

Criminaliteit in het hybride tijdperk

Robby Roks

Rutger Leukfeldt

Isabelle Klaver



Criminaliteit in het hybride tijdperk

Criminaliteit in het hybride tijdperk

Een verkennend onderzoek naar de aard en aanpak van hybride vormen van criminaliteit in Nederland, Denemarken en het Verenigd Koninkrijk

dr. R.A. Roks
prof. dr. E.R. Leukfeldt
I. Klaver, Msc

Politie en Wetenschap
Juli 2026



Netherlands Institute for the Study
of Crime and Law Enforcement



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

Lefebvre Sdu Klantenservice
telefoon: 070 - 378 98 80
website: www.sdu.nl/service

Vormgeving omslag: Robby Roks met behulp van AI

Photorealistic futuristic scene of a person holding a smartphone, surrounded by an intricate digital network connecting human body and technology. Social media interfaces floating around the person contain Dutch terms such as “DRUGS”, “GEWELD”, “FRAUDE”. The smartphone acts as a hub connecting online and offline worlds. Realistic human figure, cybernetic light patterns integrated into skin and clothing, social media feeds, network connections, urban nightscape, cinematic lighting, blue and teal color palette, ultra-detailed, high-end editorial photography style, visualizing the growing interconnectedness of humans, technology and crime on social media. Professional academic publication quality, no empty space.

ISBN: 9789012411622

© Lefebvre Sdu B.V., Den Haag, 2026

Alle rechten voorbehouden. Behalve de door de Auteurswet gestelde uitzonderingen, mag niets uit deze uitgave worden vervaelvoudigd (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). 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-uv.nl). Voor het overnemen van een gedeelte van deze uitgave ten behoeve van commerciële doeleinden dient men zich te wenden tot de uitgever.

Vanwege de aard van de uitgave gaat Lefebvre Sdu uit van een zakelijke overeenkomst; deze overeenkomst valt onder het algemene verbintenissenrecht. Uw persoonlijke gegevens worden door ons zorgvuldig behandeld en beveiligd. Wij verwerken uw gegevens voor de uitvoering van de (abonnements)overeenkomst en om u op uw vakgebied van informatie te voorzien over gelijksoortige producten en diensten van Lefebvre Sdu. Voor het toesturen van informatie over (nieuwe) producten en diensten gebruiken wij uw e-mailadres alleen als u daarvoor toestemming heeft gegeven. Uw toestemming kunt u altijd intrekken door gebruik te maken van de afmeldlink in het toegezonden e-mailbericht. Als u in het geheel geen informatie wenst te ontvangen over producten en/of diensten, dan kunt u dit laten weten aan Lefebvre Sdu Klantenservice door het contactformulier in te vullen op www.sdu.nl/service. Abonnementen gelden voor minimaal één jaar en hebben een opzegtermijn van twee maanden. Onze uitgaven zijn ook verkrijgbaar via de boekhandel. Voor informatie over onze leveringsvoorwaarden kunt u terecht op www.sdu.nl/service.

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 B.V. neither guarantees the accuracy of the data contained herein nor accepts responsibility for errors or omissions or their consequences.

Inhoudsopgave

Dankwoord / 7

1 Inleiding / 9

- 1.1 Aanleiding / 9
- 1.2 Van 'cyber' naar 'hybride' / 10
- 1.3 Criminologische concepten uit het hybride tijdperk / 12
- 1.4 Vertrekpunt en centrale onderzoeksvragen / 16
- 1.5 Methoden van onderzoek / 18
 - 1.5.1 Landselectie en drie centrale thema's / 18
 - 1.5.2 Interviews met academici en praktijkprofessionals / 19
 - 1.5.3 Een abductieve onderzoeksbenadering / 20
- 1.6 Leeswijzer / 21

2 Financieel gemotiveerde vormen van (cyber)criminaliteit / 23

- 2.1 Inleiding / 23
- 2.2 Bankhelpdeskfraude / 23
- 2.3 'Wrench attacks' / 28
- 2.4 Witwassen: de rol van geldezels / 31
- 2.5 Conclusie / 35

3 Geweld in een hybride context / 37

- 3.1 Inleiding / 37
- 3.2 Geweld tussen (groepen) jongeren / 37
- 3.3 Geweldsopdrachten via sociale media / 44
- 3.4 Conclusie / 50

4 Gedigitaliseerde drugshandel / 53

- 4.1 Inleiding / 53
- 4.2 Digitale drugsmarkten op sociale media / 53
- 4.3 'County lines' / 62
- 4.4 Conclusie / 65

5 Uitdagingen in de aanpak van hybride vormen van criminaliteit in Nederland / 67

- 5.1 Inleiding / 67

5.2	Uitdagingen in de politieorganisatie / 67
5.3	Uitdagingen in de politiecultuur / 72
5.4	Juridische uitdagingen / 76
5.5	De rol van technologiebedrijven / 79
5.6	Conclusie / 82
6	Drie landen, drie voorbeelden / 85
6.1	Inleiding / 85
6.2	Denemarken: Politiets Online Patroelje / 85
6.3	Verenigd Koninkrijk: Project Alpha / 88
6.4	Nederland: Operatie Centurion / 91
6.5	Conclusie / 93
7	Conclusie / 95
7.1	Inleiding / 95
7.2	Beantwoording deelvragen / 96
7.2.1	Financieel gemotiveerde vormen van (cyber)criminaliteit / 96
7.2.2	Geweld in een hybride context / 97
7.2.3	Digitale drugsmarkten / 97
7.2.4	Uitdagingen in de aanpak van hybride vormen van criminaliteit in Nederland / 98
7.2.5	Voorbeelden van de aanpak van hybride vormen van criminaliteit / 99
7.3	Synthese / 99
7.3.1	Kernbevindingen: een hybridiseringscontinuüm / 99
7.3.2	Nieuwe concepten: technologie-gefaciliteerde en platform-gefaciliteerde criminaliteit / 104
7.4	Implicaties: reflecties en aanbevelingen / 107
7.4.1	Reflectie op de aanpak van hybride vormen van criminaliteit / 107
7.4.2	Aanbevelingen / 109
7.5	Beperkingen van het onderzoek / 111
Literatuur / 113	
Bijlage 1 Topiclijsten / 129	
Bijlage 2 Informed consent-formulieren / 135	
Uitgaven in de reeks Politiewetenschap / 141	

Dankwoord

De centrale thematiek van dit onderzoek naar de aard en de aanpak van hybride vormen van criminaliteit houdt ons al enige tijd bezig. Wat rond 2018 begon als een serie goede gesprekken, resulteerde in meerdere publicaties over het thema hybridisering en vormde de uiteindelijke basis van dit rapport. Dit project was niet mogelijk zonder de hulp van diverse mensen die ons hebben geholpen en geïnspireerd in het verkennen van criminaliteit in het hybride tijdperk.

Allereerst bedanken wij Politie en Wetenschap voor de mogelijkheid om de oorspronkelijke ideeën verder te ontwikkelen en deze ook daadwerkelijk te vertalen naar empirisch onderzoek. In het bijzonder zijn wij Seran de Leede en Maarten Bollen zeer erkentelijk voor hun enthousiasme voor de inhoud, hun constructieve meedenken en vooral voor het geduld en begrip bij vertragingen als gevolg van persoonlijke omstandigheden en uitdagingen tijdens het veldwerk.

Bij het vormgeven van dit onderzoek hebben wij in een eerste fase veel gehad aan de waardevolle suggesties en reflecties van Bram Emmen, Barend Frans en Richard Nijboer. Voor de uitvoering hebben we dankbaar gebruik kunnen maken van ons internationale netwerk. Verschillende mensen hebben ons hierbij voorzien van gericht advies, inhoudelijke input en behulpzame introducties.

Voor Nederland willen wij Tijmen de Vreeze, Mike Loef en Aad Lenssen noemen.

In Denemarken bedanken wij Jakob Demant en andere onderzoekers en medewerkers van de Universiteit van Kopenhagen voor het hartelijke welkom en de gastvrijheid, waaronder de mogelijkheid om gebruik te maken van hun faciliteiten voor interviews en het delen van relevante contacten.

In het Verenigd Koninkrijk danken wij James Densley voor zijn suggesties ten aanzien van te interviewen respondenten.

In de afrondende fase van het onderzoek zijn wij vooral dank verschuldigd aan de leden van de leescommissie – Sjoukje van Deuren, Henk Ferwerda, Wouter Landman en Aad Lenssen – en de redactieraad van Politie en Wetenschap. Met hun scherpe, constructieve opmerkingen hebben zij ons uitgedaagd om het onderzoek verder te verdiepen en te verfijnen.

Tot slot willen wij ookilstaan bij een aantal mensen die eerder in het proces een belangrijke rol hebben gespeeld in het verder doordenken van de centrale thema's in het

onderzoek. In het bijzonder danken wij Joost Jansen, Jeroen van den Broek, Joran de Jong, Luuk Bekkers en Joeri Loggen voor het delen van inzichten, soms onbewust en ongevraagd, die van grote waarde zijn geweest.

Robby Roks
Rutger Leukfeldt
Isabelle Klaver

Juli 2026

1 Inleiding

1.1 Aanleiding

‘De criminaliteit is gedigitaliseerd. In de periode 2013-2023 is het slachtofferschap van traditionele criminaliteit sterk gedaald, terwijl het slachtofferschap van online criminaliteit sterk is gestegen. Het overgrote deel van de criminaliteit heeft tegenwoordig op de een of andere manier een online component en een deel van de misdrijven vindt volledig online plaats. Ook voor allerlei andere schadelijke en immorele gedragingen geldt dat ze meer online en minder in wijken en buurten plaatsvinden dan wel dat online en offline gedragingen sterk met elkaar zijn verweven.’ (Politie, 2025: 5)

Deze passage uit de strategische agenda van de politie (2025-2030) maakt inzichtelijk dat de politie in toenemende mate geconfronteerd wordt met delicten die op de een of andere manier een online component hebben. Voor het beschrijven van de gevolgen van de voortschrijdende digitalisering op criminaliteit worden diverse termen gebruikt. *Online criminaliteit* is de meest brede aanduiding voor delicten met een digitale component. Hieronder vallen zowel delicten die gericht zijn op ICT zoals hacken of het platleggen van websites – cybercriminaliteit in enge zin of *cyber-dependent crimes* (McGuire en Dowling, 2013a) – als *cyber-enabled crimes* (McGuire en Dowling, 2013b), oftewel gedigitaliseerde criminaliteit in de vorm van delicten waarbij ICT van belang is voor het uitvoeren van het delict, zoals in vormen van online fraude en oplichting (Schiks, Van ’t Hoff-de Goede en Leukfeldt, 2022: 11; Leukfeldt en Weulen Kranenbarg, 2017).

De gangbare terminologie die besloten ligt in online criminaliteit, cybercriminaliteit en gedigitaliseerde criminaliteit kent echter beperkingen. Opvallend hierbij is dat er een strikte scheiding wordt aangebracht tussen online en offline, alsof het hier gescheiden realiteiten betreft. Het gaat, zoals de bovenstaande passage uit de strategische agenda van de politie duidelijk maakt, echter niet altijd om volledig digitale of online delicten; de fysieke of offline wereld speelt in veel gevallen een belangrijke en soms zelfs onmisbare rol in de totstandkoming van het delict. Te denken valt bijvoorbeeld aan online fraude en phishing waarbij het ronselen van pasjes of geldezels zowel online als offline plaatsvindt en waarbij het pinnen van het geld in de fysieke wereld plaatsvindt (Politie, 2024; Bekkers, 2025). Er zijn ook delicten die niet worden aangemerkt als online criminaliteit, maar waarbij de digitale wereld wel degelijk een centrale rol heeft. De handel in verdovende middelen vindt voor een deel plaats online: na de op-

komst van cryptomarkten is tegenwoordig ook op allerlei socialemediaplatformen een levendige handel in verschillende soorten drugs (Bakken en Demant, 2019; Moyle et al., 2019; Roks en Hendriksen, 2021). Daarnaast zijn er vechtpartijen tussen jongeren die worden gefilmd en online worden verspreid en in bredere zin in het geval van rivaliserende groepen die sociale media gebruiken om elkaar uit te dagen, te bedreigen en in sommige gevallen afspraken te maken om elkaar in de offline wereld te treffen (Roks en Van den Broek, 2021; Mehlbaum et al., 2025). In dergelijke voorbeelden lijkt de aanduiding online criminaliteit te eng, evenals de term gedigitaliseerde criminaliteit. Het bovenstaande is niet alleen een semantische discussie over terminologie, maar het raakt op een fundamentele manier aan de hedendaagse aanpak van criminaliteit. Professionals in het zorg- en veiligheidsdomein worden in toenemende mate geconfronteerd met fenomenen waarbij de verwevenheid tussen online en offline of de fysieke en digitale wereld zorgt voor uitdagingen (Van den Broek en Roks, 2022; Van den Broek en Jhanjan, 2024). Onder de noemer van de digitale transformatie staat dit onderwerp ook binnen de politie hoog op de agenda. Sterker nog, dit onderwerp is aangemerkt als een van de drie doorsnijdende thema's in de eerdergenoemde strategische agenda van de politie (Politie, 2025). Het doel van de politie is om in 2030 een *'toonaangevend voorbeeld'* te zijn als het gaat om de balans tussen mens en technologie, iets dat vraagt om *'digitale vaardigheid, digitale cultuur en relationeel en digitaal leiderschap'* (Politie, 2025: 10).

Recent is er een aantal publicaties verschenen die zich richten op de gevolgen en uitdagingen van de digitalisering voor de politie(praktijk) (zie o.a. Landman en Groothuis, 2022; Mehlbaum, Van den Akker, Broekhuizen en Verweij, 2025; Stol, Strikwerda, Jansen en Schreurs, 2025; Van Steden et al., 2025). De insteek van dit onderzoek heeft raakvlakken met deze studies, maar kent een ander vertrekpunt. Voortbouwend op eerdere studies (Leukfeldt en Roks, 2020; Roks, Leukfeldt en Densley, 2020) richten we ons – net als Mehlbaum en collega's (2025) – niet op online criminaliteit, cybercriminaliteit of gedigitaliseerde delicten, maar op wat we *hybride* vormen van criminaliteit zullen noemen. We lichten dit concept, alsmede de meer theoretische achtergrond van dit hybride perspectief, in de volgende paragraaf toe.

1.2 Van 'cyber' naar 'hybride'

Sinds het ontstaan van internet is er aandacht voor wat deze digitale revolutie betekent voor criminaliteit en de bestrijding hiervan (Van der Wagen, Weulen Kranenbarg en Oerlemans, 2024: 23-36). Cybercriminaliteit kan beschouwd worden als een relatief jong, maar snelgroeiend aandachtsgebied in de criminologie (zie o.a. Holt en Bossler, 2014; Holt, 2023; Weulen Kranenbarg en Van 't Hoff-de Goede, 2023; Van der Wagen et al., 2024). Inmiddels lijkt de term 'cyber' ingebed en ingeburgerd te zijn in het criminologisch taalgebruik. Toch is het de vraag of dit bekende voorvoegsel volledig de lading dekt van fenomenen die worden getypeerd als 'cyber' (zie, o.a. Stratton, Powell en Cameron, 2017; Powell, Stratton en Cameron, 2018). Diverse auteurs betogen immers dat het gebruik van de term 'cyber' lijkt te impliceren dat het gaat om fenomenen die

volledig digitaal, virtueel of online zijn (zie o.a. Brown, 2006; McGuire, 2007; Hayward, 2012; Stratton et al., 2017; Graham et al., 2024; Kaufmann en Lomell, 2025).

Hoewel internet vaak wordt voorgesteld als een grenzeloze ruimte zonder temporele of ruimtelijke beperkingen (Van der Wagen et al., 2025, p. 33), roept de bekende term 'cyberspace' associaties op met een afzonderlijke ruimte naast of buiten de fysieke werkelijkheid (McGuire, 2007; Gordon et al., 2022). Jurgenson (2011, p. 84) duidt het gebruik van 'cyber' aan als een vorm van digitale dualiteit, waarbij cybercriminaliteit wordt beschouwd als *'a mirror or the online double of their terrestrial counterparts, differing perhaps by medium and reach, but not by nature'* (Stratton et al., 2017, p. 22). McGuire (2007; 2008; 2020) stelt dat dit een fundamenteel problematische manier is om naar de impact van digitale technologie te kijken. Moderne informatie- en communicatietechnologie (ICT) creëert volgens hem geen nieuwe, virtuele werkelijkheden, maar vergroot en intensiveert bestaande menselijke interacties (McGuire, 2007, p. 14-44; 2008, p. 8-10). Voor dit proces gebruikt hij de term 'hyperspatialisation', waarmee hij verwijst naar de wijze waarop technologie tijd en afstand comprimeert en menselijke handelingsmogelijkheden uitbreidt. De daaruit voortvloeiende sociale werkelijkheid duidt hij aan als hyperspace. Een dergelijke hyperverbonden wereld brengt eveneens nieuwe mogelijkheden voor criminaliteit met zich mee. In plaats van deze ontwikkelingen te beschrijven in termen van cybercrime, introduceert McGuire (2020, p. 23) het begrip 'hypercrime':

'In this way, a conception of cybercrime rooted in enhanced physical, social, and psychological connectivity emerges, one that arguably better links questions of human-technical agency to the new spaces of interaction created by ICT.' (McGuire, 2020, p. 23)

McGuire (2007; 2008; 2020) verwerpt hiermee een strikte scheiding tussen online en offline of tussen digitaal en fysiek. Zijn werk benadrukt juist dat digitale technologieën diep verweven zijn geraakt met alledaagse menselijke praktijken en interacties, waaronder criminaliteit, waardoor dergelijke dichotomieën steeds minder analytische waarde hebben (Gordon et al., 2022).

Nog voordat de term 'cyber' in het criminologische landschap in zwang raakte, merkte Brown (2006: 236) op vergelijkbare wijze op dat *'there is quite simply no such thing as a "technological" crime (such as a "cybercrime") as distinct from an "embodied" crime'*. Brown (2006: 224) betoogt dat dit binaire denken de discipline ontoereikend maakt voor de analyse van complexe techno-sociale kenmerken van criminologische fenomenen, waarbij sprake is van een verwevenheid tussen technologie en de mens. Om die reden pleit Brown (2006) dan ook voor een 'criminology of hybrids' (zie o.a. Van der Wagen, 2018). Tot een dergelijke hybride criminologie is het tot op heden niet gekomen. Wel valt er een andere ontwikkeling waar te nemen. In veiligheidsstudies (Futter, 2018), de antropologie (Horst en Miller, 2020), sociologie (Lupton, 2015) en criminologie (Kaufmann en Lomell, 2025; Powell et al., 2018; Stratton et al., 2017) wordt in toenemende mate het woord 'digitaal' gebruikt ten faveure van 'cyber'. Hoewel 'digitaal'

tegenwoordig verwijst naar ‘*the electronic representation of data in the discrete values of ones and zeros as established in the mid-20th century*’ (Kaufmann en Lomell, 2025: 2), stamt het woord af van het Latijnse woord voor vinger (digitus), verwijzend naar het tellen met vingers. De digitale criminologie kent daarmee, zoals Wernimont (2025: 202) betoogt, geen enge kijk op technologie, maar een ruimere blik op de techno-sociale aspecten en kenmerken van criminologische fenomenen. Met ‘techno-sociaal’ wordt in deze context gewezen op de verwevenheid tussen technologie en de mens, oftewel op het loslaten van de veel gehanteerde binaire opposities tussen online en offline en de fysieke en digitale wereld.

Deze processen van hybridisering worden in wetenschappelijke studies gesignaleerd en benoemd. In onderzoek naar cybercrime wordt bijvoorbeeld het belang onderstreept van de offline aspecten van deze delicten (Leukfeldt, 2016; Lusthaus, 2018; Lusthaus en Varese, 2021), de lokale inbedding van cybercriminele netwerken (Leukfeldt, 2016; Kruisbergen, Leukfeldt, Kleemans en Roks, 2018; Leukfeldt, Kruisbergen, Kleemans en Roks, 2019) en, meer in het algemeen, de menselijke factor van cybercriminaliteit (Leukfeldt en Weulen Kranenbarg, 2017). Waar onderzoekers van cybercriminaliteit hun perspectief verbreden van het cyberdomein naar offline en lokale contexten, lijken anderen hun onderzoeksblik eveneens te verruimen, in dit geval van het fysieke naar het online domein. Studies naar straatculturen en gangs laten bijvoorbeeld zien dat socialemediaplatformen zoals Facebook, Twitter en Instagram – ook wel aangeduid als de digitale straat (Lane, 2019) – net zo betekenisvol zijn geworden als de fysieke straat (Lauger en Densley, 2018; Moore en Stuart, 2020). Bovendien bieden digitale technologieën nieuwe mogelijkheden om traditionele straatedelicten zoals drugshandel op te schalen of om het criminele repertoire uit te breiden richting vormen van cybercriminaliteit of gedigitaliseerde delicten (Leukfeldt en Roks, 2020; Roks et al., 2021).

Er valt met andere woorden een zekere ontwikkeling te ontwaren in het denken over de impact van de digitalisering op criminologische fenomenen. Lange tijd was de zogenoemde ‘cyber era’ dominant, een tijdperk dat door Lupton (2015: 39) wordt getypeerd door de nadruk op allerhande virtuele en digitale netwerken waarin gebruikers interacteren via computertechnologie. Op basis van het bovenstaande kan betoogd worden dat we inmiddels zijn beland in het hybride tijdperk, een periode waarin er sprake is van een complexe verwevenheid tussen online en offline en het fysieke en het digitale in criminaliteitsvormen. In de volgende paragraaf geven we hiervan een aantal voorbeelden uit criminologische studies.

1.3 Criminologische concepten uit het hybride tijdperk

De criminologische literatuur brengt veelal een hard onderscheid aan tussen *cyber-dependent* en *cyber-enabled crimes* (McGuire en Dowling, 2013a; 2013b). Wall (2015) geeft echter een meer fluïde kijk op het fenomeen:

‘The range of cybercrimes described in the literature varies in terms of its mediation by technologies. At one end of the spectrum are cyber-assisted crimes that use the internet in their organisation, but which would still take place if the internet was removed. At the other end of the spectrum are cyber-dependent crimes that are of the internet. They are the spawn of the internet, and if the internet (networked technologies) is taken away, then they simply disappear. (...) In between the cyber-assisted and cyber-dependent crimes are a range of hybrid cyber-enabled crimes, that include most types of frauds.’ (Wall, 2015: 75)

Het bovenstaande verwijst naar een vorm van cybercriminaliteit die maar in beperkte mate aandacht heeft gekregen in de criminologische literatuur: zogenoemde *cyber-assisted* vormen van criminaliteit, waarbij internet vooral gebruikt wordt voor de organisatie van criminaliteit. Bovenal geeft het benaderen van cybercriminaliteit als spectrum zicht op de doorgaans poreuze grenzen tussen de veel gehanteerde categorisering van cybercriminaliteit (vgl. Lusthaus, 2024) en hybride vormen van cybercriminaliteit. Een voorbeeld hiervan vinden we in het werk van Van der Wagen (2018; 2019) over daders en slachtoffers van hightech cybercrime. Van der Wagen (2019: 164) spoort onderzoekers aan om aandacht te hebben voor wat ze ‘the hybrid’ en in het bijzonder ‘the cyborg’ noemt, vooral om te helpen identificeren op welke manieren *‘offenders and technology configure together (become one)’*. Daartoe grijpt Van der Wagen (2018; 2019) – vergelijkbaar met Brown (2006) – terug op Latours (2005) actor-netwerktheorie, met een specifieke focus op menselijke en niet-menselijke assemblages. Van der Wagen (2018: 227) stelt dat *‘technologies should be treated as active entities, mediators of participants in high-tech crime offending’*. Deze visie, in lijn met het postfenomenologische werk van Verbeek (2008; 2011; 2016) en de typering van cybercriminaliteit als een spectrum door Wall (2015: 70), onderzoekt hoe technologieën criminaliteit mediëren, maar houdt ook rekening met de wijze waarop technologieën het gedrag en de besluitvormingsprocessen van daders beïnvloeden en vormgeven (Van der Wagen, 2018: 228).

Ook in de studie van Roks, Leukfeldt en Densley (2021) zien we het gebruik van de term hybride terug, in dit geval onder de noemer van processen van hybridisering die zich in de context van de straatcultuur en -criminaliteit in Nederland voordoen. Om dit inzichtelijk te maken, wordt er in het artikel van Roks en collega’s (2021) gebruikgemaakt van een combinatie van inzichten uit een onderzoek op basis van online en offline etnografisch onderzoek naar een Nederlandse gang (Roks, 2016) en een analyse van opsporingsonderzoeken naar cybercriminele netwerken (Leukfeldt, 2016). Hybridisering is, ten eerste, zichtbaar in de vorm van een zekere digitale diversificatie van traditionele vormen van criminaliteit op straat. Hierbij valt te denken aan gangleden die op straat criminaliteit plegen en gebruikmaken van smarttelefoons en socialemediaplatformen om gestolen goederen aan te prijzen, verdovende middelen te verhandelen, maar ook om te communiceren met andere gangleden. Ten tweede wordt door Roks en collega’s (2021) beschreven dat een deel van de jongere gangleden in de studie van Roks (2016), die normaliter vooral bezig zijn met traditionele delicten op straat,

zich ook zijn gaan toeleggen op phishing en andere vormen van online fraude en oplichting. Ten slotte maakt de analyse van opsporingsonderzoeken door Leukfeldt en Roks (2020) inzichtelijk dat de cybercriminele netwerken zich niet beperken tot online vormen van criminaliteit, maar dat zij ook betrokken zijn bij meer traditionele delicten zoals de handel in verdovende middelen, vals geld en gestolen goederen. Deze betrokkenheid bij een veelvoud aan criminele activiteiten wordt in de literatuur ook wel aangeduid als *cafeteria-style offending* (vgl. Leukfeldt en Holt, 2022). Deze studies maken inzichtelijk dat technologische vooruitgang resulteert in nieuwe mogelijkheden voor criminele activiteiten, met als gevolg dat er een nadrukkelijke wisselwerking ontstaat tussen het online en offline domein.

De hybridisering die wordt beschreven in de context van straatcriminaliteit vertoont gelijkenissen met wat Di Nicola (2022) beschrijft over de impact van digitale technologie op georganiseerde misdaad. De auteur benoemt dat het in toenemende mate moeilijk is om een onderscheid te maken tussen daders die online en offline actief zijn, maar dat ook bij criminele activiteiten de vraag rijst of deze zich afspelen in de fysieke of digitale wereld. Er is, zo stelt Di Nicola (2022), immers sprake van een toenemende verwevenheid en dit vraagt om een theoretische benadering in de criminologie die recht doet aan deze complexiteit en de grote veranderingen in de digitale samenleving. De auteur introduceert hiervoor de term ‘digital organized crime’ – oftewel digitale georganiseerde criminaliteit – om te verwijzen naar:

‘(...) groups of individuals (and of individuals and machines, of actants) working together with different forms of specialization and professionalism and organizing in different ways to commit criminal activities online, offline/online, and offline that require organization of criminal work over a long, extended period of time and that are strongly influenced by the digital dimension in terms of the criminal activities they commit and the way these activities are organized, the organization of the criminal group itself, and the relationships with other criminal groups and criminal actors and machines. Within this concept, it is possible to integrate both online organized cyber-crime groups and traditional organized crime groups, both groups of human actors and networks of human and non-human actors and the socio-material objects they produce in their interaction (networks of actants).’ (Di Nicola, 2022: 13)

In deze definitie herkennen we een zekere hybridisering van cybercriminaliteit en georganiseerde criminaliteit. Di Nicola (2022) merkt in dit opzicht op dat de term digitale georganiseerde criminaliteit niet gezien moet worden als georganiseerde cybercriminaliteit, maar primair bedoeld is als concept om de diversiteit aan verschijningsvormen van georganiseerde samenwerkingsverbanden en georganiseerde vormen van criminaliteit in het digitale tijdperk te vatten.

In de literatuur over geweld vinden we eveneens een relevant concept dat raakvlakken vertoont met processen van hybridisering: *‘technology-facilitated violence’*. Het gaat in de beschikbare studies naar dit onderwerp doorgaans om vormen van interpersoonlijk geweld die worden gefaciliteerd door technologie, waaronder online intimidatie, stal-

king en het verspreiden van intieme beelden zonder toestemming (zie o.a. Henry, Flynn en Powell, 2020; Mitchell et al., 2025). Omdat er over dit concept de nodige conceptuele onduidelijkheid bestond, voerden Mitchell en collega's (2022) een conceptuele review van de wetenschappelijke literatuur over dit thema uit. Op basis van deze systematische verkenning komen de auteurs tot de volgende definitie:

‘Technology-facilitated violence refers to acts of harm that are brought about when technical artefacts, through making a harmful end easier or possible to achieve, invite actors holding this end to actualise it using the artefact.’ (Mitchell et al., 2022: 663)

Het uitgangspunt van deze definitie van technology-facilitated violence is dat technologie niet slechts een neutraal hulpmiddel is, maar actief betrokken raakt bij het ontstaan en de uitvoering van geweld. Ten eerste wordt technologie in deze definitie opgevat als een concreet artefact of object dat een tastbare rol speelt in geweldsprocessen. Daarnaast benadrukt deze definitie dat technologie het gebruik van geweld vergemakkelijkt. Ten slotte wordt technologie in deze definitie beschouwd als een actor die het gedrag van de gebruikers van de technologie beïnvloedt. Socialemediaplatformen zijn hiervan een goed voorbeeld: door anonimiteit en snelle verspreiding van berichten nodigen zij gebruikers uit om beledigende of gewelddadige content te plaatsen. Wanneer iemand al de intentie heeft om dergelijk gedrag te vertonen, kan het platform die intentie versterken en faciliteren. Het concept technology-facilitated violence maakt, met andere woorden, duidelijk dat technologie niet passief is, maar een actieve rol speelt als het gaat om geweld: technologie kan geweld uitnodigen door gedragingen te stimuleren (bijvoorbeeld anonimiteit die intimidatie vergemakkelijkt), *affordances* bieden die geweld faciliteren (zoals de mogelijkheid tot massale verspreiding van beelden) en geweld vertalen door het te herconfigureren in nieuwe vormen (zoals digitale bedreiging die verschilt van fysieke bedreiging). Hiermee wordt technologie niet langer opgevat als passief hulpmiddel, maar als actieve actor die geweld mede vormgeeft (Mitchell et al., 2025; Wood et al., 2023).

Het concept van technology-facilitated violence overstijgt, net als de andere voorbeelden in deze paragraaf, de traditionele scheidingen tussen online en offline, fysiek en digitaal, en mens en technologie. Dat geldt ook voor de notie van *platform-enabled crimes* (Hamilton, 2021) of *platform criminality* (McGuire, 2026). Met deze termen wordt verwezen naar misdrijven die niet alleen via sociale media plaatsvinden, maar waarvan de uitvoering en impact direct afhankelijk zijn van de infrastructuur, functies en beleidskeuzes van deze platforms. Hamilton (2021) gebruikt Myanmar als een casus om te laten zien hoe digitale platforms niet neutraal functioneren, maar actief kunnen bijdragen aan het ontstaan van geweld. In Myanmar was Facebook in de periode rond 2017 voor een groot deel van de bevolking de primaire, en vaak enige toegang tot nieuws, informatie en sociale communicatie. Dit betekende dat het platform een buitengewoon dominante rol speelde in het dagelijks leven en dat de algoritmes en moderatiepraktijken ervan directe maatschappelijke impact hadden. Haatdragende en op-ruiende berichten tegen de Rohingya – een etnische minderheid in Myanmar – werden

niet alleen gedeeld, maar door de algoritmische logica van het platform ook versterkt en breed verspreid. De infrastructuur van Facebook maakte het mogelijk dat propaganda razendsnel circuleerde en dat gewelddadige oproepen een groot bereik kregen. Tegelijkertijd liet het platform het na om tijdig te modereren en schadelijke content te verwijderen, hetgeen bijdroeg aan het legitimeren en coördineren van geweld in de fysieke wereld. Hamilton (2021) betoogt, in lijn met McGuire (2026), dat deze dynamiek niet kan worden begrepen als het loutere gebruik van een neutraal medium door kwaadwillende actoren: de platformstructuur zelf – het ontwerp, de algoritmische logica en de commerciële keuzes van Facebook – maakte het mogelijk dat haatcampagnes uitgroeiden tot grootschalige wredeheden. Ook hier zien we dat technologie – in dit geval de infrastructuren van socialemediaplatformen en hun zogenoemde affordances – een rol speelt. Hamilton (2021) onderscheidt in haar analyse van platform-enabled crimes zowel de in het materiele strafrecht bekende aspecten van commissie, oftewel van handelen, als van ommissie in de vorm van nalaten (zie bijvoorbeeld De Hullu en Van Kempen, 2024).

Het introduceren van de genoemde concepten kan worden gezien als bewuste pogingen om significante veranderingen in de context van criminologische verschijningsvormen te adresseren. Buiten de criminologie muntte Floridi (2015: 3) daarvoor het neologisme ‘onlife’, als verwijzing naar *‘the new experience of a hyperconnected reality within which it is no longer sensible to ask whether one may be online or offline’*. Meer in het algemeen betoogt Floridi (2015: 3) dat de opkomst en impact van ICT ons dwingen onze centrale concepten opnieuw te onderzoeken, niet alleen om te voorkomen dat onderzoekers *‘conceptually wrong-footed’* raken, maar ook omdat er een risico bestaat dat *‘we fear and reject what we fail to semanticise’*. Dit laatste is bij uitstek relevant voor de aanpak. In zijn studie naar geldezels concludeert Bekkers (2025: 173) dat lokale politieteam *‘cyber fear’* ervaren, voortkomend uit een gebrek aan noodzakelijke vaardigheden en ervaring om misdrijven waarbij digitale technologie een rol speelt effectief aan te pakken. De concepten (digital) technology-facilitated violence en platform-enabled crimes zijn op een andere manier eveneens relevant voor de aanpak. Deze inzichten benadrukken dat (digitale) technologieën en socialemediaplatformen niet slechts neutrale artefacten zijn, maar een bepalende factor kunnen zijn die geweld, of criminaliteit in bredere zin, uitnodigen, faciliteren en transformeren door hun infrastructuur, algoritmes en beleidspraktijken.

1.4 Vertrekpunt en centrale onderzoeksvragen

Het vertrekpunt in deze studie is dat de voortschrijdende digitalisering heeft geresulteerd in een nadrukkelijke verwevenheid van online en offline en het fysieke en digitale. We gebruiken hiervoor de term hybridisering en de in de vorige paragraaf gepresenteerde concepten als lens om naar specifieke criminologische verschijningsvormen te kijken, alsmede naar de consequenties en implicaties die deze verwevenheid heeft voor de aanpak ervan. Omdat de gevolgen van de digitalisering niet beperkt blijven tot onze

landsgrenzen, kent dit onderzoek een verkennende internationale vergelijking met Denemarken en het Verenigd Koninkrijk. De volgende onderzoeksvraag staat centraal:

Wat zijn de aard en aanpak van hybride vormen van criminaliteit in Nederland, Denemarken en het Verenigd Koninkrijk?

Deze centrale onderzoeksvraag hebben we geoperationaliseerd in de volgende drie deelvragen:

- 1. Welke vormen van hybride criminaliteit zijn er in Nederland, Denemarken en het Verenigd Koninkrijk?*
- 2. Welke uitdagingen worden er in Nederland ervaren als het gaat om de aanpak van hybride vormen van criminaliteit?*
- 3. Wat zijn voorbeelden van de aanpak van hybride vormen van criminaliteit in Nederland, Denemarken en het Verenigd Koninkrijk?*

Het begrip ‘hybride’ in deze vragen verdient hier een korte toelichting. Tegenwoordig kennen vrijwel alle criminele verschijningsvormen een zekere mate van hybridisering: een verwevenheid tussen de online en offline wereld. Om deze reden spreken we over criminaliteit in het hybride tijdperk. Het eerste doel van dit onderzoek is dan ook – zoals besloten ligt in de eerste deelvraag – om te komen tot een inventarisatie van voorbeelden van hybride vormen van criminaliteit in Nederland, Denemarken en het Verenigd Koninkrijk. Hoewel in verschillende onderzoeksdomeinen wordt gewezen op processen van hybridisering, zoals rondom extremisme en zedendelicten (zie bijvoorbeeld Gaudette et al., 2022; Stoeldraaijers et al., 2024), beperken we ons in deze studie tot drie thema’s: fraude, drugs en geweld. De keuze voor deze onderwerpen lichten we in de volgende paragraaf nader toe. Het gaat hierbij om criminaliteitsvormen waarin (digitale) technologie op een specifieke manier een rol speelt in de modus operandi.

Het tweede doel van deze studie komt terug in de laatste twee deelvragen. Met dit onderzoek willen we verkennen welke uitdagingen in Nederland worden ervaren bij de aanpak van hybride vormen van criminaliteit. Hoewel het hierbij gaat om uitdagingen die breder spelen in de aanpak van criminaliteit (Van den Broek en Roks, 2022; Van den Broek en Jhanjan, 2024), ligt de nadruk in dit onderzoek vooral op de uitdagingen voor de politie. Daarnaast beogen we een beeld te krijgen van bestaande, veelbelovende voorbeelden, zowel in Nederland als in Denemarken en het Verenigd Koninkrijk, opnieuw met een accent op de politie. Met deze inzichten hopen we de (politie)praktijk in Nederland te voorzien van input die gebruikt kan worden als onderdeel van de in gang gezette digitale transformatie.

1.5 Methoden van onderzoek

Voor de beantwoording van de centrale onderzoeksvraag naar de aard en aanpak van hybride vormen van criminaliteit in Nederland, Denemarken en het Verenigd Koninkrijk maken we gebruik van een exploratief, kwalitatief onderzoeksdesign. In deze paragraaf lichten we de methodologische achtergrond van dit onderzoek nader toe. We beginnen met een toelichting op de selectie van de landen in onze internationale vergelijking.

1.5.1 Landenselectie en drie centrale thema's

Het startpunt voor dit onderzoek was gelegen in Nederland. De auteurs van dit rapport zijn de afgelopen jaren betrokken geweest bij onderzoeken waarin sprake was van een zekere verwevenheid tussen online en offline aspecten, te weten naar financieel gemotiveerde cybercriminaliteit (Leukfeldt et al., 2017a, 2017b, 2017c; Leukfeldt en Roks, 2020; Roks en Monshouwer, 2020), geweld (Roks en Van den Broek, 2021; Roks, De Jong en Van den Broek, 2024) en de handel in verdovende middelen (Roks en Hendriksen, 2021), alsmede twee studies waarin diverse aanpakken in Nederland rondom deze thema's zijn geïnventariseerd (Schiks et al. 2022; Van den Broek en Roks, 2023). Op basis van deze eerdere onderzoeken hebben we een keuze gemaakt voor drie centrale thema's: financieel gemotiveerde cybercriminaliteit, geweld en de handel in verdovende middelen. Op basis van de beschikbare literatuur over deze onderwerpen en enkele verkennende gesprekken¹ in 2022 zijn er twee additionele landen geselecteerd: Denemarken en het Verenigd Koninkrijk. Naast inhoudelijke argumenten hebben we bij het maken van deze voorlopige selectie in het bijzonder rekening gehouden met haalbaarheid en met reeds bestaande contacten in onze (academische) netwerken die zouden kunnen ondersteunen bij toegang tot respondenten op deze locaties.

Onze keuze voor Denemarken is primair ingegeven door het feit dat daar al de nodige (wetenschappelijke) kennis beschikbaar is over digitale drugsmarkten op sociale media als Snapchat, Instagram en Facebook (Bakken en Demant, 2019; Bakken, 2020). Het Verenigd Koninkrijk werd geselecteerd op basis van studies op het gebied van rivaliserend groepsgedrag tussen zogenoemde drillrapgroepen, waarbij sociale media een belangrijke rol spelen (Fatsis, 2019; Irwin-Rogers en Pinkney, 2017; Ilan, 2020; Pinkney en Robinson-Edwards, 2018). Het Verenigd Koninkrijk is eveneens relevant vanwege het fenomeen van 'county lines-dealen' (Coomber en Moyle, 2017; Robinson, McLean en Densley, 2018) waarbij mobiele telefoons een belangrijke rol spelen.

1 We hebben hierbij dankbaar gebruikgemaakt van de inzichten van Barend Frans (Digitale zaken politie Amsterdam), Bram Emmen (promovendus Open Universiteit en bezig met een proefschrift over het optreden van politie en justitie in relatie tot de opkomst van het dark web) en Richard Nijeboer (Senior Liaison Cyber-crime en Digitaal Opsporen bij Politie Nederland).

1.5.2 *Interviews met academici en praktijkprofessionals*

Om zicht te krijgen op de aard en aanpak van hybride vormen van criminaliteit in Nederland, Denemarken en het Verenigd Koninkrijk hebben we gebruikgemaakt van een combinatie van interviews, media-analyse en een analyse van andere (openbare) bronnen.² We zijn in elk land begonnen met interviews met respondenten die zicht kunnen geven op concrete voorbeelden van hybride vormen van criminaliteit en hun ervaringen kunnen delen met betrekking tot de aanpak. Te denken valt aan personen die werkzaam zijn bij politie, justitie of andere relevante partners, maar ook aan academici die zich in de door ons geselecteerde landen bezighouden met het onderzoeken van hybride vormen van criminaliteit. In totaal hebben we in de periode tussen oktober 2024 en juni 2025 gesproken met 54 respondenten: 27 zijn te typeren als praktijkprofessional, 26 zijn werkzaam als wetenschapper en één respondent is zowel praktijkprofessional als betrokken bij wetenschappelijk onderzoek. De topiclijst die we hebben gebruikt is opgenomen als bijlage I.

De dataverzameling ging in oktober 2024 van start met interviews met wetenschappers en praktijkprofessionals in Nederland. In totaal hebben wij in Nederland met achttien respondenten gesproken: tien personen waren werkzaam bij de politie, vier bij het Openbaar Ministerie en twee respondenten waren op een andere manier betrokken bij de aanpak van criminaliteit. Een van hen was niet alleen werkzaam als praktijkprofessional, maar ook bezig met wetenschappelijk onderzoek. Ten slotte hebben we twee respondenten geïnterviewd die werkzaam zijn als wetenschappelijk onderzoeker. In totaal zijn zes van de achttien personen geïnterviewd via Teams, de overige gesprekken vonden plaats op een fysieke locatie. De gemiddelde duur van deze interviews was 60 minuten. Na het ondertekenen van een informed-consentformulier (zie bijlage II) zijn al deze gesprekken opgenomen en verbatim uitgewerkt.

In het Verenigd Koninkrijk hebben we in de periode van november 2024 tot en met juni 2025 gesproken met zeventien respondenten. Deze respondenten zijn geworven door gebruik te maken van het sociale netwerk van een van de onderzoekers. Een wetenschapper uit het Verenigd Koninkrijk werd geconsulteerd om een eerste lijst met mogelijk relevante gesprekspartners op te stellen op basis van een uitvoerige beschrijving van het onderzoek. Vervolgens zijn deze respondenten benaderd en werd gebruikgemaakt van de zogenaamde sneeuwbalmethode om te komen tot nieuwe mogelijke gesprekspartners. Vanwege uitdagingen in het verkrijgen van contact met praktijkprofessionals via de academici hebben we daar gesproken met vier respondenten die verbonden zijn aan de politie en dertien personen die betrokken (zijn) geweest bij wetenschappelijk onderzoek. Vier van deze dertien respondenten werkten tijdens het onderzoek nauw samen met de politie en hadden vanuit die hoedanigheid een goed beeld van de aanpak. Alle gesprekken vonden plaats via Teams en werden, op twee

2 Voor dit onderzoek is formeel goedkeuring verkregen van de Ethische Commissie van de Erasmus School of Law van de Erasmus Universiteit Rotterdam op 20 augustus 2024 (ETH2324-0715).

uitzonderingen na, met toestemming van de respondenten opgenomen en letterlijk uitgewerkt. De gemiddelde duur van deze online interviews was 49 minuten.

In Denemarken hebben we gebruikgemaakt van een vergelijkbare manier van werken. Een wetenschapper uit Denemarken is gevraagd naar een lijst met mogelijk relevante respondenten. Op basis van deze contacten zijn er op 24 en 25 februari 2025 aan de Universiteit van Kopenhagen acht respondenten geïnterviewd. Nog eens elf respondenten zijn vervolgens tussen maart en juni 2025 geïnterviewd via Teams. Van deze negentien respondenten waren er elf werkzaam in de wetenschap, zes waren verbonden aan de politie in Denemarken en twee respondenten waren op een andere manier betrokken bij de aanpak van criminaliteit. Alle gesprekken in Denemarken zijn opgenomen en vervolgens uitgewerkt. In totaal betrof de gemiddelde duur van de interviews met respondenten uit Denemarken 65 minuten.

Voorafgaand aan de interviews hebben wij online zelf gezocht naar voorbeelden van de aard en aanpak van hybride vormen van criminaliteit in Nederland, Denemarken en het Verenigd Koninkrijk. Omdat deze eerste zoekslag te weinig concrete resultaten opleverde, hebben we tijdens de interviews gevraagd om concrete voorbeelden rondom de gespreksthema's. Op basis van de input van de respondenten hebben we uiteindelijk in Nederland 23 documenten verzameld, onder andere via Lexis-Nexis en Rechtspraak.nl. Via onze Deense gesprekspartners en eigen aanvullende zoekslagen hebben we achttien relevante documenten geselecteerd, bestaande uit nieuwsartikelen op websites van Deense kranten en van de Deense politie. Ten slotte hebben we in het Verenigd Koninkrijk met een vergelijkbare manier van werken 38 documenten, afkomstig van websites van kranten, de politie en het Openbaar Ministerie, over de aard of aanpak van hybride vormen van criminaliteit verzameld.

1.5.3 *Een abductieve onderzoeksbenadering*

Omdat er nog weinig bekend is over hybride vormen van criminaliteit hebben we gekozen voor een kwalitatief onderzoeksdesign met een zogenoemde abductieve onderzoeksbenadering. Een dergelijke benadering wil zeggen dat het vertrekpunt in ons onderzoek niet zuiver exploratief of deductief was, maar dat we gedurende het analyseproces steeds hebben geprobeerd onze bevindingen te kalibreren en te verbinden met theoretische en empirische inzichten uit eerder onderzoek (Timmermans en Tavory, 2012; Van Hulst en Visser, 2024). We zijn begonnen met het inventariseren en beschrijven van processen van hybridisering in theoretische en empirische studies naar jeugd- en straatcriminaliteit, georganiseerde criminaliteit en cybercriminaliteit, met bijzondere aandacht voor financieel gemotiveerde cybercriminaliteit, geweld en de handel in verdovende middelen. Deze inzichten vormden de basis voor onze topiclijst (zie bijlage I).

De 54 interviews zijn allemaal letterlijk uitgewerkt en samen met de door ons verzamelde voorbeelden geanalyseerd in Atlas.ti 24. We hebben hierbij gebruikgemaakt van een *'thick analysis'* (Evers, 2024): een iteratieve combinatie van analysetechnieken, -tactieken en strategieën. De topiclijst en onze literatuurstudie vormden de basis van

een thematische codelijst waarmee het codeerproces is begonnen (Evers, 2024: 91-92). Vervolgens hebben we in een tweede codeerslag ook enkele open codes toegekend (Evers, 2024: 88-89). Deze fases hadden als doel om het empirische materiaal doorzoekbaar te maken en zicht te krijgen op centrale thema's (Evers, 2024: 50). We hebben daarbij met de prefix NL, DE of UK een onderscheid aangebracht per land. In de derde fase – de patroonanalyse – hebben we de verschillende codes als uitgangspunt genomen en groepscode gemaakt om overstijgende patronen in het materiaal te ontwaren (Evers, 2024: 118-119). Deze groepscode, bestaande uit 'Fraude', 'Geweld', 'Drugs', 'Aanpak Uitdagingen' en 'Aanpak Voorbeelden', vormen de structuur van de hoofdstukken van dit rapport.

Nadat de overkoepelende structuur van het rapport helder was, hebben we de segmenten van de groepscode doorgenomen en een beschrijvende analysestrategie gehanteerd om te komen tot een duidelijke beschrijving van aard en aanpak van hybride vormen van criminaliteit (Evers, 2024: 122-123). Voor de hoofdstukken over de aard van hybride vormen van criminaliteit (hoofdstukken 2 tot en met 4) hebben we een andere manier van werken gekozen dan voor de hoofdstukken over de aanpak (hoofdstuk 5 en 6). In het eerste geval hebben we per hoofdstuk (bijvoorbeeld drugs) gezocht naar deelthema's (bijvoorbeeld digitale drugsmarkten) of specifieke fenomenen (bijvoorbeeld 'county lines'). Daarbinnen was het doel om het thema of fenomeen zo goed en gedetailleerd mogelijk te beschrijven. In de beschrijving hebben we gebruik gemaakt van zowel de inzichten uit de interviews als de door ons verzamelde voorbeelden. Daarbij hebben we getracht om onze bevindingen te kalibreren en te verbinden met reeds bestaande inzichten uit eerder onderzoek, om zo verschillende aspecten van processen van hybridisering beter te begrijpen, met bijzondere aandacht voor de verwevenheid tussen online en offline, fysiek en digitaal en, meer in het algemeen, de mens en technologie. In hoofdstuk 5 hebben we, ingegeven door de deelvraag, ons in eerste instantie gericht op uitdagingen in de Nederlandse aanpak van hybride vormen van criminaliteit. Hoofdstuk 6 geeft, ten slotte, per land een beeld van concrete aanpakken.

1.6 Leeswijzer

Dit rapport is als volgt opgebouwd. We beginnen met een drietal hoofdstukken over hybride verschijningsvormen van criminaliteit. In hoofdstuk 2 beginnen we met het thema financieel gemotiveerde (cyber)criminaliteit. Vervolgens gaan we in hoofdstuk 3 in op geweld tussen (groepen) jongeren en gewelddadigheden. Hoofdstuk 4 geeft een beeld van gedigitaliseerde drugsmarkten. In de laatste twee hoofdstukken verleggen we onze aandacht naar de aanpak van hybride vormen van criminaliteit. We beginnen in hoofdstuk 5 met het schetsen van de uitdagingen die er in de Nederlandse context worden ervaren als het gaat om de aanpak van criminele verschijningsvormen met zowel een online als een offline component. In hoofdstuk 6 geven we vervolgens per land een voorbeeld van een aanpak van hybride vormen van criminaliteit. We besluiten in hoofdstuk 7 met een overzicht en synthese van de belangrijkste bevindingen en een aantal concrete aanbevelingen.

2 Financieel gemotiveerde vormen van (cyber)criminaliteit

2.1 Inleiding

Dit hoofdstuk vormt het eerste van drie hoofdstukken waarin een beeld wordt geschetst van de aard van hybride criminaliteitsvormen die we in Nederland, Denemarken en het Verenigd Koninkrijk zijn tegengekomen (deelvraag 1). We beginnen met voorbeelden die in de wetenschappelijke literatuur doorgaans bestudeerd worden onder de vlag van cybercriminaliteit en meer specifiek worden geclassificeerd als *cyber-enabled crimes* (Wall, 2007; McGuire en Dowling, 2013b), gedigitaliseerde delicten (Oerlemans, Hingh en Van der Wagen, 2024) of financieel gemotiveerde vormen van cybercriminaliteit (Bekkers, 2025; Leukfeldt en Holt, 2022; Loggen, Moneva en Leukfeldt, 2024). In paragraaf 2.2 richten we ons op wat wordt omschreven als ‘online fraude’, waarbij onder andere aandacht wordt besteed aan bankhelpdeskfraude in Nederland. Vervolgens wordt in paragraaf 2.3 het fenomeen besproken dat in het Verenigd Koninkrijk bekend staat als ‘*wrench attacks*’: smartphones die worden gestolen om vervolgens in applicaties van onder andere banken geld over te maken naar andere rekeningen. Paragraaf 2.4 behandelt de rol van zogenoemde geldezels, een verschijnsel dat in alle drie de landen wordt herkend en dat bovendien een duidelijke relatie vertoont met de onderwerpen die in de eerste twee paragrafen van dit hoofdstuk aan bod komen. We besluiten dit hoofdstuk met reflectie op de belangrijkste, overstijgende bevindingen.

2.2 Bankhelpdeskfraude

Het eerste voorbeeld dat door respondenten in zowel Nederland als Denemarken in de interviews werd benoemd, betreft bankhelpdeskfraude. Tijdens de interviews met respondenten uit het Verenigd Koninkrijk werd slechts in één gesprek gesproken over bankhelpdeskfraude en aanverwante voorbeelden van fraude en oplichting.³ Dit thema heeft de nodige aandacht in de wetenschappelijke literatuur (zie o.a. Bekkers et al., 2020; 2023; 2024; Leukfeldt et al., 2017c; Leukfeldt et al., 2020). In het recente fenomeenbeeld *Online fraude in beeld* van de Nederlandse politie (Politie, 2024: 17) wordt

3 Om deze reden beperken we ons in deze paragraaf tot de inzichten van de Nederlandse en Deense respondenten.

dit type delicten aangeduid als ‘online fraude’ en niet als ‘gedigitaliseerde criminaliteit’. Deze terminologische keuze is opmerkelijk, in het bijzonder omdat hiervoor geen nadere toelichting wordt gegeven. Een dergelijke benaming lijkt te impliceren – analoog aan wat in het eerste hoofdstuk werd opgemerkt over de bredere term ‘online criminaliteit’ – dat het gaat om fraudevormen die zich uitsluitend in digitale of online omgevingen lijken af te spelen.

Empirische studies laten echter consistent zien dat de menselijke factor, evenals lokale en offline aspecten, een cruciale rol spelen bij deze vorm van financieel gemotiveerde cybercriminaliteit (Bekkers, Leukfeldt en Kleemans, 2024; Leukfeldt en Holt, 2022; Leukfeldt en Weulen Kranenbarg, 2017; Loggen en Leukfeldt, 2022; Loggen et al., 2024). Dit punt wordt duidelijk wanneer gekeken wordt naar bankhelpdeskfraude. Slachtoffers worden bij deze vorm van oplichting telefonisch benaderd door personen die zich voordoen als bankmedewerkers, en die hen overtuigen dat hun banktegoeden onveilig zijn en hen onder druk zetten om deze zogenaamd veilig te stellen. In werkelijkheid worden de gelden overgemaakt naar rekeningen die onder controle staan van de oplichters. Een voorbeeld van een rechtszaak illustreert de rol van zowel fysieke als digitale handelingen in de modus operandi:

‘De eerste stap is dat de daders de hand weten te leggen op persoonsgegevens van slachtoffers, zogenaamde leads. Zo beschikken de daders over namen, telefoonnummers en bankrekeningnummers (van één bank; in de onderhavige zaak de Triodos Bank) van een groot aantal potentiële slachtoffers.

Vervolgens belt één van de (veelal vrouwelijke) daders, de zogenaamde social engineer, het potentiële slachtoffer. Zij stelt zich voor onder een valse naam en zegt werkzaam te zijn op de fraudeafdeling van de, in deze zaak, Triodos Bank. In de onderhavige zaak werd meerdere malen de naam [A] gebruikt; de social engineer creëert al snel een penibele situatie door het slachtoffer voor te houden dat een groot bedrag van de bankrekening was geprobeerd te halen, dat de bank dit had weten te voorkomen en de bankpassen omgeruild moeten worden omdat die besmet zijn. Haast is geboden; de social engineer biedt een helpende hand en geeft aan dat het programma Anydesk (een externe desktopapplicatie) dient te worden gedownload om de rekening en de systemen van het slachtoffer op virussen te kunnen controleren. Hoewel de social engineer aangeeft dat dit een anti-virusscanner is, is dit in werkelijkheid een remote control applicatie waarmee de social engineer op afstand kan meekijken met wat het slachtoffer op zijn/haar scherm ziet en doet; vervolgens bemachtigt de social engineer de pincodes en eventuele andere inloggegevens van de betaalpas(sen) en/of creditcard(s) van het slachtoffer door hem/haar de pincodes hetzij in te laten spreken, hetzij in te laten voeren op het scherm.

Tot slot wordt de komst aan huis van een collega van de bank aangekondigd, die zich ook daadwerkelijk kort daarna aan de deur meldt en identificeert met een alias en een controlenummer. Dit nummer heeft de social engineer aan het slachtoffer doorgegeven. Deze zogenaamde collega van de social engineer wordt (veelal) door de slachtoffers binnengelaten. Aldaar worden de bankpassen doorgeknipt, waarbij de chip in

stand gelaten wordt, waarna deze collega met de passen weer vertrekt. In enkele gevallen is ook een telefoon en/of tablet meegegeven voor controle op virussen. Doorgaans wordt in de uren na dit bezoek geld afgeschreven van de bankrekeningen van de slachtoffers. Naar later blijkt door pintransacties en aankopen.’ (Rechtspraak.nl, ECLI:NL:RBMNE:2024:5743)

Slachtoffers worden misleid en opgelicht door middel van digitale technologieën, maar de uitvoering en impact van deze delicten zijn vaak ingebed in fysieke contexten. Dit voorbeeld van bankhelpdeskfraude geeft duidelijk aan waarom de typering online fraude in dit geval te beperkt is, en dat ook het begrip gedigitaliseerde fraude onvoldoende recht lijkt te doen aan de verwevenheid van fysieke en technische handelingen. We lichten dit in het vervolg van deze paragraaf nader toe aan de hand van de vermelde stappen in de modus operandi van bankhelpdeskfraude.

Een eerste wezenlijke stap is het verkrijgen van zogenoemde *leads*, oftewel lijsten met telefoonnummers van potentiële slachtoffers. In de genoemde rechtszaak gaat het over namen, telefoonnummers en bankrekeningnummers van een specifiek bank. In Nederland vertelde een respondent dat het voorkomt dat personen een bijbaan hebben – of zoeken – bij organisaties die op grote schaal toegang hebben tot dergelijke informatie:

‘Het is gewoon een bijbaantje nemen bij een publieke organisatie zoals Vattenfall of KPN. Ik heb twee zaken gezien waar iemand gewoon de hele dag screenshots zat te maken van gegevens van mensen die wat ouder waren, van een potentieel slachtoffer dus. Daar heb je al in mijn ogen een offline component waar iemand uit een groep gewoon screenshots maakt bij zo’n publiekelijke partij.’ (RNL-3)

Hoewel technologie hier een rol speelt in de vorm van (legitieme) toegang tot computersystemen en het maken en doorsturen van screenshots, gaat het hier vooral om de menselijke toegang en verspreiding van deze informatie. We zien dit eveneens terug in de werkwijzen die door Deense respondenten werden beschreven om toegang te krijgen tot potentiële slachtoffers:

‘What they found out was an elderly lady who had just buried her husband. They saw that in the newspaper. She’s old and she’s alone and she has got all the money now. They called her. We’re from the bank. We can see that somebody is trying to move all your money. Let’s help you take all your money, put it into a safe account. To do that, we need your information. We need your bank codes. She gave them unwillingly. They were on the phone for hours trying to help this old lady, moving all her money. It could be hundreds of thousands of crones [tienduizenden euro’s, RR] moved from her account to their accounts. It happened to a lot of people.’ (RDE-5)

Een ander voorbeeld dat tijdens de interviews in Denemarken werd genoemd had betrekking op het online zoeken naar overlijdensadvertenties. Een respondent werkzaam

bij de Deense politie vertelde dat criminelen op zoek gingen naar advertenties met namen waarvan zij op basis van de voornaam vermoedden dat deze ‘oud’ klonken en dat zij vervolgens probeerden de telefoonnummers van nabestaanden te achterhalen. Als het gaat om leads werd door respondenten echter ook gewezen op de online handel in gegevens van slachtoffers die plaatsvindt op het dark web (vgl. Hutchings en Holt, 2014), maar ook op socialemediaplatform Telegram Messenger (vgl. Garkava, Moneva en Leukfeldt, 2024). Het kan daarbij zijn dat de leads verkregen zijn via een hack. Hiermee wordt duidelijk dat de grens tussen cyber-dependent en cyber-enabled crimes in de praktijk meer fluïde is dan dit onderscheid indiceert (vgl. Lusthaus, 2024). Een tweede stap in de modus operandi van bankhelpdeskfraude is het contact leggen met de potentiële slachtoffers. Dit bellen wordt volgens respondenten vaak op specifieke fysieke locaties georganiseerd. In de Nederlandse interviews werden voorbeelden gegeven van hotelkamers, een airbnb, maar ook vakantiewoningen op recreatieparken die gehuurd werden voor deze activiteit. Een respondent licht toe hoe er dan vervolgens te werk wordt gegaan:

‘Dan krijg je aan de linkerkant zo’n lijst en aan de rechterkant een belscript. Dus je moet het eigenlijk alleen maar oplezen. Natuurlijk moet je wel bepaalde skills hebben. Je moet niet zeggen dat je mevrouw De Jong van de Rabobank bent en met straattaal aankomen. Maar het is wel een stuk simpeler dan vaak gedacht.’ (RNL-3)

Met de leads wordt telefonisch contact gelegd en er wordt getracht om het vertrouwen te winnen van de slachtoffers. Respondenten noemen hierbij het vermogen om op een overtuigende manier een zorgvuldig opgesteld script te volgen. Hierbij werd bijvoorbeeld gewezen op iemand die goed ABN kan spreken of, zoals in een ander interview werd benoemd, het gebruik van vrouwen omdat dit meer overtuigend zou overkomen in het proces van oplichting.

In het proces van het benaderen van slachtoffers werd door respondenten gewezen op de centrale rol van *social engineering*: een vorm van psychologische manipulatie waarbij slachtoffers misleid worden om toegang te verkrijgen tot gevoelige informatie of digitale systemen (Politie, 2024: 149). Door zich voor te doen als een legitieme instantie wordt bewerkstelligd dat slachtoffers daadwerkelijk ergens op klikken, zoals op een zogenoemde remote access tool (Leukfeldt et al., 2017b; Lusthaus, Kleemans, Leukfeldt, Levi en Holt, 2023), of er wordt via andere overredingstechnieken geprobeerd slachtoffers zover te krijgen dat ze hun inloggegevens of andere relevante bankgegevens delen. Tijdens de interviews in Denemarken werd gewezen op het gebruik van *spoofing*, een techniek die het mogelijk maakt dat het telefoonnummer dat op het scherm van de potentiële slachtoffers verschijnt, overeenkomt met dat van een bank. Dit creëert een zekere mate van vertrouwen en versterkt het gevoel dat men de oproep moet beantwoorden, omdat deze afkomstig lijkt van een legitieme instantie zoals de bank.

De laatste wezenlijke stap in het proces van bankhelpdeskfraude betreft het verplaatsen van het geld van de rekening van de slachtoffers. In Nederland wordt door de politie

een onderscheid gemaakt tussen drie verschillende methoden (Politie, 2024: 70). Allereerst zijn er slachtoffers die na het horen dat hun bankrekening is gehackt of dat er frauduleuze transacties zijn ontdekt hun geld zelf overmaken naar een rekening die door de bellers wordt getypeerd als veilig. Een tweede meer technische methode betreft het verkrijgen van toegang tot de computers van slachtoffers middels de eerdergenoemde remote access tools. Binnen de digitale bankomgeving worden er bijvoorbeeld daglimieten verhoogd, spaargeld verplaatst naar de betaalrekening of transacties klaargezet. De slachtoffers merken dit niet omdat het scherm bewust zwart wordt gemaakt (Politie, 2024: 70). Een derde methode betreft het ophalen van de bankpas, zoals ook beschreven in de voornoemde rechtszaak. Nadat het slachtoffer is overtuigd dat de pinpas moet worden vervangen, verschijnt er iemand aan de deur om de pas op te halen. De politie (Politie 2024: 70) beschrijft dat slachtoffers instructies krijgen om de pas door te knippen of de pincode mee te geven in een envelop, waardoor de pas alsnog gebruikt kan worden. In deze laatste methode ligt de nadruk wederom op het menselijk contact, dit keer tijdens een fysieke interactie. Ook in Denemarken wordt dit waargenomen, waarbij deze wijziging in de modus operandi gezien kan worden als reactie op de meer preventieve aanpak van dit fenomeen:

‘We give them all sorts of information to prevent this. It helped. It didn't remove the problem, but it helped a lot. Then the perpetrators shifted. (...) Now, we have to cancel your credit card. We will issue a new one. You will have that one in a few days. But we need your current card and your code to prevent more crimes. We will send somebody to pick it up. And they did so and they're doing so these days.’ (RDE-5)

In Nederland wordt dit door respondenten eveneens gesignaleerd: criminelen komen aan de deur en vragen om een pinpas, bijvoorbeeld door zich voor te doen als een medewerker van een bank of door te verschijnen in een PostNL-uniform. Tijdens interviews werden daarnaast voorbeelden genoemd van nepagenten die hierbij een rol spelen.

De genoemde stappen geven zicht op verschillende personen die in de modus operandi van bankhelpdeskfraude een rol van betekenis spelen. In de interviews in Nederland werd gewezen op verschillende rollen en een zekere taakverdeling die valt te onderscheiden in de samenwerking, waaronder personen die zorg dragen voor leads, bellers, individuen die inloggen op de bankrekening en het geld verplaatsen en zogenoemde geldezels. In het fenomeenbeeld *Online fraude in beeld* spreekt de politie (Politie 2024: 148) in dit verband van criminele groeperingen met een zekere samenwerking, structuur en samenstelling. De vraag die zich opdringt is hoe dergelijke samenwerkingen tot stand komen en hoe de betrokkenen elkaar hebben leren kennen. De literatuur over cybercriminaliteit laat zien dat er binnen samenwerkingsverbanden vaak sprake is van personen die elkaar reeds langere tijd kennen (zie o.a. Dupont et al., 2017; Leukfeldt et al., 2017a; 2017b; 2017c; Roks, Leukfeldt en Holt, 2024). Ook respondenten wezen op de lokale inbedding van samenwerkingsverbanden, veelal bestaande uit vrienden en familieleden. Een Deense respondent verwoordde dit als volgt: *‘In my experience,*

within Denmark, I think that in most cases, these criminals know each other from real life’ (RDE-10). Tegelijkertijd werd beschreven dat in de zoektocht naar mededaders ook gebruik wordt gemaakt van online kanalen. In studies naar het ontstaan en de ontwikkeling van cybercriminele netwerken wordt niet alleen gewezen op de blijvende rol van de offline wereld, maar ook de rol van forums (zie o.a. Leukfeldt, 2014; Leukfeldt et al., 2017a; 2017b). Tijdens de interviews werd vooral gewezen op de rol van socialemedia-platformen. Tijdens een van de gesprekken in Nederland werd gewezen op het gebruik van Telegram Messenger, maar ook van Snapchat en Instagram om aan geschikte mededaders te komen, waaronder ook geldezels, zoals we in paragraaf 2.3 zullen toelichten.

2.3 ‘Wrench attacks’

Het tweede voorbeeld dat we in dit hoofdstuk bespreken, zijn de zogenoemde ‘wrench attacks’. Dit voorbeeld werd exclusief benoemd in meerdere gesprekken met respondenten in het Verenigd Koninkrijk als een criminaliteitsvorm waarbij sprake is van een overlap tussen het fysieke en het digitale. We beginnen met een voorbeeld uit de Britse media om dit fenomeen te introduceren:

‘On a recent night out the 28-year-old healthcare professional was kind enough to help a man who asked to borrow her phone. Less than six hours later, her £9,350 life savings had been spent by him on Apple products in London. And the final indignity: he used her Uber account to take a cab to Stansted airport.

Her story, which could almost be used by schools to teach young people how not to expose themselves to financial risk, started after a Friday night out with friends in London. While she was waiting for her 5am taxi to come and take her home, she got chatting with a man who asked if he could use her mobile, saying his had stopped working. Having unlocked her iPhone she handed it over. What happened next is a bit of a blur, she says, but it now appears she was distracted by his accomplice. When she turned around, her new friend and her phone had gone – along with her Metro Bank debit card, which she carried in her phone case.’ (Brignall, 2024)⁴

De oorsprong van het gebruik van de term ‘wrench attack’ voert volgens Ordekian en collega’s (2024: 2) terug op een webcomic: *‘The comic describes two characters discussing a physical attack using a \$5 wrench to force the victim to provide information rather than orchestrating a cyberattack’*. Het idee is dat een eenvoudige moersleutel of steeksleutel in dit beeld fungeert als metafoor voor het omzeilen van complexe encryptie door middel van fysieke dwang of misleiding (Ordekian et al., 2024: 2). In het enige beschikbare wetenschappelijke artikel over dit fenomeen richten Ordekian en collega’s (2024) zich vooral op fysieke aanvallen die zich richten op de telefoons van cryptoge-

4 <https://www.theguardian.com/money/2024/mar/02/i-was-in-despair-how-lending-a-phone-led-to-life-savings-being-stolen>, laatst bezocht op maandag 5 januari 2026.

bruikers. De interviews met respondenten in het Verenigd Koninkrijk, in het bijzonder met twee personen werkzaam bij de politie in Londen, schetsen een breder beeld. In 2022 werden er door de Metropolitan Police in Londen in totaal 256 zaken geregistreerd waarbij mobiele telefoons werden gestolen en digitale activa uit bankapplicaties en andere digitale *wallets* werden verplaatst. In 2023 steeg dit aantal tot 808 delicten, een toename van 215% ten opzichte van het voorgaande jaar.

Wrench attacks zijn te zien als een voorbeeld van een hybride delict: het gaat om fysieke vormen van criminaliteit om de barrières van digitale encryptie te slechten. Deze vorm van criminaliteit vereist, met andere woorden, geen specifieke technische vaardigheden, maar maakt eerder gebruik van traditionele delicten zoals geweld, diefstal, overvallen of afpersing (Ordekian et al., 2024: 2). Dit kan gepaard gaan met fysiek geweld, maar dat hoeft niet noodzakelijkerwijs, zoals een respondent beschreef in een concreet voorbeeld:

‘There will often be an element of social engineering. So, suspects trying to befriend victims when they’re drunk outside these nightclubs or when they’re waiting for an Uber. If they’ve got the phone unlocked and they’re standing, interacting with it or saying things like: will you, add me on social media, so that there’s a handing over of a device when it’s unlocked. And at that point, we’re seeing suspects working in groups. One of them will be engaged in the social engineering element to get that victim talking with the phone unlocked, there will potentially be somebody else videoing the inputting of the PIN number. There will then be potentially another person that’s involved in the actual taking of the phone.’ (RVK-12)

Wrench attacks vinden veelal plaats in het uitgaansleven en in de nachtelijke uren, vaak rond sluitingstijd van horecagelegenheden en niet zelden als het slachtoffer onder invloed is van alcohol. Veelvoorkomende methoden om de telefoon afhandig te maken, zijn volgens respondenten het vragen naar de tijd, het verzoek om toegevoegd te worden op sociale media of het onderscheppen van de telefoon wanneer deze wordt gebruikt voor andere doeleinden, zoals het boeken van een taxi. In sommige gevallen worden bedreigingen of fysiek geweld toegepast, maar in veel gevallen lijkt er sprake van afleidingstechnieken en social engineering om slachtoffers ertoe te bewegen hun ontgrendelde mobiele telefoons af te staan.

Volgens de respondenten worden wrench attacks vaak uitgevoerd in groepen, waarbij één persoon het slachtoffer afleidt, een ander observeert hoe de toegangscode wordt ingevoerd, en een derde de telefoon steelt. Een cruciaal element in deze delicten is dat de verdachten toegang moeten verkrijgen tot het toestel terwijl het actief is, of dat zij de toegangscode observeren om later toegang te krijgen tot financiële applicaties. Na de diefstal worden beveiligingsfuncties omzeild, waaronder het wijzigen van het aan het toestel gekoppelde e-mailadres en wachtwoorden. Vervolgens worden financiële transacties geprobeerd of uitgevoerd via accounts die aan het toestel zijn gekoppeld. In sommige gevallen is ook persoonlijke informatie op het toestel gebruikt om leningen af te sluiten (Ordekian et al., 2024). Het voorgaande maakt duidelijk dat het in het geval

van wrench attacks gaat om een vorm van criminaliteit die een zekere samenwerking vereist. Een van de respondenten licht dit nader toe:

'In some cases, we think it's the same group of suspects. If there is one that's technologically literate, then he will be the one that's doing the transferring in the phone. In other cases, we think that the phones are handed over to somebody who's then involved in the laundering of the phone funds from the phone. We also see lots of young people who would traditionally be involved in these types of thefts, then using the money to buy Apple iPhones or high value luxury goods. So, we think that those are probably going to those people, but not in some of these cases. We're seeing victims losing over hundreds of thousands of pounds from a single phone theft. So, the youths that we've seen involved in this type of street robbery aren't living the lifestyles of people who are earning that amount of money. So, we think that there will be, in the more organized networks, other people involved in the laundry.' (RVK-12)

Tijdens de interviews werd een onderscheid aangebracht tussen personen met een meer aansturende en een organisatorische rol. Andere betrokkenen, zoals degenen die daadwerkelijk telefoons stelen, ontvangen hiervoor een vastgesteld bedrag. Het vermoeden bestaat dat een ondersteunend netwerk van geldezels en tussenpersonen betrokken is bij de verdere verspreiding van gelden afkomstig van de rekeningen van slachtoffers. In bepaalde gevallen worden deze gelden eerst verplaatst tussen rekeningen van verschillende slachtoffers, alvorens zij worden omgezet in cryptovaluta of overgemaakt naar andere rekeningen. In andere gevallen zijn dezelfde verdachten zowel betrokken bij de oorspronkelijke diefstal als bij de latere verspreiding van de gelden.

Het stelen van de mobiele telefoon wordt op deze manier, zoals een respondent toelicht, extra lucratief:

'Yeah, with the but and I think the reality is that the hybridization makes it more lucrative. That's definitely something we've seen. A mobile phone robbery will get about 700, 800, with a crisper, new iPhone, second hand. But we've seen one offence where people have lost like 6 figures at £250,000 or something. So, it is a bit luck of the draw. But yeah, you can potentially, if you're the offender, really like hit the jackpot.' (RVK-15)

Het gaat hier om een vorm van criminaliteit waarmee in potentie aanzienlijke bedragen gemoeid zijn. Verliesbedragen van €10.000 zijn volgens respondenten niet ongebruikelijk; in één geval werd volgens een respondent zelfs een verlies van meer dan €150.000 gerapporteerd. Uit de interviews blijkt echter dat het niet uitsluitend gaat om het verplaatsen van geld via bankapplicaties; ook applicaties zoals Uber of andere bestelapps worden gebruikt om goederen en diensten af te nemen via de toegang tot de gestolen telefoons. Een respondent werkzaam in de academische wereld gaf hiervan een voorbeeld:

‘So, they’re just going through the phone, and I think they told him: right, you need to open your phone up like they had the knife to his stomach and they’re like: open your phone! And then I think they made him like, just remove the password on his phone. And then they just ran off. Right. So, they clearly know: everything is in the phone. The minute we get access to that, you know, and it’s quite easy too. And people aren’t, you know, particularly technologically savvy. They use the same password, or they’ve got only the password on their phone, but they’ve not got passwords for anything else.’ (RVK-8)

In dit geval werd, zoals ook in interviews met de politie naar voren kwam, de Deliveroo-app van het slachtoffer volledig leeggehaald en er werd massaal eten besteld. Respondenten werkzaam bij de politie noemden daarnaast een ander voorbeeld waarbij informatie op mobiele telefoons werd gebruikt om leningen af te sluiten, bijvoorbeeld omdat er foto’s van paspoorten of rijbewijzen op het toestel waren opgeslagen.

In de interviews werd, net als in het artikel van Ordekian en collega’s (2024), gesignaleerd dat dergelijke wrench attacks zich voor een deel lijken te concentreren op cryptovaluta. In dergelijke gevallen lijkt het dat bezitters van cryptovaluta in hun telefoon heel nadrukkelijk worden gezocht of geselecteerd als slachtoffer:

‘This is all anecdotal, but we’ve seen several instances where the victims have been identified through breach data, so they’re buying breach data online, identifying people who they’ve got reason to believe, have large crypto holdings and then targeting them. And that is already a methodology.’ (RVK-15)

Een andere respondent gaf het voorbeeld van online informatie die wordt verzameld over personen met aanzienlijke hoeveelheden cryptovaluta: *‘But this starts online potentially with these ones, and similarly other ways we’ve seen victims identified as through social media activity. If they’re advertising crypto wealth’* (RVK-15). Deze variant maakt de verwevenheid tussen de online en offline dimensie in het geval van wrench attacks nog duidelijker: de verkregen informatie via een datalek of het doorzoeken van social media-accounts wordt vervolgens benut om deze personen in de fysieke wereld te lokaliseren. In meer extreme situaties leidt dit volgens respondent zelfs tot het opzoeken van slachtoffers in hun woningen en het toepassen van geweld.

2.4 Witwassen: de rol van geldezels

Het laatste onderwerp dat we in dit hoofdstuk bespreken zijn zogenoemde geldezels, een fenomeen dat door respondenten in alle drie de landen werd genoemd als voorbeeld van een criminele verschijningsvorm met een duidelijke verwevenheid tussen online en offline dimensies. Geldezels zijn personen die een cruciale rol spelen in het witwassen van verdiensten die op een illegitieme manier zijn verkregen (Bekkers, 2025: 14), bijvoorbeeld geld dat verkregen is via de twee criminele verschijningsvormen die we eerder in dit hoofdstuk bespraken. Tot op heden krijgt het fenomeen van

geldezers vooral aandacht in de wetenschappelijke bestudering van cybercriminaliteit (zie voor een overzicht Bekkers, 2025: 14). Alhoewel respondenten de rol van geldezers veelal benoemden in de context van cybercriminele activiteiten zoals bankhelpdesk-fraude of phishing, werd eveneens benadrukt dat hun rol zich niet beperkt tot deze vormen van criminaliteit.

In de interviews werden verschillende voorbeelden gegeven van de activiteiten van geldezers, waarbij er per land verschillen werden benoemd. Een respondent uit het Verenigd Koninkrijk gaf het volgende voorbeeld:

‘They will put out a message and just be like, does anybody fancy making some money? DM me, you know, on their story. And what happens is they say: give us your bank account details, or even in some instances, sell us your bank account details. And what happens is £500 comes in and then £450 comes out. Right? But they do it multiple times. So, for the kid that’s just given up their bank account, I mean all they’ve done is just like receive some money then move some money on. It’s pretty easy. And they’ve earned £50 and they do it a couple of times a week.’ (RVK-8)

In het Verenigd Koninkrijk werd naar deze witwaspraktijken verwezen als *‘deets and squares’*: het eerste als aanduiding voor de details (*‘deets’*) van bancaire gegevens en het tweede als verwijzing naar de vierkante vorm van bankpasjes (*‘squares’*) die in sommige gevallen door geldezers ter beschikking worden gesteld. Ook in de Deense context werd gesproken over een dergelijke manier van handelen. Sterker nog, de politie in het Deense Noord-Jutland publiceerde in 2022 een bericht op haar website waarin nadrukkelijk werd gewaarschuwd voor deze praktijken:

“Laat anderen je telefoon niet gebruiken”, zegt politiecommissaris Simon Hjorth Jacobsen van de politie van Noord-Jutland, toen hem werd gevraagd zijn belangrijkste preventieve boodschap samen te vatten voor jongeren die in deze vrolijke kersttijd in het nachtleven feesten. De jongeren dreigen – als een zeer onaangenaam ‘dankjewel’ voor hun overigens vriendelijke gebaar – te eindigen als criminele geldezers. Van zogenoemde geldezelffraude is sprake wanneer mensen (vaak te goeder trouw) op de een of andere manier hun rekening ter beschikking stellen aan criminelen die er op deze manier in slagen om geld wit te wassen. Dit kan bijvoorbeeld gebeuren door in de voetgangersstraat te worden aangehouden en te worden gevraagd geld op te nemen voor iemand in ruil voor het mobiel overmaken van een bedrag naar je rekening. “Wat we nu zien, is dat het zich afspeelt in het nachtleven, waar sluwe criminelen misbruik maken van de dronkenschap van mensen om hun mobiele telefoons te lenen en hen zo te betrekken bij het witwassen van geld”, legt de politiecommissaris die aan het hoofd staat van de preventieafdeling van de politie in Aalborg uit. De fraude kan in verschillende fasen plaatsvinden: een persoon slaagt erin de mobiele telefoon van de geldezel te lenen en maakt vervolgens een veel groter bedrag over dan afgesproken aan een andere persoon. Deze andere persoon maakt het geld vervolgens over aan een

*derde persoon, die de taak heeft het geld op te nemen en vervolgens de gestolen creditcard te melden bij de bank en de politie.*⁵

Een concreet voorbeeld hiervan werd geschreven in een nieuwsartikel in een populaire Deense krant:

‘Een paar tienerjongens, beiden uit Haderslev, van 16 en 17 lopen het risico een straf te krijgen nadat ze zijn beschuldigd van het witwassen van geld. Beide beschuldigden zijn, volgens de politie in Zuid-Jutland, gecontacteerd door onbekende mannen via Snapchat voor hulp om een groter bedrag aan contanten te krijgen. De 17-jarige stelde zijn account beschikbaar zodat de man een bedrag van 9500 kronen kon overmaken, dat vervolgens werd verhoogd en overgedragen op het treinstation van Vojens (...). De politie waarschuwt burgers voor het beschikbaar stellen van hun account, MobilePay of NemID aan anderen. Het risico bestaat dat je een geldezel wordt voor criminelen. In sommige gevallen lijkt de hulp misschien onschuldig als iemand bijvoorbeeld uitlegt dat hij zijn creditcard is verloren en hulp zoekt van iemand aan wie geld kan worden overgemaakt en die dat geld vervolgens voor hem kan opnemen. In andere gevallen zijn er berichten op Snapchat, waar het lijkt dat je snel en gemakkelijk geld kunt verdienen door je account beschikbaar te stellen, legt politiecommissaris Dennis Holst uit van de politie in Zuid-Jutland.’ (Eriksen, 2022)⁶

Voorbeelden van het ter beschikking stellen van bankgegevens, waarop vervolgens geld wordt gestort en doorgesluisd naar een andere rekening, werden in de interviews met Nederlandse respondenten niet expliciet genoemd: zij wezen vooral op het uitleenen van bankpasjes om geld op te nemen bij een automaat. Ook gaven zij voorbeelden van geldezels die cadeaukaarten aanschaffen of met geld dat op hun rekening wordt gestort dure goederen kopen zoals iPhones. Alhoewel de specifieke handeling van een geldezel aldus kan verschillen, zien we dat zij in alle voorbeelden nadrukkelijk in beeld komen bij opsporingsinstanties. Bovendien faciliteert deze manier van werken dat betrokkenen, die veelal een organisatorische of aansturende rol hebben bij de (cyber) criminele activiteiten, buiten beeld blijven (vgl. Bekkers, 2025).

De handelingen van geldezels vereisen, zo maakt het bovenstaande duidelijk, niet direct enige technische kennis of vaardigheden, of zoals een respondent uit het Verenigd Koninkrijk benadrukte: *‘You may have zero technical ability whatsoever. I mean, you could maybe use an ATM. I mean, that’s not really technical’* (RVK-13). De hybridisering die er in het geval van geldezels kan worden waargenomen ziet vooral op het rekruteringsproces (Bekkers, 2025). Respondenten uit alle drie de landen gaven aan dat

5 We hebben een deel van het oorspronkelijke bericht geraadpleegd op maandag 5 januari 2026 via <https://politi.dk/nordjyllands-politi/nyhedsliste/politiet-advarer-unge-lad-ikke-andre-bruge-din-telefon-i-natteliv/>2022/12/08 en naar het Nederlands laten vertalen door Google Translate.

6 We hebben een deel van het oorspronkelijke bericht, geraadpleegd op maandag 5 januari 2026 via <https://ekstrabladet.dk/krimi/teenagere-sigtet-for-hvidvask-kontaktet-paa-snapchat/9569636> naar het Nederlands laten vertalen door Google Translate.

sprake is van een combinatie van online en offline manieren waarop geldezels worden geworven. Daarbij werd benadrukt dat de online wereld, en in het bijzonder socialemediaplatformen, vooral relevant zijn vanwege het bereik. Dit sluit aan bij eerdere studies naar de rol van sociale media in de context van criminaliteit waarin wordt beschreven hoe platformen als Instagram, Snapchat en Telegram Messenger gebruikt worden in het rekruteringsproces en fungeren als *online offender convergence settings* (Bekkers et al., 2024; Bekkers en Leukfeldt, 2022; Bergers et al., 2026; Leukfeldt et al., 2017a; Roks et al., 2021; Soudijn en Zegers, 2012). Tijdens een van de interviews in Nederland werd dit geïllustreerd aan de hand van een concreet voorbeeld uit het onderzoek van een respondent:

‘Ik had één geval, één netwerk, die meer dan vier miljoen hebben gestolen van slachtoffers en daar meer dan 400 geldezels voor hebben gebruikt. Want ja, je kan natuurlijk maar beperkt geld wegsluizen via een geldezelrekening, dus je hebt er heel veel nodig. En ja, om dan alle 400 op straat te vinden, dat is gewoon bijna onmogelijk. Dus de online omgeving die verbreedt gewoon je publiek eigenlijk, waardoor je door heel het land geldezels kan rekruteren. Maar daarbij zie je dus nog steeds dat ze daarbij afhankelijk zijn van de lokale fysieke omgeving. Want je ziet dan bijvoorbeeld van die ronseladvertenties van: wil je nou geld vinden met je pas, neem contact met ons op? Maar dat ze dus in dat soort berichten dus nog steeds verwijzen naar postcodes of naar steden waar ze nog actief zijn.’ (RNL-4)

Sociale media bieden de mogelijkheid tot schaalvergroting. Een respondent van de politie in Nederland haalde hierbij een voorbeeld aan van jongeren uit Oost-Nederland die reageerden op een bericht op sociale media en vervolgens naar de Randstad reisden om hun bankpassen ter beschikking te stellen. Ondanks dat een deel van de werving van geldezels zich afspeelt op socialemediaplatformen, wordt uit zowel de interviews als de wetenschappelijke literatuur duidelijk dat de zoektocht naar geldezels ook nog steeds plaatsvindt in de fysieke wereld, bijvoorbeeld op straat, bij metrostations, op school of in het nachtleven. Er is, kortom, sprake van zowel rekrutering via online als offline wegen, iets dat door respondenten in alle drie de landen werd benadrukt.

Wel kwamen er in de gesprekken verschillen tot uitdrukking als het gaat om de personen die in beeld komen als geldezels. Respondenten uit het Verenigd Koninkrijk verwezen in het bijzonder naar jongeren tussen de 14 en 18 jaar, met sporadische voorbeelden van personen die begin twintig waren. Ook plaatsten zij de activiteiten van geldezels niet zozeer in de context van cybercriminele netwerken, maar van gangs, zoals het volgende voorbeeld illustreert:

‘Well, an older person in a street gang will ask a younger person to do a favor, and they will say, “I need you to hold something for me for three days or a week and then give it back to me. But it’s not a physical thing. It has to go into your bank account, and it has to sit there for a few days, and then I’ll take it out. Uh, but I’ll leave you £100 or

€100. I'll leave that in your account. And that's your reward for helping me." And they will make elaborate excuses as to why this is done. You know, they're changing banks or, um, they're changing their address. They'll create some crazy excuse. And, the money will go into the young person's account, maybe £5000, £10,000. It will stay for 48 hours, and then it will be taken out. It will go. And it creates a problem because the audit trail cannot be traced back to the criminal. It sits with the young person. So, in three or four months' time, the young person's contacted by the bank to say, well, what's been going on with this?' (RVK-7)

In zowel Nederland als Denemarken verwezen respondenten naar geldezels als kwetsbare personen. Soms betreft dat jongeren, maar respondenten gaven ook voorbeelden van geldezels die benaderd worden rondom opvanglocaties of instellingen voor jeugdbescherming.

2.5 Conclusie

In dit hoofdstuk hebben we drie criminaliteitsvormen beschreven die geclassificeerd (kunnen) worden als financieel gemotiveerde (cyber)criminaliteit. In de interviews met respondenten uit Nederland en Denemarken werd allereerst gewezen op bankhelpdeskfraude. Alhoewel dit fenomeen recent door de politie werd getypeerd als online fraude, geven de beschrijvingen in dit hoofdstuk eerder zicht op processen van hybridisering. Op het spectrum van cybercriminaliteit kunnen bepaalde onderdelen van de modus operandi van bankhelpdeskfraude geplaatst worden in de richting van cyber-dependent crimes. Hierbij valt onder andere te denken aan hacks om aan leads te komen, het gebruik van spoofing om slachtoffers te bellen en gebruik van remote access tools om toegang tot de computers van slachtoffers te verkrijgen. Vooral toont zich in het geval van bankhelpdeskfraude de menselijke factor in cybercriminaliteit (Leukfeldt en Weulen Kranenbarg, 2017): er is in de uitvoering van dit fenomeen sprake van een nadrukkelijke wisselwerking tussen mens en (digitale) technologie.

Iets vergelijkbaars zien we op een andere manier terugkomen in het tweede voorbeeld dat we in dit hoofdstuk bespraken. Bij de wrench attacks, een verschijningsvorm die alleen tijdens interviews met respondenten uit het Verenigd Koninkrijk werd benoemd, wordt duidelijk dat de mobiele telefoon de sleutel is tot persoonlijke informatie en met name tot bancaire gegevens. Door de (ontgrendelde) telefoon te stelen, soms onder dreiging met geweld, kan geld van rekeningen overgemaakt worden of kan via andere applicaties goederen of eten besteld worden. In het geval van wrench attacks werden er ook voorbeelden genoemd van personen die op basis van hun socialemediaccontent over cryptovaluta konden worden geïdentificeerd als potentieel slachtoffer.

Het laatste voorbeeld van geldezels vormt een verbindende schakel tussen de twee andere verschijningsvormen van financieel gemotiveerde (cyber)criminaliteit. Het gaat hier om personen die in alle landen op de een of andere manier werden getypeerd als kwetsbaar, die hun persoonlijke informatie, bancaire gegevens of betaalpassen ter beschikking stellen om het illegaal verkregen geld wit te wassen. Ook in dit geval is het de

mens die technische handelingen mogelijk maakt. Daarnaast werd duidelijk dat in de zoektocht naar geldezels gebruik wordt gemaakt van zowel fysieke contacten als van socialemediaplatformen.

Een terugkerende term rondom de verschijningsvormen in dit hoofdstuk is social engineering. Hiermee wordt de socio-technische uitvoering van diverse handelingen benadrukt: het is de mens die centraal staat en gebruikmaakt van de (nieuwe) mogelijkheden van (digitale) technologie om slachtoffers of uitvoerders te overtuigen, te overreden, te misleiden en te werven. Dit komt naar voren in uiteenlopende praktijken, zoals het ophalen of ter beschikking stellen van bankpasjes, het stelen van mobiele telefoons of het inzetten van geldezels. Hiermee wordt zicht gegeven op processen van hybridisering waarin technische infrastructuur en menselijke interactie elkaar versterken. In het volgende hoofdstuk, waarin de nadruk ligt op het thema geweld, wordt dit op een andere manier eveneens duidelijk.

3 Geweld in een hybride context

3.1 Inleiding

Het tweede thema waar we processen van hybridisering waar kunnen nemen is geweld. In de wetenschappelijke literatuur worden online uitingsvormen van geweld aangeduid als *cyber violence* binnen de oorspronkelijke typologie van cybercriminaliteit van Wall (2001). In studies naar straat- en gangculturen zijn dergelijke vormen van digitaal geweld benoemd als ‘*cyberbanging*’ (Haut, 2014), ‘*internet banging*’ (Patton et al., 2013), de digitalisering van de straatcode (Lane, 2019), de *code of the Tweet* (Stuart, 2020a) en meer recent als ‘hybride straatgeweld’ (Mehlbaum et al., 2024). In paragraaf 3.2 gaan we eerst in op geweld tussen (rivaliserende) groepen jongeren en de rol die sociale media hierbij spelen. We richten ons daarbij vooral op voorbeelden uit Nederland en het Verenigd Koninkrijk waarbij sociale media niet alleen fungeren als communicatiemiddel, maar ook gezien kunnen worden als katalysator voor fysieke confrontaties. Vervolgens wordt in paragraaf 3.3 aandacht besteed aan geweldsopdrachten. Dit fenomeen wordt geïllustreerd aan de hand van voorbeelden uit Denemarken en Nederland waarin zichtbaar wordt hoe socialemediaplatformen worden ingezet om personen te werven om gewelddadige handelingen uit te voeren. Het hoofdstuk besluit met meer algemene reflecties op het thema, waarbij de nadruk ligt op de verwevenheid van online en offline dimensies.

3.2 Geweld tussen (groepen) jongeren

In alle drie de landen werd gewezen op geweld tussen groepen jongeren waarbij sprake was van hybridisering. Sociale media spelen hierbij in het bijzonder een rol: conflicten tussen (groepen) jongeren lijken daar te escaleren omdat er over en weer gedigitaliseerde provocaties worden uitgewisseld en afspraken voor fysieke ontmoetingen en vechtpartijen worden gemaakt. Op basis van de interviews werd duidelijk dat dit onderwerp in het Verenigd Koninkrijk al langer op de agenda staat. Een onderzoeker die al meer dan tien jaar geleden publiceerde over dit thema, was destijds als professional werkzaam met jongeren en maakte zich, net als haar collega's, zorgen over ‘*young people being stabbed or killed or raped or sexually assaulted as a result of things that were happening on social media*’ (RVK-4). Op dat moment was er echter nog weinig aandacht voor dit fenomeen in het Verenigd Koninkrijk, iets dat mede naar aanleiding van enkele geweldsincidenten onder (groepen) jongeren zou veranderen (Pinkney en Ro-

binson-Edwards, 2018; Fatsis, 2019; Ilan, 2020). Ook in de andere twee landen werd benoemd dat het gaat om conflicten tussen jongeren die zich vanwege de online component voor een deel aan het oog van professionals onttrekken. Een respondent werkzaam bij de Deense politie gaf hiervan een concreet voorbeeld:

'We had a situation in the district where, out of nowhere, two groups of people met up at a skate park. Young people between the 13 and about 17 or 18 years old. All of them were underage, and they met up with the axes or knives or what do you call the iron fists thing you can put on to? And they just started a beating on each other. And then one got killed, got stabbed, and then they disappeared in all directions, and it came out of nowhere. We didn't know the people. In hindsight, we the police weren't really familiar with the youngsters. Only a couple of them, but nothing in this category. And the investigation, as I recall, took us back to Snapchat, where two groups of people had been trash talking each other and then decided to meet up at the skate park. And I think they actually discussed that we kind of meet up and we're gonna fist fight this out, and no one brings any weapons to it. But they didn't really trust each other, so they both brought different kind of weapons. And then it just turned out horrendous. And a youngster, I'm not sure. 14 or 15, got killed.' (RDE-11-1)

De jongeren in dit voorbeeld waren niet eerder in beeld wegens geweldsdelicten, maar waren bij de politie wel bekend als geldezels. Respondenten verwezen naar dit incident als de Snapchat-moord en het vormt een voorbeeld van een geweldsincident in de fysieke wereld die voor de politie in eerste instantie uit het niets kwam, maar bij nader onderzoek al een duidelijke digitale aanloop kende.

Een respondent in Nederland schetst een vergelijkbare dynamiek zoals werd beschreven in Denemarken:

'Professionals worden vaak ineens geconfronteerd met een geweldsincident of een ander delict en weten dan totaal niet hoe dit heeft kunnen plaatsvinden. Nadat de politie daar onderzoek naar heeft gedaan in gegevensdragers en soms zelfs in openbare bronnen, blijkt dan dat dat allemaal te maken heeft met een online uiting of met iets wat op sociale media heeft plaatsgevonden.' (RNL-2)

De zorg over geweldsincidenten waarbij groepen jongeren betrokken zijn, werd in Nederland expliciet geplaatst in de context van rivaliserende drillrapgroepen. In september 2019 vond in Amsterdam een geweldsincident plaats waarbij een 18-jarige jongeman om het leven kwam. Bij nader onderzoek bleek dat er sprake was van een al langer bestaand conflict met een andere groep uit Amsterdam (De Jong, 2021). De fysieke confrontatie bleek echter niet gepland te zijn, zoals bleek tijdens de rechtszaak:

'Ook de groepen van [medeverdachte], [verdachte] en [slachtoffer] hebben zich meermaals bedreigend tegen elkaar uitgelaten en er hebben in het verleden (steek)incidenten plaatsgevonden waarvan het vermoeden bestaat dat de rivaliteit tussen [drillrap-

groep A] en [drillrapgroep B] daaraan ten grondslag heeft gelegen. Het onderhavige incident echter, blijkt op grond van de stukken in het dossier geen vooraf afgesproken ontmoeting te zijn geweest waarbij de tussen deze groepen bestaande vete uitgevochten moest worden. In die zin is het hof van oordeel dat de rivaliteit tussen [drillrapgroep A] en [drillrapgroep B] in beperkte mate van invloed is geweest op het incident dat op 3 september 2019 heeft plaatsgevonden. Maar deze context is wel de reden dat [medeverdachte], [verdachte] en [slachtoffer] op straat grote messen en machetes bij zich droegen en niet schroomden deze wapens toen tegen elkaar te gebruiken. In zoverre kan de onderhavige strafzaak worden geplaatst tegen de achtergrond van de zorgelijke ontwikkelingen omtrent drillrap in Nederland.’ (Rechtspraak.nl, ECLI:NL:GHAMS:2022:1424)

Een ander Nederlands voorbeeld is een geweldsincident dat plaatsvond in de zomer van 2020. Al langere tijd was er sprake van een conflict tussen een groepering uit Rotterdam en een uit Amsterdam (Roks en Van den Broek, 2020). Op 10 augustus 2020 kwam het, zo is te lezen in een uitspraak van het gerechtshof Den Haag, tot een confrontatie tussen jongeren die zich schaarden achter een van beide groeperingen:

‘Op 9 augustus 2020 heeft [persoon 1] via sociale media een bericht geplaatst waarin hij ook de bedreigingen aan zijn vriendin en familie heeft genoemd:

“[drillrapgroep 2], ksb, en iedereen die linkt met hun zijn kanker flikker ze durven niks te doen bij mij en mijn members enigste stoere wat deze jongens doen is me vriendin bedreigen en onze families exposen terwijl wij willen hun eraf en niet met hun meisjes.

Jullie zijn hun fans toch zeg tegen hun kom ergens midden van Amsterdam en Rotterdam meeten dan gaan we die beef daar regelen in 1x

Ik [bijnaam persoon 1] herhaal ik wil met hun allemaal tegelijk ergens meeten dan gaan we het daar regelen

Ik weet dat ze dit niet willen doen en door gaan gaan met me vriendin pesten [rapper 1] ze vriendin pesten ZEG DIE MANNEN KOM MEETEN

Vandaag vandaag regelen we het nog.

Trouwens volgende snap kijk wat er gebeurd als je pokoes met hun maakt.”

Na deze oproep volgden twee filmpjes waarop te zien is dat [rapper 3] wordt geslagen. [persoon 3] heeft op diezelfde dag op Snapchat een bericht geplaatst met de tekst: “Morgen ben IK Skiffa3 en me loca gaat aan, niemand Wacked mij.”

Het hof stelt vast dat vanwege het conflict door de Rotterdammers en Amsterdammers in berichten over en weer werd bedreigd met geweld en dat in de uitdaging van [persoon 1] niet alleen [drillrapgroep 2] werd uitgedaagd maar ook iedereen die bevriend met hen is. Uit de reactie van [persoon 3] volgt dat hij ingaat op de oproep van [persoon 1].’ (Rechtspraak.nl, ECLI:NL:GHDHA:2025:596)

Anders dan het eerdergenoemde voorbeeld uit Nederland, werd deze confrontatie in zekere zin aangekondigd via sociale media. Op de dag van het incident zelf verschijnen er op diverse accounts op sociale media berichten over een incident dat zich op de Pier van Scheveningen zou hebben afgespeeld, inclusief een video waarop een persoon te zien is die met een vuurwapen door een menigte van jongeren rent. Ook worden er foto's geplaatst van het slachtoffer die bebloed op grond ligt en medische hulp krijgt (vgl. Roks en Van den Broek, 2020: 104-106).

Het thema geweld onder (groepen) jongeren werd in alle drie de landen benoemd, waarbij aangetekend dient te worden dat dit vooral met respondenten uit het Verenigd Koninkrijk en Nederland werd uitgediept met concrete voorbeelden en zorgen. Geweld in het hybride tijdperk is in deze landen – en ook in de Verenigde Staten – in toenemende mate onderwerp van studie. Een respondent uit het Verenigd Koninkrijk vat de stand van zaken in de literatuur als volgt samen:

'I think just to kind of summarize a lot of what the research says, obviously there can be something of an acceleration effect towards violence for kind of two main factors. The first being that the virtual space can create an audience that might otherwise not exist. The second one being that it can archive evidence that might otherwise be forgotten.' (RVK-10)

Veel van het beschikbare onderzoek benoemt sociale media als een katalysator of trigger voor fysiek geweld (zie o.a. Patton et al., 2013; Lauger en Densley, 2018; Moule et al., 2017; Irwin-Rogers et al., 2018; Urbanik en Haggerty, 2018). Bestaande studies illustreren dat sociale media nieuwe en aanvullende mogelijkheden bieden om rivalen uit te dagen en om reputaties binnen straat- en gangculturen op te bouwen (Lane en Stuart, 2022: 2). Sociale media maken conflicten tussen (groepen) jongeren meer zichtbaar en zijn ook toegankelijker voor een breder publiek. Dit kan het verloop van conflicten op een negatieve manier beïnvloeden en kan in sommige gevallen zelfs uitmonden in fysiek geweld (Roks en Van den Broek, 2020; Mehlbaum et al., 2024). Een respondent werkzaam binnen de academische wereld in het Verenigd Koninkrijk, en daarnaast incidenteel betrokken bij advisering van de politie in de aanpak van deze problematiek, verwoordde dit als volgt:

'And in London alone, I can point to maybe 9 or 10 murders where people have seen a video and thought, okay, we're going to come for you now, we're going to come after you because of what you posted. And it's led to people being killed. And that has become a big challenge.' (RVK-7)

Door deze respondent werd nadrukkelijk gewezen op de rol van online content als aanleiding van conflicten die uiteindelijk resulteren in fysiek geweld onder jongeren, soms zelfs met dodelijke afloop. Een voorbeeld hiervan werd breed uitgemeten door de BBC op 3 maart 2020:

‘When a video of an attack on one of the UK’s biggest rap stars went viral, three young people were murdered in the London borough of Haringey over the next 10 weeks. Tensions have long existed between rival gangs in Wood Green and Tottenham, but they rapidly escalated two years ago as tit-for-tat attacks were filmed and posted on Snapchat and YouTube.’⁷

Het bericht op de website van de BBC is een chronologische weergave van de drie geweldsincidenten, inclusief de socialemediaposts die een relevante rol hebben gespeeld in de escalatie van dit conflict. De directe oorzaak van conflicten tussen (rivaliserende) groepen jongeren wordt lang niet altijd duidelijk, zo geven respondenten uit zowel Nederland als het Verenigd Koninkrijk aan. Online circuleren er echter wel de nodige geruchten en brengen jongeren hun ideeën over de herkomst van ruzies, soms ondersteund met allerlei (online) bewijsmateriaal, wel naar voren (Roks en Van den Broek, 2020; Roks, De Jong en Van den Broek, 2024).

De rol van content op sociale media blijft echter niet beperkt tot de aanloopfase, zoals wordt geïllustreerd in een rechtszaak over een geweldsdelict tussen rivaliserende gangleden uit het Verenigd Koninkrijk:

‘Matters did not even stop with the horrific hammer attack and associated kicking to Cemerens’s head and body. You Ramon Djauna actually filmed part of this attack on Snapchat and published that Snapchat video on the internet. I have no difficulty in rejecting your equally ludicrous version of events that you videoed what you were both doing accidentally whilst trying to turn your mobile phone flashlight on and then accidentally published it when you were climbing over a fence as you made good your escape. I am sure that you made that video deliberately, and did so as a trophy, and as a warning to any others who might shame the gang with which you were associated, that they would be met with extreme violence if they crossed you.’ (R-v Aaron Miller, Jacob Morgan, Ramon Djauna and Caleb Brown – 21 May 2019)

In dit voorbeeld wordt de fysieke confrontatie tussen jongeren gefilmd en vervolgens verspreid via sociale media (vgl. Mehlbaum et al., 2024; Roks en Van den Broek, 2020; De Jong, 2021; Van den Broek, De Jong en Moussaid, 2022; Weerman, Roks, Van den Broek en Willink, 2022). Dit kan, zoals een respondent werkzaam bij de Nederlandse politie benadrukte, resulteren in een vicieuze cirkel van geweld:

‘Een cirkel waarin er steeds op elkaar gereageerd wordt. Nou ja, de ene keer begint dat online en de andere keer begint dat fysiek. En het is natuurlijk binnen die rivaliserende jeugd ook een doorlopend verhaal, dus er is al een conflict gaande en dan is er weer een incident en dan zet dat conflict zich weer voort.’ (RNL-6-1)

7 <https://www.bbc.com/news/stories-51722066>, laatst bezocht op maandag 5 januari 2026.

Wanneer gewelddadige content online wordt geplaatst, heeft dit de potentie om viraal te gaan. Het gevolg kan zijn dat de (online) groepsdruk dermate groot wordt, onder andere omdat het online publiek op de digitale straat vele malen groter en anoniemer is dan offline (Urbanik en Haggerty, 2018), dat jongeren zich genooddaakt voelen om met geweld te reageren (Irwin-Rogers e.a., 2018, 406). Dit kan resulteren in 'vicious online-offline violence' (Irwin-Rogers et al., 2018: 404). Mehlbaum en collega's (2024) typeren het geweld onder jongeren tegen deze achtergrond daarom als een 'track', oftewel een keten aan gebeurtenissen die soms plaatsvinden in de fysieke wereld en soms zich vooral afspelen op sociale media.

In de interviews werd door respondenten uit met name het Verenigd Koninkrijk gereflecteerd op de veranderende manier waarop er naar de rol van sociale media in de context van geweld wordt gekeken. Een respondent beschreef dat sociale media in het begin van de wetenschappelijke aandacht vooral werden gezien als '*an addendum or an addition to the ecosystem. Most of the action was still occurring on the streets in person*' (RVK-11). Dit sluit aan bij het werk van Lane (2019) die beschrijft hoe straatculturen de afgelopen jaren zijn losgekoppeld van een geografische locatie en zijn opgesplitst in een fysieke en een digitale straat. Dit denken in twee gescheiden werelden lijkt echter niet langer op te gaan. Tegenwoordig is er, in de woorden van dezelfde respondent, eerder sprake van '*this complete merger where the online and the offline world are not sort of two distinct entities, but they are one and the same*' (RVK-11). Voor deze versmelting wordt in toenemende mate gebruikgemaakt van de aanduiding 'hybride'. Toch is het de vraag of er ook gesproken kan worden van 'hybride straatgeweld' (Mehlbaum et al., 2024). Een deel van de online content, in de vorm van beledigingen, scheldpartijen, provocaties en bedreigingen, zou getypeerd kunnen worden als aspecten van geweld (Schinkel, 2010). Het geweld tussen jongeren waar Mehlbaum en collega's (2024) verslag van doen, is echter hoofdzakelijk lichamelijk en fysiek van aard.

Eerder lijkt er sprake te zijn van processen van hybridisering rondom fysiek geweld onder jongeren, iets dat eveneens wordt geïllustreerd in het werk van Stuart (2020a, 2020b). Op basis van etnografisch onderzoek in de Verenigde Staten laat Stuart (2020a, 2020b) zien hoe jongeren zich in toenemende mate rekenschap geven van de performativiteit van hun gedrag op sociale media, onder andere omdat zij zelf (ook) online content plaatsen waarin zij zichzelf beter, sterker en gevaarlijker voordoen dan ze in werkelijkheid zijn. Als reactie hierop proberen jongeren een zogenoemde '*context collapse*' – een term die verwijst naar het publiekelijk maken van (compromitterende) informatie die funest is voor de manier waarop iemand zich online presenteert (boyd, 2014) – te bewerkstelligen om de gevaarlijke en gewelddadige poses in de digitale content van hun rivalen openlijk op sociale media te betwisten. Ze doen dit aan de hand van het verzamelen, genereren en publiceren van informatie die de online uitingen van hun rivalen tegenspreken of in twijfel trekken (Stuart, 2020a, 2020b).

De studie van Stuart (2020a, 2020b) illustreert dat jongeren gebruikmaken van verschillende strategieën om de performativiteit of de 'fakeness' van de digitale content te laten zien. De eerste strategie betreft '*cross referencing*'. Hiermee verwijst Stuart (2020a, 2020b) naar het proces waarbij door het digitaal verspreiden van informatie in de vorm

van socialemediaposts uit het verleden of privé-informatie of beeldmateriaal waar niet alle volgers van op de hoogte zijn, openlijk vraagtekens worden geplaatst bij online claims van geweld. ‘*Calling bluffs*’, de tweede strategie die Stuart (2020a, 2020b) onderscheidt, gaat een stapje verder. Hierbij worden jongeren die gewelddadige claims op sociale media plaatsen publiekelijk uitgedaagd om de daad bij het (digitale) woord te voegen. ‘*Catching lacking*’ vertegenwoordigt de laatste strategie. ‘*To catch someone lacking*’ wil zeggen dat jongeren worden geconfronteerd in een niet-gang-gerelateerde sociale context, zoals op school of werk, tijdens niet-gang-gerelateerde activiteiten. Het idee hierachter is dat zelfs personen met de meest gewelddadige reputaties zich niet gedurende de gehele dag op deze manier gedragen. Het zijn deze momenten waarop jongeren hopen hun rivalen te treffen zonder de bescherming van andere gangleden of vuurwapens.

Stuart (2020a) beschrijft dat deze drie strategieën verschillen in de mate waarin de uitdagingen resulteren in fysiek geweld, waarbij ‘*catching lacking*’ vanwege het risico op een fysieke confrontatie de hoogste waarschijnlijkheid kent om uit te monden in geweld. In het merendeel van de gevallen resulteren de online uitdagingen echter niet in geweld, maar worden (online) reputaties op sociale media hersteld op innovatieve en niet-gewelddadige wijze. De studie van Stuart (2020a) laat hiermee zien dat sociale media ook nieuwe mogelijkheden bieden om gewelddadige uitdagingen te de-escaleren of te vermijden. Lane en Stuart (2022) wijzen op vergelijkbare wijze op de rol van socialemediaplatformen in het bieden van nieuwe mogelijkheden om geweld te de-escaleren. Met behulp van het concept *communication visibility* benadrukken zij dat stedelijk geweld moet worden begrepen als onderdeel van een breder, digitaal gemedieerd ecosysteem, waarin derden kunnen optreden als beschermende actoren. Hun onderzoek toont zowel directe als indirecte effecten van toeschouwers aan. Bij directe effecten gaat het om interventies van derden die erin slagen potentiële strijders weg te trekken van gewelddadige confrontaties, ondanks hun ogenschijnlijke loyaliteit aan de straatcode (Lane en Stuart, 2022: 471). Indirecte effecten verwijzen naar het fenomeen waarbij potentiële strijders hun communicatiegedrag proactief aanpassen, in de verwachting dat derden meekijken en mogelijk zouden kunnen ingrijpen (Lane en Stuart, 2022: 468). Deze studie illustreert hoe digitale technologieën gedrag beïnvloeden en laat zien dat jongeren niet alleen daders van geweld kunnen zijn, maar ook actief kunnen bijdragen aan vreedzame oplossingen.

In veel studies naar het thema geweld in het hybride tijdperk overheerst echter nog een zekere lineaire of sequentiële kijk op de relatie tussen sociale media en fysiek geweld. Ook in de geweldsketen van Mehlbaum en collega’s (2024: 102-103) is fysiek geweld het vertrekpunt van het onderzoek, maar in zekere zin ook het eindpunt. Het werk van Stuart (2020a, 2020b) laat echter zien dat de verschillende strategieën die jongeren hanteren sterk variëren in de mate waarin zij kunnen leiden tot fysiek geweld. Een belangrijk deel van de online interacties, ook met een meer gewelddadige inslag, blijft uiteindelijk beperkt tot het digitale domein en resulteert niet in fysiek geweld. Bovendien waarschuwt Stuart (2020a, 2020b) dat het schier onmogelijk is om op basis van posts op sociale media vast te stellen of dit resulteert in fysieke vormen van geweld,

omdat het buitenstaanders in veel gevallen ontbreekt aan de (achtergrond)kennis – of straatgeletterdheid (Ilan, 2020) – om de digitale content goed te kunnen begrijpen en duiden. In gesprekken met respondenten in het Verenigd Koninkrijk werd bovendien kritisch gereflecteerd op de manier waarop online content door professionals, en in het bijzonder de opsporingsdiensten, wordt geïnterpreteerd en welke betekenis daaraan wordt toegekend – een onderwerp dat in hoofdstuk 6 nader zal worden uitgediept.

3.3 Geweldsopdrachten via sociale media

Een tweede verschijningsvorm van geweld met zowel een online als een offline component werd enkel in de gesprekken met respondenten uit Nederland en Denemarken benoemd: geweldsopdrachten die via sociale media worden uitgezet. Dit sluit aan bij de aandacht die Europol eind 2024 vroeg voor rekrutering van jongeren voor criminele activiteiten door georganiseerde criminaliteitsgroeperingen, waarbij in het bijzonder gewezen werd op de rol van sociale media. Een voorbeeld uit Denemarken:

*'According to the prosecutor, a 16-year-old Swedish boy traveled all the way from Luleå last spring to carry out a murder assignment in Denmark. On Tuesday, he will be brought before the court in Copenhagen's city court (district court). According to the Danish prosecution authority, the 16-year-old was stopped by Swedish police at the first attempt to enter Denmark in April last year. He was sent back to Luleå, but five days later he traveled to Denmark again. A 30-year-old woman is charged with having received the boy at Copenhagen Airport on the evening of April 22, providing him with a pistol and ten cartridges and driving him to another part of Copenhagen. According to the indictment, the plan was for the teenager to shoot one or more people connected to the Comanches motorcycle gang's clubhouse in Brøndby. However, there was no shooting, as the clubhouse was empty. Both the woman and the boy deny any wrongdoing. Last week, the trial began against another Swedish teenager, who is also charged with having taken on the assignment to murder one or more people at the same clubhouse. He was arrested by Danish police on April 16. In both cases, a 21-year-old Swedish man is suspected of having acted as an intermediary in connection with the recruitment of the youths.'*⁸

Tijdens de interviews met Deense respondenten werd dit verschijnsel aangeduid als 'crime-as-a-service' of 'torpedo's' om expliciet te verwijzen naar de jongeren die het geweld plegen. De Deense minister Peter Hummelgaard verklaarde in augustus 2024 dat er sinds april al 25 voorbeelden bekend waren van bendes uit Denemarken die jonge Zweden zouden hebben ingehuurd om geweld te plegen in de Deense hoofdstad.⁹

8 <https://swedenherald.com/article/16yearold-swedish-national-in-court-in-copenhagen>, laatst bezocht op maandag 5 januari 2026.

9 <https://tpo.nl/2024/08/09/denemarken-voert-strengere-grenscontroles-in-met-zweden-na-schietincidenten/>, laatst bezocht op maandag 5 januari 2026.

De hybride component heeft in het geval van deze geweldsopdrachten betrekking op de manier waarop jongeren hierbij betrokken raken. In een ander nieuwsbericht uit Denemarken over dit fenomeen werd dit als volgt beschreven: *'We have seen that organized criminals on social media demand people who are willing to carry out dangerous crimes and that young Swedes have unfortunately taken on the task for a fee'*.¹⁰ Door Deense respondenten werd eveneens beschreven hoe socialemediaplatformen fungeren als schakel tussen georganiseerde misdaadgroepen en de uitvoerders van het geweld:

'They recruit all these young people in Sweden, they have a lot of young people who live by themselves or have run away from home. And that's usually the ones they recruit. And they just want to make some quick money. They don't really care how. A lot of them do not have that big of a criminal history but are ready to go over here to Denmark and maybe commit murder or whatever they're going to do over here.' (RDE-11-2)

De vraag rijst hoe jongeren via sociale media aan dergelijke geweldsopdrachten worden blootgesteld en op welke platformen dit gebeurt. Een respondent beschreef dit als volgt:

'I think that may have actually been on Telegram. But there was also, now that we're talking about how this is communicated, that they were posted as advertisements as we need someone to go to Copenhagen and, do this and you get this amount for firing a grenade. You get this amount for shooting a building. You get this amount for shooting a person and then you could apply for it. So that's also this discussion about crime as a service. So, this is really a form of marketization. Whereas before social media and these encrypted communications, this was something you do in your social network. You would ask people: you know someone that would do this? But now you can open it up and tons more people can see it. It's much more efficient. Some of these torpedoes did not fit the profile that maybe we would expect for someone desperate enough to do that. So maybe the people that posted the advertisement could actually pick a person that would better go under the radar to do this kind of thing.' (RDE-13)

In berichten in de media werd gewezen op het gebruik van code- en beeldtaal in de communicatie, waarbij bijvoorbeeld 'appel' stond voor een handgranaat en 'pistool' voor een moord. Op basis van de interviews werd het echter niet helder via welke platformen dergelijke geweldsopdrachten verspreid werden. Sommige respondenten benadrukten dat dit vooral via het dark web gebeurde, terwijl anderen wezen op Telegram Messenger, Snapchat en Instagram.

10 <https://cphpost.dk/2024-08-02/news/police-swedish-boys-are-hired-for-serious-crime-in-denmark/>, laatst bezocht op maandag 5 januari 2026.

Over het algemeen resteerde er bij respondenten uit Denemarken de nodige onduidelijkheid over de precieze mechanismen van werving en rekrutering van jongeren voor deze vormen van criminaliteit. Wel benoemden zij duidelijk dat de uitvoerders doorgaans jonge en kwetsbare personen zijn. Een van de respondenten gaf een voorbeeld van een jongere die werd voorgehouden dat hij zijn schulden zou kunnen aflossen door in Denemarken geweld te plegen:

'And he was told to go and do this. He called her, said: don't do it, don't do it. And he told his father, I'm going away. I have to do something very bad. And if I don't, they will kill you.' (RDE-5)

Naast een zekere mate van dwang die volgens respondenten op deze kwetsbare jongeren wordt uitgeoefend, spelen ook financiële motieven een rol. In een krantenbericht uit Denemarken werd een bedrag genoemd van tussen de 300.000 en 500.000 Deense kronen (circa € 39.000 tot € 65.000) als vergoeding voor het uitvoeren van gewelddadige opdrachten.

Het Deense voorbeeld van torpedo's sluit nadrukkelijk aan bij de eerdergenoemde zorgen die Europol (2024) heeft geuit over de inzet van jongeren voor georganiseerde en zware misdaad. Ook in Nederland verscheen begin 2025 een voorbeeld dat vergelijkbaar is met de Deense torpedo's. Mike F., een minderjarige jongen uit Nederland, kreeg via Snapchat een gewelddadige opdracht en pleegde vervolgens in Duitsland een schietincident. Hij werd daarbij zelf beschoten, belandde in een Duitse gevangenis en is inmiddels uitgeleverd aan Nederland (Tieleman en Timmersmans, 2025). Empirisch onderzoek naar de rol van sociale media bij de betrokkenheid van jongeren bij zware en georganiseerde criminaliteit is schaars (Bergers et al., 2026). In een studie van Bervoets en collega's (2024) wordt benadrukt dat de online wereld een van de leefgebieden vormt waarin jongeren worden benaderd. In hun interviews met jongeren die betrokken raakten bij georganiseerde criminaliteit en met hulpverleners kwamen meerdere voorbeelden naar voren van hoe jongeren via sociale media zoals Snapchat of Telegram werden verleid om 'snel geld te verdienen', met name in de drugshandel. Enkele jaren eerder gaven Van den Berg en Rekers (2022) in een verkennende studie zicht op de jongeren die benaderd worden voor strafbare feiten. Een vragenlijst onder schoolgaande jongeren maakte duidelijk dat 12 procent van de ondervraagde jongeren wel eens benaderd was voor een criminele opdracht. Een kwart hiervan werd benaderd via sociale media (Van den Berg en Rekers, 2022).

In een recente studie van Bergers en collega's (2026) ging de aandacht expliciet uit naar de rol van sociale media bij het betrokken raken van jongeren bij zware en georganiseerde vormen van misdaad. De resultaten van een vragenlijst onder jongeren laten zien dat bijna één op de vijf jongeren (19,6%) tussen de 16 en 27 jaar op sociale media weleens berichten heeft gezien waarin personen werden gezocht voor het plegen van drugs- of geweldsdelicten. Deze blootstelling aan dergelijke berichten op sociale media is echter anders dan daadwerkelijk benaderd worden voor drugs- of geweldsdelicten. In totaal gaf 6,1 procent van de ondervraagde jongeren aan zelf benaderd te zijn voor

dergelijke criminele activiteiten. Bergers en collega's (2026) beschrijven dat jongeren vooral worden geworven voor drugsgerelateerde klussen, zoals het dealen of vervoeren van drugs, en minder vaak voor zware geweldsdelicten. Daarbij verschilt de aard van de criminaliteit per platform: Snapchat wordt voornamelijk gebruikt voor drugsdelicten, terwijl TikTok vaker wordt ingezet voor geweldsdelicten. Telegram en Discord worden in de vragenlijst nauwelijks genoemd als platforms waarop jongeren worden benaderd voor het plegen van drugs- of geweldscriminaliteit. De berichten waarin jongeren worden benaderd om een criminele klus uit te voeren zijn meestal afkomstig van onbekenden, maar als de afzender wel bekend is, betreft het doorgaans een vriend of schoolgenoot (Bergers et al., 2026).

In de interviews met respondenten uit Nederland werden enkele voorbeelden gegeven van jongeren die via sociale media betrokken raakten bij een geweldsopdracht. Een voorbeeld hiervan zien we terug in de volgende rechtszaak:

'In de telefoon van [medeverdachte 1] is te zien dat hij op 15 december 2021 om 00:54 uur een foto ontvangt van [accountnaam]. Dit betreft een foto van het slachtoffer [slachtoffer]. [medeverdachte 1] heeft verklaard dat rondom dit moment ook het adres van [slachtoffer] werd gedeeld. Verder zijn in zijn telefoon foto's aangetroffen van gesprekken op 15 december 2021 met de tijdstippen 01:08 uur, 13:36 uur en 13:41 uur. Dit betreffen foto's van het scherm van een andere telefoon, waarvan [medeverdachte 1] heeft verklaard dat hij die in gebruik had. Op de foto's zijn gesprekken te zien tussen [medeverdachte 1] en [accountnaam]. In één van deze gesprekken wordt door [accountnaam] [woonplaats slachtoffer] (de rechtbank begrijpt: [woonplaats slachtoffer]) genoemd, de woonplaats van het slachtoffer. Om 01:08 uur is het volgende gesprek zichtbaar:

[accountnaam]: Tamara kom ik met iets waardoor je vrijdag kan

NN-gebruiker: Ai ns

[accountnaam]: Easy toch?

[accountnaam]: Oke en met een capuchon aanbellen is niet slim

[accountnaam]: Met een doos ofzo snap je

[accountnaam]: Er zijn geen camera's in de straat

NN-gebruiker: Ja Drm Ga hem zeggen Doe alsofje iets gaat bezorgen

[accountnaam]: Top

De rechtbank interpreteert dit gesprek zo dat [accountnaam] morgen met iets komt waardoor zij vrijdag kunnen. Daarnaast geeft [accountnaam] instructies over hoe aan te bellen.

Om 13:36 uur wordt het volgende gesprek gevoerd:

NN-[accountnaam]: (Ik stuurde je gister)

NN-[accountnaam]: O van p haha so

NN-[accountnaam]: Si

NN-gebruiker: (lachende emoji)

NN-[accountnaam]: [adres] NN-gebruiker: Aii

De rechtbank interpreteert dit gesprek zo dat wordt gesproken over de plek waar p, het pistool, moet worden opgehaald. Dit sluit aan op de verklaring van [medeverdachte 1] dat hij en de mededader het wapen hebben opgehaald nabij het adres [adres] en vervolgens met dit wapen hebben proefgeschoten in het Bijlmerpark.’ (Rechtspraak.nl, ECLI:NL:RBAMS:2023:8315)

Dit voorbeeld maakt inzichtelijk dat sociale media niet alleen kanalen zijn via welke jongeren benaderd worden voor een criminele klus, iets dat in deze zaak verliep via Snapchat, maar ook dat een deel van de onderlinge communicatie en de concrete instructie via dergelijke platformen verloopt (vgl. Van Berkel et al., 2025).

In de Nederlandse context gaat het echter vooral om specifieke vormen van geweld waarbij jongeren als uitvoerder in beeld komen, te weten bij het plaatsen van explosies, doorgaans met behulp van zwaar vuurwerk, bij woningen, restaurants en soms voertuigen. Bij de werving van uitvoerders, maar ook voor het verkrijgen van zwaar vuurwerk voor deze geweldsklussen, spelen sociale media een prominente rol (Van Berkel et al., 2025; Bergers et al., 2026). Een voorbeeld hiervan zien we in een rechtszaak tegen een Rotterdamse man die werd veroordeeld tot een gevangenisstraf wegens het voorbereiden van een explosie bij een woning en een auto in Amsterdam. In deze zaak werd een gedetailleerde beschrijving gegeven van de manier waarop de benadering en instructie via sociale media verliepen:

‘Uit onderzoek aan Snapchatgegevens blijkt dat [naam minderjarige 1] op 23 februari 2024 een bericht kreeg van een persoon [gebruikersnaam] dat er gewerkt kon worden. Ze zouden met een chauffeur (“driver”) naar Amsterdam (“Damsco”) gaan. Het ging om het tot ontploffing brengen van een explosief (“plakken” van een “cobra met een fles er aan vast” in een auto (“waggie”) en een deur.

Op 24 februari 2024 om 22.50 uur stuurde een persoon [gebruikersnaam] in een groepsgesprek met onder andere [naam minderjarige 1] dat hij een klus (“job”) had, een auto (“waggie”). Er werd gesproken over een te verdienen bedrag van (in totaal) 700,- en [naam minderjarige 1] vroeg of ze geld zouden krijgen als de klus geklaard was (“Krijgen we gwn nadat we job hebben geklaard in waggie pap”). Om 23.23 uur zei [gebruikersnaam] in het groepsgesprek dat de chauffeur er was (“Driver staat der all. Hij wacht”), waarna [naam minderjarige 1] om 23.28 uur bevestigde dat hij bij de chauffeur was.

Om 23.32 uur vroeg een persoon [gebruikersnaam] aan [naam minderjarige 1] of hij hem nog kwam ophalen, waarop [naam minderjarige 1] zei: “Hij zegt alleen jij en iemand zit hier”. In het groepsgesprek zei [gebruikersnaam] vervolgens: “Korte zegt ik kan niet meer fzo want er is een andere boy”, waarop [gebruikersnaam] reageerde: “Seri dan is driver met bully gekomen [...] ’K maak goed met je morgen nieuwe job.” Om 23.28 uur werden aan [naam minderjarige 1] duidelijke instructies gegeven in het groepsgesprek: “[adres] [...] waggie raampje tikken. Cobra met fles erin. Benzine fles over heen gooien en aansteken. Dan cobra voor deur zetten. Aanteken en wegren-

nen. Der moet goed gefilmd worden vanaf begin [...] Als alles goed is mag je morgen ochtendgeldkomenhalen.Ofstraksnog”(Rechtspraak.nl,ECLI:NL:RBAMS:2025:3921)

In dit concrete geval kwam het uiteindelijk niet tot de uitvoering van het geweld omdat de twee minderjarige verdachten door de politie werden betrappt.

De rol van socialemediaplatformen bij geweldsopdrachten vertoont een zekere gelijkenis met de werving van geldezels; bij beide verschijnselen zorgen sociale media voor een groter bereik. Dit punt werd ook benadrukt tijdens een van de interviews in Nederland:

‘Zo’n opdracht uitzetten kan natuurlijk heel makkelijk. Je kunt een hele grote groep in bijvoorbeeld een Telegram Group of via Snapchat benaderen. Via vrienden kun je heel snel in contact komen met anderen. Tot tien jaar terug had je natuurlijk wel WhatsApp en dat soort apps, maar het is nu veel, veel groter, veel breder geworden. Dus ja, als ik nu iets wil. Ik wil zo’n bom aan zo’n deur laten hangen, heb ik vuurwerk nodig. Ik heb iemand nodig die het doet. Iemand die dit organiseert, of iemand die dat organiseert. Je bent zo makkelijk in contact met elkaar. Ook over onze grenzen heen. En dan heb ik het over onze Amsterdamse politiegrenzen van een eenheid. Ik bedoel, ik kan iemand regelen uit Almere vanuit Amsterdam of ik kan iemand regelen vanuit Brabant die voor mij die klus doet of die het vuurwerk levert voor die bom.’ (RNL-3)

Sociale media zijn in staat om een grotere pool van geschikte of gemotiveerde uitvoerders aan te boren (vgl. Van Berkel et al., 2025). De functionaliteiten van bepaalde platformen kunnen dit bereik daarbij faciliteren. Te denken hierbij valt bijvoorbeeld aan de functie ‘Vrienden zoeken’ (voorheen ‘Snel toevoegen’) op Snapchat waarmee gebruikers eenvoudig andere personen aan hun vriendenlijst kunnen toevoegen op basis van algoritmisch gegenereerde aanbevelingen (Bergers et al., 2026). Op deze manier maken platforms als Snapchat het mogelijk om door onbekenden te worden benaderd (Van Berkel et al., 2025). Toch concluderen Van Berkel en collega’s (2025) op basis van de bestudering van zes afgesloten opsporingsdossiers dat werving vaak gericht is op personen uit vertrouwde sociale kringen, een bevinding die overeenkomt met studies naar de werving van geldezels (Bekkers, 2025), uithalers (Roks en Ter Weijden, 2026) en de online betrokkenheid van jongeren bij zware en georganiseerde vormen van criminaliteit in het algemeen (Bergers et al., 2026).

Een van de vragen die rijst is of jongeren daadwerkelijk weten wat zij moeten gaan doen wanneer zij via sociale media worden benaderd voor criminele opdrachten. In het onderzoek van Bergers en collega’s (2026) wordt beschreven dat de berichten soms hele specifieke verwijzingen of emoji’s bevatten die zicht geven op de aard van de klus, bijvoorbeeld door het gebruik van de term ‘hitten’ als verwijzing naar vuurwapengeweld of termen als ‘c6’ (cobra 6) of ‘bomba’s’ voor het plaatsen van explosieven. Ook in de interviews werden hiervan voorbeelden gegeven, zoals een icoontje van een auto in combinatie met een vuuremoji. Toch werd in de interviews door respondenten ook benadrukt dat sommige jongeren slechts gedeeltelijk of zelfs nauwelijks inzicht hebben

in de precieze aard van de opdracht waarvoor zij via sociale media worden benaderd. Een respondent gaf hiervan het volgende voorbeeld:

‘Maar die jongen die had een telefoon, zeg maar open mee. Je ziet gewoon dat hij constant iemand op de hoogte aan het houden is van wat hij aan het doen is. Oh ja, en hij stuurt op een gegeven moment ook iets en dan zie je ook dat hij gewoon geen idee heeft. Hij stuurt van: wow dit is het meest beveiligde huis waar ik ooit ben geweest, dat zegt wel iets over dat hij het vaak heeft gedaan, maar hij weet helemaal niet bij wie of wat hij iets aan het doen is. Hij krijgt gewoon een klusje.’ (RNL-1-2)

Op een vergelijkbare manier beschrijven Bergers en collega's (2026) dat de berichten waarop jongeren reageren weinig zicht geven op de concrete opdracht: de posts blijven beperkt tot termen als ‘fitte boys’ en er wordt simpelweg verwezen naar ‘jobs’ of ‘werk’. Dit betekent dat een deel van de jongeren vaak niet volledig weet wat zij gaan doen. In de interviews werd echter ook benoemd dat de uitvoerders niet altijd op de hoogte zijn of er andere personen betrokken zijn bij de uitvoering:

‘Die worden aan elkaar gekoppeld. Vanuit Tilburg hadden we een groep, vanuit Almere hadden we een groep, vanuit Utrecht hadden we een groep en die komen naar Veendam. Ja, niemand weet waar het ligt als ik jullie vraag naar Veendam om daar bommen te plaatsen. Ja, zo fluide is het. En die mensen die stappen bij elkaar in de auto, maar die kennen elkaar ook niet.’ (RNL-12-3)

Ook werd uit de interviews duidelijk dat de uitvoerders zelden weten hebben van de daadwerkelijke opdrachtgevers en vooral contact onderhouden met tussenpersonen. Een studie naar betrokkenen bij liquidaties van Adjiembaks en collega's (2024) schetst een vergelijkbaar beeld: bij de organisatie en uitvoering van liquidaties wordt soms (bewust) een strikte scheiding aangebracht, in het bijzonder tussen organisatoren en uitvoerders. Deze ‘compartimentering’ maakt dat uitvoerders niet direct in contact staan of weten hebben van de opdrachtgever, iets dat het risico op identificatie of aanhouding van personen met een organisatorische rol verkleint (Adjiembaks et al., 2024: 104-105).

3.4 Conclusie

In dit hoofdstuk zijn twee verschijningsvormen van geweld besproken die vanwege de dynamiek tussen het online en offline domein niet slechts getypeerd kunnen worden als cyber violence (Wall, 2001). Allereerst hebben we een beschrijving gegeven van conflicten tussen (groepen) jongeren waarbij sociale media een wezenlijke rol spelen. In de gesprekken met respondenten uit zowel Nederland, Denemarken als het Verenigd Koninkrijk werden concrete voorbeelden gegeven van (dodelijk) geweld tussen jongeren met een online aanloop of escalatie. Meer in het algemeen bleek deze dynamiek geenszins eenduidig: conflicten kunnen op sociale media beginnen, zich ontwik-

kelen door digitale berichten over en weer, en op enig moment uitmonden in fysieke confrontaties. Tegelijkertijd zijn er ook gevallen waarin conflicten juist offline aanvangen, vervolgens worden uitvergroot op sociale media en daarna opnieuw fysiek eindigen in geweld. Daarbij speelt ook het fenomeen dat fysiek geweld wordt gedigitaliseerd doordat foto's en video's van incidenten als content circuleren. In die zin ontstaat een keten van gebeurtenissen, zoals Mehlbaum en collega's (2024) beschrijven, waarbij rondom het fysieke geweld processen van hybridisering vallen waar te nemen.

De tweede verschijningsvorm die we in dit hoofdstuk hebben besproken zijn geweldsopdrachten door jongeren, een onderwerp waar Europol (2024) recentelijk aandacht voor vroeg. In zowel Nederland als Duitsland bestaan zorgen over jongeren die betrokken raken bij ernstige vormen van geweld. In Nederland gaat het daarbij onder andere om het gebruik van explosieven, terwijl in Denemarken gesproken werd over de zogenoemde 'torpedo's': jongeren die vanuit Zweden in Denemarken geweld kwamen plegen. Socialemediaplatformen spelen een cruciale rol doordat zij worden gebruikt om opdrachten uit te zetten en de communicatie richting uitvoering te faciliteren. Soms weten jongeren precies wat van hen wordt gevraagd, ze kennen de verhullende code-taal en emoji's, en sommigen zijn zelfs actief op zoek naar dergelijke opdrachten. In andere gevallen blijft de aard van de opdracht vaag of wordt deze verhuld in codetaal en emoji's.

De hier besproken voorbeelden van hybridisering verschillen van die in het voorgaande hoofdstuk, maar illustreren eveneens dat online en offline domeinen niet los van elkaar kunnen worden gezien. Sterker nog, de voorbeelden in dit hoofdstuk wijzen op de verwevenheid van online en offline, hetgeen inzichtelijk maakt dat geweld in de hedendaagse samenleving niet langer kan worden begrepen zonder de digitale infrastructuur die het faciliteren.

4 Gedigitaliseerde drugshandel

4.1 Inleiding

Het laatste thema dat we behandelen is de handel in drugs. Gezien de centrale rol van Nederland als productie- en doorvoerland voor verdovende middelen (Staring et al., 2019; Roks, Kleemans en Blokland, 2021), is het opmerkelijk dat dit onderwerp in de interviews met Nederlandse respondenten maar in beperkte mate werd benoemd¹¹ als voorbeeld van een verschijningsvorm met hybride elementen. Voor dit hoofdstuk concentreren we ons daarom vooral op inzichten uit de interviews die betrekking hadden op Denemarken en het Verenigd Koninkrijk. Technologische innovaties hebben historisch gezien een bepalende rol gespeeld in de wijze waarop de handel in verdovende middelen wordt georganiseerd. Waar het einde van de twintigste eeuw vooral zicht geeft op de opkomst van de mobiele telefoon als essentieel hulpmiddel voor drugshandel (Natarajan et al., 1995; Anderson, 1999: 30; Barendregt et al., 2006), wordt de meest ingrijpende technologische verandering toegeschreven aan de introductie van cryptomarkten (Van Hout en Bingham, 2014; Martin, 2014; Aldridge en Décary-Héту, 2016). Meer recent is een verschuiving zichtbaar naar socialemediaplatformen en mobiele applicaties als nieuwe arena's voor de handel in verdovende middelen (Demant et al., 2019; Korshøj en Søgaard, 2024; Moyle et al., 2019; Salinas, 2018; Søgaard, 2019). We beginnen dit hoofdstuk in paragraaf 4.2 met het verschijnsel van digitale drugsmarkten op sociale media. Vervolgens gaan we in paragraaf 4.3 in op een fenomeen dat in het Verenigd Koninkrijk wordt aangeduid als 'county lines', waarbij mobiele telefoons en socialemediaplatformen een rol van betekenis spelen (Coomber en Moyle, 2017; Robinson, McLean en Densley, 2018; Spicer, 2021). De belangrijkste bevindingen van dit hoofdstuk bespreken we in paragraaf 4.4.

4.2 Digitale drugsmarkten op sociale media

De eerste verschijningsvorm die we behandelen in dit hoofdstuk zijn digitale drugsmarkten op sociale media. Moyle en collega's (2019) bieden een eerste systematische verkenning van socialemediaplatformen en apps die momenteel worden ingezet voor drugshandel. Deze platformen functioneren niet enkel als communicatiemiddel tussen

11 Dit is, zoals we in de conclusie van dit rapport uitgebreider zullen benadrukken, ook een directe consequenties van onze selectie van respondenten.

bekenden – bijvoorbeeld voor het regelen van drugsdeals –, maar, afhankelijk van hun technische mogelijkheden, ook als commerciële marktplaatsen voor drugs. Dealers benutten deze digitale infrastructuur om producten en diensten aan te prijzen en zo nieuwe klanten aan te trekken. Zij maken gebruik van berichten, foto's, video's en statusupdates om hun aanbod te promoten, terwijl tijdelijke 'stories' worden ingezet om beschikbare substanties, hoeveelheden en prijzen kenbaar te maken. Hoewel deze ontwikkeling steeds meer aandacht krijgt, blijft het aantal empirische studies dat inzicht biedt in de wijze waarop sociale media worden ingezet voor de handel in verdovende middelen vooralsnog beperkt (Bakken en Demant, 2019; Demant et al., 2019; Moyle et al., 2019; Bakken, 2020). Bakken en Demant (2019: 255) typeren dit onderzoeksgebied om die reden dan ook als een *'absolute research gap'*.

Met name in de Scandinavische landen is er de nodige kennis over digitale drugsmarkten op sociale media als Snapchat, Instagram en Facebook. Volgens een onderzoeker die zich al langere tijd met dit onderwerp bezighoudt, werden onderzoekers hier door de politie op geattendeerd. Drugs dealen op sociale media zorgde in eerste instantie bij deze onderzoeker voor enige verbazing:

'I remember, we were kind of starting the project saying like: people dealing drugs on social media are stupid, like they should do it in crypto markets, like it's so safe. You can read about people, you have like you encrypted money, like you have all these security measures, and then you do it on Snapchat, like it's just ... it's stupid. And then we got all these reasons for why that is actually the best solution for many people.' (RDE-16)

Voor al omdat er allerlei technologische afschermingsmechanismen voorhanden zijn op bijvoorbeeld cryptomarkten, wekte de openlijk zichtbare communicatie over drugshandel verbazing:

'Like, it's not coded for us and it's not a strong code. For instance, if you sell MDMA on social media, it needs to be called 'now'. Then in order not to be detected, it needs to be whatever. And then a postal number. Yeah, that's coded. Um, but here it's only coded in a way more traditional, like slang.' (RDE-4)

Naast het gebruik van specifieke slang wordt er ook gebruikgemaakt van digitale beeldtaal, zoals emoji's om te verwijzen naar verschillende soorten drugs, zoals emoji's van sneeuw of ijs voor cocaïne (vgl. Moyle et al., 2019; Roks en Hendriksen, 2021).

Differentiatie is een centraal begrip om drugsmarkten in het algemeen en digitale drugsmarkten in het bijzonder te begrijpen. Coomber (2015: 11-12) wijst er met dit begrip op dat drugmarkten sterk gedifferentieerd zijn – niet alleen naar soort drugs, maar ook naar tijd en plaats, alsook de soorten dealers en consumenten die op de verschillende markten actief zijn. Niet alle drugs worden op dezelfde wijze verhandeld, noch kennen zij dezelfde sociale en economische contexten (Coomber, 2015). Een respondent licht dit nader toe:

'Whereas the vast majority of dealing and market activity that's going on is, you know, around recreational drugs. And those markets, they don't operate in the same way that the heroin crack cocaine markets do.' (RVK-6)

Op dit punt komen we in paragraaf 4.2 nader terug als het gaat om het zogenoemde county lines-dealen. Het concept differentiatie toont zich ook uiterst relevant als het gaat om digitale drugsmarkten. Technologie bepaalt immers de wijze van communicatie tussen koper en verkoper, zoals een respondent benadrukte:

'But the main reason why they use it is because of the people that they're retailing the drugs to are vulnerable users, right? So, at least when I speak to a lot of police, they will say, look, as cheap as smartphones are nowadays, you know, you're a vulnerable user. That is somebody that has a dependency on crack cocaine or heroin or synthetic opioids. To put it crudely, he would probably sell on a smartphone if they were to use it.' (RVK-8)

Deze inzichten leiden ertoe dat drugdealers zich moeten aanpassen aan de digitale voorkeuren en praktijken van hun klanten. Voor sommigen betekent dit het gebruik van socialemediaplatformen en mobiele applicaties om hun aanbod te promoten en transacties te organiseren, terwijl anderen juist vasthouden aan meer traditionele en fysieke vormen van contact. Deze differentiatie in consumptiepatronen en communicatiemiddelen maakt duidelijk dat technologie niet uniform werkt, maar uiteenlopende effecten heeft op de organisatie van de handel.

Differentiatie manifesteert zich daarnaast op een andere manier, namelijk in de variatie tussen de platformen en de typen dealers die daar actief zijn. Bakken en Demant (2019) maken een onderscheid tussen gesloten en (semi)publieke digitale drugsmarkten. Op gesloten digitale drugsmarkten is de communicatie tussen gebruikers van het platform niet openlijk zichtbaar voor iedereen met toegang tot internet. Gebruikers van deze applicaties moeten een zekere online connectie hebben – ze moeten elkaar volgen of hebben geaccepteerd – om een-op-een te communiceren (Bakken en Demant, 2019: 260). Andere socialemediaplatformen of applicaties zijn te typeren als publieke digitale drugsmarkten omdat ze gekenmerkt worden door één-op-veel communicatie, spontane en onpersoonlijke sociale relaties en een hoge mate van openheid (Bakken en Demant, 2019: 260). Omdat het hier gaat om communicatie met onbekenden met doorgaans anonieme online identiteiten, kan er niet teruggevallen worden op eerdere positieve ervaringen of op iemands (online) reputatie. Het ontbreekt met andere woorden aan manieren om een goede inschatting te maken van de betrouwbaarheid van aanbieders en potentiële afnemers van verdovende middelen (Bakken en Demant, 2019; Bakken, 2020).

Uit het voorgaande volgt dat er verschillende soorten drugsmarkten zijn op de verschillende soorten socialemediaplatformen. De uiteenlopende functionaliteiten van de platformen brengen in deze context immers een eigen dynamiek teweeg, zoals de volgende respondent uit het Verenigd Koninkrijk beschrijft:

'And that's primarily Snapchat in the British context. At least when I was doing a little research on that kind of more street-based form of offending, Snapchat was a big one. For the most part, because it's ephemeral. So, you know, there's a perception that it's kind of encrypted in a sense. And so, when that message disappears, it disappears, right? Unless somebody screenshots it. So amongst sort of young kids, Snapchat was the main application I was seeing.' (RVK-8)

Hier zien we dat de vluchtigheid van content op Snapchat, die op een door gebruikers ingesteld moment weer wordt verwijderd, bepaalde praktijken faciliteert, waaronder het aanbieden van verdovende middelen. Volgens een respondent uit Denemarken trekt Snapchat om deze redenen bepaalde dealers aan:

'So now what we do when we are seeing drug dealing, especially on Snapchat, these are commercial dealers. They are likely gang related. Basically, it's really difficult, because we don't know, but it seems from how they are operating if you just take the data traces, then we see that there's 24/7 sales. It's very different quantities. It's professionally set up, the delivery is professional and so on. There's a lot of indications that these are professionals. And the small timers seem to be moving out, not totally moving out of the drug sales, but not using the same places as the professionals.' (RDE-4)

Onderzoekers in Denemarken signaleren bovendien, in lijn met wat er in de laatste zinnen van het bovenstaande citaat wordt benoemd, dat de digitale drugshandel bijzonder dynamisch is in termen van de platformen die worden gebruikt:

'Regarding the social media platforms, we see a lot of change in what platforms they use. There can be kind of migration from one platform to another if it's suddenly deemed unsafe. But it seems like the text message is more like a stable, fixed thing in a way that's not as likely to just change. We saw a migration from Telegram. Reddit was also very popular at one point, and it turned to Telegram. Now Telegram is deemed unsafe, so it kind of moves away. So, it's also ever changing. It seems like with these online platforms in a way.' (RDE15-1)

Telegram Messenger had lange tijd de naam een veilige berichtendienst te zijn, in het bijzonder vanwege de mogelijkheden om in 'secret chats' anonimiteit een-op-een te communiceren of, meer in het algemeen, via end-to-end-encryptie versleutelde berichten, foto's en videobestanden te delen die een zelfvernietigingsfunctie toegewezen kunnen krijgen (Roks en Hendriksen, 2021). Na de arrestatie van Telegram-oprichter Durov zien respondenten een verandering in het gebruik van Telegram en wordt dit platform door sommige gebruikers als onveilig gezien. In die context werd WhatsApp genoemd door een respondent uit het Verenigd Koninkrijk: *'But now what I see is basically just simple groups. You know, it's the WhatsApp groups, people inviting people and they join the group, you know, so somebody will usually vouch for them'* (RVK-3).

Het bovenstaande maakt inzichtelijk dat verschillende applicaties eigen functionaliteiten bieden die voor het dealen of aanschaffen van verdovende middelen van nut zijn. Een van de respondenten uit Denemarken geeft echter een additionele verklaring voor het gebruik van bepaalde socialemediaplatformen voor de verkoop van drugs:

'I think to a large extent that that sort of parallels where the people are sort of going. Drug dealers will be using the same apps everyone uses. People will be using the same apps to get their drugs as they used to talk with their friends. So, I think there's been a transformation there. In broad terms, the transformation we've seen technologically is that in a sense people have followed the same trends we see in, let's say, the legitimate web. (...) You don't perhaps choose the most well-functioning app. You choose the one your friends use. You might avoid the ones that have a cringe name. So, I mean, in your day-to-day life, you don't optimize on, let's say, encryption or all of these other aspects. Perhaps it's a bit too much to expect people who commit crimes to do the same.' (RDE-12)

Deze respondent benadrukt dat zowel consumenten als dealers niet altijd kiezen voor de platformen met de beste functionaliteiten en mogelijke afschermingsmechanismen: zij maken vooral gebruik van de digitale infrastructuren die populair zijn onder consumenten. Een respondent uit het Verenigd Koninkrijk benadrukte dat deze ontwikkeling in zekere zin de logica volgt van wat breder in de retailsector valt waar te nemen:

'The way in which digital services et cetera tend to be designed, is for a lack of delay, a kind of a flow, a smoothness of experience. And, you know, I imagine that that's something that will increasingly sort of enter the illegal capitalism and license capitalism. And so, you see the stickers on the whatever lamp posts or electric boxes side of the road. The QR codes, you know, all of these sorts of things. And again, you know, whereas we might have said a few years ago: this is a hybrid drug market. You know, it's online again, you know. Is that how younger people experience it as some sort of innovation, or do they just see it as part of everyday life? And I think it's the latter.' (RVK-10)

Deze respondent benadrukt dat de handel in verdovende middelen niet los gezien kan worden van bredere maatschappelijke en economische ontwikkelingen. Een andere respondent uit het Verenigd Koninkrijk trok een vergelijkbare analogie met Britse equivalenten van Thuisbezorgd en de bredere manier waarop consumenten tegenwoordig aan goederen en diensten komen:

'The other thing is that in our study, the people we spoke to, it tended to be: they were sitting in a pub or something and then they would think, oh, I could use a smoke or I want a tablet. They then just looked online and then they just would say, oh, that one's nearby. So, their discretion, you know, despite the fact that there are potentially warnings on a forum or whatever. They are probably not going to take notice of that or see

it a lot of the time, because they just want the person who's literally five minutes away.' (RVK-6)

Hier wordt met name de aandacht gevestigd op het gemak waarmee verdovende middelen, net als andere consumptiegoederen, tegenwoordig besteld kunnen worden. Net als bij enkele van de andere verschijningsvormen die we bespraken in hoofdstuk 2 en 3 blijken sociale media ook in het geval van de handel in verdovende middelen het afzetgebied en het bereik van berichten te vergroten, in dit geval van dealers. Dit maakt dat, zoals een onderzoeker uit Denemarken beschreef, de drugshandel een nieuwe schaal en dynamiek krijgt:

'At least if it's drugs that you aren't comfortable sending with the mail. Right. But even posting it with the GLS or something is also forcing some kind of physicality on it. But everything else is kind of online. Right. That's how I got into the hybrid thing. Because you have to, we have to turn it over. But when you sell it on Snapchat or Facebook or even like the SMS lists, there's hugely different social affordances to who you can reach and what you can sell and what kind of niche clientele you can serve.' (RDE-1)

Met digitale drugsmarkten vallen de beperkingen van geografische nabijheid en het belang van sociale contacten grotendeels weg. Waar traditionele handel vaak afhankelijk was van fysieke nabijheid en persoonlijke relaties, maken digitale infrastructuren het mogelijk om een veel breder en meer divers publiek te bereiken. Daarmee verandert niet alleen het afzetgebied, maar ook de manier waarop vraag en aanbod elkaar vinden. Belangrijk om hier te benadrukken is dat deze verschuiving niet uitsluitend gaat over bereik, maar volgens respondenten ook over de werking van algoritmen:

'And there's a recommendation algorithm that does a lot of heavy lifting. So, then the profiles tend to offer one thing, right? Then you're recommended easy money or cocaine 24/7. And those are like individual businesses in some sort of way.' (RDE-1)

Ook andere respondenten stellen dat de werking van algoritmen op deze manier behulpzaam is in de verkoop, namelijk omdat *'network based algorithms of Snapchat will do the selling'* (RDE-4). Ook een respondent in Nederland, werkzaam bij de politie, gaf hiervan een duidelijk voorbeeld in de voorgestelde contacten bij Snapchat: *'Bij een uitgelezen telefoon van een meisje van vijftien zie ik gewoon de dealer van de wijk. Zo noemt hij zichzelf ook en die staat netjes in haar voorgestelde vriendenlijst'* (RNL-10).

In de beschikbare literatuur wordt benadrukt dat deze ontwikkelingen ertoe kunnen leiden dat de drempel om drugs te kopen via digitale kanalen aanzienlijk lager is (McCulloch en Furlong, 2019; Aagesen en Demant, 2025). McCulloch en Furlong (2019) laten bijvoorbeeld zien dat jongeren die geen eerdere ervaringen hadden met drugs, toch in aanraking komen met drugsverkoop via sociale media zonder dat zij hier bewust naar op zoek zijn. De auteurs beschrijven dat één op de vier jongeren (24%) tussen de 16 en 24 jaar illegale drugsadvertenties via sociale media heeft gezien. Volgens

McCulloch en Furlong (2019) kan deze blootstelling en beschikbaarheid ertoe leiden dat jongeren verleid worden om drugs te kopen en te gebruiken. Daarbij speelt mee dat in veel groepen op sociale media waar voornamelijk cannabis wordt aangeboden, ook harddrugs worden verkocht. Dit resulteert erin dat mensen verschillende soorten drugs kopen waarnaar zij niet specifiek op zoek waren. Meer recent krijgt deze dynamiek aandacht in een studie van Aagesen en Demant (2025) waarin is onderzocht hoe algoritmische aanbevelingssystemen op sociale media gebruikers ongemerkt kunnen sturen van grijze, semilegale markten, zoals de handel in vapes, naar zwarte markten zoals digitale drugsmarkten. De auteurs laten zien dat sociale media, en in het bijzonder Snapchat, niet slechts neutrale communicatiemiddelen zijn, maar zelf een actieve rol spelen in het faciliteren van illegale netwerken. Zij creëerden veertig profielen die zich oriënteerden op grijze markten en observeerden vervolgens hoe Snapchats algoritmes deze profielen door middel van aanbevelingen en suggesties verder leidden. Binnen vier dagen bleek dat 65 procent van de profielen door het algoritme in aanraking werd gebracht met aanbieders van illegale drugs, zonder dat er vooraf interactie met dergelijke content had plaatsgevonden. De auteurs concluderen op basis hiervan dat algoritmes criminogene potentie bezitten: zij creëren digitale drift door gebruikers van semilegale naar illegale markten te sturen, zelfs wanneer die gebruikers daar niet actief naar op zoek zijn. Daarmee wordt duidelijk dat sociale media niet slechts infrastructuur zijn waar illegale handel toevallig plaatsvindt, maar actoren die deze handel mede vormgeven (Aagesen en Demant, 2025).

Veel van het voorgaande maakt inzichtelijk dat de handel in verdovende middelen onder invloed van technologische ontwikkelingen van karakter verandert. Een respondent werkzaam bij de Deense politie vat een deel van deze evolutie als volgt samen:

'Back in the day when I was a street cop in Copenhagen, we had, like what we call the shop Corner. It was in a place called Easter Girl, next to the central station, two blocks away from there. There was this corner. All the drug abuse, drug addicts stood on the corner. Because if you were a dealer, you know, those who stood on that corner would like to buy heroine from you. And they got in contact and they met somewhere and they did a deal. Today you get a phone number, you call the number and you ask for whatever it is and you meet somewhere random. So back in the days, we knew where to pick them up. Now they are everywhere.' (RDE-5)

Ondanks de nieuwe mogelijkheden die (digitale) technologie biedt, geven respondenten aan dat er geen sprake is van een volledige online verplaatsing van de handel van verdovende middelen of dat het gebruik van sociale media de fysieke en lokale aspecten van het dealen in drugs volledig naar de achtergrond heeft gedrukt. Een respondent uit het Verenigd Koninkrijk licht dit toe:

'In a strange way, the use of apps and selling via apps and social media, on the one hand, may have decreased the number of open markets, but it hasn't necessarily completely decreased the amount of open selling. And one of the things that we mentioned

in that paper was to our surprise that people laid themselves open to being contacted by the police and just, you know, sort of they don't know until they turn up to that. So, it's kind of open selling, facilitated by apps and their reliance on the police or other users who are just going to rob them.' (RVK-6)

Op een vergelijkbare manier schetst een onderzoeker uit Denemarken dat het dealen in drugs onderhevig lijkt te zijn aan een andere dynamiek dan reguliere consumptiegoederen:

'But what we also see is that, for example, people tend to come back to the same drug dealers again and again and again. And there's a very good reason for that. You purchase something and you confirm that this person is honest. They're trustworthy. Now they have an edge over all of their competitors because, and this is in a very uncertain market, that their product is good. So, I do think the experience of being confirmed that you can trust someone is crucial to understanding these economies. And how do people learn to trust someone? Well, they do that by sort of a physical encounter in some way. That physical encounter might be you trying out the drugs, might be you meeting them, but you need some affirmation that you can trust someone. So, I think that might also be a good explanation of why some of the patterns we see when we see illicit online commerce is that people tend to go back to the same sellers, which again, is a little bit counterintuitive, if we think of Amazon or other legal economies.' (RDE-12)

Deze hang naar het bekende en vertrouwde, ondanks de grenzeloze mogelijkheden die internet biedt, wordt ook beschreven in de beschikbare literatuur. Norbutas (2018) benadrukt bijvoorbeeld dat mensen eerder geneigd zijn om drugs te kopen van dealers die in hun eigen land gevestigd zijn, hetgeen een geografische clustering tot gevolg heeft (vgl. Leukfeldt et al., 2019). Norbutas (2018) geeft aan dat dit effect opvallend is, omdat als er alleen vanuit technisch oogpunt wordt gekeken, drugsgebruikers nu juist toegang hebben tot wereldwijde drugsmarkten. Kennelijk lijken gebruikers toch een voorkeur te hebben voor lokale markten.

Een dergelijke lokale verankering wordt echter ook benoemd in het onderzoek van Korshøj en Søgaard (2024). Vanwege de duidelijk verwevenheid tussen online en offline en fysieke en digitale aspecten, maken Korshøj en Søgaard (2024) gebruik van de term 'hybrid drug dealing'. Op basis van interviews met 25 respondenten en data afkomstig van platforms als Facebook, Snapchat, Wickr, Reddit en Telegram Messenger, geeft deze studie een beeld van de rol van sociale media en versleutelde berichtenapps in het vinden van dealers en het organiseren van transacties. Socialemediaplatformen blijken belangrijke toegangspoorten te zijn voor dealers: ze maken het mogelijk om snel contact te leggen en nieuwe klanten te bereiken. Maar, zo benadrukte een respondent uit Denemarken, deze platformen fungeren vooral als aanvulling:

'When I interviewed a lot of these people, it became very clear that there were so many overlaps, like this idea that drug dealing via social media is this entirely new phenomenon that is different. It kind of unraveled in a way. I mean, there's new ways they can advertise and there is some differences, but also, they didn't distinguish, they also talked about it as one sales phone. They didn't distinguish in the same way that we as researchers do. For them, it was just a phone, and they used it to text and for social media. (...) It's just seems like an extension of what is already happening. And they just have new ways of advertising in more colorful ways than maybe they could on the normal or analogue text.' (RDE-15-1)

Dealers maken met andere woorden gebruik van nieuwe mogelijkheden om hun handel onder de aandacht te brengen. In de manier waarop mensen betrokken raken als dealer zien we gelijkenissen met centrale bevindingen uit hoofdstuk 2 en 3. Beginnen in deze handel gebeurt vaak via bestaande sociale contacten, bijvoorbeeld vrienden of kennissen. Korshøj en Søgaard (2024) beschrijven dat het aantrekken van extra 'personeel' deels verloopt via digitale kanalen, maar deels ook nog steeds via persoonlijke relaties, omdat vertrouwen en competentie doorslaggevend blijven. Deze traditionele, offline werving van nieuwe dealers richt zich meestal op langdurige relaties die als relatief veilig worden gezien. Tegelijkertijd laten de onderzoekers zien dat sommige klanten via sociale media zelf aangeven interesse te hebben in koerierswerk.

Ondanks de relevantie van de digitale infrastructuur voor de handel in verdovende middelen eindigen transacties doorgaans in fysieke ontmoetingen (vgl. Korshøj en Søgaard, 2024). Met name het aspect van de betaling is daarin relevant, zoals een respondent uit Denemarken uitlegt:

'It's very fascinating, but they run into the problem that they don't have a virtual payment solution. Almost all payments in Denmark are done using apps. So mobile pay is the big one we have. So, I think they're also sort of like forced to meet physically, to exchange, to use cash, to trade physically. So, I think they do that a lot, because there are not very good digital payment options, I think they're also sort of restricted to using more cash and meeting physically.' (RDE-12)

Over de manier van betalen voor verdovende middelen – of de betaling rondom criminele activiteiten meer in het algemeen – is nog relatief weinig bekend, maar voor een belangrijk deel blijkt deze handel nog steeds afhankelijk van contante betalingen (vgl. Kruisbergen et al., 2018; Kruisbergen et al., 2019). In een van de Nederlandse interviews werd echter duidelijk dat ook digitale betaalmethoden hun intrede doen: *'En die kwamen er wel op uit dat je qua betalingen heel vaak uitkomt op cash, maar dat je in heel veel gevallen ook gewoon met een tikkie kan betalen. Dus dat je ook gewoon geld kan overmaken'* (RNL-10). Deze observatie wijst erop dat de handel in verdovende middelen zich niet alleen verplaatst naar digitale communicatiemiddelen, maar dat ook de financiële afwikkeling steeds vaker via reguliere betaalapps verloopt. Dit biedt enerzijds gemak voor koper en verkoper, maar creëert anderzijds ook nieuwe mogelijkhe-

den voor opsporing omdat digitale transacties sporen achterlaten voor de opsporingsdiensten.

4.3 ‘County lines’

Een tweede verschijningsvorm met hybride elementen rondom de handel in drugs is een fenomeen dat uitsluitend in de interviews met respondenten uit het Verenigd Koninkrijk werd benoemd: *county lines dealing*. Het gaat hier om georganiseerde drugs-handel, zoals de volgende respondent toelicht:

‘When it comes to the so-called sort of county lines drug dealing in the UK, a lot of attention is around the involvement of young people, and young people becoming involved as drug runners. So being sent often from metropolitan areas to more provincial areas to sell drugs.’ (RVK-9)

In het Verenigd Koninkrijk gebruikt de overheid de term ‘county lines’ om te verwijzen naar de activiteiten van criminele netwerken en gangs, alhoewel hier kritisch op wordt gereflecteerd in de wetenschappelijke literatuur (Andell, 2019; Koch, Williams en Wroe, 2023; McLean, Robinson en Densley, 2020; Spicer, 2021). De benaming ‘county lines’ komt voort uit de telefoonlijnen – vaak prepaid mobieltjes – die worden gebruikt om drugs over geografische grenzen heen te verhandelen, vanuit grote steden naar regio’s. Deze technologie kan gezien worden als een essentieel onderdeel van county lines-dealen (Coomber en Moyle, 2017; Fawell, Davies, Stubbings en Payne, 2024; Robinson, McLean en Densley, 2018). Dealers brengen hun drugshandel onder de aandacht via massale sms-berichten. Een respondent uit het Verenigd Koninkrijk beschreef dit fenomeen om deze reden dan ook als een traditionele vorm van drugshandel, die anders functioneert dan de digitale drugshandel die in paragraaf 4.2 is besproken.

In meer recente studies wordt echter ook melding gemaakt van het gebruik van sociale media om de verdovende middelen te verhandelen (McLean et al., 2019; Storrod en Densley, 2017). In de interviews werd de rol van sociale media echter vooral genoemd in relatie tot jongeren die bij deze handel betrokken raken. In de media in het Verenigd Koninkrijk verscheen in april 2021 een voorbeeld dat illustreert hoe jongeren worden benaderd:

‘A teenager has told how he was groomed by criminals to sell heroin and crack cocaine after being recruited through a post on Snapchat. Two years ago, aged 14 and wanting to run away from home, he responded to a message offering cash-in-hand work and accommodation on the social media app. Within 80 minutes, a gang collected him and drove him elsewhere to sell drugs. (...) The teenager, who said he spotted the post on another person’s Snapchat story, said: “It was from a simple text to be honest with

you ... Within an hour and 20 minutes of me texting them, they was [sic] already here.” (Campbell, 2021)¹²

Respondenten benadrukten in de voorbeelden van de werving van jongeren voor county lines-dealen verschillende aspecten. Allereerst de laagdrempeligheid van populaire platforms zoals Snapchat. Net als voor digitale drugsmarkten in het algemeen, werd er hier in het bijzonder gewezen op het feit dat socialemediaplatformen de mogelijkheid bieden om op grote schaal contact te leggen. Hierdoor neemt volgens respondenten de kans toe dat jongeren in aanraking komen met dergelijke praktijken, vaak zonder dat zij daar bewust naar op zoek zijn zoals de volgende respondent uitlegt:

‘Sometimes more senior drug dealers will almost kind of advertise opportunities for young people to become involved. Almost kind of like informal or illicit job postings. That will be posted out and that young people can respond to. So, I think the role of the online world can be viewed there in terms of the recruitment aspect of it. I think we can see it in terms of the glamorization of that life as well. So young people consuming content which depicts drug supply. Or more specifically, I guess, depicts the often material goods that have come from being involved in drug supply. And that can come in various forms, sometimes that can come in the form of people sending small Snapchat images of bundles of cash that they may have made that weekend, having gone to this area and sold drugs for the weekend, and suddenly they’ve got like a big wad of cash and stuff like that.’ (RVK-9)

Een tweede aspect waar door deze respondent op wordt gewezen, is de manier waarop sociale media een rol spelen in het presenteren van een bepaalde manier van leven. Het beeld dat wordt neergezet, benadrukt financieel succes en status, aspecten die voor jongeren aantrekkelijk kunnen zijn en op sociale media zichtbaar zijn (Roks en Van den Broek, 2017; 2020; Storrod en Densley, 2017). In een nieuwsbericht op de website van de Standard wordt dit als volgt beschreven:

‘Snapchat is the main tool being used by gangs to recruit children into county lines drug rings, police warned on Thursday after they seized £1 million worth of drugs in a crackdown. Teenagers are being lured in by offers of cash, mobile phones, vapes and clothes in messages sent on the app and other social media platforms and then made to courier cocaine, heroin and cannabis from London to smaller town and cities.’¹³

Respondenten gaven in de interviews aan dat het niet alleen gaat om deze blootstelling en verheerlijking van een zekere criminele levensstijl, maar ook om meer directe vormen van werving. Op sociale media worden oproepen geplaatst die jongeren uitnodi-

12 <https://www.bbc.com/news/uk-england-kent-56717403>, laatst bezocht op maandag 5 januari 2026.

13 <https://www.standard.co.uk/news/crime/county-lines-gangs-snapchat-teenagers-metropolitan-police-london-b1066084.html>, laatst bezocht op maandag 5 januari 2026.

gen om deel te nemen, op een vergelijkbare manier zoals we eerder beschreven bij de zoektocht naar geldezels (hoofdstuk 2) en uitvoerders voor geweldsopdrachten (hoofdstuk 3).

Een nadrukkelijk verschil dat in de context van county lines werd benoemd, betreft het actief benaderen van jongeren. Een respondent beschreef dit als volgt:

'If gangs are going to schools and recruiting from schools and they're looking them up on their Facebook pages and finding things out, you know, that is purposeful recruitment for the purpose of exploitation.' (RVK-6)

Het gaat hier om wat in de literatuur wordt beschreven als actieve rekrutering, waarbij het initiatief ligt bij leden van een georganiseerde criminele groep (Adamse et al., 2024; Smith, 2014). Deze benadering van jongeren vindt volgens respondenten zowel online als offline plaats. In de interviews werd echter ook gewezen op 'zelfselectie': jongeren die zichzelf aanmelden (Adamse et al., 2024), of in de woorden van een respondent *'There are absolutely people who are presenting themselves to the gangs and being like, hey, what can I do? How can I make money?'* (RVK-4). Tegelijkertijd benadrukte deze respondent dat er in de praktijk vaak sprake is van een mix, bestaande uit zowel jongeren die actief zijn benaderd en personen die zichzelf, en hun diensten, kenbaar hebben gemaakt. In alle interviews, alsook in de literatuur (Fawell et al., 2024), werd echter benadrukt dat het in beide gevallen gaat om kwetsbare jongeren:

'Many of these kids are what we call in care in the UK. They're not in the family home. They're being looked after. They're not being very well looked after. Their futures are quite glum. Their futures are poor. And they will know this to some degree. I mean, they're not in education. They're not in work. They're not in the family home. They don't feel loved. And therefore a move into a world where they can have the thing, they're often going to be poor. So to have the things that they see other kids on social media.' (RVK-6)

Wel stelt een respondent dat contacten die enkel zijn ontstaan via sociale media, bijvoorbeeld omdat jongeren hebben gereageerd op een oproep, in de praktijk de nodige risico's met zich mee kunnen brengen:

'I think, despite them being young people and being kind of used by these more senior drug dealers, you still need to kind of trust these young people. You know, you're giving them often quite a lot of drugs. They're going to be handling quite a lot of cash. They're going to need to be able to kind of manage themselves within a potentially quite difficult environment coming across erratic people who use drugs and all the rest of it. So, I think relying on online communication too much probably reduces the capacity for those older drug dealers to be able to make those decisions about, is this young person going to be able to do what we want them to do? Are they, if they get arrested by the police, are they going to tell them about what's going on?' (RVK-9)

Respondenten gaven aan dat dealers en anderen betrokkenen soms om die reden op zoek gaan naar online informatie over jongeren.

Maar digitale technologie speelt in de context van county lines ook op een andere manier een rol, zoals een respondent beschrijft:

'Like this has got more sophisticated, as phones have got more sophisticated. So, we're thinking like at one point we were using BlackBerry messenger, and then we have like iPhones. And then so the remote monitoring that I was seeing was like one to one basis through find my iPhone. And it was only like two phones at that point that could connect. Whereas now you have stuff like the app 360 and stuff like that can connect multiple people. And not only can it connect multiple people, it can also share location. It can share things like whether the battery is dying or like how many minutes they have left on their battery, like where they've just been like, it's so much more sophisticated. So that means that cyberstalking in this kind of abuse is even more stringent. It's easier for them to do. And it also gives them access to much more information, in terms of the people that they're stalking, and it connects whole networks of people.' (RVK-4)

In de literatuur wordt dit aangeduid als *remote mothering*, oftewel *'the ability to monitor where someone is, what they are doing, and who they are with at all times via locations tags, GPS tracking, pictures and video calling'* (Storrod en Densley, 2017: 688). Vergelijkbaar als rondom de geweldsopdrachten die beschreven werden in het vorige hoofdstuk, zien we hier hoe (digitale) technologie gebruikt wordt om zicht en controle te houden op de activiteiten van jongeren.

4.4 Conclusie

In dit hoofdstuk hebben we een beschrijving gegeven van de laatste verschijningsvorm waarbij processen van hybridisering een rol spelen: drugsmarkten. Dit terrein is van oudsher nauw verweven met technologie: aanvankelijk via mobiele telefoons en later ook door het gebruik van cryptovaluta. Van meer recente datum is de opkomst van digitale drugsmarkten op socialemediaplatformen. Over het algemeen is er op uiteenlopende platformen sprake van een levendige handel in verdovende middelen. Daarbij is het van belang te wijzen op differentiatie (Coomber, 2015). Er bestaan namelijk duidelijke verschillen tussen drugsmarkten, en dit geldt ook voor de digitale varianten. Niet alleen de soorten en hoeveelheden drugs die per platform worden aangeboden variëren, maar ook de functionaliteit van de platformen resulteert in uiteenlopende typen verkopers en afnemers op respectievelijk Snapchat en Telegram Messenger. Alhoewel er veel verschillen zijn tussen de verschijningsvormen in dit hoofdstuk en de eerder besproken voorbeelden van geweld, zijn er ook overeenkomsten. Net als bij geweld gaat het uiteindelijk om fysieke handelingen: de transactie van drugs en de betaling zijn cruciaal. Het betreft dus geen volledig online fenomeen, maar technologie vervult wel een faciliterende rol. Illustratief hiervoor is de werking van algoritmes op

bepaalde platforms, waardoor gebruikers sneller en vaker met drugsgerelateerde content worden geconfronteerd.

Een tweede specifieke verschijningsvorm binnen dit domein is het fenomeen van county lines dat enkel ter sprake kwam in de interviews met respondenten uit het Verenigd Koninkrijk. Het gaat hier bij uitstek om een technologisch verschijnsel, waarbij drugslijnen buiten de stad worden georganiseerd en jongeren via telefoonnummers contact onderhouden met klanten. Ook hier is sprake van een duidelijke verwevenheid van online en offline processen. Net als bij geldezels en geweldsopdrachten spelen sociale media een rol in de werving en het leggen van contacten. Jongeren worden via digitale kanalen blootgesteld aan bepaalde leefstijlen en verleid om hieraan deel te nemen. Via digitale middelen kan bovendien worden nagegaan waar jongeren zich bevinden. Met andere woorden: ook in deze context wordt zichtbaar dat technologie niet alleen de communicatie faciliteert, maar ook controle en toezicht mogelijk maakt.

5 **Uitdagingen in de aanpak van hybride vormen van criminaliteit in Nederland**

5.1 **Inleiding**

In dit hoofdstuk verplaatsen we onze aandacht naar de aanpak van hybride vormen van criminaliteit in Nederland. Hoewel dit thema ook in gesprekken met respondenten in Denemarken en het Verenigd Koninkrijk werd benoemd, ligt de nadruk omwille van de praktische relevantie van de inzichten in dit hoofdstuk op de Nederlandse context. We richten ons in het bijzonder op het beantwoorden van de tweede onderzoeksvraag: welke uitdagingen worden er in Nederland ervaren als het gaat om de aanpak van hybride vormen van criminaliteit? Het doel daarbij is niet om een volledig overzicht te bieden van alle uitdagingen in de politiepraktijk als het gaat om de digitale transformatie. Het thema van de digitale transformatie van de politie krijgt in meerdere onderzoeken expliciet aandacht (zie o.a. Landman en Groothuis, 2022; Landman, 2023; Stol et al., 2025; Van Steden et al., 2025). Waar deze studies vooral de nadruk leggen op cybercriminaliteit en digitale dimensies van de politiepraktijk, richten we ons in dit onderzoek juist op de verwevenheid tussen de fysieke en digitale aspecten van criminaliteit en de uitdagingen die dit in de praktijk voor politieprofessionals met zich meebrengt. Onze scope beperkt zich, mede vanwege het aantal geïnterviewde respondenten, tot het bieden van een inkijk in enkele uitdagingen die door respondenten in de context van hybride vormen van criminaliteit als relevant en urgent worden benoemd. We beginnen dit hoofdstuk met het schetsen van enkele uitdagingen in de structuur van de politieorganisatie (paragraaf 5.2). Paragraaf 5.3 behandelt daarna uitdagingen in de politiecultuur. Juridische uitdagingen staan centraal in paragraaf 5.4. Ten slotte bespreken we in paragraaf 5.5 de rol van technologiebedrijven en de uitdagingen die dat oplevert in de samenwerking met de politie. We besluiten met een overzicht en duiding van de centrale uitdagingen die tijdens de interviews naar voren werden gebracht.

5.2 **Uitdagingen in de politieorganisatie**

Binnen de politieorganisatie in Nederland zijn er veel initiatieven gaande die onderdeel uitmaken van de zogenoemde digitale transformatie, oftewel wat de opkomst van nieuwe technologieën vraagt van de politieorganisatie, iets dat volgens Landman (2023: 187) zowel betrekking heeft op veranderende veiligheidsvraagstukken als de

toepassing van technologie in het politiewerk. Van Steden en collega's (2025: 10) geven voorbeelden op landelijk en lokaal niveau van wat er rondom het thema digitalisering binnen de politie gebeurt. Zo zijn er cybercentra om medewerkers te ondersteunen, digitaal wijkagenten, digitale districten, digitale flexteams, digi-kamers, cybersupportteams, taakaccenthouders cyber, IT-coaches en cybervrijwilligers. Tegelijkertijd concluderen Van Steden en collega's (2025: 10) dat *'het handhaven van de orde op straat meestal meer aandacht [krijgt] dan het reguleren van de online wereld'*, iets wat eerder ook al werd geconstateerd met betrekking tot de afhandeling van cybercriminaliteit in Nederland (Ruiter et al., 2023; Leukfeldt et al., 2025). De digitale transformatie bij de politie wordt om deze reden door de onderzoekers aangeduid als een worsteling.

De typering van een worsteling is ook in het onderhavige onderzoek van toepassing. In de interviews werd door respondenten aan de ene kant benadrukt dat er binnen de politie stappen worden gezet, maar zij benoemden ook dat de politieorganisatie als geheel achterloopt als het gaat om de bredere digitalisering van de criminaliteit. Een respondent die al langer werkzaam is bij de politie zei daarover *'Ik heb ook gezien dat de politie daar niet heel erg goed in is meegegroeid en nog steeds niet.'* (RNL-11-2). Wanneer we vertrekken vanuit een meer traditioneel perspectief op de politietaak, lag de nadruk volgens een respondent lange tijd vrijwel uitsluitend op de offline wereld, die als het belangrijkste werd beschouwd (vgl. Van Steden et al., 2025: 10). Deze prioritering van de fysieke dimensie heeft ertoe geleid dat digitale en hybride vormen van criminaliteit minder structureel in de organisatie zijn verankerd. Een respondent licht dit toe:

'Ook door burgemeesters, ook door beleid. Dat ze nog steeds denken: ja jongens, ik heb een probleem met de echte wereld. En de offline wereld, dat zijn voor sommigen nog twee hele gescheiden werelden. (...) Terwijl je dan eigenlijk hiermee kunt aantonen, ja maar wacht eens even, die dodelijke schietpartij, die is wel waarschijnlijk ontstaan, of het gevolg van iets wat uiteindelijk met online ellende te maken heeft.' (RNL-7)

In hoofdstuk 3 bespraken we voorbeelden uit Nederland, Denemarken en het Verenigd Koninkrijk van geweldsincidenten die een duidelijke online aanloop kenden. Dergelijke incidenten zijn fysiek en traditioneel van aard, maar laten zien dat het online domein, of in dit geval activiteiten op socialemediaplatformen, een belangrijke rol spelen in het begrijpen van dit geweld. Enkele respondenten merkten cynisch op dat er doorgaans pas iets gebeurt binnen organisaties wanneer er zich incidenten voordoen. Daarbij onderstrepen dergelijke incidenten het belang van een sterke online informatiepositie om dit soort fenomenen te begrijpen en te adresseren (Mehlbaum et al., 2024; Van den Broek en Roks, 2022; Van den Broek en Jhanjan, 2024).

De toenemende aandacht voor de digitale wereld brengt volgens respondenten ook een andere uitdaging mee. Binnen de organisatie ontstaan tal van initiatieven, vaak vanuit bevoegenheid en met focus op de eigen eenheid. Hoewel dit veel goede dingen oplevert, leidt het ook tot fragmentatie: projecten lopen langs elkaar heen, zoals een van de respondenten beschrijft:

‘Bijvoorbeeld dat dit team hier in deze eenheid bestaat. En daarmee is het het enige team. En dat betekent niet dat andere eenheden helemaal niks doen op rivaliserende jeugd of niet online actief zijn op dit thema, maar zij zijn wel veel minder echt gestructureerd met eenzelfde soort aanpak bezig als wij dat zijn. En dat betekent ook wel dat wij vaak inderdaad een discussie hebben over deze groep uit [plaats]. Eh ja, we zien wel linkjes met onze eenheid, maar aan de andere kant waar stopt dat? Dus laat deze maar gaan. Een heel concreet voorbeeld is dat we een tijd geleden online filmpjes zagen van iemand in een politie-uniform die met automatische vuurwapens stond te rappen; we wisten dit van de eenheid [plaats]. En nou ja, als dat hier zou gebeuren: meteen schakelen, wordt er meteen actie ondernomen. Wij geven het signaal af. En daar? Nou ja, wij hebben er niks meer van gehoord.’ (RNL-6-1)

Soms zijn er simultane en vergelijkbare projecten of initiatieven op andere plekken in het land, maar vaak ontbreekt het aan overzicht. Bovendien is er volgens respondenten weinig structurele uitwisseling van *good of best practices*, succes- en faalfactoren (Schiks et al., 2021). Dit wordt door respondenten voor een deel gerelateerd aan het ontbreken van een strategische visie op het thema. Omdat veel initiatieven bottom-up ontstaan, zijn fragmentatie en versnippering volgens de geïnterviewden een logisch gevolg.

Veel initiatieven die te maken hebben met digitalisering binnen de politie lijken specifiek gericht op cybercriminaliteit of gedigitaliseerde vormen van criminaliteit. Van de relevantie van de aanpak van cybercriminaliteit is de politie inmiddels volledig doordrongen. Er zijn gespecialiseerde teams zoals Team High Tech Crime, het onderwerp cybercriminaliteit heeft prioriteit en het staat stevig op de agenda. Meerdere respondenten noemden daarbij ook Project Centurion¹⁴ als positief voorbeeld van de manier waarop de politie bezig is met het vraagstuk van digitalisering. Aanzienlijk minder aandacht gaat echter uit naar de verwevenheid van online en offline. Bovendien zorgen technologische ontwikkelingen ervoor dat het onderscheid tussen cybercrime, gedigitaliseerde criminaliteit en andere vormen van criminaliteit niet altijd duidelijk is (vgl. Lusthaus, 2024). Voor de politie heeft dit belangrijke consequenties:

‘Vroeger toen we begonnen was cybercrime in enge zin, dat was duidelijk. En nu is het wat breder geworden. Gedigitaliseerde criminaliteit heeft gewoon veel meer vermenigving met traditionele criminaliteit en dat maakt het onderscheid maken tussen die twee wel heel lastig. Ik denk ook meer dat wij gewoon bepaalde thema's naar ons toe hebben getrokken, van dat zien wij als online criminaliteit. Dat valt dan onder ons. Er is echt meer per thema gekeken, per soort delict en ook qua impact op de maatschappij en dat er toch veel slachtoffers van dat soort delicten zijn en dat je daar dus ook een focus op wilt hebben.’ (RNL-9-1)

14 In het volgende hoofdstuk gaan we nader op Project Centurion in.

Het fluïde karakter van hybride vormen van criminaliteit brengt daarbij specifieke uitdagingen met zich mee, omdat dit raakt aan verschillende organisatorische domeinen binnen de politie. Een respondent vatte dit samen als: *‘er is geen doordacht politieplan in Nederland over hoe we met die verschillende criminele takken van sport online aan de slag gaan’* (RNL-10). Voor cybercrime bestaan inmiddels gespecialiseerde teams, maar de uitdaging ligt volgens respondenten juist in de manier waarop digitale technologie verweven raakt met traditionele delicten. Hierdoor worden bepaalde aspecten van de modus operandi wel online zichtbaar, maar is het delict niet volledig digitaal van aard, zoals enkele van de verschijningsvormen die we in de vorige drie hoofdstukken hebben beschreven. Juist de wisselwerking tussen online en offline maakt het complex om te bepalen wie binnen de politie de verantwoordelijkheid draagt en waar de prioriteit moet liggen. Dit werd tijdens een interview geïllustreerd door een voorbeeld van een grote bankhelpdeskfraudezaak die uiteindelijk werd ondergebracht bij de eenheid waar de respondent in kwestie werkzaam is. De moeilijkheid hierbij is dat dergelijke zaken niet eenduidig onder cybercrime vallen, maar ook kenmerken van traditionele fraude en georganiseerde criminaliteit bevatten: *‘het is eigenlijk te groot voor een districtsrecherche. Maar het is dan voor een cybercrime-team niet complex genoeg. Dat maakt dat zo’n zaak nergens echt goed kan landen’* (RNL-9-1). Dit ‘hokjesdenken’ werd in de context van digitale criminaliteit eerder ook gesignaleerd door Van Steden en collega’s (2025: 94).

Respondenten signaleren daarnaast een additionele uitdaging waar de uitdagingen in de politieorganisatie raken aan de prioritering van bepaalde onderwerpen. In lijn met de fluïditeit van deze fenomenen kan het strafrecht bepaalde delicten op verschillende manieren aanvliegen. Dit leidt tot spanning tussen kwantitatieve doelstellingen en de complexiteit van hedendaagse delicten. Daarbij komt dat er onderscheid wordt gemaakt tussen cyber en ‘gedigitaliseerde’ delicten, waarbij soms meerdere wetsartikelen beschikbaar zijn om dezelfde concrete handeling onder te scharen:

‘Maar wat ik daarin wel interessant vond, was dat de cyber-officier zei: we hebben meerdere mogelijkheden. Het ging over het in bezit hebben van leads, het in het bezit hebben van contactgegevens. Dat is al strafbaar. Je kan het via verschillende artikelen vervolgen als Openbaar Ministerie. Dat kan onder een artikel gedigitaliseerde criminaliteit, maar het kan ook onder een cybercriminaliteit-artikel. En ze zeggen: nou we hebben meer kans onder het artikel gedigitaliseerde criminaliteit, maar we vervolgen het onder het cybercrime-artikel aangezien we cijfers hebben die we dit jaar moeten halen op het gebied van cybercriminaliteit.’ (RNL-2)

Een respondent werkzaam bij het Openbaar Ministerie gaf hier een ander concreet voorbeeld van: phishing-panels kunnen juridisch via artikel 139d lid 2 van het Wetboek van Strafrecht (Sr) als technisch hulpmiddel worden vervolgd, maar ook via artikel 234 Sr (diefstal door middel van een valse sleutel of oplichting). Een keuze, met andere woorden, tussen een cyberdelict en een gedigitaliseerd delict. Relevant in het maken van deze keuze worden dan prestatienormen:

‘Eerlijk gezegd zijn we ons, omdat we dus ook die cijfers moeten halen, meer bewust van het feit dat als iedereen zaken als gedigitaliseerde criminaliteit ten laste legt, we misschien een zaakje missen in het kader van de cybercrimencijfers. Dus soms is het ook gewoon: we moeten verantwoording afleggen. Dan komt het handiger uit als we dat artikel kiezen als er verder geen verschil in zit.’ (RNL-8-1)

Het voornoemde kan ertoe leiden dat bepaalde zaken meer aandacht en prioriteit krijgen dan andere.

Respondenten wijzen ten slotte nog op een andere uitdaging die raakt aan de organisatie van de politie. Zij signaleren namelijk dat individuen of groeperingen zich niet uitsluitend bezighouden met één type criminaliteit, maar juist actief zijn op meerdere terreinen. Zo zijn er groeperingen die zich zowel met cyberactiviteiten als met geweld bezighouden (vgl. Bekkers en Leukfeldt, 2025). Daarnaast kwamen in de interviews voorbeelden naar voren van netwerken die zich zowel bezighielden met cybercriminaliteit als met drugshandel, of waarbij vanuit drugsactiviteiten werd overgestapt naar phishing (vgl. Loggen, Veenstra en Leukfeldt, 2026). Deze verwevenheid van verschillende criminele domeinen benadrukt dat hybride criminaliteit niet alleen gaat om de combinatie van online en offline, zoals een respondent toelicht:

‘De politie ziet ook deze overlap, dus dat die netwerken zich gewoon met verschillende dingen bezighouden, maar zij weten ook niet zo goed hoe ze daarmee om moeten gaan. En zeker op lokaal niveau krijgen die cybercrimezaken gewoon geen voorrang. Ze weten gewoon niet zo goed wat ze daarmee moeten. Dus gaan ze maar iets anders doen. Gaan ze maar een traditionele zaak oppakken, daar zijn ze iets beter bekend mee, dat is iets makkelijker. Dus dat zie je op lokaal niveau zeker gebeuren. En ja, we hebben natuurlijk van die cybercrimeteams, elke regio heeft er eentje, maar dat is specifiek dan voor de technische delicten. Dus om echt die mix van de gedigitaliseerde criminaliteit met de traditionele criminaliteit te maken ... ze weten heel goed dat dit een heel belangrijk punt is. Ze zijn er ook, ze willen daar graag meer over weten, maar ze weten niet zo goed hoe ze dat moeten doen, hoe ze dat op moeten pakken.’ (RNL-4).

Waar het gaat om criminaliteit met nadrukkelijke technische aspecten is de afbakening duidelijker, maar bij de minder eenduidige verschijningsvormen blijkt dit lastiger. Het fenomeen ‘nepagenten’ was een ander voorbeeld dat tijdens de interviews werd genoemd om het bovenstaande te illustreren. Een respondent schetst dat er over dit onderwerp discussie ontstond: ‘Mensen gingen zeggen, nepagenten, is dat digitale criminaliteit? Dat is toch eigenlijk gewoon de klassieke babbeltruc?’ (RNL-7). Een andere respondent beschreef iets vergelijkbaars:

‘Bij die nepagenten is er vaak helemaal niks digitaals aan voorafgegaan, dus ook geen telefoontje of iets dergelijks. Nee, telefoontjes soms nog wel. Nou goed, er was heel veel discussie in ieder geval over van hoort het nu wel bij ons cyber-intelcluster of niet? Uiteindelijk heeft er daarover ook landelijk veel overleg plaatsgevonden en is besloten

dat dat niet het geval is. Maar je ziet wel de dadergroepen die erachter zitten, dat er overeenkomsten in zitten en dat er mogelijk slachtoffers geselecteerd kunnen worden op basis van die leadlijst. Ja, en dat gaat op het dark web, dus dan heb je daar al een cybercrime-component. Dus het is niet altijd heel erg duidelijk waar het bij hoort.’ (RNL-9-1)

De vraag waarnaar verwezen wordt, heeft betrekking op veranderingen in de modus operandi, waarbij de nadruk steeds meer verschuift naar online maar tegelijkertijd ook fysiek aanwezig blijft, hetgeen de vraag oproept waar dergelijke fenomenen organisatorisch thuishoren. Dit zorgt voor moeilijkheden rond prioritering en verantwoordelijkheden. In die zin wordt de politie door respondenten soms gezien als een logge organisatie waarin het niet altijd duidelijk is wie zich met deze hybride vraagstukken moet bezighouden.

5.3 Uitdagingen in de politiecultuur

De voortschrijdende digitalisering vraagt het nodige van de politie (Landman, 2023). Een respondent vergeleek de politie in dit opzicht met een olietanker: er gebeurt inmiddels veel op verschillende plekken, maar het kost tijd en moeite om de koers daadwerkelijk te wijzigen. Dit vormt een uitdaging omdat het, zoals duidelijk werd in de vorige paragraaf, raakt aan meerdere onderdelen van de politieorganisatie. Respondenten geven aan dat specialisten op het gebied van digitalisering binnen de politie goed in staat zijn om de digitale transformatie vorm te geven, maar dat er buiten deze groep nog winst te behalen is. Bovendien bleek uit de interviews dat de specialisten die wel over de nodige digitale expertise beschikken vaak overvraagd worden: *‘Ze roepen vaak “hebben we geen tijd voor, geen capaciteit”. De lopende dingen die via de reguliere weg binnenkomen zijn eigenlijk al te veel. We zijn er gewoon niet op ingericht’* (RNL-10). Door deze respondent wordt een punt aangestipt dat deels gezien kan worden als uitdaging binnen de politieorganisatie: er zijn volgens deze respondent letterlijk niet genoeg mensen met specialistische kennis om hybride verschijningsvormen van criminaliteit adequaat op te pakken. Naast dat dit raakt aan de politieorganisatie, heeft het ook betrekking op de politiecultuur, oftewel op de waarden en ideeën van de politie (Janssen et al., 2022; Van Hulst et al., 2016). Door respondenten wordt gesignaleerd dat het binnen diverse onderdelen van de politieorganisatie schort aan de nodige digitale vaardigheden en kennis. Van Steden en collega’s (2025: 87) wijzen hierbij bijvoorbeeld op de rol van de basisteams, iets dat een van de respondenten eveneens toelicht:

‘In verband met het opnemen van aangiftes en meldingen zie je nu weleens dat mensen ten onrechte worden weggestuurd omdat de betrokken agent denkt dat iets niet strafbaar is, dat het meer civielrechtelijk is. Dus je moet degene die die aangiftes opneemt heel duidelijke instructies meegeven of checken dat zijn kennis op peil is.’ (RNL-9-1)

De prioriteit binnen de basisteams gaat volgens Van Steden en collega's (2025) voornamelijk uit naar de aanpak van fysieke en meer traditionele vormen van criminaliteit en digitale criminaliteit komt daar volgens de onderzoekers 'bij'.

Respondenten in het onderhavige onderzoek signaleren dat er op dit punt ruimte voor verbetering is, met name in de manier waarop moet worden omgegaan met het online domein, iets wat voor velen nog (steeds) nieuw is in de context van hun werk. Digitale expertise lijkt daarbij beperkt tot gedreven enkelingen (vgl. Van Steden et al., 2025: 88-89). Een respondent werkzaam bij de recherche signaleert op dit vlak een andere uitdaging:

'Wat we deden, kunnen we fantastisch, terugkijken; rechercheren betekent ook letterlijk terugkijken en dan hebben we onze gereedschapskist. Maar die gereedschapskist, die zit nog vol met een handzaag en een spijker en een hamer, terwijl de rest van de wereld allang elektrisch is en kunststof gebruikt.' (RNL-12-1)

Respondenten gaven hierbij voorbeelden van politiecomputers zonder toegang tot Telegram, Snapchat of Marktplaats en bijzondere bureaucratische procedures om dergelijk digitaal gereedschap te verkrijgen. Meer in het algemeen bestaat er behoefte aan ondersteuning in de vorm van kennisproducten en bijscholing, maar respondenten signaleren een bredere uitdaging die betrekking heeft op de politiecultuur: *'We blijven klasjes en kennissessies geven aan de politiemensen die er nu zitten. En de één zegt net iets harder tegen je dan de ander van: ach doe mij maar gewoon weer een straatroof'* (RNL-8-1). Het beeld dat politiewerk zich zou moeten afspelen op straat lijkt hardnekkig te zijn, zo klinkt er ook door in het volgende citaat:

'Ik merk ook wel dat we online nog niet zo'n 24/7-mentaliteit hebben die we verder in de organisatie wel hebben. (...) Het zou ondenkbaar zijn als de politie op straat alleen tussen negen en vijf zou werken. Dat zou heel raar zijn. Op straat is gewoon 24/7 patrouille. Terwijl we dat online eigenlijk helemaal niet echt doen. Dat wordt belegd bij specialisten die daarmee bezig zijn op verschillende thema's. Dus dat kan cyber zijn, maar datzelfde geldt zeker voor serious organized crime. (...) Maar dat zijn eigenlijk kantoorbanen. Dus je ziet dat we dat dan doen van 9 tot 5, en niet op vrijdag, want we werken niet op vrijdag. Ja, dat is natuurlijk eigenlijk heel gek. En er zijn natuurlijk uitzonderingen op. Dus als het echt om hele ernstige gedragingen gaat, dan wordt daar wel 24/7 op gemonitord, bijvoorbeeld als je het hebt over terroristische bewegingen. Maar dan heb je het over echt hele serieuze criminaliteit en met de meer mainstream-criminaliteit zijn we niet online 24/7 bezig als organisatie. Nee, terwijl we dat op straat wel doen. Ja, dat is eigenlijk best gek.' (RNL-6-1)

De huidige tijd vraagt een andere manier van werken en daarmee ook een andere mentaliteit, waarbij de werkzaamheden van de politie zich niet langer (alleen) op straat afspelen, maar ook achter het bureau.

In meerdere interviews werd door respondenten de term ‘koudwatervrees’ gebruikt om te verwijzen naar de manier waarop men binnen de politie omgaat met de online wereld en het thema digitalisering in bredere zin. In veel gevallen speelt hierbij de gehanteerde terminologie een rol. Alleen al het benoemen van het fenomeen in cybertermen kan in bepaalde gevallen leiden tot koudwatervrees, omdat het als complex en technisch wordt ervaren, zoals een respondent toelicht: *‘We merken dat zodra we het woord cyber gebruiken, ook naar collega’s toe, dat ze meteen denken: oké, wow, technisch ingewikkeld. Hackers, zolderkamers zeg maar.’* (RNL-8-1). Een vergelijkbare spanning werd opgemerkt door Bekkers en collega’s (2025) en dit kan gezien worden als complicerende factor in de aanpak. Relevant in deze context is dat er binnen het Openbaar Ministerie bewust voor is gekozen om niet te spreken over cyber, maar over digitale criminaliteit, in de hoop dat dit de koudwatervrees tempert. Van Steden en collega’s (2025: 92) roepen in hun onderzoek op dat digitale criminaliteit gezien moet worden als veelvoorkomende criminaliteit. Daarbij zou het helpen als, in de woorden van een respondent, *‘we het gewoon beschouwen als hetzelfde en de online omgeving en de online leefwereld ook beschouwen als onze leefwereld’* (RNL-3). Een dergelijke manier van kijken kan helpen om het digitale meer te normaliseren en te zien als een kerntaak van de politie. Een respondent die al langere tijd werkzaam is binnen de politie verwoordde dit als volgt:

‘Maar dat het aan het einde van de dag toch nog vooral gewoon boeven vangen is. Dan zeggen ze: ik wist niet dat jij zo’n digitale nerd was. Nou, dan heb ik nieuws voor je: dat ben ik nog steeds niet, lullig gezegd, weet je wel. Ik zit in allerlei overlegjes, ik ga naar congressen. Kijk, die jongens die telefoons uit elkaar halen, die bestanden terugvinden, de digi-jongens, zeg maar, dat ben ik nog steeds niet. Maar waar ik wel heel sterk in ben, en dat is wel leuk dat jij dat zegt, is dat als ik natuurlijk voor die gasten sta, ik zeg: jongens, ik wil nog steeds boeven vangen. Dit zijn gewoon serieus boeven, want ze zoeken willens en wetens kwetsbare mensen uit. Wijkagenten zeggen, maar ik heb niks met digitaal. Dan denk ik: ja, maar, je bent bij de politie gegaan om mensen te helpen en boeven te vangen. En dat is het nog steeds, alleen je doet het nu op een andere manier.’ (RNL-7)

Het bovenstaande vat in de volle breedte de uitdagingen in de politiecultuur samen die waar te nemen vallen rondom het vraagstuk digitalisering. Het gaat hierbij om bepaalde beelden van de veranderende digitale wereld, alsof digitale expertise uitsluitend het domein is van ‘nerds’ met zeer specialistische kennis. Tegelijkertijd geven respondenten aan dat zij zich in de loop der jaren op allerlei manieren hebben ontwikkeld, omdat zij zagen dat hun beroepspraktijk veranderde en dat digitalisering noodzakelijk werd om ‘boeven te vangen’. Daarbij beschikken zij zelf niet altijd over alle kennis, maar maken zij gebruik van collega’s binnen de organisatie die wel over specifieke technische expertise beschikken of die weten waar dergelijke kennis te vinden is. Respondenten signaleren dat hier ruimte voor verbetering ligt omdat handleidingen, tips en kennis niet altijd gemakkelijk beschikbaar of toegankelijk zijn.

Koudwatervrees speelt ook op een andere manier een rol. Een respondent die altijd op straat had gesurveilleerd, gaf aan dat het voor hem niet duidelijk was hoe hij zich op sociale media moest bewegen, hoe hij online moest opereren en waar hij moest beginnen. Een vergelijkbare spanning werd in de interviews op verschillende niveaus benoemd. Eerder noemden we al de basisteam, maar in de interviews werd duidelijk dat dit ook speelt bij de recherche, zoals de volgende respondent toelicht: ‘Wij noemen dat koudwatervrees. Het is nodig om daarvan af te komen en om gewoon die zaken te gaan oppakken. En dan ervaar je dat het gewoon regulier recherchewerk is.’ (RNL-9-2). Ook volgens een andere respondent is de oplossing gelegen in ‘het gewoon doen’:

‘De digitale fitheid van de recherche is al jaren een speerpunt in allerlei plannen. En dat is het nog steeds. Dus wij moeten daar nog heel veel in leren. Maar aan de andere kant moet je het ook gewoon doen, want ik heb het gedaan en ik ben al wat ouder. Het is echt niet ingewikkeld. Het past prima in een normaal rechercheproces. Dat artikel 138ab [Sr, RR] is echt niet ingewikkelder dan 312. Dat [artikel 312 Sr, RR] kunnen we heel goed, maar die 138ab strafrecht vindt iedereen nu nog wat spannend. Ik chargeer een beetje, terwijl we allemaal mensen hebben die daar bewijs voor gaan leveren. Forensisch dus. Zo ingewikkeld is dat nog niet. Alleen voordat dat kwartje ging vallen, dat is een missie geweest. Heb ik drie jaren voor gevochten en een grote bijdrage aan geleverd. Inmiddels gaat het beter. Maar ja, we hebben nog wel een weg te gaan.’ (RNL-12-1)

Weer een andere respondent signaleert eveneens dat er stappen gemaakt zijn, maar ook dat er nog steeds de nodige ruimte voor verbetering is:

‘Dat is ook de reden waarom ik ook nog steeds zeg, ook binnen onze eigen organisatie, bij nog te veel collega’s moet er nog steeds de knop om. Van joh, het is allemaal niet zo ingewikkeld. Ja, tuurlijk hebben we die hele geavanceerde digitale cyberdingen, maar dit soort is eigenlijk de VVC, de veelvoorkomende criminaliteit in digitale vorm. En wat die gasten doen, natuurlijk zullen ze best wel een aantal knaapjes hebben die echt wel meer thuis zijn in computers, maar uiteindelijk wat je ziet, is dat ze gewoon lopen te rommelen met bankpasjes, met bankrekeningen, met telefoontjes, en je kan natuurlijk tegenwoordig heel veel op het internet vinden, phishing panels, tools.’ (RNL-7).

De rode draad in deze bespiegelingen is dat digitale fitheid van de politie niet alleen draait om kennis en vaardigheden, maar ook om een zeker pragmatisme: pas door het doen, kan ervaren worden dat de werkzaamheden niet altijd spannend, complex of wezenlijk anders hoeven te zijn.

Digitale fitheid binnen de politie vraagt, met andere woorden, om een gedeelde taal en visie, waarbij zowel werkvloer als leidinggevenden betrokken zijn. Voor sommige aspecten heeft dit namelijk andere consequenties en vraagt het van de organisatie om zich niet uitsluitend digitaal te positioneren, maar om een balans te vinden tussen digitale en traditionele werkwijzen. Het voorgaande betekent volgens respondenten

eveneens dat selectie en werving anders moeten worden ingericht. Enerzijds gaat het om het digitaal fit maken van zittende medewerkers, anderzijds om het aannemen van voldoende nieuwe mensen die al affiniteit hebben met digitalisering. Daarbij is het, zoals Landman en collega's (2024) benadrukken, cruciaal dat leidinggevendenden zelf voldoende digitaal fit zijn en de noodzaak voelen om dergelijke profielen binnen de organisatie te brengen. Dit benadrukt dat digitale fitheid niet alleen een technische kwestie is, maar ook een vraagstuk van personeelsbeleid en leiderschap. Of, in de woorden van een respondent: *'Je moet bij hen tussen de oren krijgen dat we misschien op zoek zijn naar politiemannen en -vrouwen die om andere redenen bij de politie gaan dan op straat bij de noodhulp willen zitten.'* (RNL-8-1).

5.4 Juridische uitdagingen

Een majeure uitdaging die door respondenten wordt gesignaleerd doorkruist de eerdergenoemde onderwerpen. In bredere zin gaat het hier om de wettelijke kaders en juridische vraagstukken die samenhangen met de voortschrijdende digitalisering van de samenleving. Centraal staat daarbij de vraag welke bevoegdheden, normen en beperkingen gelden binnen digitale en online omgevingen. Over deze ontwikkelingen is het nodige geschreven (zie bijvoorbeeld Landman en Groothuis, 2022, p. 21-38). Op dit terrein zijn er belangrijke ontwikkelingen gaande, waaronder de invoering van het nieuwe Wetboek van Strafvordering dat naar verwachting op 1 april 2029 in werking treedt en op verschillende onderdelen rekening houdt met de toenemende digitalisering van opsporing en strafvordering. Dat is relevant, want tijdens de interviews signaleren respondenten vooral onduidelijkheden op juridisch vlak. Volgens de geïnterviewden is de wetgeving verouderd, vooral waar het gaat om strafvordering en het opsporingsproces. Dit levert uitdagingen op, bijvoorbeeld als het gaat om het gebruik van data afkomstig van sociale media:

'De wet is hierin natuurlijk ook gewoon behoorlijk verouderd. En ja, niet heel erg uitgekristalliseerd. Dus wat mag je als politieorganisatie wel en niet doen? En wanneer ga je dan de grenzen over richting infiltratie? Of loop je tegen privacywetgeving aan? Daar zijn gewoon geen hele duidelijke regels over. Hoe meer het openbaar is, als jij dat zelf in de openbaarheid hebt gedeeld, dan moet je er rekening mee houden dat de politie dat ook kan zien. Nou, dan mogen wij dat dus ook zien. Ja, en hoe meer het gesloten wordt, hoe ingewikkelder dat wordt. Bij het ene platform leidt dat tot meer discussie dan bij het andere platform. Je ziet bijvoorbeeld op Telegram, zeker na de stappen die in Frankrijk zijn genomen, dat best wel heel veel groepen gesloten zijn. De vraag is dan in hoeverre het nog openbaar is. Dat het openbaar is kan je misschien bij een groep met tienduizend leden beter beargumenteren dan bij een groep met twintig leden. Dat is iedere keer weer een nieuwe discussie.' (RNL-6-1)

In meerdere gesprekken werd het monitoren van sociale media genoemd, waarbij met name verschillen tussen platforms duidelijk naar voren werden gebracht. Het gaat

daarbij vooral om reactieve manieren van werken, zoals de volgende respondent toelicht:

‘Dat vaak professionals ineens geconfronteerd worden met een geweldsincident of een ander delict en dat ze totaal niet weten hoe dit heeft kunnen plaatsvinden. En dat achteraf ineens blijkt dat dat allemaal te maken heeft met een online uiting of met iets wat op sociale media heeft plaatsgevonden nadat de politie daar onderzoek naar heeft gedaan, in gegevensdragers en soms zelfs in openbare bronnen. Dus dat het allemaal best wel achterafwerk is. Terwijl je natuurlijk veel liever aan de voorkant dit soort zaken wilt signaleren.’ (RNL-2)

Het monitoren en volgen van mensen aan de voorkant – dus proactief en preventief – roept in het bijzonder vragen op over bevoegdheden en juridische kaders. Op dit vlak is de situatie complex: er bestaat de wens om beter zicht te krijgen, maar juridisch blijkt dit vaak niet te verantwoorden. In het Verenigd Koninkrijk wordt dit wel gedaan, iets waar in het volgende hoofdstuk nader op wordt teruggekomen als voorbeeld van hoe daaraan in die context invulling wordt gegeven.

Een tweede uitdaging heeft te maken met het uitlezen van telefoons die bij verdachten worden aangetroffen. Zo viel er bij een respondent werkzaam in de digitale opsporing enige frustratie te bemerken over het feit dat telefoons lang niet altijd worden uitgelezen, terwijl daar wel een juridische basis voor bestaat. In sommige gevallen is die basis echter niet bekend, bijvoorbeeld wanneer iemand wordt aangehouden met 200 gram cocaïne en xtc. Een bijkomende ingewikkeldheid is dat, wanneer een telefoon wél wordt uitgelezen, er ook iemand moet zijn die met de verkregen data aan de slag gaat. Juist de opvolging wordt door respondenten gezien als een uitdaging. Een concreet voorbeeld waar in de Nederlandse context naar werd verwezen, is het zogenoemde *Landeck-arrest* (ECLI:NL:HR:2025:409) dat door de Hoge Raad is gewezen op 18 maart 2025. Volgens respondenten, met name zij die rond dezelfde periode als dit arrest zijn geïnterviewd, heeft het *Landeck-arrest* – over de toegang tot gegevens, bewaard op inbeslaggenomen smartphones (zie o.a. Parkins-Ozephius en Van Toor, 2024) – grote gevolgen voor de manier waarop digitale gegevensdragers zoals smartphones mogen worden onderzocht in strafrechtelijke zaken. Zij gaven aan dat dit arrest resulteerde in nieuwe juridische uitdagingen voor politieonderzoek, omdat het de bestaande praktijkvoering en bevoegdheden opnieuw ter discussie stelt:

‘We hadden een heel mooie tool voor, bijvoorbeeld, contact. Ik denk dat iedereen de context hier wel kent. Je kon een entiteit door het digitaal beslag halen en dan krijg je in ieder geval te horen: joh dit account komt in die telefoon van dat onderzoek voor, die moet je misschien even bellen. Nou, door het Landeck-arrest is daar gewoon de stekker uit getrokken. Eigenlijk kan ik nu dus geen onderzoek doen naar online entiteiten en accounts. Dat ik denk: eigenlijk zijn we nu in een paar weken vijftien jaar terug in de tijd gegaan. Maar dat is mijn persoonlijke frustratie. Ik denk echt: dat helpt ons niet. Sterker nog: dat belemmert de opsporing enorm. Wat verwacht je nog

van de opsporing als je met een Landeck-arrest komt en dingen niet meer deelbaar maakt? Dan komen we helemaal nergens.’ (RNL-12-1)

Het overstijgende gevoel dat hierin naar voren komt, sluit aan bij wat in de vorige paragraaf werd geschetst: respondenten werkzaam binnen de opsporing geven aan te werken met een gereedschapskist vol oude tools, terwijl digitalisering vraagt om nieuwe instrumenten en methoden. Dit leidt tot het gevoel dat men achterloopt, omdat de juridische kaders en opsporingspraktijken niet altijd synchroon lopen met de digitale realiteit.

Volgens respondenten is er in juridische zin in het algemeen vooral sprake van onduidelijkheid. Het gaat niet zozeer om zaken die nadrukkelijk verboden zijn, maar om het feit dat de beschikbare wetgeving niet specifiek is toegesneden op de omstandigheden waarmee de politie in de praktijk wordt geconfronteerd. In de gesprekken werd duidelijk dat met deze onduidelijkheden op twee manieren wordt omgegaan. Allereerst werd gesignaleerd dat de afwezigheid van duidelijke kaders kan resulteren in praktijken die minder wenselijk zijn. Zo werd genoemd dat wijkagenten, die weten dat relevante informatie op sociale media te vinden is, soms met privéaccounts gaan kijken en screenshots maken. Respondenten benadrukken dat dergelijke praktijken niet handig zijn voor de informatiepositie en bovendien niet bruikbaar zijn in het strafproces. Dit werd nadrukkelijk gezien als onwenselijk. Daarbij werd ook gesignaleerd dat dit probleem niet beperkt blijft tot de politie, maar dat ook andere ketenpartners soms met privéaccounts informatie zoeken of volgen.

Respondenten benoemen daarnaast een tweede manier om met onduidelijkheden om te gaan, namelijk door gebruik te maken van bestaande kaders. Een respondent licht dit toe aan de hand van de inzet van virtuele agenten op sociale media:

‘We zetten maximaal in op de virtuele agenten. Er staat nu weer een heel stuk op intranet en dat werkt ook prima. Het zijn echt slimme gasten in al die besloten groepjes waar ze wat kunnen en dan gaan we ook dingen zien en meemaken. Alleen wij hebben iemand die die kar trekt, die komt van de WOD (de afdeling Werken onder dekmantel) en die is heel erg van artikel drie Politiewet. Nou, dat is fijn want daardoor kunnen we nog veel meer doen en daar krijg ik hem ook steeds in mee, dus dat gaat goed. Maar ook daar heb je de wettelijke belemmering. Ik zeg niet dat we een politie-staat moeten worden, helemaal niet, maar de weegschaal is nog niet helemaal mooi in evenwicht en dat maakt het moeilijk.’ (RNL-12-2)

Een andere respondent geeft een vergelijkbaar antwoord op de vraag hoe er met de juridische uitdagingen wordt omgegaan:

‘Het is lastig dat al die wetten niet specifiek zijn geschreven voor deze situatie. Dus ook niet voor zo’n stelselmatige informatie-inwinning. Als je naar het artikel kijkt, dan moet je wel drie keer nadenken voordat je denkt: dat is van toepassing op het deelnemen door de politie op socialemediaplatformen. Dat is niet in eerste instantie vrij

obvious. Het is eigenlijk gewoon het artikel dat het dichtste bij komt en dat inmiddels in de jurisprudentie is uitgemaakt als zijnde de basis om dat te doen. Maar goed, wij zijn natuurlijk ook continu wel aan het kijken op welke manier we die informatie toch kunnen gebruiken. En dat betekent in ons geval vaak, als we denken van dat is echt belangrijk, dat we bijvoorbeeld ook gewoon een proefproces beginnen. We willen bijvoorbeeld meer met Telegram en bekijken dan of we met artikel drie Politiewet iets kunnen. Dus gewoon zonder allerlei bevoegdheden eraan ten grondslag te leggen om dat te doen. Nou, en dan kiezen we een specifieke zaak waarvan we denken: het is geen drama als het verkeerd uitpakt, zal ik maar zeggen.’ (RNL-8-1)

In de praktijk betekent dit dat de politie en het OM bepaalde werkwijzen uitproberen en deze vervolgens aan de rechter voorleggen, juist omdat binnen de organisaties lang niet altijd helder is wat wel en niet binnen het bereik van de huidige wetgeving valt. Wanneer de rechter vervolgens uitspraak doet, geeft dat meer duidelijkheid over wat er wel en wat er niet kan en mag. Dit kan gezien worden als een direct gevolg van het feit dat de juridische kaders nog niet zijn uitgekristalliseerd en dat voor een aantal relevante zaken geen duidelijke richtlijnen bestaan.

5.5 De rol van technologiebedrijven

Ten slotte werd door respondenten gewezen op een ander thema dat nauw verbonden is met de bovenstaande juridische uitdagingen: de rol van technologiebedrijven. Respondenten benadrukken dat opsporing en vervolging in digitale contexten vaak afhankelijk zijn van de medewerking van ‘big tech’. In de vorige drie hoofdstukken kwam op verschillende manieren naar voren dat de communicatie tussen verdachten op socialemediaplatformen belangrijke informatie bevat voor de opsporingsdiensten. Een respondent werkzaam bij het OM licht dit als volgt toe:

‘Wat we heel veel zien is dat Snapchat echt machtig populair is. Het wordt echt heel veel gebruikt en het is supervluchtig. Heel vaak zien we dat Snapchat wordt gebruikt. We weten bijvoorbeeld dat er ‘gesnapt’ is, maar we hebben geen idee wat de inhoud van dat Snapchat-bericht is. Dus een van de grootste uitdagingen is wat mij betreft dat we ook gewoon daadwerkelijk kunnen zien wat er gecommuniceerd wordt of is in het verleden omdat we gewoon heel vaak de inhoud niet weten. En daar is natuurlijk de digitale opsporing altijd heel druk mee en dat is altijd de wens van ons. Oké, wat hebben ze nou naar elkaar gestuurd?’ (RNL-1-1)

Wanneer een telefoon wordt aangetroffen bij een verdachte en die kan worden uitgelezen, is het relatief eenvoudig: alle data kunnen veilig worden gesteld en de telefoon geeft toegang tot communicatie en activiteiten op sociale media. Maar wanneer dit niet het geval is, moet de politie proberen de informatie te vorderen bij de betreffende platformen of bedrijven. Het verkrijgen van dergelijke informatie wordt volgens respondenten gezien als een grote uitdaging. Een respondent uit Denemarken verwoordde dit

als volgt: wanneer zich in een woning een verdachte situatie voordoet, beschikt de politie over de bevoegdheid om binnen te treden. In de digitale context is deze bevoegdheid echter minder vanzelfsprekend, waardoor opsporingsinstanties regelmatig stuiten op ‘gesloten deuren’ in de vorm van technische of juridische barrières (RDE-8). Op een vergelijkbare manier signaleerde een respondent uit Nederland het volgende: *‘Heel veel van die platforms zijn niet ontzettend happig op informatie delen, zelfs in opsporingsonderzoeken niet, dat duurt echt heel lang’* (RNL-6-1). Als de technologiebedrijven wel bereid zijn om data te delen, duurt dat doorgaans erg lang. Technologiebedrijven zijn in dezen, in de woorden van Lehdonvirta (2022), verworpen tot *cloud empires* met meer macht dan de overheid.

Alhoewel de rol van techbedrijven wordt benoemd als een uitdaging in de context van de aanpak van hybride vormen van criminaliteit, deelt een deel van de respondenten ook goede ervaringen en positieve ontwikkelingen. In het bijzonder wezen zij op directe contacten met mensen werkzaam bij bepaalde socialemediaplatformen, zoals de volgende respondent toelicht:

‘We hebben bij de politie een afdeling die verzoeken met die providers regelt. Single point of contact, zo heet dat. Als je het mij vraagt, is dat een van de meest ondergewaardeerde afdelingen binnen de Nederlandse politie. Daar kun je de hoeveelheid collega’s, ze zijn nu geloof ik met z’n zessen of zo iets, makkelijk verdubbelen, want je zou veel meer kunnen investeren in een goede samenwerking met die grote partijen. En die willen dat ook vaak graag.’ (RNL-10)

Aan de ene kant benoemen respondenten, ook in Denemarken en het Verenigd Koninkrijk, dat er wordt samengewerkt met sommige techbedrijven, zeker in levensbedreigende zaken waar via goede contacten direct geschakeld kan worden. Tegelijkertijd signaleren respondenten dat de mate van medewerking sterk afhangt van het type criminaliteit en van het socialemediaplatform. Een respondent licht dit toe:

‘Nou ja, laatst natuurlijk weer met Telegram, dan denk je daar is weer wat mogelijk. Nou, daar gaan we weer. Voordat iedereen massaal een vordering richting Telegram stuurt, wordt er geprobeerd om daar wat coördinatie op uit te voeren. Dus dit is iets wat continu beweegt en ook afhangt van welk platform populairder wordt. Het is belangrijk om daar goede afspraken mee te maken. Bij Snapchat was het in het begin ook veel lastiger. Daar zijn volgens mij inmiddels betere afspraken mee, zodat ik nu best wel snel resultaat krijg. Dus het verandert ook naarmate de tijd vordert, zal ik maar zeggen. En als zo’n platform dan belangrijker wordt, dan is het natuurlijk belangrijk voor ons om de prioriteit daarop te krijgen.’ (RNL-8-1)

Ook andere respondenten gaven aan dat Snapchat doorgaans meewerkt. Maar het hangt daarbij wel heel erg af van wat er door de opsporingsdiensten wordt gevorderd. Zo gaf de voornoemde respondent aan dat het verkrijgen van de inhoud van berichten op Snapchat ‘een mijl op zeven is’, omdat dit via de Verenigde Staten loopt, waardoor

het doorgaans een langdurige procedure is. Het vorderen van gebruikersgegevens en metadata bij Snapchat, zoals waar en wanneer iemand is ingelogd, gaat volgens respondenten doorgaans sneller. Dit staat in contrast met Telegram Messenger dat lange tijd geen medewerking verleende en zelfs nadrukkelijk de bescherming en anonimiteit van gebruikers boven samenwerking met autoriteiten stelde. Sinds de aanhouding van Pavel Durov in augustus 2024, zo gaven respondenten in Nederland en de andere landen aan, lijkt er echter een duidelijke verandering zichtbaar. Binnen Telegram-groepen zou er volgens respondenten inmiddels zelfs sprake zijn van een afname van bepaalde berichten in open groepen. Dit betekent niet dat Telegram niet meer wordt gebruikt, maar dat activiteiten zich verplaatsen naar afgeschermd, gesloten groepen.

Een breder thema dat werd benoemd als het gaat om de rol van technologiebedrijven is dat van platformverantwoordelijkheid. Respondenten benadrukten dat naast het strafrecht en het vorderen van gegevens ook de richtlijnen van socialemediaplatformen zelf een rol spelen. In de interviews met respondenten uit Denemarken werd dit punt een aantal keer expliciet genoemd. Het ging daarbij over wat er op sociale media wordt geplaatst en wat platformen zelf doen in termen van moderatie. Waar dit tijdens de interviews in Nederland niet of nauwelijks aan de orde kwam, werd dit door respondenten in Denemarken benoemd als een belangrijk punt. Een respondent zei daarover het volgende:

'It's not very impressive, the amount of moderation, but there's definitely more moderation on Meta than, for example, on Snapchat. And you can see the effect of moderation all the time in the languages, like the code words changing. And right now, they're mostly in group chats in Facebook groups. Okay, this is where moderation is weak right now.' (RDE-1)

Artikel 8 van de (Europese) Digital Service Act (DSA) stelt aan platformen geen verplichting om alle content op een proactieve manier te monitoren. Toch is er wel degelijk sprake van moderatie, en dat is ook iets waar de socialemediaplatformen op hun websites verslag van uitbrengen. Door het gebruik van emoji's in plaats van woorden en bepaalde slang is moderatie echter moeilijk. Tegelijkertijd geldt dat moderatie zich niet uitstrekt tot privégesprekken, zoals directe berichten (DM's) of gesloten chatgroepen. Daar kan niet op worden ingezet, wat een belangrijke uitdaging vormt. Meer in het algemeen geldt dat moderatie afhankelijk is van de manier waarop bedrijven zelf hierin investeren. Voor de Deense context werd geschetst dat het in de praktijk slechts gaat over een beperkt aantal mensen per platform en dat in toenemende mate AI en algoritmen worden ingezet om content te modereren. Een wezenlijke vraag daarbij is of de content die in strijd is met de richtlijnen van de platformen vervolgens ook wordt doorgegeven aan de politie, zoals een respondent uit Denemarken benadrukte:

'Normally you would say that if someone will be flagged and if it's a criminality, the platform should report it to the local police. And I think it would be really interesting to ask the central point of contact, like the Danish cyber police, if the platforms actu-

ally report criminality to them. And I don't think so, and then what they do is they take it down. They have a policy of takedown and then remove all the evidence.'
(RDE-4)

Het onderwerp moderatie bevat een relevante uitdaging. Wanneer moderatie plaatsvindt, betekent dit vaak dat berichten of accounts offline worden gehaald en volledig verwijderd. Dit leidt er niet toe dat de informatie wordt veiliggesteld en doorgestuurd naar de politie om in een strafrechtelijk proces te gebruiken. Wel kan dit in termen van disruptie effectief zijn, omdat het criminele activiteiten tijdelijk onderbreekt. Op dit punt wordt in het volgende hoofdstuk nader ingegaan.

5.6 Conclusie

In dit hoofdstuk hebben we een beschrijving gegeven van enkele uitdagingen in de aanpak van hybride vormen van criminaliteit in Nederland. Op basis van gesprekken met respondenten werkzaam in dit domein worden verschillende niveaus onderscheiden waarop deze uitdagingen zichtbaar worden. Binnen de politieorganisatie is de afgelopen jaren meer aandacht ontstaan voor digitalisering. Toch blijkt dat de organisatie als geheel niet altijd in hetzelfde tempo is meegegroeid met de digitale en technologische ontwikkelingen. Er zijn initiatieven binnen de politie die specialistisch van aard zijn, evenals bottom-up-praktijken om het hoofd te bieden aan meer recente ontwikkelingen, maar het blijft vaak onduidelijk hoe en waar in de politieorganisatie deze inspanningen structureel zijn of moeten worden ingebed. Dit probleem wordt versterkt wanneer fenomenen veranderen en nieuwe vormen van criminaliteit zich aandienen, waardoor de vraag rijst hoe de organisatie daarop moet reageren en wie er binnen de politie verantwoordelijk is voor de aanpak.

Naast organisatorische vraagstukken speelt ook de politiecultuur een rol van betekenis. Enerzijds zijn er binnen de politie specialisten met diepgaande kennis, bijvoorbeeld op het gebied van cybercrime. Deze groep is goed in staat om digitalisering vorm te geven, maar wordt vaak overvraagd omdat de bredere organisatie onvoldoende digitaal is meegegroeid. Voor veel medewerkers geldt dat zij koudwatervrees ervaren, niet zozeer vanwege de inhoud, maar door de terminologie en onbekendheid met digitale werelden. Dit geldt zowel voor basisteams als voor de recherche. Deze uitdaging vraagt om praktische ervaring, maar ook om investeringen in trainingen, om aandacht van leidinggevend en om beleid dat gericht is op werving en selectie van medewerkers met digitale competenties.

Een derde uitdaging betreft de juridische dimensie. Respondenten signaleren dat wetgeving vaak verouderd is en niet specifiek toegesneden op digitale omstandigheden. Dit leidt tot onduidelijkheden en improvisatie, waarbij politie en Openbaar Ministerie soms in afwachting zijn van uitspraken van rechters om richting te geven aan hun werkzaamheden. Het recente *Landeck*-arrest illustreert daarbij hoe jurisprudentie sturend kan worden in het digitale domein en daardoor nieuwe uitdagingen oproept voor opsporing en bewijsvoering. Het beeld dat men werkt met een gereedschapskist vol

verouderde werktuigen, terwijl nieuwe tools dringend nodig zijn, is in dezen betekenisvol.

Ten slotte is aandacht besteed aan de rol van technologiebedrijven. Alhoewel positieve ervaringen werden gedeeld, noemden respondenten ook de nodige uitdagingen. Zo verschilt de medewerking per platform: Snapchat wordt gezien als relatief coöperatief, terwijl Telegram lange tijd nadrukkelijk de anonimiteit van gebruikers boven samenwerking stelde. Recente ontwikkelingen, zoals de aanhouding van Pavel Durov, lijken hierin verandering te hebben gebracht, maar leiden vooral tot een verplaatsing van activiteiten naar gesloten groepen.

Kortom: alhoewel het vraagstuk van digitalisering binnen de politie de afgelopen jaren nadrukkelijk meer aandacht heeft gekregen, overheerst het beeld dat de organisatie als geheel vooral de nodige uitdagingen ervaart als het gaat om de snelheid waarmee digitale en technologische innovaties zich ontwikkelen en criminele verschijningsvormen beïnvloeden. In het volgende hoofdstuk verleggen we onze aandacht naar een drietal voorbeelden van de aanpak van hybride vormen van criminaliteit, waarmee deels inzichtelijk wordt gemaakt hoe in de drie landen wordt omgegaan met de in dit hoofdstuk geschetste uitdagingen.

6 Drie landen, drie voorbeelden

6.1 Inleiding

In dit voorlaatste hoofdstuk besluiten we met een aantal concrete voorbeelden van aanpakken waarmee (deels) wordt getracht het hoofd te bieden aan de uitdagingen die beschreven zijn in het vorige hoofdstuk. We geven hiermee antwoord op de derde en laatste deelvraag naar voorbeelden van de aanpak van hybride vormen van criminaliteit in Nederland, Denemarken en het Verenigd Koninkrijk. Per land lichten we een specifieke aanpak uit die in de interviews in de respectievelijke landen werd genoemd als voorbeeld. Het gaat hier nadrukkelijk niet om aanpakken die een zekere wetenschappelijke evidentie kennen of geëvalueerd zijn. Eerder zijn het voorbeelden, elk met een andere focus, die een beeld geven van de manier waarop de politie bezig is met de aanpak van fenomenen die op de een of andere manier een digitale component hebben. In de volgende paragrafen zetten we op hoofdlijnen uiteen wat deze aanpakken behelzen. We beginnen in paragraaf 6.2 met het Deense voorbeeld: POP, oftewel *Politiets Online Patrulje* (online politiepatrouille). In paragraaf 6.3 bespreken Project Alpha uit het Verenigd Koninkrijk. Paragraaf 6.4 geeft een beschrijving van Operatie Centurion in Nederland. In paragraaf 6.5 maken we de balans op en benoemen we enkele overeenkomsten en verschillen tussen de drie voorbeelden.

6.2 Denemarken: Politiets Online Patrulje

In het recente rapport ‘*Policing in an online world. Relevance in the 21st century*’ van Europol (2025) wordt een reeks initiatieven beschreven die vallen onder de noemer van ‘online policing’. Hiermee wordt verwezen naar uiteenlopende praktijken waarin politiediensten proberen hun rol te pakken in de digitale context. Online policing wordt gezien als een belangrijk domein voor politiewerk:

‘If online communities are seen as lawless spaces “by creating online safe havens of impunity”, ungoverned areas of life will eventually be ruled by the strongest, resulting in the law of the jungle. The police, therefore, must move into these spaces before they become lawless, in order to protect the rights of citizens and reintroduce the safeguards that underpin life in 21st century Europe.’ (Europol, 2025: 5)

Onder de noemer van *online policing* wordt een domein aangeduid waarover tot op heden relatief weinig geschreven is. Europol (2025: 6-7) beschouwt dit als een veld in opkomst, dat nog verdere ontwikkeling behoeft om daadwerkelijk effectief te kunnen functioneren. Daarbij wordt verwezen naar eerste studies op dit gebied, zoals het onderzoek uit Noorwegen van Vrist Rønn (2023), waarin *online police patrolling* centraal staat. Deze vorm van digitale surveillance kent vooral een nadruk op preventie, waarbij getracht wordt de kern van lokaal en community policing in fysieke ruimtes te reproduceren. Het gaat dan om lokale verankering in een specifieke gemeenschap, het uitvoeren van concrete politietaken zoals criminaliteitspreventie en het optreden tegen alledaagse overtredingen, evenals het opbouwen van relaties en het versterken van publiek vertrouwen (Vrist Rønn, 2023).

In het rapport van Europol (2025) over online policing worden verschillende initiatieven belicht die onder deze noemer vallen. Denemarken wordt in het rapport van Europol genoemd als een voorbeeld van een land waar het politiewerk zich succesvol heeft aangepast aan het digitale tijdperk. Daar heeft men een innovatieve en geïntegreerde aanpak ontwikkeld voor online patrouilles en digitale preventie onder de naam POP: *Politiets Online Patrulje*. Deze Deense online politiepatrouille vormt een gespecialiseerde eenheid binnen de nationale politie die zich richt op digitale handhaving en preventie. Tijdens een bezoek aan Denemarken in februari 2025 spraken wij uitgebreid met een betrokkene bij de start en ontwikkeling van POP, dat sinds april 2022 actief is. Deze eenheid liet zich in sterke mate inspireren door een vergelijkbaar voorbeeld uit Noorwegen dat al eerder was gestart (Vrist Rønn, 2023). De eenheid bestaat uit tien leden – zeven politieagenten, een civiele analist, een communicatiespecialist en een hoofd van de afdeling – en opereert op uiteenlopende online platforms, afhankelijk van doelgroep en context. Binnen het team zelf is sprake van een zekere specialisatie: in het team richt ieder zich op een eigen focusgebied, zoals radicalisering of de handel in verdovende middelen. De enorme hoeveelheid online activiteiten op verschillende platformen vormt gezien dit beperkte aantal medewerkers een uitdaging.

Het primaire doel van POP is het zichtbaar maken van politieaanwezigheid in de digitale ruimte en het vergroten van de veiligheid van burgers daarin (Europol, 2025: 8-9). POP is online herkenbaar op socialemediaplatformen, waarbij zij opereert onder officiële accounts. Enerzijds richt men zich op het leggen van contact met jongeren, vergelijkbaar met de wijze waarop wijkagenten offline relaties opbouwen. In Denemarken gebeurt dit onder meer door zichtbaar als politie deel te nemen aan online activiteiten, zoals gamen. Daarbij wordt gebruikgemaakt van herkenbare avatars, handles en uniformen, zodat duidelijk is dat het om politiefunctionarissen gaat. Dit draagt bij aan het creëren van dialoog en gezamenlijke activiteiten, zoals ook op buurtniveau gebruikelijk is, en beoogt vooral het leggen van contact en het opbouwen van vertrouwen. Online krijgt dat echter wel anders vorm dan in de fysieke wereld:

'It's more difficult to do it online than in the offline world. You can have a police officer as myself, I can go down to the youth club or something and have a talk with the youth because I will be there. They can see the uniform, but online I have to get them to the

place before I can talk to them. And they won't come in there if I'm not going to talk right way. So that's a little bit different compared to the physical world.' (RDE-8)

Door proactief aanwezig te zijn online beoogt POP het veiligheidsgevoel te versterken en het vertrouwen in de politie te vergroten. De werkwijze is gebaseerd op actieve interactie met gebruikers: agenten reageren op vragen en opmerkingen, organiseren Q&A-sessies en delen informatieve content over actuele risico's zoals cyberpesten, online fraude en sexting. De communicatie wordt afgestemd op verschillende doelgroepen, met name jongeren, en ondersteund door visuele middelen zoals video's en infographics. Deze aanpak maakt het mogelijk om op een laagdrempelige manier in contact te komen met burgers. Een belangrijk werkterrein betreft jongeren en kinderen die veelvuldig actief zijn op gamingplatforms. De patrouille sluit hierop aan door zelf deel te nemen aan online spellen, zoals Roblox, Minecraft en Fortnite. Via livestreams op Twitch bereikt men bovendien een aanzienlijk breder publiek, waardoor interactie met duizenden burgers mogelijk wordt binnen enkele uren (Europol, 2025: 8-9).

De zichtbare aanwezigheid van de politie in online ruimtes kan op zichzelf gezien worden als een vorm van preventie. Net zoals de fysieke aanwezigheid van politie op straat een signaalfunctie vervult, geldt dit ook in digitale contexten. Toch levert dit niet altijd het gewenste resultaat op:

'It's quite different. Some of the groups are actually welcoming us and say: oh, great to see the police, if they don't have so much illegal stuff going on there. Really welcoming us, mostly. But we also see, especially when we started patrolling Reddit, also a special place, they want to confront the police also. We had a lot of that in the beginning. We had a big group in and on Reddit, and they kicked us out in the beginning and said, we don't want the police here.' (RDE-8)

Waar op het ene platform de nadruk ligt op open dialoog en laagdrempelige interactie, kan op een ander platform de dynamiek juist meer gesloten of vluchtig zijn. Soms wordt er positief gereageerd op de online aanwezigheid van de politie, maar op andere platformen, zoals ook Telegram, aanzienlijk minder. Met de arrestatie van Pavel Durov in augustus 2024 is hierin wel een verandering gekomen.

Naast preventie speelt open-source intelligence (OSINT) een centrale rol in de opsporing van online criminaliteit. Burgers kunnen meldingen doen van verdachte activiteiten, waarna OSINT wordt ingezet om verdachten te identificeren of aanvullende informatie te verzamelen (Europol, 2025: 8-9). Bovendien richt POP zich inmiddels niet meer alleen op preventie:

'We are patrolling the internet like we are patrolling the streets. If we come across something illegal or something, then we can go deeper into it, and try to do an investigation to build up cases or to try to disrupt the crime.' (RDE-8)

Deze meer gerichte patrouilles worden door Europol (2025: 18) beschreven als een manier om online criminaliteit te verstoren. Het idee achter deze manier van werken is dat deze gebaseerd is op politie-inlichtingen, tips en een bredere kennis van welke digitale ruimtes relevant zijn om te monitoren. Wanneer POP bijvoorbeeld kennis vergaart over een specifieke online omgeving waar criminele activiteiten plaatsvinden, kan zij actief deelnemen aan gesprekken via publieke profielen om het verloop van die activiteiten te onderbreken. Dit kan daders ontmoedigen om op dat specifieke platform aanwezig te blijven en kan resulteren in een verplaatsing naar andere platformen. Hoewel dit ertoe kan leiden dat zij zich verplaatsen naar sterker versleutelde berichten-diensten, wat het onderzoek bemoeilijkt, verkleint dit tegelijkertijd hun potentiële klantenkring en vertraagt het hun activiteiten.

Juist dit disruptieve element is relevant in een digitale context. Het laat zien dat online policing niet alleen gericht is op preventie en relationele verankering, maar ook op het actief verstoren van criminele activiteiten op sociale media. Daarvoor wordt gebruikgemaakt van een 'single point of contact' die POP heeft bij socialemediaplatformen waarmee *'we're going to try, on their own terms of service, to put down the profiles'* (RDE-8). Zo worden illegale Facebookgroepen, gebruikt voor de handel in verboden middelen, in samenwerking met het Deense single point of contact verwijderd. Ook in meer anonieme omgevingen zoals Telegram wordt disruptie toegepast. De patrouille wist daar daders van de verspreiding van kindermisbruikmateriaal te identificeren en vervolgen. Vervolgens werd in diverse groepen gecommuniceerd dat een operatie had plaatsgevonden en dat meerdere gebruikers waren aangeklaagd. Deze strategie had een afschrikkend effect: gebruikers verlieten massaal de groepen en de verspreiding van beeld- of videomateriaal waarin kinderen seksueel worden misbruikt of uitgebuit en van wraakpornografie daalde aanzienlijk (Europol, 2025: 17).

6.3 Verenigd Koninkrijk: Project Alpha

Het tweede voorbeeld betreft *Project Alpha* uit het Verenigd Koninkrijk. Project Alpha is momenteel een door de National Police Chiefs' Council (NPCC) gesponsorde en door het Home Office gefinancierde operatie, ondergebracht bij de Metropolitan Police (Met) in Londen. Het initiatief werd in juni 2019 gestart als een socialemedia-intelligenceproject met als doel het monitoren, analyseren en rapporteren van online content, in het bijzonder in relatie tot ernstige jeugddelicten en county lines-criminaliteit (Metropolitan Police, 2024). Het project beschikt over circa 42 vaste posities, bestaande uit politieagenten en ondersteunend personeel en verdeeld tussen het zogenoemde Online Harm Referral Team (OHRT) en de Social Media Hub (SMH) (Metropolitan Police, 2024). Binnen Project Alpha is sprake van een gespecialiseerde organisatorische structuur die zich richt op het monitoren en analyseren van digitale content.

Project Alpha beoogt een nauwkeurig beeld te schetsen van socialemedia-activiteiten die zich vertalen naar ernstige geweldsincidenten in de fysieke wereld. Daarmee wordt een expliciete link gelegd tussen digitale dynamieken en offline geweldscriminaliteit. Het doel van Project Alpha is dan ook het versterken van de operationele capaciteit van

de politie in het bestrijden van geweldscriminaliteit via sociale media. Volgens het hoofd van deze afdeling was er namelijk een duidelijke toename in geweld zichtbaar nadat bepaalde online content, in het bijzonder muziek, werd gedeeld en verspreid. Een centrale activiteit van Project Alpha betreft het volgen van drill- en rapvideo's, met name vanwege hun potentieel gewelddadige inhoud. Dat begon op YouTube en later ook op Instagram en andere platformen die op dit moment populair zijn. Door deze content systematisch te monitoren, kan het team spanningen tussen rivaliserende groepen identificeren en vroegtijdig signaleren. Cruciaal daarbij is dat de betrokken medewerkers beschikken over kennis van de lokale context, zoals het hoofd van de afdeling toelichtte:

'As an organization, what we started doing was that we had officers that understood, so police officer who worked in sort of gang's units that were street cops. We brought them into a team to go online and look at incitement of violence in the online space.' (RVK-5-1)

Zonder dergelijke kennis van het fenomeen en de context, iets dat belangrijk is om de betekenis van online uitingen te kunnen doorgronden en correct te kunnen interpreteren (Ilan, 2020), bestaat immers het risico dat digitale signalen verkeerd worden geïnterpreteerd en dat hun waarde voor intelligence en opsporing beperkt blijft.

Volgens het hoofd van de afdeling heeft de werkwijze van Project Alpha een zekere parallel met de manier waarop offline politiewerk zou worden uitgevoerd. Hij lichtte dit als volgt toe:

'In case there would have been a stabbing last night in the south of Rotterdam, I would have got high visibility police officers stopping and searching people physically in that area, watching what's going on. Why wouldn't I be looking at what's going on in the online space when it's open and public? I'm not intercepting. I'm not specifically targeting a person but moving the case forward. Until say that the stabbing in the south of Rotterdam was done by [naam respondent 2]. We would like to specifically target [respondent 2] and effectively take his digital world apart. Maybe follow him online, look at his posts, etc. We would then get an authority that's the same level as a normal surveillance authority. It is the same level of authority as if we would follow him around the street. I have to add him as a friend on social media. So, there is oversight and governance during a review period.' (RVK-5-1)

Door Project Alpha wordt hierbij ook gebruikgemaakt van heimelijke openbrontechnieken om kansen voor inlichtingenvergaring en bewijsverzameling te identificeren als aanvulling op de bestaande OSINT-teams.

De activiteiten van Project Alpha omvatten het verzamelen van criminele inlichtingen, het signaleren van content die mogelijk in strijd is met de richtlijnen van platformen, en het bieden van ondersteuning aan onderzoeks- en opsporingsteams. Een belangrijk onderdeel van de aanpak betreft het versturen en delen van informatie met technolo-

giebedrijven. Dit wordt vooral uitgevoerd door het Online Harm Referral Team (OHRT), dat fungeert als schakel tussen politie en socialemediaplatformen. Het hoofd van de afdeling beschreef dit als volgt:

'But then we started engaging with Google, who obviously owns YouTube, and then Meta, who's got Instagram. And more recently we've done some really positive engagement with Snapchat and TikTok, to the point where we have something called a trusted flagging system. We have a special portal where we can go into Google i.e. YouTube and say this track, we think, breaches your terms and conditions because YouTube will have terms and conditions that say you can't put violent material, you can't show knives, you can't show guns on our platform. So, we're not using our policing powers. We're looking at the track or we're looking at the visuals. It's mainly the visuals, and we say: we think this is breaching your terms of service. Could you please review it and consider taking it down? And we had lots of removals, and we built quite a good relationship.' (RVK-5-1)

Het team van Project Alpha identificeert online content die mogelijk schadelijk of illegaal is en draagt deze gericht aan bij de betreffende bedrijven, zodat zij maatregelen kunnen nemen om materiaal te verwijderen of accounts te blokkeren. Daarbij wordt toegelicht waarom de medewerker van Project Alpha meent dat de inhoud in strijd is met de richtlijnen, inclusief context, bijvoorbeeld songteksten die verwijzen naar eerdere misdrijven. Belangrijk is dat er geen politie-informatie wordt gedeeld met het platform. Alleen gegevens uit het materiaal zelf of publiek beschikbare bronnen, zoals mediaberichten over geweldsincidenten, worden gebruikt. Zo blijft de verwijzing beperkt tot feitelijke en openbare informatie, terwijl het platform kan beoordelen of de inhoud verwijderd moet worden.

In zowel het interview met het hoofd van Project Alpha als in openbare beschikbare documentatie werd gewezen op het belang van duidelijke grenzen die aan deze vorm van online politiewerk moeten worden gesteld. In de praktijk kwam het voor dat politiefunctionarissen zelfstandig online optraden, zonder duidelijke grenzen. Tijdens het interview werd een voorbeeld gegeven van een agent die een nepaccount aanmaakte op Instagram en gangleden ging toevoegen. Omdat hij werkte met twee verschillende accounts, koppelde algoritmes zijn nepaccount aan dat van zijn echte vrienden en zijn familie. Dergelijke ongecoördineerde acties zijn niet alleen ineffectief, maar kunnen ook risico's met zich meebrengen voor de legitimiteit en veiligheid van het politiewerk. Meer in het algemeen is er fundamentele kritiek geuit op de werkwijze van Project Alpha. Zo kopte *The Guardian* op 3 augustus 2022 (Crisp en Dodd, 2022) *'Met police profiling children "on a large scale", documents show'*. Uit interne documentatie zou blijken dat de politie op grote schaal persoonlijke gegevens van kinderen verzamelt en op grote schaal online profileert. Critici, aldus de journalisten van *The Guardian* (Crisp en Dodd, 2022), waarschuwen voor de maatschappelijke risico's van deze onevenredige focus op jonge zwarte kinderen, een sentiment dat ook naar voren werd gebracht tijdens enkele interviews met respondenten in het Verenigd Koninkrijk. Mensenrechten-

organisaties stellen bovendien vragen over de mate waarin platforminteracties, zoals harm referrals en contentverwijdering, kunnen worden gezien als vormen van censuur of stigmatisering van specifieke groepen (Crisp en Dodd, 2022). In een reactie op deze kritiek gaf het hoofd van het Project Alpha het volgende aan:

‘I suppose one of the learnings from that is better engagement with the community about why and what we’re doing, because the perception was that we were just deleting, you know, we had the big red button that just deleted tracks. And it was if you’re a young black man in London, we were going to delete your track. And that simply wasn’t the case. It was purely based on what the track is talking about and what it can do.’ (RVK-5-1)

In aanvulling hierop distantieert de Londense politie zich in een ‘freedom of information request’ – vergelijkbaar met een Woo-verzoek (Wet open overheid) in Nederland – van etnisch gericht queren en onderstreept dat drillmuziek nooit wordt beschouwd als ‘criminal in nature’.¹⁵

6.4 Nederland: Operatie Centurion

Het derde en laatste voorbeeld dat we in dit hoofdstuk bespreken betreft Operatie Centurion. Dit Nederlandse initiatief is expliciet gericht op het versterken van de aanpak van gedigitaliseerde criminaliteit. Zoals ook in het fenomeenbeeld *Online fraude in beeld* van de politie (2024: 16) wordt benadrukt, gaat het hier om een verschijnsel dat veel voorkomt en een grote impact heeft op slachtoffers. Tegelijkertijd betreft het een thema dat, juist vanwege de digitale component, binnen de politie niet altijd de aandacht heeft gekregen die het verdient. Dit heeft onder andere te maken met de noodzaak tot prioritering, de schaarste aan capaciteit en de vereiste vaardigheden om effectief met digitale criminaliteit om te gaan – facetten die in het vorige hoofdstuk als uitdagingen zijn benoemd. Tegen deze achtergrond werd Operatie Centurion op 1 januari 2022 gelanceerd als onderdeel van de bredere digitale transformatie binnen de politie. De aandacht daarbij ligt, zoals in het vorige hoofdstuk ook benoemd, op veelvoorkomende digitale criminaliteit, te weten aan- en verkoopfraude, phishing, bankhelpdeskfraude en hulpvraagfraude. Deze delicten, ook wel aangeduid als Centurion-delicten of -feiten, zijn voor een deel te typeren als hybride criminaliteitsvormen omdat zij zowel online als offline componenten hebben en meer in het algemeen een wisselwerking tussen mens en techniek kennen.

Het doel van Operatie Centurion is om de aanpak van gedigitaliseerde criminaliteit bij de politie en het Openbaar Ministerie te bespoedigen en te komen tot een gezamenlijke, landelijk gecoördineerde strategie (Politie, 2025: 16). Om dit te realiseren is het noodzakelijk dat basisteams worden ondersteund bij het opvolgen van meldingen van

¹⁵ <https://www.met.police.uk/foi-ai/metropolitan-police/disclosure-2024/june-2024/project-alpha/>, laatst bezocht op maandag 5 januari 2026.

digitale criminaliteit, maar dat ook informatie bijeen wordt gebracht waarmee criminele verbanden zichtbaar worden gemaakt om vervolgens aangepakt te kunnen worden (Van Steden et al., 2025: 21). Binnen de politie blijft schaarste echter een structureel probleem. Ook bij de aanpak van gedigitaliseerde criminaliteit was het daarom noodzakelijk om zaken te prioriteren, omdat niet alle signalen en casussen tegelijkertijd kunnen worden opgepakt. Een respondent betrokken bij de start van Operatie Centurion lichtte dit als volgt toe:

‘Maar wij hebben wel gezegd: elke eenheid moet eigenlijk wel, en ik weet, capaciteit is een vies woord, maar we zeggen wel, wil je deze slag een beetje maken, dan moet je in elke eenheid eigenlijk toch wel een dedicated capaciteitsframe maken om hiermee aan de gang te gaan. Want als je dit gewoon maar laat doen, van ja: we doen het wel tussen de bedrijven door, dan is de ervaring toch heel vaak, en dat wil ik wel even zeggen, dan zal het altijd moeten wedijveren met weer een explosief aan een deur, en dan gaat zo’n zaak van tafel. En daar is Rotterdam niet uniek in, want dat gebeurt ook in Groningen, dat gebeurt ook in Zeeland.’ (RNL-7)

Binnen diverse eenheden zijn gespecialiseerde teams en hubs ingericht die zich specifiek richten op de bestrijding van de Centurion-delicten (Van Steden, 2025: 21). In het Nederlandse politielandschap vertegenwoordigt Operatie Centurion een omslag in de manier waarop digitale criminaliteit wordt benaderd. In meerdere gesprekken in Nederland werd om deze reden verwezen naar Operatie Centurion als een goed voorbeeld. Een respondent gaf hiervan het volgende voorbeeld:

‘Je ziet wel, en dat vind ik het mooie, dat we ook gewoon resultaten hebben. Want als je nu echt kijkt, nou ja, ik zie geregeld in de krant artikelen staan. En ik weet dat dan niet alleen vanuit de krant, maar ik zie geregeld gelukkig ook nu in de krant dat er weer gewoon vier, vijf gasten worden aangehouden die tientallen van dit soort zaken [Centurion-delicten, RR] gepleegd he.’ (RNL-7)

Tussen december 2023 en september 2024 vond een externe, onafhankelijke evaluatie van Operatie Centurion plaats (Oosterheert, 2025). Er werd, onder andere, geconcludeerd dat Operatie Centurion heeft bijgedragen aan een versnelling van de digitale transformatie in de eenheden. Over het algemeen hebben medewerkers in de basisteams meer ervaring en kennis opgedaan met betrekking tot het oppakken van gedigitaliseerde criminaliteit (Van Steden et al., 2025). Toch zijn er ook uitdagingen die voor een deel al benoemd werden in het vorige hoofdstuk. Van Steden en collega’s (2025: 95) concluderen dat de aanpak van digitale criminaliteit goed van de grond komt als er sprake is van gedreven politiemedewerkers die beschikken over *‘improvisatievermogen en de benodigde kennis van het digitale werk op basisteams’*. Alhoewel er binnen Operatie Centurion stappen zijn gezet met betrekking tot de aanpak van de Centurion-delicten, zijn er meer digitale fenomenen die aandacht vragen, waaronder ook een deel van de verschijningsvormen die in deze rapportage zijn benoemd. Ook werd benoemd dat

het van belang is dat de politie op dit punt flexibel blijft, want, in de woorden van een respondent, *‘over vier maanden hebben ze misschien wel weer iets bedacht, maar wij nu nog niet’* (RNL-7).

Op basis van de aanbevelingen uit de evaluatie van Operatie Centurion is begin 2025 het programma *Gedigitaliseerde Criminaliteit* gestart. Dit programma heeft als doel de politie in staat te stellen digitale criminaliteit op een effectieve manier te bestrijden. De beoogde effecten zijn dat digitale criminaliteit met de grootste maatschappelijke impact gericht wordt aangepakt, waarbij de politie datagedreven samenwerkt om de bestrijding te versterken. Daarnaast wordt ingezet op een effectieve samenwerking tussen politie, ketenpartners en het publiek-private stelsel, zowel nationaal als internationaal, zodat actuele vormen van digitale criminaliteit gezamenlijk en slagvaardig bestreden kunnen worden (Oosterheert, 2025).

6.5 Conclusie

In dit hoofdstuk hebben we een beschrijving gegeven van drie projecten die door respondenten in de respectievelijke landen genoemd werden als positieve illustraties in de context van de aanpak van hybride criminaliteit. Alle drie de voorbeelden maken inzichtelijk hoe in verschillende landen invulling wordt gegeven aan politiewerk in een digitale context. In Denemarken richt de Politiets Online Patroelje (POP) zich vooral op preventie en zichtbare online aanwezigheid van de politie in zijn algemeenheid en agenten in het bijzonder. Bij Project Alpha uit het Verenigd Koninkrijk staat een meer heimelijke vorm van online politiewerk centraal, onder andere om verbanden te leggen tussen digitale uitingen en geweldscriminaliteit in de fysieke wereld. Het Nederlandse voorbeeld, Operatie Centurion, vertegenwoordigt ten slotte een meer strategische en organisatorische omslag bij de politie voor bepaalde gedigitaliseerde vormen van criminaliteit.

Ondanks de verschillen in focus – preventie en dialoog bij POP, intelligence en disruptie bij Project Alpha en een meer strategische insteek bij Operatie Centurion – zijn er overeenkomsten. Alle drie de projecten benadrukken de noodzaak van een digitale transformatie, het combineren van preventieve en repressieve elementen en het belang van samenwerking met externe actoren zoals technologiebedrijven. Gezamenlijk laten deze voorbeelden zien dat de werkzame bestanddelen van politiewerk in een hybride context zijn gelegen in online en offline zichtbaarheid, prioritering van digitale en gedigitaliseerde delicten, intelligence over online en offline verschijningsvormen en samenwerking met technologiebedrijven. Deze elementen vormen de kern van politiewerk in een breder digitaal transformatieproces waarin de politie niet alleen reageert op digitale criminaliteit, maar ook actief vormgeeft aan de manier waarop veiligheid en rechtshandhaving in het digitale tijdperk worden georganiseerd.

7 Conclusie

7.1 Inleiding

De voortschrijdende digitalisering heeft geresulteerd in criminaliteitsvormen die een sterke verwevenheid kennen tussen online en offline, en fysieke en digitale componenten. Voor deze bredere ontwikkeling hanteren we in deze studie de term hybridisering, een ontwikkeling die bij vrijwel alle criminaliteitsvormen in meer of mindere mate kan worden waargenomen. In dit rapport doen we verslag van een verkennend onderzoek naar hybride vormen van criminaliteit, met aandacht voor zowel de aard als de aanpak van deze fenomenen in Nederland, Denemarken en het Verenigd Koninkrijk. De volgende onderzoeksvraag staat centraal in deze studie:

Wat zijn de aard en aanpak van hybride vormen van criminaliteit in Nederland, Denemarken en het Verenigd Koninkrijk?

Om de centrale onderzoeksvraag te beantwoorden, hebben we de volgende drie deelvragen geformuleerd:

- 1. Welke vormen van hybride criminaliteit zijn er in Nederland, Denemarken en het Verenigd Koninkrijk?*
- 2. Welke uitdagingen worden er in Nederland ervaren als het gaat om de aanpak van hybride vormen van criminaliteit?*
- 3. Welke voorbeelden van de aanpak van hybride vormen van criminaliteit zijn er in Nederland, Denemarken en het Verenigd Koninkrijk?*

In de periode oktober 2024 tot juni 2025 hebben wij in totaal 54 respondenten geïnterviewd om antwoord te krijgen op deze vragen. Deze 54 respondenten waren als volgt verdeeld over de drie landen: 18 respondenten waren afkomstig uit Nederland, 19 uit Denemarken en 17 uit het Verenigd Koninkrijk. Deze respondenten zijn geworven via onze academische en professionele netwerken, met in het bijzonder hulp van academici in Denemarken en het Verenigd Koninkrijk om zicht te krijgen op relevante gesprekspartners en om contacten te faciliteren. We hebben hierbij gestreefd naar een evenwichtige verdeling tussen respondenten werkzaam in de wetenschap en in de praktijk. Van de 54 respondenten werken er 27 als praktijkprofessional, 26 respondenten zijn wetenschapper en één respondent combineert beide rollen. Op basis van de

inzichten uit de interviews en suggesties van respondenten hebben wij openbaar beschikbare voorbeelden verzameld van hybride criminaliteitsvormen of aanpakken gericht op digitale of hybride criminaliteit. Over Nederland hebben we in totaal 23 documenten verzameld, over Denemarken 18 documenten en over het Verenigd Koninkrijk zijn er in totaal 38 documenten verzameld die betrekking hebben op de aard en aanpak van hybride vormen van criminaliteit.

In dit onderzoek hebben we gekozen voor een kwalitatief onderzoeksdesign met een abductieve benadering. Dit houdt in dat het vertrekpunt van ons onderzoek niet louter exploratief of deductief was, maar dat wij tijdens het analyseproces voortdurend hebben geprobeerd onze bevindingen te verbinden met theoretische en empirische inzichten uit eerder onderzoek (Timmermans en Tavory, 2012; Van Hulst en Visser, 2024). In paragraaf 7.3 van dit hoofdstuk wordt nader ingegaan op de resultaten van deze abductieve werkwijze. We beginnen in de volgende paragraaf met de beantwoording van de centrale deelvragen uit dit onderzoek.

7.2 Beantwoording deelvragen

In deze paragraaf worden de deelvragen van het onderzoek beantwoord. Daarbij richten wij ons uitsluitend op de belangrijkste bevindingen per hoofdstuk. De beantwoording van deelvraag 1 volgt in paragraaf 7.2.1 tot en met 7.2.3. Deelvraag 2 zal worden beantwoord in paragraaf 7.2.4. Ten slotte volgt de beantwoording van de derde en laatste deelvraag in paragraaf 7.2.5.

7.2.1 *Financieel gemotiveerde vormen van (cyber)criminaliteit*

In hoofdstuk 2 zijn drie vormen van criminaliteit besproken die kunnen worden geclassificeerd als financieel gemotiveerde (cyber)criminaliteit. Het eerste voorbeeld, aangedragen door respondenten uit Nederland en Denemarken, betreft bankhelpdeskfraude. Binnen het spectrum van cybercriminaliteit vertonen onderdelen van de modus operandi van bankhelpdeskfraude kenmerken van cyber-dependent crimes. Hierbij gaat het onder meer om het hacken om leads te verkrijgen, het gebruik van spoofing om slachtoffers telefonisch te benaderen en het inzetten van remote access tools om toegang te krijgen tot computers van slachtoffers. Een tweede voorbeeld, uitsluitend genoemd door respondenten uit het Verenigd Koninkrijk, betreft de zogenoemde wrench attacks. Hierbij fungeert de mobiele telefoon als sleutel tot het verkrijgen van persoonlijke en in het bijzonder bancaire gegevens. Door een ontgrendelde telefoon te stelen, soms onder dreiging van geweld, kan geld van rekeningen worden overgemaakt of kunnen via applicaties goederen en diensten worden besteld. Daarnaast zijn gevallen genoemd waarin personen op basis van hun socialemediaprofielen, bijvoorbeeld met betrekking tot cryptovaluta, werden geïdentificeerd als potentiële slachtoffers. Het derde voorbeeld betreft geldbezels die een verbindende schakel vormen tussen de eerdergenoemde verschijningsvormen van financieel gemotiveerde (cyber)criminaliteit. Het gaat hierbij om personen die in alle onderzochte landen als kwetsbaar werden

getypeerd en die hun persoonlijke gegevens, bankinformatie of betaalpassen beschikbaar stellen om illegaal verkregen geld wit te wassen. Ook hier is het de menselijke factor die technische handelingen mogelijk maakt. Bovendien blijkt dat de werving van geldezels zowel via fysieke contacten als via socialemediaplatformen plaatsvindt.

7.2.2 *Geweld in een hybride context*

Het thema geweld stond centraal in hoofdstuk 3. Het eerste voorbeeld dat werd besproken betrof conflicten tussen jongeren(groepen) waarin sociale media een centrale rol spelen. Respondenten uit Nederland, Denemarken en het Verenigd Koninkrijk gaven concrete voorbeelden van (dodelijk) geweld dat een online aanloop of escalatie kende. Deze dynamiek blijkt echter complex: conflicten kunnen aanvankelijk op sociale media ontstaan, zich ontwikkelen via digitale interacties en uiteindelijk uitmonden in fysieke confrontaties. Tegelijkertijd zijn er gevallen waarin conflicten offline beginnen, vervolgens worden versterkt door sociale media en opnieuw eindigen in fysieke geweldsincidenten. Daarbij komt het voor dat fysiek geweld wordt gedigitaliseerd doordat foto's en video's van incidenten circuleren als content.

Het tweede voorbeeld betreft geweldsopdrachten onder jongeren, een fenomeen waar Europol (2024) recentelijk aandacht voor heeft gevraagd. Zowel in Nederland als in Duitsland bestaan zorgen over jongeren die betrokken raken bij ernstige vormen van geweld. In Nederland gaat het onder meer om het gebruik van explosieven, terwijl in Denemarken werd gesproken over zogenoemde 'torpedo's': jongeren die vanuit Zweden geweld kwamen plegen in Denemarken. Socialemediaplatformen vervullen hierbij een cruciale functie doordat zij worden ingezet om opdrachten te verspreiden en communicatie richting uitvoering te faciliteren. Soms is voor jongeren duidelijk wat van hen wordt verwacht, terwijl in andere gevallen de aard van de opdracht verhuuld blijft in codetaal en emoji's. Er zijn eveneens voorbeelden van jongeren die actief op zoek gaan naar dergelijke opdrachten (vgl. Bergers et al., 2026).

7.2.3 *Digitale drugsmarkten*

In hoofdstuk 4 stond de laatste onderzochte verschijningsvorm centraal waarin processen van hybridisering een rol spelen: drugsmarkten. Dit domein is van oudsher nauw verbonden met technologie, aanvankelijk via mobiele telefoons en later door online markten op het dark web. Een meer recente ontwikkeling is de opkomst van digitale drugsmarkten op socialemediaplatformen. Op uiteenlopende platformen blijkt sprake van een levendige handel in verdovende middelen. Daarbij is differentiatie van belang (Coomber, 2015): er bestaan duidelijke verschillen tussen drugsmarkten. Niet alleen variëren de soorten en hoeveelheden drugs die per platform worden aangeboden, maar ook de functionaliteit van de platformen leidt tot uiteenlopende typen verkopers en afnemers, bijvoorbeeld op Snapchat en Telegram Messenger. Een tweede specifieke verschijningsvorm binnen dit domein is het fenomeen 'county lines', dat uitsluitend naar voren kwam in de interviews met respondenten uit het Ver-

enigd Koninkrijk. Dit betreft bij uitstek een technologisch verschijnsel, waarbij drugslijnen buiten stedelijke gebieden worden georganiseerd en jongeren via telefoonnummers contact onderhouden met klanten. Ook hier is sprake van een nauwe verwevenheid tussen online en offline processen. Net als bij geldezels en geweldsopdrachten spelen sociale media een rol in de werving en het leggen van contacten. Jongeren worden via digitale kanalen blootgesteld aan bepaalde leefstijlen en verleid om hieraan deel te nemen. Digitale middelen maken bovendien mogelijk dat hun locatie wordt gevolgd.

7.2.4 *Uitdagingen in de aanpak van hybride vormen van criminaliteit in Nederland*

Hoofdstuk 5 gaf een overzicht van enkele uitdagingen in de aanpak van hybride vormen van criminaliteit in Nederland. De interviews gaven zicht op verschillende niveaus waarop in de huidige aanpak deze knelpunten zichtbaar worden. Binnen de politieorganisatie is de afgelopen jaren weliswaar meer aandacht ontstaan voor digitalisering, maar de organisatie als geheel blijkt niet altijd in hetzelfde tempo te zijn meegegroeid met technologische ontwikkelingen. Er bestaan specialistische initiatieven en bottom-uppraktijken om recente fenomenen het hoofd te bieden, maar vaak blijft onduidelijk hoe en waar deze inspanningen structureel zijn ingebed. Dit probleem wordt versterkt wanneer nieuwe vormen van criminaliteit opkomen, waardoor de vraag rijst hoe de organisatie daarop moet reageren en wie binnen de politie verantwoordelijk is voor de aanpak.

Naast organisatorische vraagstukken speelt ook de politiecultuur een belangrijke rol. Enerzijds zijn er specialisten met diepgaande kennis, bijvoorbeeld op het gebied van cybercrime. Deze groep wordt echter vaak overvraagd omdat de bredere organisatie onvoldoende digitaal is meegegaan. Voor veel medewerkers geldt dat zij koudwaterrees ervaren, niet zozeer vanwege de inhoud, maar door onbekendheid met terminologie en digitale werelden. Dit geldt zowel voor basisteams als voor de recherche. Het vraagt om praktische ervaring, gerichte trainingen, aandacht van leidinggevenden en beleid dat inzet op werving en selectie van medewerkers met digitale competenties.

Een derde uitdaging betreft de juridische dimensie. Respondenten signaleren dat wetgeving vaak verouderd is en onvoldoende toegesneden op digitale omstandigheden. Dit leidt tot onduidelijkheden en improvisatie, waarbij de politie en het Openbaar Ministerie soms wachten op rechterlijke uitspraken om richting te krijgen. Het recente *Landeck*-arrest illustreert hoe jurisprudentie sturend kan zijn in het digitale domein en nieuwe uitdagingen oproept voor opsporing en bewijsvoering (ECLI:NL:HR:2025:409). Respondenten spraken in deze context over een gereedschapskist vol oude instrumenten, terwijl nieuwe tools dringend nodig zijn.¹⁶

16 Hierbij dient te worden opgemerkt dat het nieuwe Wetboek van Strafvordering momenteel in voorbereiding is en naar verwachting op 1 april 2029 in werking treedt, waarmee aan een aantal van de gesignaleerde juridische uitdagingen tegemoet wordt gekomen.

Ten slotte kwam de rol van technologiebedrijven aan bod. Hoewel positieve ervaringen zijn gedeeld, werden ook aanzienlijke uitdagingen genoemd. De mate van medewerking verschilt per platform: Snapchat wordt gezien als relatief coöperatief, terwijl Telegram lange tijd nadrukkelijk de anonimiteit van gebruikers boven samenwerking stelde. Recente ontwikkelingen, zoals de arrestatie van de oprichter van Telegram, lijken hierin verandering te brengen, maar leiden vooral tot een verplaatsing van activiteiten naar gesloten groepen.

7.2.5 *Voorbeelden van de aanpak van hybride vormen van criminaliteit*

In hoofdstuk 6 zijn drie projecten beschreven die door respondenten in de respectieve landen zijn aangedragen als positieve voorbeelden in de aanpak van hybride criminaliteit. Elk van deze initiatieven laat zien hoe politiewerk met een digitale component in verschillende nationale contexten vorm krijgt. In Denemarken richt de Politie's Online Patroelje (POP) zich primair op preventie en op de zichtbare online aanwezigheid van de politie en individuele agenten. In het Verenigd Koninkrijk staat bij Project Alpha een meer heimelijke vorm van online politiewerk centraal, gericht op het leggen van verbanden tussen digitale uitingen en geweldscriminaliteit in de fysieke wereld. Operatie Centurion, het Nederlandse voorbeeld, vertegenwoordigt ten slotte een strategische en organisatorische omslag in de aanpak van bepaalde gedigitaliseerde vormen van criminaliteit.

7.3 *Synthese*

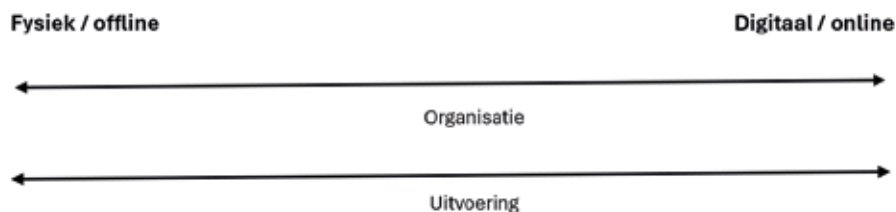
In deze paragraaf formuleren we een antwoord op de centrale onderzoeksvraag op basis van een synthese van de wetenschappelijke literatuur, de inzichten uit de interviews en de concrete voorbeelden uit de openbare bronnen. We beginnen in paragraaf 7.3.1 met het presenteren van een hybridiseringscontinuüm op basis van de kernbevindingen ten aanzien van de aard van hybride vormen van criminaliteit. Deze centrale thema's bieden een overkoepelende samenvatting van de belangrijkste inzichten van dit onderzoek en vormen de opmaat tot de meer theoretische duiding van de onderzoeksresultaten in paragraaf 7.3.2.

7.3.1 *Kernbevindingen: een hybridiseringscontinuüm*

In de criminologische literatuur wordt de aanduiding 'hybride' in toenemende mate gebruikt om te verwijzen naar processen waarin sprake is van een verwevenheid tussen online en offline, het fysieke en het digitale, of de mens en de techniek. Wanneer we kijken naar de bestaande wetenschappelijke literatuur waarin hybride concepten worden gebruikt, blijkt dat het proces van hybridisering betrekking kan hebben op verschillende aspecten van criminaliteit. Di Nicola (2022) wijst bijvoorbeeld op criminele samenwerkingsverbanden die bestaan uit actoren én uit niet-menselijke entiteiten ('actanten') zoals machines (Latour, 2005) met uiteenlopende technische vaardighe-

den. Individuen met specialistische digitale kennis werken daarbij samen met personen zonder dergelijke expertise. Deze samenwerkingsverbanden kunnen hun oorsprong hebben in de fysieke wereld, maar kunnen ook online zijn ontstaan (vgl. Leukfeldt et al., 2017a, 2017b, 2017c). In dergelijke gevallen spreken we van hybride criminele samenwerkingsverbanden, oftewel van processen van hybridisering in de organisatie van criminaliteit.

Hoewel deze ontwikkelingen ook in dit onderzoek worden gesignaleerd, geeft deze studie vooral zicht op een verandering in de modus operandi van de drie verschijningsvormen die centraal hebben gestaan: financieel gemotiveerde (cyber)criminaliteit, geweld en de handel in verdovende middelen. In deze verschijningsvormen zien we dat op verschillende manieren sprake is van verwevenheid tussen menselijk handelen en technologische middelen. Afhankelijk van de specifieke vorm van criminaliteit is deze verwevenheid anders van aard. Bovendien verschilt de mate waarin technologie de dynamiek van delicten beïnvloedt per verschijningsvorm, maar ook per handeling binnen de modus operandi van de specifieke verschijningsvorm. Meer in het algemeen dienen deze processen van hybridisering begrepen te worden als een continuüm: een schaal waarop criminaliteitsvormen variëren in de mate waarin fysieke en digitale elementen met elkaar verweven zijn. Dit hybridiseringscontinuüm, visueel weergegeven in figuur 1, breekt allereerst met de klassieke binaire oppositie van fysiek versus digitaal of online versus offline. De drie centrale verschijningsvormen, te weten financieel gemotiveerde (cyber)criminaliteit, geweld en de handel in verdovende middelen, kennen wat betreft de modus operandi – opgedeeld naar de organisatie en de uitvoering van het delict – een ander vertrekpunt op het hybridiseringscontinuüm: geweld bevindt zich meer aan de linkerkant, de handel in verdovende middel neemt meer een middenpositie in en financieel gemotiveerde (cyber)criminaliteit kan meer aan de rechterzijde van het continuüm worden geplaatst. We maken binnen de modus operandi een onderscheid tussen de organisatie en de uitvoering van de specifieke verschijningsvorm, omdat de respectievelijke plek op het continuüm hierbij per verschijningsvorm niet per definitie hetzelfde hoeft te zijn.



Figuur 1 Hybridiseringscontinuüm

Dit onderzoek maakt inzichtelijk dat aspecten van de modus operandi van deze criminaliteitsvormen onder invloed van processen van digitalisering bewegen op het hybridiseringscontinuüm. Er zijn, aan de ene kant van het continuüm, aspecten van de door ons beschreven verschijningsvormen die voor wat betreft de uitvoering nog steeds sterk leunen op fysieke handelingen. Hierbij valt te denken aan geweld, zowel tussen

jongeren als in de vorm van geweldsopdrachten, maar ook aan het ophalen van bankpassen en het fysiek pinnen van geld in het geval van financieel gemotiveerde (cyber) criminaliteit en de fysieke transactie bij verdovende middelen. Ook de uitvoering van de zogenoemde wrench-attacks bevindt zich aan deze kant van het continuüm. Wat betreft de organisatie van deze verschijningsvormen valt aan de fysieke/offline-kant te denken aan het gebruik van sociale relaties uit de buurt of het bredere netwerk voor het vinden van mededaders of gemotiveerde uitvoerders. Aan de meer digitale kant van het continuüm staan voorbeelden waarin (digitale) technologie een grotere rol speelt in de uitvoering, zoals het hacken voor leads, het gebruik van remote access tools en spoofingtechnieken in het geval van financieel gemotiveerde (cyber)criminaliteit. Voor de organisatie van deze verschijningsvormen zien we aan de rechterzijde van de figuur bijvoorbeeld het online adverteren van verdovende middelen op digitale drugsmarkten of de zoektocht naar uitvoerders via socialemediaplatformen in de context van witwassen (geldezels), geweldsopdrachten en het dealen van drugs (county lines) of geweldsopdrachten.

Het hybridiseringscontinuüm vormt de basis voor het belichten van een tweetal kernbevindingen waarmee de herconfiguratie van de dynamiek van de drie criminaliteitsvormen nader kan worden toegelicht. Het gaat hier om twee simultane bewegingen: aan de ene kant zien we binnen de door ons onderzochte verschijningsvormen ontwikkelingen binnen de modus operandi die we kunnen typeren als *digitalisering* en die zich bewegen richting de rechterzijde van het hybridiseringscontinuüm. Aan de andere kant zien we tegelijkertijd ook processen van wat we materialisering noemen en waarbij we bestendinging of ontwikkeling van het digitale naar het fysieke en het lokale zien.

Digitalisering: nieuwe mogelijkheden en schaalvergroting

De voorbeelden van geweld tussen groepen jongeren en de handel in verdovende middelen laten zien dat de uitvoering van deze traditionele vormen van criminaliteit onder invloed van digitale technologie niet langer beperkt blijft tot de fysieke wereld. Ook het vinden van mededaders of uitvoerders van criminele activiteiten verliep lange tijd voornamelijk via offline contacten en interacties. In die zin kunnen we spreken van een digitalisering van de criminaliteitsvormen die in dit onderzoek centraal staan. Digitale technologie biedt nieuwe mogelijkheden, met name voor het vinden van geschikte mededaders. Dit sluit aan bij eerder onderzoek naar het ontstaan en de ontwikkeling van cybercriminele netwerken (Leukfeldt et al., 2017a, 2017b, 2017c) en komt in dit onderzoek onder meer terug bij bankhelpdeskfraude en geldezels. Deze studie wijst echter vooral op de rol van sociale media bij het vinden van uitvoerders van meer klassieke, offline criminele activiteiten, zoals geweldsopdrachten en de handel in verdovende middelen. Net als bij cybercriminaliteit fungeren socialemediaplatformen in deze context als een 'digital offender convergence setting' (vgl. Bekkers, 2025; Roks en Monshouwer, 2020; Soudijn en Zegers, 2012): op verschillende platformen worden criminele klussen uitgezet – soms breed en algemeen als advertentie, soms gericht op specifieke personen (vgl. Bergers et al., 2026) – terwijl potentiële uitvoerders actief

zoeken naar manieren om snel geld te verdienen. Via sociale media kan relatief eenvoudig een grote, potentieel geïnteresseerde groep uitvoerders worden bereikt. Tegelijkertijd bieden dezelfde kanalen mogelijkheden voor mededaders en uitvoerders om hun motivatie en diensten kenbaar te maken.

Hiermee raken we aan een centraal punt: technologische ontwikkelingen, en momenteel in het bijzonder socialemediaplatformen, faciliteren een schaalvergroting van criminele verschijningsvormen (McGuire, 2007; 2026). Dit zien we bijvoorbeeld bij de handel in verdovende middelen, waar technologie leidt tot een toename van het aantal potentiële klanten en daarmee tot een grotere afzetmarkt (vgl. Bakken en Demant, 2019; Moyle et al., 2019; Roks en Hendriksen, 2021). Het wordt eveneens zichtbaar in de manier waarop via sociale media wordt gezocht naar geldezels, uitvoerders van geweldsopdrachten of andere uitvoerders: het potentiële bereik is groter wanneer gebruik wordt gemaakt van populaire platformen zoals Snapchat. Daarbij wordt nadrukkelijk gebruikgemaakt van specifieke functionaliteiten van platformen, zoals grote thematische groepen op Telegram of de 'snel toevoegen'-functie op Snapchat (Bergers et al., 2026), die het eenvoudig maken om snel een groot publiek te bereiken en online (afgeschermd) te communiceren. Bovendien helpen algoritmes om content verder te verspreiden en zichtbaar te maken (vgl. Aagesen en Demant, 2025).

Dit onderzoek bevestigt daarmee dat de voortschrijdende digitalisering nieuwe mogelijkheden met zich meebrengt voor criminaliteit. In de huidige studie wordt duidelijk dat, hoewel in de hoofdstukken 2 tot en met 4 afzonderlijke thema's worden besproken, dezelfde personen en groepen zich met uiteenlopende vormen van criminaliteit bezighouden. Er is daarbij niet zozeer sprake van specialisatie, maar eerder van wat in de wetenschappelijke literatuur wordt aangeduid als 'cafeteria style offending' (Klein, 1995; Leukfeldt en Holt, 2022; Bekkers, Loggen, Keja, Bijmans en Leukfeldt, 2025). De spreekwoordelijke 'menukaart' van mogelijke criminele activiteiten om geld mee te verdienen is uitgebreid als gevolg van de voortschrijdende digitalisering, waardoor er zich meer en andere mogelijkheden voordoen om geld te verdienen. Voor jeugdgroepen of gangs, maar eveneens in de bredere context van de straatcultuur, kan dit resulteren in een zekere digitale diversificatie van activiteiten, waaronder vormen van online fraude en oplichting – ook wel 'F-game' (Roks en Monshouwer, 2020; Bekkers, 2025) – naast meer traditionele vormen van straatcriminaliteit zoals de handel in verdovende middelen (Leukfeldt en Roks, 2020; Loggen et al., 2026; Roks et al., 2021).

Materialisering: lokale inbedding en de-digitalisering

Te midden van processen van digitalisering zien we ook een beweging die kan worden getypeerd als materialisering. In de digitale antropologie, waar we het gebruik van de term materialisering aan ontlenen (Horst en Miller, 2020; Pink, Ardèvol en Lanzeni, 2020), wordt materialiteit ('*materiality*') gebruikt om de nadruk niet alleen op het digitale te leggen, maar ook op de fysieke, technische en materiële voorwaarden die online gedragingen mogelijk maken. Horst en Miller (2020: 25) beschouwen het materiële om die reden als het fundament van de digitale antropologie. In dit onderzoek zien we eveneens het (blijvende) belang van het materiële. In deze studie heeft de nadruk daar-

bij niet zozeer gelegen op fysieke apparaten – computers en mobiele telefoons – en fysieke infrastructures zoals datacenters en netwerk-hardware achter socialemediaplatformen die digitale technologie mogelijk maken (vgl. Horst en Miller, 2012). Onze bevindingen wijzen met name op een tweetal andere voorbeelden van materialisering. Allereerst zien we dat, parallel aan de schaalvergroting die digitale technologie mogelijk maakt, de drie centrale criminaliteitsvormen in dit onderzoek nog steeds een sterke lokale component kennen. Dit geldt zowel voor de handel in verdovende middelen, die doorgaans afgebakend blijft binnen een lokale context, als voor de zoektocht naar uitvoerders. Hoewel er voorbeelden zijn van jongeren die uit andere regio's worden betrokken, benadrukken respondenten dat lokale inbedding en bestaande sociale netwerken – zoals binnen families, buurten, op school en op straat – nog steeds een belangrijke rol spelen in het vinden van mededaders en uitvoerders (vgl. Bergers et al., 2026; Kruisbergen et al., 2019; Leukfeldt et al., 2020; Roks en Ter Weijden, 2026). Deze bevinding wijst, met andere woorden, op het blijvende belang van de lokale, fysieke context voor hybride vormen van criminaliteit.

Materialisering zien we daarnaast terug binnen criminele verschijningsvormen die al een technologische of digitale component bevatten, zoals bij vormen van financieel gemotiveerde (cyber)criminaliteit. De eerste Nederlandse studies op dit terrein lieten zien dat phishing en banking malware primair waren gericht op het digitale betalingsverkeer, met als doel het legen van online bankrekeningen (Leukfeldt, 2015; Leukfeldt et al., 2017a, 2017b, 2017c). Een latere analyse door Loggen en Leukfeldt (2022) liet echter zien dat de modus operandi van phishing veranderde. Malware werd minder ingezet omdat banken dergelijke aanvallen sneller detecteren en blokkeren. Bovendien zijn digitale beveiligingsmaatregelen verbeterd: banken monitoren betalingsverkeer intensiever en spamfilters houden phishingberichten effectiever tegen. Hierdoor is de kans op succesvolle benadering van slachtoffers via deze technische wegen afgenomen, waardoor er volgens Loggen en Leukfeldt (2022) werd teruggevallen op alternatieve en meer klassieke methoden, zoals de telefonische benadering van slachtoffers.

Het bovenstaande vormt een illustratief voorbeeld van de constatering van Loggen en Leukfeldt (2022) dat voortschrijdende digitalisering niet noodzakelijk leidt tot steeds meer technische handelingen. Integendeel: in sommige gevallen worden criminele activiteiten juist minder technologisch van aard. Deze adaptatie wijst met andere woorden op een zekere mate van *de-digitalisering*. In dit onderzoek werd dat zichtbaar bij bankhelpdeskfraude. In plaats van de inzet van complexe technologie bellen daders met slachtoffers of gaan ze fysiek langs, al dan niet vermomd als nepagent. Ook de wrench attacks zijn te beschouwen als een voorbeeld van de-digitalisering. In plaats van technologie om de beveiliging van mobiele telefoons te slechten, wordt teruggevallen op afleiding, misleiding of fysieke dwang of dreiging om de telefoon letterlijk in handen te krijgen. Dit zou voor een deel ook het gevolg kunnen zijn van het ontbreken van bepaalde technologische kennis. Hoewel vervolgens vaak wél technologische handelingen worden verricht, zoals het wijzigen van gebruikersinstellingen om toegang te verkrijgen tot bancaire gegevens of andere applicaties, is de kern van een wrench attack fysiek.

Deze processen van materialisering maken inzichtelijk dat de *modus operandi* van criminaliteitsvormen niet per definitie een incrementele digitaliseringslijn op het hybridiseringcontinuüm hoeven te volgen. Het is goed denkbaar dat daders bewust gebruikmaken van of terugvallen op meer klassieke, minder technische methoden in zowel de organisatie als de uitvoering, juist omdat deze minder risico's met zich meebrengen, bijvoorbeeld doordat er minder digitale sporen worden achtergelaten in een context waarin opsparing steeds verder digitaliseert.

7.3.2 *Nieuwe concepten: technologie-gefaciliteerde en platform-gefaciliteerde criminaliteit*

In hoofdstuk 1 van dit rapport constateerden wij dat de gehanteerde termen om te verwijzen naar de impact van (digitale) technologie op criminaliteit veelal tekortschieten. Begrippen als *cyber*, gedigitaliseerd en online criminaliteit roepen beelden op van fenomenen die volledig digitaal zijn. Deze drie concepten kunnen worden beschouwd als uitingen van wat Lupton (2015) het cybertijdperk noemt, met nadruk op digitale technologieën en infrastructuur. Voor bepaalde verschijningsvormen heeft de term cybercriminaliteit in het bijzonder waarde binnen het onderzoeksveld van cybercriminaliteit binnen de criminologie. Dergelijke termen doen echter onvoldoende recht aan fenomenen waarin sprake is van een wisselwerking tussen fysiek en digitaal, en tussen online en offline. Het betreft hier, zoals ook in de inleiding werd betoogd, niet slechts een semantische discussie of een academisch streven om onderscheidend te zijn. Wezenlijker is het, in lijn met oproepen van Floridi (2015) en Mitchell en collega's (2025), dat de gehanteerde taal een adequate typering geeft van de fenomenen die wij waarnemen. Waar in het cyber-tijdperk lange tijd termen werden gehanteerd die daaraan verbonden waren, vraagt de huidige hybride context om socio-technische concepten om voorbij binaire opposities te denken. Dit is bovendien van wezenlijk belang voor de aanpak van deze vormen van criminaliteit, zoals we in de volgende paragraaf nader zullen toelichten.

Tegen deze achtergrond hebben we in dit onderzoek gebruikgemaakt van de term hybride. Een hybride lens kan behulpzaam zijn om te kijken naar de gevolgen van de voortschrijdende digitalisering op criminaliteit, maar vraagt ook om terughoudendheid: wanneer elke vorm van verwevenheid of versmelting tussen technologie – of in engere zin sociale media – en criminaliteit als hybridisering wordt bestempeld, dreigt de analytische (meer)waarde van het begrip verloren te gaan. Het is van belang te beschikken over een taal en terminologie die recht doet aan wat empirisch wordt waargenomen. In het restant van deze paragraaf bespreken we een tweetal concepten die naar ons idee recht doen aan de specifieke rol van technologie in relatie tot criminele activiteiten: technologie-gefaciliteerde criminaliteit en platform-gefaciliteerde criminaliteit.

Technologie-gefaciliteerde criminaliteit (en geweld)

In hoofdstuk 1 hebben we het concept 'technology-facilitated violence' besproken (Mitchell et al., 2025). Deze term wordt in de wetenschappelijk literatuur veelal ge-

bruikt om te verwijzen naar interpersoonlijke vormen van geweld, maar is ook voor het bredere onderwerp van deze studie van waarde. Het gaat hierbij immers om een bepaalde manier van kijken naar (digitale)¹⁷ technologie: niet slechts als neutraal medium, maar als actor die op uiteenlopende wijzen een actieve rol speelt in het geweld. Deze studie laat zien dat het idee van ‘technologie-gefaciliteerd’ relevant is voor meer dan alleen geweld, zoals ook al eerder betoogd door Demant en Bakken (2019) in de context van de handel in verdovende middelen via sociale media. De verschijningsvormen in dit onderzoek kunnen worden geschaard onder de brede noemer van *technology-facilitated crime*. Anders dan de brede aanduiding *cybercriminaliteit*, of varianten als *cyber-dependent*, *cyber-enabled* of *cyber-assisted crimes*, positioneert dit concept technologie niet slechts als object of hulpmiddel, maar nadrukkelijk als actor binnen socio-technische constellaties.

Diverse voorbeelden in dit rapport kunnen worden beschouwd als uitingen van technologie-gefaciliteerde criminaliteit. Zo wordt in de context van bankhelpdeskfraude veelal gewezen op het belang van social engineering. Dit benadrukt de socio-technische uitvoering van uiteenlopende handelingen: de mens staat centraal en benut (digitale) technologie om slachtoffers of uitvoerders te overtuigen, te misleiden of te werven. Soms betreft dit meer hightech verschijningsvormen die binnen het spectrum van cybercriminaliteit als *cyber-dependent crimes* worden geplaatst, zoals hacken om leads te verkrijgen, spoofing om slachtoffers te bellen, of het gebruik van remote access tools om toegang te krijgen tot computers van slachtoffers. Daarnaast zijn er ook onderdelen die niet of nauwelijks technisch van aard zijn, zoals het bellen van slachtoffers, het ophalen van bankpassen of het laten pinnen door geldezels. Dat geldt ook voor wrench attacks, waarbij een telefoon wordt gestolen door afleiding of onder dreiging van geweld. Het zijn allemaal manieren waarop de mens omgaat met de technologische beveiliging van telefoons om toegang te verkrijgen tot bancaire of andersoortige relevante gegevens of applicaties. Kortom, de voorbeelden in hoofdstuk 2 laten zien dat de uitvoering berust op een voortdurende interactie tussen mens en (digitale) technologie, oftewel om technologie-gefaciliteerde criminaliteit.

De meer specifieke term technologie-gefaciliteerd geweld is relevant om conflicten tussen groepen jongeren te duiden, zoals in hoofdstuk 3. Mehlbaum en collega's (2024) spreken in dit verband van *hybride straatgeweld*. Hoewel de hybride lens hier bij uitstek van toepassing lijkt, kan zij ook vertroebelen werken. Het geweld waarover Mehlbaum en collega's (2024) schrijven, evenals de voorbeelden in hoofdstuk 3, betreft immers fysiek geweld: het gaat om slaan, steken, en in sommige gevallen het gebruik van vuurwapens. Ontegenzeggelijk kan de digitale content opgevat worden als, om met Schinkel (2010) te spreken, een aspect van geweld, maar de aanduiding hybride straatgeweld lijkt vooral te blijven verwijzen naar fysieke geweldsuitingen. Wanneer we kijken naar de voorbeelden in hoofdstuk 3, zien we vooral dat er in de keten van gebeur-

17 Mitchell en collega's (2025) bekritiseren dat technologie tegenwoordig vooral wordt opgevat als digitale technologie en roepen op tot een bredere blik op technologische ontwikkelingen, waaronder ook kunstmatige intelligentie, om recht te kunnen blijven doen aan toekomstige iteraties van *technology-facilitated crimes*.

tenissen rondom fysiek geweld sprake is processen van hybridisering. Het geweld zelf is echter niet hybride, maar onverminderd fysiek. Hier is eerder sprake van technology-facilitated violence, omdat digitale technologie en sociale media in het bijzonder de zichtbaarheid en verspreiding vergroten, het voor een breder publiek toegankelijk maken en door archivering het gewelddadige potentieel laten voortbestaan (boyd, 2014; Roks en Van den Broek, 2021; 2023).

Platform-gefaciliteerde criminaliteit

Voor het merendeel van de verschijningsvormen in dit onderzoek kunnen sociale media worden gezien als de specificatie van de bredere term technologie. We raken daarbij aan een ander begrip dat in hoofdstuk 1 werd geïntroduceerd: platform-enabled crimes (Hamilton, 2021) of platform criminality (McGuire, 2026). Diverse voorbeelden uit dit onderzoek maken inzichtelijk dat socialemediaplatformen door hun handelen faciliterend werken voor bepaalde vormen van criminaliteit, in het bijzonder rondom de organisatie en uitvoering van deze activiteiten. Sociale media maken het mogelijk dat op grotere schaal geschikte uitvoerders of mededaders kunnen worden gevonden en dat hiermee kan worden gecommuniceerd. Dit zien we bij de geldezels uit hoofdstuk 2, bij uitvoerders van geweldsopdrachten uit hoofdstuk 3, en in hoofdstuk 4 bij jongeren die betrokken raken bij county lines-dealen van verdovende middelen in het Verenigd Koninkrijk en meer in het algemeen bij digitale drugsmarkten. Vanuit het perspectief van personen die op zoek zijn naar uitvoerders – in het dagelijks taalgebruik ook wel aangeduid als ronselaars – vervullen platformen een faciliterende functie.

We zien hierbij, analoog aan wat Coomber (2015) beschrijft in de context van drugsmarkten, een zekere differentiatie als het gaat om socialemediaplatformen: verschillende platformen hebben uiteenlopende functionaliteiten en gebruiksvormen. Zo is Snapchat populair vanwege de mogelijkheid om snel mensen in of rondom dezelfde locatie toe te voegen, berichten te sturen en gebruik te maken van zelfvernietigende functies bij het plaatsen van digitale content. Telegram biedt een zekere mate van encryptie en groepen waarin lange tijd zonder veel moderatie allerlei vormen van criminele handel konden plaatsvinden. Bovendien werd Telegram lange tijd geroemd door de beperkte samenwerking met autoriteiten. Meer in het algemeen spelen algoritmen hierbij een belangrijke faciliterende rol: wanneer gebruikers eenmaal worden blootgesteld aan bepaalde content, worden zij frequenter geconfronteerd met criminogene inhoud (Aagesen en Demant, 2025).

Naast deze faciliterende rol is er ook sprake van een zeker nalaten door socialemediaplatformen. Posts op sociale media waarin wordt gezocht naar geldezels, uitvoerders van geweld of klanten voor verdovende middelen op Snapchat en Telegram zijn in strijd met de richtlijnen van platformen. Toch vindt er slechts in beperkte mate moderatie plaats van deze content op de delen van platformen die toegankelijk zijn voor iedereen met een account en internetverbinding. In directe berichten of groepschats lijkt in het geheel geen sprake van moderatie. Ook leeftijdsgrenzen worden vaak niet gehandhaafd. Met andere woorden: techbedrijven laten na om de regels die van kracht

zijn op hun platformen ook daadwerkelijk te handhaven. In combinatie met de functionaliteiten en werking van de algoritmes maakt dit dat het concept platform-gefaciliteerde criminaliteit relevant is als aanduiding voor een deel van de hybride verschijningsvormen in dit onderzoek.

7.4 **Implicaties: reflecties en aanbevelingen**

In de synthese in de vorige paragraaf lag het zwaartepunt op de aard van de hybride vormen van criminaliteit, oftewel op de fenomeenkant van dit onderzoek. Een onvermijdelijke vervolgvraag is wat deze bevindingen betekenen voor de praktijk. Allereerst dient opgemerkt te worden dat het hier gaat om een breder maatschappelijk vraagstuk in de aanpak van criminaliteit (zie o.a. Van den Broek en Roks, 2022; Van den Broek en Jhanjan, 2024; De Jong et al., 2026). In dit onderzoek richten we ons echter in het bijzonder op de implicaties voor de aanpak van hybride criminaliteit in de politiepraktijk. In paragraaf 7.4.1 delen we enkele reflecties op de huidige aanpak en de digitale transformatie binnen de politie in het bijzonder. Deze reflecties bouwen voort op de hybride verschijningsvormen die in dit onderzoek zijn geïdentificeerd, maar ook op de uitdagingen die in de huidige praktijk zichtbaar zijn geworden en op de voorbeelden van aanpakken van hybride vormen van criminaliteit in de landen in onze selectie. In de daaropvolgende paragraaf formuleren we vervolgens meer concrete aanbevelingen voor de aanpak van hybride vormen van criminaliteit door de politie.

7.4.1 ***Reflectie op de aanpak van hybride vormen van criminaliteit***

Dit onderzoek bevestigt allereerst dat de digitalisering binnen de politie de afgelopen jaren meer aandacht heeft gekregen (Landman en Groothuis, 2022; Landman, 2023; Stol et al., 2025; Van Steden et al., 2025). Dat is positief, iets dat evenzeer geldt voor het feit dat het thema digitalisering is aangemerkt als een van de drie centrale thema's in de strategische agenda van de politie (Politie, 2025). Wanneer we kijken naar de ontwikkelingen in dit rapport, dan ontstaat echter ook het gevoel dat de politieorganisatie als geheel moeite heeft om gelijke tred te houden met de snelheid waarmee de digitalisering zich voltrekt. Dit is niet uniek voor Nederland: de voorbeelden die in dit rapport worden genoemd, leveren interessante inzichten en lessen op, maar vormen geen pasklare oplossing voor de meer fundamentele vragen die de aanpak van hybride vormen van criminaliteit voor de politie oproept. Ook in Denemarken en het Verenigd Koninkrijk zien we namelijk vergelijkbare uitdagingen in wat hybridisering van de politie vraagt.

Wanneer we kijken naar hoe digitalisering het politiewerk raakt, lag het accent de afgelopen jaren veelal op cyber, en krijgen in de slipstream daarvan inmiddels ook gedigitaliseerde delicten in toenemende mate aandacht. Alhoewel dit in de digitale transformatie van de politie beschouwd kan worden als een goed startpunt, en hieruit zeker waardevolle lessen zijn te trekken, maken de verschijningsvormen in deze studie eveneens duidelijk dat de huidige focus van de politie als het gaat om de voortschrijdende

digitalisering te beperkt is. Bovendien zijn er buiten onze beperkte selectie van thema's nog veel meer fenomenen die de kern van dit onderzoek raken, waaronder radicalisering, extremisme en zedendelicten (zie bijvoorbeeld Gaudette et al., 2022; Stoeldraaijers et al., 2024). Dit roept nadrukkelijk de vraag op of de huidige aandacht voor en inzet op de digitale transformatie voldoende is om de inhaalslag te maken die in de volle breedte van de politieorganisatie nodig is.

De uitgesproken ambities van de politie op dit vlak zijn groot. In de strategische agenda is het doel gesteld om in 2030 een toonaangevend voorbeeld te zijn van een organisatie die een goed evenwicht weet te vinden tussen mens en technologie. Aan de ene kant is het positief dat hiermee, wellicht meer impliciet, wordt voorbijgegaan aan het binaire denken over mens en technologie. Aan de andere kant is het, afgaande op wat in dit onderzoek is gesignaleerd en breder in recente studies die raken aan het thema van deze studie (Landman en Groothuis, 2022; Landman, 2023; Stol et al., 2025; Van Steden et al., 2025), een bijzonder grote opgave. Het is daarbij zelfs de vraag of dit wel een realistische doelstelling is: het vraagt immers om de ontwikkeling van digitale vaardigheden en het bevorderen van een digitale cultuur binnen de politie op een manier waarbij de digitale transformatie niet wordt gezien als een taak die naast het bestaande werk komt, maar als een fundamenteel onderdeel van het politiewerk. Hoewel er de afgelopen jaren stappen zijn gezet op dit vlak, laten de resultaten van dit onderzoek ook zien dat digitalisering nog steeds wordt benaderd als een specialistisch domein en (nog) niet als een integraal onderdeel van het politiewerk.

Een fundamentele digitale transformatie vraagt bovendien om een meer drastische hervorming binnen de bredere politiecultuur. Archaïsche opvattingen waarin digitale expertise wordt gezien als een niche of als het domein van enkele specialisten, hebben een vertragend effect op de digitale transformatie. Het doorbreken hiervan is cruciaal om te voorkomen dat specialisten binnen de politie voortdurend overvraagd worden en andere onderdelen van de organisatie onvoldoende digitaal meebewegen. Hier ligt een taak voor leidinggevendenden om voorbeeldgedrag te tonen, maar het is ook nadrukkelijk een opgave bij de werving en selectie van nieuw personeel dat – om de doelstellingen te halen – zou moeten beschikken over digitale competenties en affiniteit met (digitale) technologie.

Daarnaast vraagt digitale transformatie om blijvende en structurele investeringen in training, coaching en ondersteuning van alle politiemedewerkers op het thema digitalisering en bij voorkeur ook op het thema hybridisering. Digitale vaardigheden mogen niet incidenteel worden aangeboden (vgl. Brynjolfsson en McAfee, 2014), maar moeten – zeker voor politiefunctionarissen met minder kennis, ervaring of interesse in technologie – ingebed zijn in loopbaanontwikkeling en voortdurend worden bijgewerkt. Dit betekent dat tijd en middelen expliciet moeten worden vrijgemaakt voor digitale bijscholing en innovatie. Dit kan in de vorm van e-learningmodules en online platformen, waardoor medewerkers flexibel en laagdrempelig toegang hebben tot training en expertise. Dit vereist ook een andere manier van nadenken over digitale technologie. Het is niet de ambitie dat alle medewerkers specialist worden of specialistische kennis ontwikkelen, maar wel dat binnen de bredere politieorganisatie een basisoniveau

van digitale geletterdheid en digitale fitheid aanwezig is. Het is de vraag of dit rond het jaar 2030 daadwerkelijk te realiseren valt.

Opvallend is dat een aanzienlijk deel van de in deze reflectie benoemde punten ook in andere onderzoeken naar voren is gekomen. Dit roept de vraag op waarom het, ondanks deze eerdere constatering, niet is gelukt deze vraagstukken afdoende te adresseren. De huidige onderzoeksopzet leent zich niet voor een beantwoording van deze vraag. Vervolgonderzoek zou daarom expliciet aandacht moeten besteden aan de onderliggende factoren die maken dat dergelijke knelpunten blijven bestaan. Meer inzicht in de wijze waarop juridische, organisatorische en operationele omstandigheden de politiepraktijk beïnvloeden, kan bijdragen aan een beter begrip van de uitdagingen die samenhangen met de digitale transformatie van het politiewerk.

7.4.2 *Aanbevelingen*

We besluiten deze paragraaf over de aanpak van hybride vormen met een tweetal aanbevelingen voor de politiepraktijk die voortvloeien uit enerzijds de gesignaleerde uitdagingen in Nederland en anderzijds de voorbeelden uit Denemarken en het Verenigd Koninkrijk.

Van bestraffen naar verstoren

Een belangrijke les uit de voorbeelden uit Denemarken en het Verenigd Koninkrijk is dat klassieke vormen van politiewerk in de digitale context vaak moeilijk uitvoerbaar zijn. De enorme hoeveelheid content, de complexiteit van het achterhalen van verantwoordelijken en de hoge eisen aan bewijsvoering maken opsporing, vervolging en veroordeling complex. De aanbeveling is om voor een deel van de thema's in dit onderzoek, bijvoorbeeld waar het gaat om digitale advertenties gericht op jongeren voor criminele klussen, drugsmarkten op sociale media en content met risico op gewelddadige conflicten, een andersoortige manier van werken te prioriteren. Hoewel opsporing en vervolging noodzakelijk blijven waar dit haalbaar is, lijkt het beperken van schade en het verstoren van activiteiten met een online component een effectiever en realistischer alternatief. Te denken valt aan het snel offline halen van accounts of groepen en het op grotere schaal verwijderen van schadelijke online content, waarbij de werkwijzen van de Deense Politie Online Patroelje (POP) en Project Alpha uit het Verenigd Koninkrijk als voorbeeld kunnen fungeren. In de context van de bestrijding van terroristische online content is dit al iets dat op EU-niveau plaatsvindt.¹⁸ Een dergelijke aanpak vraagt om nauwe samenwerking met technologiebedrijven die de infrastructuur beheren waarop criminele activiteiten plaatsvinden. Alleen door structurele afspraken over data-uitwisseling, prioritering van verzoeken en gezamenlijke interventies kan verstoring effectief worden ingezet. Wezenlijk daarvoor is echter de samen-

18 <https://www.consilium.europa.eu/en/infographics/terrorist-content-online/>, laatst bezocht op dinsdag 19 mei 2026.

werking met platformen, iets dat gezien kan worden als een cruciaal onderdeel van de aanpak van hybride vormen van criminaliteit.

Samenwerking met platformen

In de wetenschappelijke literatuur worden technologiebedrijven vaak omschreven als cloud empires (Lehdonvirta, 2022): entiteiten die beschikken over een macht die in veel opzichten groter is dan die van nationale overheden. Dit geldt ook in de context van criminaliteit: politie en justitie zijn in hoge mate afhankelijk van de infrastructuur en data die door deze bedrijven worden beheerd. Een belangrijke uitdaging is dat de snelheid waarmee de politie toegang nodig heeft tot data om tot vervolging en bewijsvoering te komen, niet altijd overeenkomt met de snelheid waarmee platformen bereid of in staat zijn deze informatie te delen. Er bestaan echter, zo maakt dit onderzoek eveneens duidelijk, ook positieve voorbeelden. In sommige gevallen is er via een single point of contact direct en effectief overleg tussen politie en een sociaalmediumplatform, waardoor samenwerking mogelijk wordt gemaakt en content sneller kan worden verwijderd. Dit laat zien dat nauwe samenwerking niet alleen wenselijk, maar ook haalbaar is, mits er voldoende menskracht binnen de politie beschikbaar wordt gesteld om deze relaties te onderhouden.

Daarnaast speelt de vraag naar contentmoderatie door de platformen zelf. Hoewel de technologiebedrijven hierover rapporteren op hun websites, blijft de moderatie vaak achter bij de omvang van de problematiek. Algoritmen die content detecteren en filteren moeten voortdurend worden getraind en beoordeeld, wat een intensief en kwetsbaar proces is. Het Verenigd Koninkrijk en Denemarken bieden goede voorbeelden van directe samenwerking via *trusted flaggers*: actoren die op basis van OSINT-accounts en posts kunnen signaleren, waardoor content sneller offline wordt gehaald dan via reguliere rapportageprocedures. Dit model zou breder kunnen worden toegepast, niet alleen binnen de politie, maar ook binnen gemeenten, ngo's of andere maatschappelijke organisaties.

Fundamenteel is de vraag of technologiebedrijven bereid zijn substantieel te investeren in moderatie. Uit artikel 8 van de Digital Service Act (DSA) volgt voor platformen immers geen verplichting om alle content proactief te monitoren. Telegram heeft lange tijd populariteit genoten juist omdat het nauwelijks verantwoording nam voor de inhoud die werd gedeeld. Snapchat toont meer bereidheid tot samenwerking, maar beschikt volgens respondenten niet altijd over de menskracht en daadkracht om een substantieel deel van de schadelijke content te verwijderen. Daarbij spelen ook kwesties als leeftijdsverificatie, waar platformen wel beleid op formuleren, maar waarvan de feitelijke uitvoering vaak achterblijft.

Ook in dit verband is een andere taal relevant. Het concept platform-enabled crime wijst nadrukkelijk op de verantwoordelijkheid van platformen zelf en de rol die zij spelen in het faciliteren en mogelijk maken van bepaalde vormen van criminaliteit (Hamilton, 2021). Dit sluit aan bij bredere discussies over maatschappelijk verantwoord ondernemen: technologiebedrijven kunnen niet langer volstaan met het slechts aanbieden van infrastructuur, maar zouden – conform hun eigen richtlijnen – actief

moeten bijdragen aan het beperken van misbruik en het beschermen van de gebruikers van hun platformen. Voor de politiepraktijk betekent dit dat samenwerking met platformen niet alleen gericht moet zijn op toegang tot data, maar ook op het gezamenlijk ontwikkelen van normen en praktijken voor contentmoderatie en veiligheid. Wanneer overheden merken dat platformen hierin onvoldoende verantwoordelijkheid nemen, ontstaat de noodzaak voor een bredere lobby om druk uit te oefenen en bedrijven te wijzen op hun maatschappelijke verantwoordelijkheid en eigen richtlijnen (zie o.a. Flew, Martin en Suzor, 2019).

7.5 Beperkingen van het onderzoek

Dit onderzoek kent, tot slot, enkele beperkingen. Allereerst is er over het thema van hybride verschijningsvormen nog relatief weinig geschreven. Om deze reden is dit onderzoek deels gebaseerd op interviews en openbare bronnen die voorbeelden van verschijningsvormen bieden. De verschijningsvormen die in dit onderzoek worden gepresenteerd zijn daarmee selecties. Hierbij speelt ook de internationale component een rol: per land is slechts een beperkt aantal interviews afgenomen. Hoewel dit een zekere inkijk verschaft, blijft het onderzoek daardoor verkennend van aard. Daarnaast zijn er beperkingen in de perspectieven die centraal staan. Wetenschappers bieden een beeld van fenomenen op basis van hun eigen onderzoek, maar hebben minder zicht op de praktijk en de concrete aanpak. Praktijkprofessionals beschikken daarentegen over kennis van de aanpak, maar hun blik op de fenomenen is sterk gekleurd door wat zij in hun dagelijkse werk tegenkomen. Bovendien heeft de wijze van werving van respondenten in de verschillende landen geleid tot een zekere selectie. Voor vervolgonderzoek is het daarom van belang om per land meer respondenten te betrekken, nadrukkelijk samen te werken met lokale contacten en ook praktijkprofessionals sterker in het onderzoek te integreren. Tevens verdient het aanbeveling om de focus uit te breiden naar meer landen, zodat zowel de analyse van fenomenen als van aanpakken aan diepgang wint.

Een tweede beperking betreft de inhoudelijke focus. Dit onderzoek richt zich primair op financieel gemotiveerde (cyber)criminaliteit, geweld en drugs. Er zijn echter veel meer onderwerpen die vergelijkbare relevantie hebben. Het feit dat deze buiten beschouwing zijn gelaten, vormt een duidelijke beperking. Voor vervolgonderzoek is het daarom wenselijk om ook radicalisering, zedendelicten, meer georganiseerde vormen van criminaliteit en andere thema's te betrekken. Op die manier kan een vollediger beeld worden verkregen van verschijningsvormen van criminaliteit in het hybride tijdperk.

Literatuur

Aagesen, K. & Demant, J.J. (2025). From Gray to Black markets – A quasi-experimental study on algorithmically driven digital drift opportunities on social media. *Deviant Behavior*, 1-14.

Adjiembaks, S., Boerman, F., Roks, R.A. & Stoffers, E. (2023). *Liquidaties in Nederland: Ontwikkelingen en achtergronden van schutters en andere betrokkenen*. Politie & Wetenschap. <https://www.politieenwetenschap.nl/uploads/Politiewetenschap/pw-130.pdf>. Politie & Wetenschap/

Adamse, I., Eichelsheim, V., Blokland, A. & Schoonmade, L. (2024). The risk and protective factors for entering organized crime groups and their association with different entering mechanisms: A systematic review using ASReview. *European Journal of Criminology*, 21(6), 859-886. <https://doi.org/10.1177/14773708241250278>

Aldridge, J. & Décary-Héty, D. (2016). Hidden wholesale: how drug cryptomarkets may transform traditional online drug markets. *International Journal of Drug Policy*, 35, 7-15.

Andell, P. (2019). Addressing county lines: praxis for community safety practitioners. *Safer Communities*, 18(2), 43-53. <https://doi.org/10.1108/sc-02-2019-0006>

Anderson, E. (1999). *Code of the Street*. Norton and Co.

Bakken, S.A. (2020). Drug dealers gone digital: using signalling theory to analyse criminal online personas and trust. *Global Crime*, 1-23. <https://doi.org/10.1080/17440572.2020.1806826>

Bakken, S.A. & Demant, J.J. (2019). Sellers' risk perceptions in public and private social media drug markets. *International Journal of Drug Policy*, 73, 255-262. <https://doi.org/10.1016/j.drugpo.2019.03.009>.

Barendregt, C., Poel, A. van der & Mheen, D. van de (2006). The rise of the mobile phone in the hard drug scene of Rotterdam. *Journal of Psychoactive Drugs*, 38(1), 77-87.

Bekkers, L.J. (2025). *Recruiting money mules: Exploring the offline and online involvement mechanisms of cybercrime*. [Dissertation]. Vrije Universiteit Amsterdam.

Bekkers, L.J. & Leukfeldt, E.R. (2022). Recruiting money mules on instagram: a qualitative examination of the online involvement mechanisms of cybercrime. *Deviant Behavior*, 1-17.

Bekkers, L., Leukfeldt, E.R. & Kleemans, E.R. (2025). Police Investigations into Financial-Economic Cybercriminal Networks: The Experiences and Perceptions of Dutch Law Enforcement. *European Journal on Criminal Policy and Research*. <https://doi.org/10.1007/s10610-025-09615-2>

Bekkers, L. & Leukfeldt, E.R. (2025). Specialization in cybercrime and offense versatility during early adolescence and the role of criminogenic needs. *Crime Law and Social Change*, 83(1). <https://doi.org/10.1007/s10611-025-10232-7>

Bekkers, L., Loggen, J., Keja, N., Bijmans, H. & Leukfeldt, E.R. (2025). Exploring cybercrime and traditional crime on Telegram in the Netherlands. *Global Crime*, 1-23.

Bekkers, L., Moneva, A. & Leukfeldt, E.R. (2024). Understanding cybercrime involvement: a quasi-experiment on engagement with money mule recruitment ads on Instagram. *Journal of Experimental Criminology*, 20(2), 375-394. <https://doi.org/10.1007/s11292-022-09537-7>

Bekkers, L., Schiks, J. & Leukfeldt, E.R. (2020). *Naar een interventie tegen geldezels*. De Haagse Hogeschool. https://www.dehaagsehogeschool.nl/sites/hhs/files/images/naar-een-interventie-tegen-geldezels_een-pilot-in-de-gemeente-haarlem.pdf

Bekkers, L., Van Houten, Y., Spithoven, R. & Leukfeldt, E.R. (2023). Money Mules and Cybercrime Involvement Mechanisms: Exploring the Experiences and Perceptions of Young People in the Netherlands. *Deviant Behavior*, 44(9), 1368-1385. <https://doi.org/10.1080/01639625.2023.2196365>

Bergers, J., Van Deuren, S., Roks, R.A., Habets, S., Leukfeldt, E.R. & Eichelsheim, V. (2026). *De rol van sociale media in de betrokkenheid van jongeren bij zware en georganiseerde drugs- en geweldscriminaliteit*. Politie en Wetenschap

Bervoets, E., Van den Akker, K., Oude Lansink, M., Schuitema, B., Van Bohemen, R. & Tielens, J. (2024). *KNEL: jongeren en jongvolwassenen over het betrokken raken bij georganiseerde criminaliteit*. Bureau Bervoets & RIEC. <https://www.hetckm.nl/wp-content/uploads/2024/07/KNEL-digi-2024.pdf>

- boyd, D. (2014). *It's Complicated: The Social Lives of Networked Teens*. Yale University Press.
- Brown, S. (2006). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, 10(2), 223-244.
- Brynjolfsson, E. & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. WW Norton & company.
- Coomber, R. & Moyle, L. (2017). The Changing Shape of Street-Level Heroin and Crack Supply in England: Commuting, Holidaying and Cuckooing Drug Dealers Across 'County Lines'. *The British Journal of Criminology*, 58(6), 1323-1342. <https://doi.org/10.1093/bjc/azx068>
- Crisp, W. & Dodd, V. (2022, 3 juli). Met police profiling children 'on a large scale', documents show. *The Guardian*. Geraadpleegd op 6 januari 2026 via: <https://www.theguardian.com/uk-news/2022/jun/03/met-police-project-alpha-profiling-children-documents-show>.
- De Jong, J. (2021). *Favourite rappers or favourite cappers?* [ongepubliceerde masterscriptie]. Universiteit Utrecht.
- De Jong, J., Terpstra, J. Van Aggelen, M., & Herder, F. (2026). *Routekaart Samenwerken bij online jeugdcriminaliteit*. NHVeilig/het CCV/Partner in Crime, https://b414ba1d-9de0-4cf9-b056-1f9076d9845a.filesusr.com/ugd/d99537_61a0f2de643b4bf98390fe-1fe8ce1a78.pdf
- De Hullu, J. & Van Kempen, P.H.P.H.M.C. (2024). *Materieel strafrecht*. Wolters Kluwer.
- Demant, J., Bakken, S.A., Oksanen, A. & Gunnlaugsson, H. (2019). Drug dealing on Facebook, Snapchat and Instagram: a qualitative analysis of novel drug markets in the Nordic countries. *Drug and Alcohol Review*, 38(4), 377-385.
- Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*, <https://doi.org/10.1007/s12117-022-09457-y>
- Dupont, B., Côté, A.M., Boutin, J.L. & Fernandez, J. (2017). Darkode: Recruitment patterns and transactional features of 'the Most Dangerous Cybercrime Forum in the World'. *American Behavioral Scientist*, 61(11), 1219-1243.
- Europol (2025). *The changing DNA of serious and organised crime: EU Serious and Organised Crime Threat Assessment 2025 (EU-SOCTA)*. Publication Office of the

European Union. <https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf>

Evers, J. (2024). *Handboek kwalitatieve analyse: theorie en praktijk van thick analysis*. Evers Research and Training

Fatsis, L. (2019). Policing the beats: The criminalisation of UK drill and grime music by the London Metropolitan Police. *The sociological review*, 67(6), 1300-1316.

Fawell, L., Davies, J.L., Stubbings, D. & Payne, L. (2024). How vulnerable are people to victimisation of County Lines drug dealing? *Crime Prevention and Community Safety*, 26(3), 285-300. <https://doi.org/10.1057/s41300-024-00212-9>.

Flew, T., Martin, F. & Suzor, N. (2019). Internet regulation as media policy: Rethinking the question of digital communication platform governance. *Journal of Digital Media & Policy*, 10(1), 33-50.

Floridi, L. (2015). *The onlife manifesto: Being human in a hyperconnected era*. Springer nature.

Futter, A. (2018). 'Cyber' semantics: why we should retire the latest buzzword in security studies. *Journal of Cyber Policy*, 3(2), 201-216.

Garkava, T., Moneva, A. & Leukfeldt, E.R. (2024). Stolen data markets on Telegram: a crime script analysis and situational crime prevention measures. *Trends in Organized Crime*. <https://doi.org/10.1007/s12117-024-09532-6>

Gaudette, T., Scrivens, R. & Venkatesh, V. (2022). The role of the internet in facilitating violent extremism: insights from former right-wing extremists. *Terrorism and Political Violence*, 34(7), 1339-1356.

Gordon, F., McGovern, A., Thompson, C. & Wood, M.A. (2022). Beyond cybercrime: New perspectives on crime, harm and digital technologies. *International Journal for Crime, Justice and Social Democracy*, 11(1), i-viii.

Graham, R., Humer, S.G., Lee, C.S. & Nagy, V. (Eds.). (2024). *The Routledge international handbook of online deviance*. Routledge, Taylor & Francis Group.

Hamilton, R.J. (2021). Platform-Enabled crimes. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3905351>

Haut, F. (2014). Cyberbanging: When Criminal Reality and Virtual Reality Meet. *International Journal on Criminology*, 2(2), 22-27.

- Hayward, K.J. (2012). Five spaces of cultural criminology. *The British Journal of Criminology*, 52(3), 441-462.
- Henry, N., Flynn, A. & Powell, A. (2020). Technology-Facilitated Domestic and Sexual Violence: A Review. *Violence Against Women*, 26(15-16), 1828-1854. <https://doi.org/10.1177/1077801219875821>
- Holt, T.J. (2023). Understanding the state of criminological scholarship on cybercrimes. *Computers in Human Behavior*, 139, 107493.
- Holt, T.J. & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant behavior*, 35(1), 20-40.
- Horst, H. & Miller, D. (2012). Normativity and materiality: A view from digital anthropology. *Media International Australia*, 145(1), 103-111.
- Horst, H.A. & Miller, D. (Eds.). (2020). *Digital anthropology*. Routledge.
- Hutchings, A. & Holt, T.J. (2014). A Crime Script Analysis of the Online Stolen Data Market: Table 1. *The British Journal of Criminology*, 55(3), 596-614. <https://doi.org/10.1093/bjc/azu106>
- Ilan, J. (2020). Digital street culture decoded: why criminalizing drill music is street illiterate and counterproductive. *The British Journal of Criminology*, 60(4), 994-1013.
- Irwin-Rogers, K., Densley, J. & Pinkney, C. (2018). Gang violence and social media. In *The Routledge international handbook of human aggression* (pp. 400-410). Routledge.
- Irwin-Rogers, K. & Pinkney, C. (2017), *Social Media as a Catalyst and Trigger of Youth Violence*, Catch 22, London.
- Janssen, J., Defrancq, B., Schaap, D. & Ponsaers, P. (2022). Voor een multidimensionele visie op politiecultuur. *Cahiers Politiestudies*, (64), 7-16.
- Jurgenson, N. (2011). Digital dualism versus augmented reality. *The Society Pages*, 24.
- Kaufmann, M. & Lomell, H.M. (2025). An introduction to digital criminology. In *De Gruyter Handbook of Digital Criminology* (pp. 1-20). <https://doi.org/10.1515/9783111062037-001>
- Koch, I., Williams, P. & Wroe, L. (2023). 'County lines': racism, safeguarding and statecraft in Britain. *Race & Class*, 65(3), 3-26. <https://doi.org/10.1177/03063968231201325>

Korshøj, N.T. & Søgaaard, T.F. (2024). Hybrid drug dealing: Merging on-and offline spheres when dealing drugs via social media. *International Journal of Drug Policy*, 130, 104509.

Kranenbarg, M.W. & Van 't Hoff-de Goede, S. (2023). Online criminaliteit in criminologisch perspectief. *Tijdschrift Voor Criminologie*, 65(4), 400-419. <https://doi.org/10.5553/tvc/0165182x2023065004002>

Kruisbergen, E.W., Leukfeldt, E.R., Kleemans, E.R. & R. Roks (2018) Georganiseerde criminaliteit en ICT: Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit. Den Haag/Amsterdam: WODC/NSCR

Kruisbergen, E.W., Leukfeldt, E.R., Kleemans, E.R. & Roks, R. (2019). Money talks. Money laundering choices of organized crime offenders in a digital age. *Journal of Crime and Justice*, 42(5), 569-581. <https://doi.org/10.1080/0735648x.2019.1692420>

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

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

Lane, J. (2019). *The Digital Street*. Oxford University Press.

Lane, J. & Stuart, F. (2022). How social media use mitigates urban violence: Communication visibility and third-party intervention processes in digital urban contexts. *Qualitative Sociology*, 1-19.

Latour, B. (2005), *Reassembling the Social. An introduction to Actor-Network-Theory*. Oxford University Press.

Lauger, T.R. & Densley, J.A. (2018). Broadcasting badness: Violence, identity, and performance in the online gang rap scene. *Justice Quarterly*, 35(5), 816-841.

Lehdonvirta, V. (2022). Cloud empires. How Digital Platforms Are Overtaking the State and How We Can Regain Control. In *The MIT Press eBooks*. <https://doi.org/10.7551/mitpress/14219.001.0001>

Leukfeldt, E.R. (2014). Cybercrime and social ties: Phishing in Amsterdam. *Trends in Organized Crime*, 17(4), 231-249.

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

Leukfeldt, E.R. (2017). *Research agenda the human factor in cybercrime and cybersecurity*. Eleven International Publishing.

Leukfeldt, E.R. & Holt, T.J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behavior*, 126, 106979.

Leukfeldt, E.R., Kleemans, E.R. & Stol, W.Ph. (2017a). Origin, growth and criminal capabilities of cybercriminal networks: An international empirical analysis. *Crime, Law and Social Change*, 67(1), 39-53.

Leukfeldt, E.R., Kleemans, E.R. & Stol, W.Ph. (2017b). The use of online crime markets by cybercriminal networks: A view from within. *American Behavioral Scientist*, 61(11), 1387-1402.

Leukfeldt, E.R., Kleemans, E.R. & Stol, W.Ph. (2017c). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology*, 57(3), 704-722.

Leukfeldt, E.R., Kleemans, E.R., Kruisbergen, E.W. & Roks, R.A. (2019). Criminal networks in a digitised world: on the nexus of borderless opportunities and local embeddedness. *Trends in Organized Crime*, 22(3), 324-345. <https://doi.org/10.1007/s12117-019-09366-7>

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

Leukfeldt, E.R. & Roks, R.A. (2020). Cybercrimes on the streets of the Netherlands? An exploration of the intersection of cybercrimes and street crimes. *Deviant Behavior*, 42(1), 1-12. DOI:10.1080/01639625.2020.1755587

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

Leukfeldt, E.R., Van Leuken, M., Van Ruitenburg, T., Schiks, J. & Ruiter, S. (2025). Bottlenecks and Opportunities for Improvement in Cybercrime Handling: Insights from Dutch Police Practice. *Deviant Behavior*, 1-17.

Loggen, J. & Leukfeldt, R. (2022). Unraveling the crime scripts of phishing networks: an analysis of 45 court cases in the Netherlands. *Trends in Organized Crime*, 25(2), 205-225.

Loggen, J., Moneva, A. & Leukfeldt, R. (2024). A systematic narrative review of pathways into, desistance from, and risk factors of financial-economic cyber-enabled crime. *Computer Law & Security Review*, 52, 105858.

Loggen, J., Veenstra, S. & Leukfeldt, E.R. (2026). *Criminele jeugdgroepen: een onderzoek naar het ontstaan, de groei en de aanpak van criminele jeugdgroepen in een digitaliserende samenleving*. Politie & Wetenschap.

Lupton, D. (2015). *Digital sociology*. Routledge.

Lusthaus, J. (2018). *Industry of anonymity: Inside the business of cybercrime*. Harvard University Press.

Lusthaus, J. (2024). Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime?. *Annual Review of Law and Social Science*, 20(1), 369-385.

Lusthaus, J., Kleemans, E.R., Leukfeldt, E.R., Levi, M. & Holt, T. (2023). Cybercriminal networks in the UK and Beyond: Network structure, criminal cooperation and external interactions. *Trends in Organized Crime*. <https://doi.org/10.1007/s12117-022-09476-9>

Lusthaus, J. & Varese, F. (2021). Offline and Local: The Hidden Face of Cybercrime. *Policing A Journal of Policy and Practice*, 15(1), 4-14. <https://doi.org/10.1093/police/pax042>

Martin, J. (2014). Lost on the silk road: Online drug distribution and the 'cryptomarket'. *Criminology and Criminal Justice*, 14, 351-367.

McCulloch, L. & Furlong, S. (2019). DM for Details: Selling Drugs in the Age of Social Media. In *Volteface*. <https://www.drugsandalcohol.ie/31036/1/DM-for-Details-1-5-2.pdf>.

McGuire, M.R. (2007). *Hypercrime: The new geometry of harm*. Routledge-Cavendish.

McGuire, M.R. (2008, January). From Hyperspace to Hypercrime: new Technologies and the Geometries of Control. In: *papers from the British Criminology Conference 2008* (Vol. 8, pp. 3-17).

McGuire, M.R. (2019). It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. In: Leukfeldt, E.R. en T.J. Holt (red). *The human factor of cybercrime* (pp. 3-28). Routledge.

- McGuire, M.R. (2026). *Platform Criminality and Post-Crime: How Cybercrime (and Everything Else) Changed*. Taylor & Francis.
- McGuire, M.R. & Dowling, S. (2013a). Chapter 1: Cyber-dependent crimes. In *Cyber crime: A review of the evidence* (1-34). Home Office, <https://doi.org/10.1016/j.echo.2011.03.004>.
- McGuire, M.R. & Dowling, S. (2013b). Chapter 2: Cyber-enabled crimes – fraud and theft. In *Cyber crime: A review of the evidence*. Home Office, <https://doi.org/10.1080/11356405.2016.1269500>.
- McLean, R., Robinson, G. & Densley, J.A. (2020). County lines. Criminal Networks and Evolving Drug Markets in Britain. *Springer Cham*. <https://doi.org/10.1007/978-3-030-33362-1>
- Mehlbaum, S., Van Den Akker, K., Broekhuizen, J., Verweij, A. & Van Lochem, M. (2025). *Geklapt, gefilmd en gedeeld: Onderzoek naar hybride straatgeweld onder jongeren*. Politie & Wetenschap.
- Metropolitan Police (2024). Project Alpha. Geraadpleegd op 6 januari 2026 via: <https://www.met.police.uk/foi-ai/metropolitan-police/disclosure-2024/june-2024/project-alpha/>.
- Mitchell, M., Wood, J., O'Neill, T., Wood, M., Pervan, F., Anderson, B. & Arpke-Wales, W. (2025). Technology-facilitated violence: A conceptual review. *Criminology & Criminal Justice*, 25(2), 649-669. <https://doi.org/10.1177/17488958221140549>
- Moore, C.L. & Stuart, F. (2022). Gang research in the twenty-first century. *Annual Review of Criminology*, 5(1), 299-320.
- Moyle, L., Childs, A., Coomber, R. & Barratt, M.J. (2019). #Drugsforsale: an exploration of the use of social media and encrypted messaging apps to supply and access drugs. *International Journal of Drugs Policy*, 63, 101-110. doi:10.1016/j.drugpo.2018.08.005
- Natarajan, M., Clarke, R. & Johnson, B. (1995). Telephones as Facilitators of Drug Dealing: A Research Agenda. *European Journal of Criminal Policy*, 3(3), 137-154.
- Norbutas, L. (2018). Offline constraints in Online Drug Marketplaces: An Exploratory analysis of a Cryptomarket trade network. *International Journal of Drug Policy*, 56, 92-100. <https://doi.org/10.1016/j.drugpo.2018.03.016>
- Oerlemans J., Hingh A.E. de & Van der Wagen, W. (2024). Types of cyber-enabled crime and their criminalisation. In: Van der Wagen, W., Oerlemans, J. & Weulen Kra-

nenbarg, M. (Eds.), *Essentials in cybercrime: a criminological overview for education and practice* (pp. 97-144). Eleven.

Oosterheert, A. (2025, 1 oktober). *Gespreksnotitie rondetafelgesprek publiek-private samenwerking online fraude*. Tweede Kamer, Vaste Commissie voor Justitie & Veiligheid.

Ordekian, M., Atondo-Siu, G., Hutchings, A. & Vasek, M. (2024). Investigating wrench attacks: Physical attacks targeting cryptocurrency users. *Leibniz-Zentrum Für Informatik (Schloss Dagstuhl)*. <https://doi.org/10.4230/lipics.aft.2024.24>

Patton, D.U., Eschmann, R.D. & Butler, D.A. (2013). Internet banging: New trends in social media, gang violence, masculinity and hip hop. *Computers in Human Behavior*, 29(5), A54-A59. <https://doi.org/10.1016/j.chb.2012.12.035>

Parkins-Ozephilus, C. T. & van Toor, D. (2024). My phone is my castle: Over de voorwaarden voor onderzoek aan een smartphone in strafrechtelijke context. *Nederlands Tijdschrift voor Strafrecht*, 2024(4/5), 194-203.

Pink, S., Ardèvol, E. & Lanzeni, D. (2020). Digital materiality. In *Digital materialities* (pp. 1-26). Routledge.

Pinkney, C. & Robinson-Edwards, S. (2018). Gangs, music and the mediatization of crime: Expressions, violations and validations. *Safer Communities*, 17, 103-111.

Politie. (2024). *Online fraude in beeld: Fenomeenbeeld 2024*.

Politie. (2025). *Stevig staan in deze tijd: Strategische agenda politie 2025-2030*. Geraadpleegd op 10 december 2025 via: <https://www.politie.nl/informatie/strategische-agenda-politie-stevig-staan-in-deze-tijd.html>

Powell, A., Stratton, G. & Cameron, R. (2018). *Digital criminology: Crime and justice in digital society*. Routledge.

Robinson, G., McLean, R. & Densley, J. (2018). Working County Lines: Child Criminal Exploitation and Illicit Drug Dealing in Glasgow and Merseyside. *International Journal of Offender Therapy and Comparative Criminology*, 63(5), 694-711. <https://doi.org/10.1177/0306624x18806742>

Roks, R.A. (2016). *In de h200d. Een eigentijdse etnografie over de inbedding van criminaliteit en identiteit*. [Ongepubliceerd proefschrift]. Erasmus Universiteit Rotterdam (EUR).

Roks, R.A., De Jong, J. & Van den Broek, J. (2024). Zijn gwn UK fans die zijn gaan leven wat ze rappen ipv rappen wat ze leven: De multimediale performance van authenticiteit in de Nederlandse (online) drillcultuur. *Tijdschrift voor Criminologie*, 66(3), 294-314.

Roks, R.A. & Hendriksen, J. (2021). Laat je niet misleiden door afwijkende prijzen: Een exploratieve studie naar de ambiguïteit van betrouwbaarheid van cocainedealers op Telegram Messenger. *Tijdschrift voor Criminologie*, 63(2), 212-235.

Roks, R.A., Kleemans, E.R. & Blokland, A.A.J. (2021). Drugscriminaliteit in de lage landen: De omvang(schatting) van de drugseconomie en de verwevenheid met de wettige wereld in Nederland en België. *Tijdschrift voor Criminologie*, 63(2), 115-128. <https://doi.org/10.5553/TvC/0165182X2021063002001>

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

Roks, R.A., Leukfeldt, E.R. en T. Holt (2024). Cybercriminele samenwerkingsverbanden. In W. van der Wagen, J. Oerlemans & M. Weulen Kranenbarg (red.) *Cybercriminaliteit: Een criminologisch overzicht voor studie en praktijk*. Boom Criminologie.

Roks, R.A. & Monshouwer, N. (2020). F-gamers die ‘mapsen’, ‘swipen’ en ‘bonken’: een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger. *Justitiële Verkenningen*, 46(2), 44-58.

Roks, R.A. & Ter Weijden, C. (2026). *Zicht op Rotterdamse uithalers: Een verkennend onderzoek naar de achtergronden, risicofactoren en ingroeimechanismen van Rotterdammers die betrokken zijn bij uithalen*. Gemeente Rotterdam

Roks, R.A. & Van den Broek, J.B. (2017). #HOUHETSTRAAT: straatcultuur op social media? *Tijdschrift Over Cultuur & Criminaliteit*, 7(3), 31-50. <https://doi.org/10.5553/tcc/221195072017007003003>

Roks, R.A. & Van den Broek, J.B.A. (2020). *Cappen voor Clout? Een verkennend onderzoek naar Rotterdamse jongeren, drill en geweld in het digitale tijdperk*. Erasmus Universiteit Rotterdam.

Roks, R.A. & Van den Broek, J.B.A. (2022). De online drillcultuur in Rotterdam: provocaties, bedreigingen en beefs op social media. In I. Weijers (Ed.), *Jeugdcriminaliteit. Achtergronden van jeugdcriminaliteit* (4e ed., pp. 447-468). Boom criminologie.

Ruiter, S., Leuken, M.V., Ruitenburg, T.V., Schiks, J. & Leukfeldt, E.R. (2023). In-en doorstroom van online criminaliteit in de strafrechtsketen. WODC.

Rønn, K.V. (2023). Mediated Proximity: Community Policing in the Digital Age. *Nordic Journal of Studies in Policing*, 10(1), 1-15. <https://doi.org/10.18261/njsp.10.1.8>

Salinas, M. (2018). The unusual suspects: an educated, legitimately employed drug dealing network. *International Criminal Justice Review*, 28(3), 226-242.

Schiks, J.A.M., Van 't Hoff-de Goede, S. & Leukfeldt, E.R. (2022) *Op zoek naar de parels bij de lokale aanpak van cybercriminaliteit en gedigitaliseerde criminaliteit. Een verkennend onderzoek* (P&W verkenningen 89). Politie & Wetenschap.

Schinkel, W. (2010). *Aspects of Violence. A Critical Theory*. Palgrave Macmillan.

Smith R.G. (2014) Responding to organised crime through intervention in recruitment pathways. *Trends and Issues in Crime and Criminal Justice* 473: 1-9.

Søgaard, T.F. (2019). Drop-off drug distribution: why users choose to source illegal drugs from delivery dealers. *Nordic Journal of Criminology*, 20(2), 213-222.

Soudijn, M.R.J. & Zegers, B.C.H.T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime*, 15(2-3), 111-129. <https://doi.org/10.1007/s12117-012-9159->

Spicer, J. (2020). Between gang talk and prohibition: The transfer of blame for County Lines. *International Journal Of Drug Policy*, 87, 102667. <https://doi.org/10.1016/j.drugpo.2020.102667>

Staring, R., Bisschop, L., Van de Bunt, H., Brein, E. & Roks, R. (2019). Drugscriminaliteit in de Rotterdamse haven: aard en aanpak van het fenomeen. Boom Criminologie.

Stoeldraaijers, C., Rodermond, E., Thijs, F., Leukfeldt, R. & Weerman, F. (2024). Radicale reclame op sociale media Een onderzoek naar online rekrutering. WODC.

Stol, W., Strikwerda, L., Jansen, J. & Scheurs, W. (2025). *Politiestraatwerk en informatiegebruik*. Politie & Wetenschap.

Storrod, M.L. & Densley, J.A. (2016). 'Going viral' and 'Going country': the expressive and instrumental activities of street gangs on social media. *Journal Of Youth Studies*, 20(6), 677-696. <https://doi.org/10.1080/13676261.2016.1260694>

Stratton, G., Powell, A. & Cameron, R. (2017). Crime and justice in digital society: Towards a digital criminology?. *International Journal for Crime, Justice and Social Democracy*, 6(2), 17-33

Stuart, F. (2020a). *Ballad of the Bullet. Gangs, Drill Music, and The Power of Online Infamy*. Princeton, NJ: Princeton University Press.

Stuart, F. (2020b). Code of the tweet: Urban gang violence in the social media age. *Social problems*, 67(2), 191-207

Timmermans, S. & Tavory, I. (2012). Theory construction in qualitative research. *Sociological Theory*, 30(3), 167-186. <https://doi.org/10.1177/0735275112457914>

Tieleman, Y. & C. Timmersmans (2025, 17 augustus). Ouders van aanslagpleger Mike (15) probeerden alles, maar verloren hem toch aan de onderwereld. *Algemeen Dagblad*. Geraadpleegd op 6 januari 2026 via: <https://www.ad.nl/binnenland/ouders-van-aanslagpleger-mike-15-probeerden-alles-maar-verloren-hem-toch-aan-de-onderwereld~a141c6c1/>.

Tollenaar, L.S.A., Lopriore, E., Middeldorp, J.M., Haak, M.C., Klumper, F.J., Oepkes, D. & Slaghekke, F. (2018). Improved prediction of twin anemia-polycythemia sequence by delta middle cerebral artery peak systolic velocity: new antenatal classification system. *Ultrasound in Obstetrics and Gynecology*, 53(6), 788-793. <https://doi.org/10.1002/uog.20096>

Urbanik, M. & Haggerty, K.D. (2017). ‘#It’s Dangerous’: The Online World of Drug Dealers, Rappers and the Street Code. *The British Journal of Criminology*, 58(6), 1343-1360. <https://doi.org/10.1093/bjc/azx083>

Van Berkel, S., Kleemans, E. & Mooij, A. (2025). Social media and organizing violent crime against persons and properties: a qualitative analysis of online criminal communication between young offenders based on seized telephone information. *Trends in Organized Crime*, 1-22.

Van den Berg, P. & Rekers, M. (2022). Criminelen ronselen jongeren. Leerlingenalert

Van den Broek, J.B.A., De Jong, J. & Moussaid, Y. (2022). Handreiking Rivaliserend Groepsgedrag in een Hybride Werkelijkheid. *Partner in Crime, in opdracht van Gemeente Delft, Den Haag en Zoetermeer*. <https://www.partnerincrime.nl/wp-content/uploads/2023/01/Handreiking-rivaliserend-groepsgedrag-in-een-hybride-werkelijkheid-2022-Origineel.pdf>

Van den Broek, J.B.A. & Jhanjan, J.H. (2024). Straatcultuursensitief werken in het digitale tijdperk. In *Werken in gedwongen kader Methodiek voor het forensisch sociaal werk*. SPW.

Van den Broek, J.B.a. & Roks, R. (2023). Inspiratiedocument aanpak problematisch groepsgedrag in het digitale tijdperk. *Partner in Crime, in opdracht van Gemeente Zoetermeer, Den Haag en Delft*.

Van der Wagen, W. (2018). Het 'cyborg crime'-perspectief Theoretische vernieuwing in het digitale tijdperk. *Tijdschrift over Cultuur en Criminaliteit*, 8(1),19-34.

Van der Wagen, W. (2019). The Significance of 'Things' in Cybercrime How to Apply Actor-network Theory in (Cyber) criminological Research and Why it Matters. *Journal of Extreme Anthropology*.

Van der Wagen, W., Oerlemans, J.J. & Weulen Kranenbarg, M. (2024). *Basisboek Cybercriminaliteit: Een criminologisch overzicht voor studie en praktijk*. Boom.

Van Hout, M.C. & Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy*, 25, 183-189. doi:10.1016/j.drugpo.2013.10.009.

Van Hulst, M., Terpstra, J. & Kolthoff, E. (2016). Politiecultuur als kernbegrip en discussiethema. *Tijdschrift Voor Veiligheid*, 15(2-3), 3-14. <https://doi.org/10.5553/tvv/187279482016015203001>

Van Hulst, M. & Visser, E.L. (2024). Abductive analysis in qualitative research. *Public Administration Review*, 85(2), 567-580. <https://doi.org/10.1111/puar.13856>

Van Steden, R., Ter Woerds, S., 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*. Politie & Wetenschap.

Verbeek, P.P. (2008). Cyborg intentionality: Rethinking the phenomenology of human-technology relations. *Phenomenology and the cognitive sciences*, 7(3), 387-395.

Wall, D.S. (2001). Cybercrimes and the internet. In D. S. Wall (Ed.), *Crime and the internet* (pp. 1-17). Routledge.

Wall, D.S. (2007). Cybercrime. *The Transformation of Crime in the Information Age*. Polity.

Wall, D.S. (2015). Dis-organised crime: Towards a distributed model of the organization of cybercrime. *The European Review of Organised Crime*, 2(2).

Weerman, F., Roks, R.A., Van den Broek, J. & Willink, J. (2022). 'Het is een probleem, maar niet voor mij': Een onderzoek naar de achtergronden van wapens en wapengeweld onder jongeren in Rotterdam. Erasmus School of Law (ESL).

Werninmont, J. (2025). *Digital*. In Kaufmann, M. & Mork Lomell, H. (red). *De Gruyter Handbook of Digital Criminology* (pp. 197-204). De Gruyter.

Wood, M.A., Mitchell, M., Pervan, F., Anderson, B., O'Neill, T., Wood, J. & Arpke-Wales, W. (2023). Inviting, affording and translating harm: Understanding the role of technological mediation in technology-facilitated violence. *The British Journal of Criminology*, 63(6), 1384-1404.

Bijlage 1 Topiclijsten

Interviews in Nederland

Inleiding

Hartelijk dank voor uw deelname aan dit onderzoek. Dit interview is onderdeel van een studie naar de hybridisering van criminaliteit uitgevoerd door het lectoraat Cybercrime & Cybersecurity van de Haagse Hogeschool, en de Erasmus Universiteit Rotterdam. Het onderzoek richt zich op de verwevenheid van online en offline elementen in de organisatie en uitvoering van criminaliteit in groepsverband en de uitdagingen die dit met zich meebrengt voor de aanpak.

Het doel van dit onderzoek is om de aard en aanpak van hybride vormen van criminaliteit in kaart te brengen, met als focus Nederland en enkele omliggende landen in Europa. We zijn voor dit interview niet geïnteresseerd in namen of andere tot personen herleidbare informatie. Het interview zal ongeveer 60 tot 90 minuten in beslag nemen. Alles wat u met ons deelt, is vertrouwelijk en alleen toegankelijk voor de onderzoekers. De gedeelde informatie wordt gepseudonimiseerd en versleuteld opgeslagen.

Informed consentformulier laten ondertekenen

1. Algemeen

Voordat we beginnen, zouden we graag eerst wat meer over uw achtergrond en functie willen weten.

Kunt u zich kort voorstellen?

- Organisatie/functie
- Doorvragen naar vorige functies/ervaringen

2. Aard van hybride criminaliteit

Graag stellen wij u een aantal specifieke vragen om meer inzicht te krijgen in (de aard van) de delicten waarbij de verwevenheid van traditionele en online criminaliteit zichtbaar wordt.

Aard van hybride criminaliteit algemeen

Op welke manier ziet u de invloed van digitale technologie terug in vormen van criminaliteit waar u tijdens uw werk mee in aanraking komt?

- Welke vormen van criminaliteit ziet u waarbij zowel een online als offline component aanwezig is? (Doorvragen op concrete voorbeelden en probeer te achterhalen hoe de respondent zicht heeft gekregen op deze voorbeelden)
- In hoeverre ziet u hierbij een verandering in de complexiteit van deze vormen van criminaliteit?

De volgende vragen per vorm van criminaliteit die door de respondent wordt genoemd langslopen. Expliciet vragen naar wat deze voorbeelden nieuw/anders maken.

Voorbeelden van criminaliteit waarbij sprake is van een zekere hybridisering. Let op: niet alles hoeft uitgevraagd te worden.

Ontstaan samenwerkingsverband

Wat is er bekend over het samenwerkingsverband?

- Hoeveel leden/daders?
- Leeftijd leden/daders?
- Criminele achtergrond leden/daders?
- Herkomst van leden/daders?
- Wat is er bekend over hoelang deze daders al samenwerken?
- Met welke vormen van criminaliteit houden de leden zich bezig?
- In hoeverre is er sprake van een specialisme?

Hoe kennen de daders in het samenwerkingsverband elkaar?

- Offline: zo specifiek mogelijk uitvragen
- Online: zo specifiek mogelijk uitvragen (welke socialemediaplatformen bijvoorbeeld)

Organisatie

Hoe werken de daders in het samenwerkingsverband samen?

- Offline: zo specifiek mogelijk uitvragen
- Online: zo specifiek mogelijk uitvragen

Wat is er bekend over het netwerk?

- In hoeverre is er een taakverdeling? (subgroepen, kernfuncties, ondersteunende functies)
- In hoeverre was er sprake van een hiërarchie?
- In hoeverre is er sprake van een wisselende samenstelling?

Hoe vond de communicatie tussen leden van het netwerk plaats?

- Offline: zo specifiek mogelijk uitvragen
- Online: zo specifiek mogelijk uitvragen (naar platformen etc.)

Uitvoering van criminele activiteiten

Wat is bekend over de manier waarop de criminele activiteiten worden uitgevoerd?

- Doorvragen op modus operandi
- In hoeverre is er een online component? (Zo concreet mogelijk uitvragen)
- In hoeverre is er een offline component? (Zo concreet mogelijk uitvragen)

Waar worden de criminele activiteiten hoofdzakelijk gepleegd?

- In hoeverre is sprake van internationale aspecten bij de uitvoering van deze delicten?
- In hoeverre speelt geweld een rol?

3. Aanpak van hybride criminaliteit

Ook zijn we geïnteresseerd in de aanpak van hybride vormen van criminaliteit. We stellen u vragen over zowel de huidige aanpak als mogelijkheden voor de aanpak in de toekomst. Ook gaan wij in op uw mening over zowel de sterke punten als verbeterpunten van deze aanpak.

Hoe ziet de aanpak eruit voor de door u genoemde voorbeelden?

- Wat is de focus van deze initiatieven? (preventie, opsporing, verstoring van criminele netwerken)
- Indien opsporing: op welke wijze worden deze zaken afgedaan, strafrechtelijk of anderszins?
- In hoeverre is deze aanpak delictspecifiek?
- In hoeverre is de aanpak gericht op individuele daders of het gehele netwerk?
- Met welke actor(en) werkt u samen in deze aanpak?
- Welke rol vervullen betrokken organisaties in deze aanpak?
- Hoe verloopt de samenwerking? (Doorvragen naar voorbeelden)

Effectieve aangrijpingspunten

Waar in dit voorbeeld zitten naar uw idee effectieve aangrijpingspunten voor preventie, verstoring en opsporing?

- In hoeverre is hier een verschil in aangrijpingspunten online of offline? Waarom?
- Hoe zien deze aangrijpingspunten eruit en welke actoren zijn hiervoor verantwoordelijk?
- Wat zijn naar uw mening de sterke punten van de huidige aanpak?
- Wat zijn naar uw mening verbeterpunten van de huidige aanpak?
- In hoeverre zijn er bij uw organisatie interventies nog in ontwikkeling? Hoe zien deze eruit?

- Bent u bekend met de aanpak van de hybridisering van criminaliteit buiten Nederland? Hoe verschilt de aanpak van hybride criminaliteit ten opzichte van traditionele criminaliteit of cybercriminaliteit in engere zin?

4. Uitdagingen en belemmeringen

Tot slot willen we graag uw perspectief horen op de uitdagingen en belemmeringen die gepaard gaan met de hybridisering van criminaliteit. We zijn benieuwd naar uw persoonlijke inzichten en ervaringen op dit gebied.

- Wat zijn volgens u de grootste uitdagingen bij de aanpak van de hybride vormen van criminaliteit in Nederland?
- Welke belemmeringen ondervindt u of uw organisatie bij de preventie, verstoring, of opsporing van deze delicten?
- In hoeverre zijn internationale samenwerkingen belangrijk in de aanpak van hybride criminaliteit?
- In hoeverre zijn er juridische uitdagingen die de aanpak bemoeilijken?
- In hoeverre zijn er andere specifieke problemen of uitdagingenbarrières die voortkomen uit de combinatie van online en offline criminaliteit?
- Wat zijn mogelijke verbeteringen of innovaties om effectiever op te treden tegen hybride criminaliteit?

Dit is het einde van het interview.

Heeft u nog opmerkingen of dingen die u wilt toevoegen?

Suggesties voor andere respondenten?

Interviews in Denemarken en Verenigd Koninkrijk

This interview is part of a study on the hybridization of crime carried out by the Cyber-crime & Cybersecurity research group of The Hague University of Applied Sciences and Erasmus University Rotterdam. The research focuses on the overlap between on-line and offline aspects of crime – with a focus on violence, fraud, and drug dealing - and the challenges that this entails for the approach.

The aim of this research is to map the nature and approach of hybrid forms of crime, with a focus on the Netherlands, Denmark, and the United Kingdom. For this interview, we are not interested in names or other personally identifiable information. The interview will take approximately 60 to 90 minutes. Everything you share with us is confidential and only accessible to the researchers. The shared information is stored pseudonymously and encrypted.

Informed consent form signed

(Can we record this conversation? It is for our own use only, so we don't have to write everything down)

1. General

Before we start, we would like to know a bit more about your background and position.

- Can you briefly introduce yourself?
- Organisation/ position
- Previous positions/ experiences

2. Nature of hybrid crimes

We would like to ask you a number of specific questions to gain more insight into (the nature of) the crimes in which the overlap between online and offline becomes visible.

- How do you see the influence of digital technology in forms of crime (or victimization) that you come across during your research (or work more in general)?
- Which forms of crime do you see in which both an online and offline component?
 - Organisation?
 - Parts of the *modus operandi* of the crime?
 - And also: on or via what platforms?
- To what extent do you see a change in the complexity of these forms of crime?

3. The approach to hybrid crimes

We are also interested in the approach to hybrid forms of crime. We will ask you questions about both the current and future approaches.

- What does the approach look like for the above examples?
- What is the focus of these initiatives? (prevention, detection, disruption of criminal networks)
- If detection: how are these cases dealt with, criminally or otherwise?

- To what extent is this approach specific to the offence?
- To what extent is the approach focused on individual perpetrators or the entire network?
- Which actor(s) do you work with in this approach?
- What role do the organisations involved play in this approach?
- How does the collaboration proceed? (Ask for examples)
- Effective points of attack
- Where in this example do you think there are effective points of attack for prevention.

4. Challenges and barriers

Finally, we would like to hear your perspective on the challenges and barriers that come with the hybridization of crime. We are curious about your personal insights and experiences in this area.

- What do you think are the biggest challenges in tackling hybrid forms of crime?
- What barriers do you or your organization encounter in the prevention, disruption, or detection of these crimes?
- To what extent are international collaborations important in tackling hybrid crime?
- To what extent are there legal challenges that complicate the approach?
- To what extent are there other specific problems or challenges barriers that arise from the combination of online and offline crime?
- What are possible improvements or innovations that are needed to act more effectively against hybrid crime?

This concludes the interview

- Do you have any comments or things you would like to add?
- Suggestions for other respondents?

Bijlage 2 Informed consent-formulieren

Formulier voor interviews in Nederland

INFORMED CONSENT

Geachte heer/mevrouw,

Met deze brief willen wij uw medewerking vragen aan een interview in het kader van het onderzoek 'Hybridisering van criminaliteit' dat momenteel uitgevoerd wordt door de Haagse Hogeschool en de Erasmus Universiteit Rotterdam in opdracht van Politie & Wetenschap.

Doel onderzoek

In dit onderzoeksproject richten we ons op de hybridisering van criminaliteit, oftewel op de verwevenheid tussen online en offline in de context van criminaliteit. Dit kan bijvoorbeeld betrekking hebben op de samenwerking in de uitvoering van criminele activiteiten die bijvoorbeeld hun oorsprong kunnen vinden in de fysieke wereld, maar ook tot stand kunnen komen via contacten op socialemediaplatformen zoals Instagram, TikTok en Telegram Messenger. Een ander voorbeeld zijn de modus operandi van bepaalde soorten criminaliteit die zowel online als offline aspecten bevatten. In dit project gaat onze aandacht in het bijzonder uit naar geweld, de handel in verdovende middelen, en fraude en oplichting.

Door deel te nemen aan een interview hopen we meer te weten te komen over uw kennis over en ervaring met de online-offlineverwevenheid in de context van criminaliteit, zowel in termen van het fenomeen als de aanpak ervan.

Interview

Een interview duurt ongeveer 60 tot 90 minuten. In overleg wordt vastgesteld op welke manier (online of fysiek), datum en tijdstip het interview wordt gehouden. Met uw toestemming zal er een geluidsopname van het interview gemaakt worden en zullen er tijdens het interview schriftelijke aantekeningen gemaakt worden.

Privacy

De informatie die u in het interview geeft, wordt alleen voor dit onderzoek gebruikt. Uw gegevens worden anoniem verwerkt. Dit betekent dat u niet met naam en toenaam

in een onderzoekpublicatie wordt genoemd: u blijft volledig onbekend. Ook zal de informatie die u deelt niet rechtstreeks naar u herleidbaar zijn.

Mochten er onduidelijkheden zijn, dan lichten we die met veel plezier toe.

Onderzoekers

Isabelle Klaver – De Haagse Hogeschool

Robby Roks – Erasmus Universiteit

Rutger Leukfeldt – De Haagse Hogeschool/Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving

INFORMED CONSENT

voor het interview en het onderzoek:

Hybridisering van criminaliteit

- Ik ben over het interview en het onderzoek geïnformeerd.
- Ik heb de schriftelijke informatie gelezen.
- Ik ben in de gelegenheid gesteld om vragen over het interview en het onderzoek te stellen.
- Ik heb over mijn deelname aan het interview en het onderzoek kunnen nadenken.
- Ik geef toestemming voor het maken van een geluidsopname en schriftelijke aantekeningen tijdens het interview.
- Mijn deelname aan het onderzoek is vrijwillig.
- Ik heb het recht om mijn toestemming op ieder moment weer in te trekken, zonder dat ik daarvoor een reden hoeft op te geven.

Ik stem toe met deelname aan het onderzoek.

Naam :

Datum :

Handtekening :

Formulier voor interviews in Denemarken en het Verenigd Koninkrijk

INFORMED CONSENT

With this letter we would like to ask for your cooperation in an interview for the research project titled 'The hybridization of crime' by the Erasmus University Rotterdam and The Hague University of Applied Sciences on behalf of Police & Science.

Aim of research

In this research project, we focus on the hybridization of crime – the overlap between online and offline aspects of crime – with a focus on violence, fraud, and drug dealing. The aim of this research is to map the nature and approach of hybrid forms of crime, with a focus on the Netherlands, Denmark, and the United Kingdom. For this interview, we are not interested in names or other personally identifiable information. The interview will take approximately 60 to 90 minutes. Everything you share with us is confidential and only accessible to the researchers. The shared information is stored pseudonymously and encrypted.

By participating in an interview, we hope to learn more about your knowledge and experience of the online-offline nexus in the context of crime, both in terms of the phenomenon and how to deal with it. Our goal is to collect examples of the hybridization of crime, good practices when it comes to the approach, but also experiences or challenges when it comes to tackling hybrid forms of crime.

Interview

An interview lasts approximately 60 to 90 minutes. In consultation, it will be determined in what way (online or physical), and on what date and time the interview will be held. With your permission, an audio recording will be made of the interview, and written notes will be made during the interview.

Privacy

The information you provide in the interview will only be used for this research. Your data will be processed anonymously. This means that you will not be mentioned by name in a research publication: you will remain completely unknown. The information you share will also not be directly traceable to you.

If there are any questions, we will be happy to answer them.

Researchers

Isabelle Klaver – De Haagse Hogeschool

Dr. Robby Roks – Erasmus University Rotterdam

Prof. dr. Rutger Leukfeldt – The Hague University of Applied Sciences/Netherlands Study Centre for Crime and Law Enforcement

INFORMED CONSENT

for the interview and the research project titled:

‘The hybridization of crime’

- I have been informed about the interview and the research project.
- I have read the written information.
- I have been given the opportunity to ask questions about the interview and the research.
- I have had time to reflect on my participation in the interview and the research project.
- I give permission for audio recording and written notes to be made during the interview.
- My participation in the study is voluntary.
- I have the right to withdraw my consent at any time, without giving any reason.

I agree to participate in the research.

Name :

Date :

Signature :

Uitgaven in de reeks Politiewetenschap

1. Kerntaken van de politie. Een inventarisatie van heersende opvattingen

C.D. van der Vijver, A.J. Meershoek & D.F. Slobbe, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2001

2. Bevoegdheden overd(r)acht. Een onderzoek naar delegatie en mandaat van beheersbevoegdheden in de politiepraktijk

H.B. Winter & N. Struiksmā, Pro Facto B.V., Universiteit Groningen, 2002

3. Sturing van politie en politiewerk. Een verkennend onderzoek tegen de achtergrond van een veranderende sturingscontext en sturingsstijl

J. Terpstra, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2002

4. Woninginbrekers en zware jongens. Daders vanuit het voormalig Joegoslavië aan het woord

M. van San, E. Snel & R. Boers, Risbo, Erasmus Universiteit Rotterdam, 2002

5. Zeg me wie je vrienden zijn. Allochtone jongeren en criminaliteit

F.M.H.M. Driessen, B.G.M. Völker, H.M. Op den Kamp, A.M.C. Roest & R.J.M. Molenaar, Bureau Driessen, Utrecht, 2002

6. Op deugdelijke grondslag. Een explorerende studie naar private forensische accountancy

J. van Wijk, W. Huisman, T. Feuth & H.G. van de Bunt, Vrije Universiteit, Amsterdam, 2002

7. Voorbij de dogmatiek. Publiek-private samenwerking in de veiligheidszorg

A.B. Hoogenboom & E.R. Muller, COT, Den Haag, 2003

8. Hennepteelt in Nederland. Het probleem van de criminaliteit en haar bestrijding

F. Bovenkerk, W.I.M. Hogewind, D. Korf & N. Milani, Willem Pompe Instituut, Universiteit Utrecht, 2003

9. Politiekennis in ontwikkeling. Een onderzoek naar het verzamelen en veredelen van informatie voor het Politie Kennis Net

Bakker & C.D. van der Vijver, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2003

10a. Politie en geweld. Een verkenning van politiereacties op geweldsincidenten in vier Nederlandse regiokorpsen

C.J.E. In 't Velt, W.Ph. Stol, P.P.H.M. Klerks, H.K.B. Fobler, R.J. van Treeck & M. de Vries, NPA-Politie Onderwijs- en Kenniscentrum, LSOP, Apeldoorn, 2003

10b. Geweldige informatie? Onderzoek naar de informatiehuishouding van geweldsmeldingen bij de politie

R. van Overbeeke, O. Nauta, A. Beerepoot, S. Flight & M. Rietveld, DSP-groep, Amsterdam, 2003

11. Blauwe Bazen. Het leiderschap van korpschefs

R.A. Boin, P. 't Hart & E.J. van der Torre, Departement Bestuurskunde, Universiteit Leiden/COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2003

12. Over de grens. Een verkenning van projecten voor probleemjeugd in Duitsland, Engeland en Zweden

van Leiden, G. Verhagen & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem, 2003

13. Integriteit in het dagelijkse politiewerk. Mening en ervaringen van politiemensen

J. Naeyé, L.W.J.C. Huberts, C. van Zweden, V. Busato & B. Berger, Centrum voor Politiewetenschappen, VU Amsterdam, 2004

14. Politiestraatwerk in Nederland. Noodhulp en gebiedswerk: inhoud, samenhang, verandering en sturing

W. Ph. Stol, A.Ph. van Wijk, G. Vogel, B. Foederer & L. van Heel, Nederlandse Politie-academie, Onderzoeksgroep, LSOP, Apeldoorn, 2004

15. De kern van de taak. Kerncompetenties van de politie als criterium voor de afbakening van kerntaken in de praktijk

Mein, A. Schutte & A. van Sluis, ES&E, Den Haag, 2004

16. Professionele dienstverlening en georganiseerde criminaliteit. Hedendaagse integriteitsdilemma's van advocaten en notarissen

F. Lankhorst & J.M. Nelen, Vrije Universiteit Amsterdam, Faculteit der Rechtsgeleerdheid, Sectie Criminologie, Amsterdam, 2004

17. Paradoxaal Politiebestel. Burgemeesters, Openbaar Ministerie en Politiechefs over de sturing van de politie

L.W.J.C. Huberts, S. Verberk, K. Lasthuizen & J.H.J. van den Heuvel, Vrije Universiteit Amsterdam/B&A Groep, 's-Gravenhage, 2004

18. Illegale vuurwapens in Nederland: smokkel en handel

A.C. Spapens & M.Y. Bruinsma, IVA, Tilburg, 2004

19. Samenwerking en netwerken in de lokale veiligheidszorg

J. Terpstra & R. Kouwenhoven, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2004

20. Uit balans: politie en bestel in de knel. State-of-the-art: bundeling van kennis en inzicht

H.G. van de Bunt, A.B. Hoogenboom, L.W.J.C. Huberts, E.R. Muller, J. Terpstra, C.D. van der Vijver & C. Wiebrens, 2004 Redactie: G.C.K. Vlek, C. Bangma, C. Loeff & E.R. Muller

21. Politie en media. Feiten, fictie en imagopolitiek

H. Beunders & E.R. Muller, Erasmus Universiteit Rotterdam/COT, Instituut voor Veiligheids- en Crisismanagement, Leiden, 2005 (2e druk 2009)

22. Integriteit van de politie. State-of-the-art: wat we weten op basis van Nederlands onderzoek

L.W.J.C. Huberts & J. Naeyé, Centrum voor Politie- en Veiligheidswetenschappen/Vrije Universiteit, Amsterdam, 2005

23. De sociale organisatie van mensensmokkel

R. Staring, G. Engbersen, H. Moerland, N. de Lange, D. Verburg, E. Vermeulen & A. Weltevrede; m.m.v. E. Heyl, N. Hoek, L. Jacobs, M. Kanis & W. van Vliet, Erasmus Universiteit Rotterdam: Criminologie – Sociologie – Risbo, 2005

24. In elkaars verlengde? Publieke en private speurders in Nederland en België

U. Rosenthal, L. Schaap J.C. van Riessen, P. Ponsaers & A.H.S. Verhage, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag/Universiteit Gent, 2005

25. De strafrechtelijke rechtshulpverlening van Nederland aan de lidstaten van de Europese Unie. De politieke discussie, het juridische kader, de landelijke organisatie en de feitelijke werking

C.J.C.F. Fijnaut, A.C. Spapens & D. van Daele, Universiteit van Tilburg, Vakgroep Strafrechtwetenschappen, 2005

26. Niet zonder slag of stoot. De geweldsbevoegdheid en doorzettingskracht van de Nederlandse politie

J. Naeyé, Faculteit der Rechtsgeleerdheid, Vrije Universiteit Amsterdam, 2005

27. Preventief fouilleren. Een analyse van het proces en de externe effecten in tien gemeenten

E.J. van der Torre & H.B. Ferwerda, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag/Advies- en Onderzoeksgroep Beke, Arnhem, 2005

28. Zedenmisdrijven in Nederland. Aangiften- en verdachtenanalyses op basis van HKS-gegevens

A.Ph. van Wijk, S.R.F. Mali, R.A.R. Bullens, L. Prins & P.P.H.M. Klerks, Politieacademie Onderzoeksgroep, Apeldoorn, Vrije Universiteit Amsterdam. KLPD, 2005

29. Groepszedenmisdrijven onder minderjarigen. Een analyse van een Rotterdamse casus

Van Leiden & J. Jakobs, Advies- en Onderzoeksgroep Beke, Arnhem, 2005

30. Omgaan met conflictsituaties: op zoek naar goede werkwijzen bij de politie

O. Adang, N. Kop, H.B. Ferwerda, J. Heijnemans, W. Olde Nordkamp, P. de Paauw & K. van Woerkom, Onderzoeksgroep Politieacademie, Apeldoorn/Advies en Onderzoeksgroep Beke, Arnhem, 2006

31. De strategische analyse van harddrugsscenes. Hoofdlijnen voor politie en beleid

E.J. van der Torre, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2006

32a. Cijfers en stakeholders. Prestatiesturing en de gevolgen voor de maatschappelijke en politiekbestuurlijke relaties van de politie

Van Sluis, L. Cachet, L. de Jong, C. Nieuwenhuyzen & A. Ringeling, Centre for Local Democracy, Erasmus Universiteit Rotterdam, 2006

32b. Operationele betrokkenheid. Prestatiesturing en bedrijfsvoering Nederlandse politie

A.B. Hoogenboom, Nivra-Nyenrode, Breukelen, 2006

32c. Op prestaties gericht. Over de gevolgen van prestatiesturing en prestatieconvenanten voor sturing en uitvoering van het politiewerk

M.P.C.M. Jochoms, F. van der Laan, W. Landman, P.S. Nijmeijer & A. Sey, Politieacademie, Apeldoorn/Twynstra Gudde, Amersfoort/Universiteit van Amsterdam, 2006

33. Het nieuwe bedrijfsmatig denken bij de politie. Analyse van een culturele formatie in ontwikkeling

J. Terpstra & W. Trommel, IPIT Instituut voor Maatschappelijke Veiligheidsvraagstukken, Universiteit Twente, 2006

34. De legitimiteit van de politie onder druk? Beschouwingen over grondslagen en ontwikkelingen van legitimiteit en legitimiteitstoekenning

Bundel onder redactie van C.D. van der Vijver & G.C.K. Vlek, IPIT Instituut voor Maatschappelijke Veiligheidsvraagstukken, Universiteit Twente/Politie & Wetenschap, 2006

35. Naar beginselen van behoorlijke politiezorg

M.J. Dubelaar, E.R. Muller & C.P.M. Cleiren, Faculteit der Rechtsgeleerdheid, Universiteit Leiden, 2006

36a. Asielmigratie en criminaliteit

J. de Boom, G. Engbersen & A. Leerkes, Risbo Contractresearch BV/Erasmus Universiteit, Rotterdam, 2006

36b. Criminaliteitspatronen en criminele carrières van asielzoekers

M. Althoff & W.J.M. de Haan, m.m.v. S. Miedema, Vakgroep Strafrecht en Criminologie, Faculteit der Rechtsgeleerdheid, Rijksuniversiteit Groningen, 2006

36c. 'Ik probeer alleen maar mijn leven te leven'. Uitgeprocedeerde asielzoekers en criminaliteit

Leerkes, Risbo Contractresearch BV/Erasmus Universiteit, Rotterdam; Amsterdamse School voor Sociaal Wetenschappelijk Onderzoek/Universiteit van Amsterdam, Amsterdam, 2006

37. Positie en expertise van de allochtone politiemedewerker

J. Broekhuizen, J. Raven & F.M.H.M. Driessen, Bureau Driessen, Utrecht, 2007

38. Lokale politiechefs. Het middenkader van de basispolitiezorg

E. J. van der Torre, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2007

39. Niet verschenen

40. Conflict op straat: strijden of mijden? Marokkaanse en Antilliaanse jongeren in interactie met de politie

N. Kop, Martin Euwema, m.m.v. H.B. Ferwerda, E. Giebels, W. Olde Nordkamp & P. de Paauw, Politieacademie, Apeldoorn, Universiteit Utrecht, 2007

41. Opsporing onder druk

Liedenbaum & M. Kruijsen, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2008

42. Symbolen van orde en wanorde. Broken windows policing en de bestrijding van overlast en buurtverval

van Stokkom, Centrum voor Ethiek, Radboud Universiteit Nijmegen, 2008

43. Verkeershandhaving: prestaties leveren, problemen aanpakken

G. Meershoek & M. Krommendijk, IPIT, Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2008

44. De frontlinie van opsporing en handhaving. Stelselmatige bedreigingen door burgers als contrastrategie

M.J.G. Jacobs, M.Y. Bruinsma & J.W.M.J. van Poppel, IVA Tilburg, 2008

45a. 'Kracht van meer dan geringe betekenis'. Deel A: Politiegeweld in de basispolitiezorg

R. Bleijendaal, J. Naeyé, P. Chattellon & G. Drenth, Vrije Universiteit, Amsterdam, 2008

45b. 'Kracht van meer dan geringe betekenis'. Deel B: Sturing en toetsing van de politieke geweldsbevoegdheid

G. Drenth, J. Naeyé & R. Bleijendaal, Vrije Universiteit, Amsterdam, 2008

45c. Agressie en geweld tegen politiemensen. Beledigen, bedreigen, tegenwerken en vechten

J. Naeyé & R. Bleijendaal, Vrije Universiteit, Amsterdam, 2008

45d. Belediging en bedreiging van politiemensen

J. Naeyé, m.m.v. M. Bakker & C. Grijzen, Vrije Universiteit Amsterdam, 2009

45e. Uitgangspunten voor politieoptreden in agressie- en geweldssituaties

J. Naeyé, Vrije Universiteit Amsterdam, 2010

46. Wijkagenten en hun dagelijks werk. Een onderzoek naar de uitvoering van gebiedsgebonden politiewerk

J. Terpstra, 2008

47. Bijzonder zijn ze allemaal! Vergelijkend onderzoek naar reguliere en bijzondere opsporing

W. Faber, A.A.A. van Nunen & C. la Roi, Faber Organisatievernieuwing, Oss, 2009

48. Gouden bergen. Een verkennend onderzoek naar Nigeriaanse 419-fraude: achtergronden, daderkenmerken en aanpak

Y.M.M. Schoenmakers, E. de Vries Robbé & A.Ph. van Wijk, Politieacademie, Apeldoorn/Bureau Beke, Arnhem, 2009

49. Het betwiste politiestel. Een vergelijkend onderzoek naar de ontwikkeling van het politiestel in Nederland, België, Denemarken, Duitsland, Engeland & Wales

Cachet, A. van Sluis, Th. Jochoms, A. Sey & A. Ringeling, Erasmus Universiteit Rotterdam/Politieacademie, Apeldoorn/Korps landelijke politiediensten, Driebergen, 2009

50. Leven met bedreiging. Achtergronden bij aangiften van bedreiging van burgers
Bieleman, W.J.M. de Haan, J.A. Nijboer & N. Tromp, Intraval & Rijksuniversiteit Groningen, 2010

51a. Het publieke belang bij private preventie. Een economische analyse van inbraakpreventiebeleid

B.A. Vollaard, TILEC/Universiteit van Tilburg, 2009

51b. Het effect van langdurige opsluiting van veelplegers op de maatschappelijke veiligheid

B.A. Vollaard, TILEC/Universiteit van Tilburg, 2010

52. Lokale politiek over politie

T.B.W.M. van der Torre-Eilert, H. Bergsma & M.J. van Duin, met medewerking van R. Eilert, LokaleZaken, Rotterdam, 2010

53a. Trainen onder stress. Effecten op de schietvaardigheid van politieambtenaren

R.R.D. Oudejans, A. Nieuwenhuys & G.P.T. Willemsen, Vrije Universiteit Amsterdam, 2010

53b. Schieten of niet schieten? Effecten van stress op schietbeslissingen van politieambtenaren

Nieuwenhuys, G.P.T. Willemsen & R.R.D. Oudejans, Vrije Universiteit, Amsterdam, 2012

53c. Politievaardigheden onder stress. Het optimaliseren van aanhouding en zelfverdediging in de praktijk

P.G. Renden, A. Nieuwenhuys, G.P.T. Willemsen & R.R.D. Oudejans, Vrije Universiteit, Amsterdam, 2015

53d. Effectief omgaan met acute stress. Effecten van aanleg en trainingservaring op de schietprestatie onder druk

Landman, A. Nieuwenhuys & R.R.D. Oudejans, Vrije Universiteit, Amsterdam, 2015

54. Politie en publiek. Een onderzoek naar de communicatievormen tussen burgers en blauw

H.J.G. Beunders, M.D. Abraham, A.G. van Dijk & A.J.E. van Hoek, DSP-groep, Amsterdam/Erasmus Universiteit, Rotterdam, 2011

55. Managing collective violence around public events: an international comparison

O.M.J. Adang with cooperation from: S.E. Bierman, E.B. Brown, J. Dietermann, C. Putz, M. Schreiber, R. van der Wal, J. Zeitner, Police Science & Research Programme, Apeldoorn, 2011

56. Stads- en regioscan in de grootste Brabantse gemeenten. De achtergronden van onveilige GVI-scores

B.M.W.A. Beke, E.J. van der Torre, M.J. van Duin, COT, Den Haag; LokaleZaken, Rotterdam & Beke Advies, Arnhem, 2011

57. De mythe ontrafeld? Wat we weten over een goed politieleiderschap

W. Landman, M. Brussen & F. van der Laan, Twynstra Gudde, Amersfoort, 2011

58. Proactief handhaven en gelijk behandelen

J. Svensson, H. Sollie & S. Saharso, Vakgroep Maatschappelijke Risico's en Veiligheid, Institute of Governance Studies, Universiteit Twente, Enschede, 2011

59a. De sterkte van de arm: feiten en mythes

J.H. Haagsma, T.M. Rumke, I. Smits, E. van der Veer & C.J. Wiebrens, Andersson Elffers Felix, Utrecht, 2012

59b. Blauw, hier en daar. Onderzoek naar de sterkte van de politie in Nederland, België, Denemarken, Engeland & Wales en Nordrhein-Westfalen

J.H. Haagsma, I. Smits, H. Waarsing & C.J. Wiebrens, Andersson Elffers Felix, Utrecht, 2012

60. De nachtdienst 'verlicht'

M.C.M. Gordijn, Rijksuniversiteit Groningen, 2012

61. Opsporing Verzocht. Een quasi-experimentele studie naar de bijdrage van het programma Opsporing Verzocht aan de oplossing van delicten

J.G. van Erp, F. van Gastel & H.D. Webbink, Erasmus Universiteit, Rotterdam, 2012

62. Jeugdige zedendelinquenten en recidive. Een onderzoek bij jeugdige zedendelinquenten naar de voorspellende waarde van psychiatrische stoornissen en psychosociale problemen voor (zedend)recidive

Boonmann, L.M.C. Nauta-Jansen, L.A. 't Hart-Kerkhoffs, Th.A.H. Doreleijers & R.R.J.M. Vermeiren, VUmc De Bascule, Duivendrecht, 2012

63. Hoe een angstaas een jokkebrok herkent

J. Jolij, Rijksuniversiteit Groningen, 2012

64. Politie en sociale media. Van hype naar onderbouwde keuzen

Meijer, S. Grimmelhuijsen, D. Fictorie, M. Thaens, P. Siep, Universiteit Utrecht, Center for Public Innovation, Rotterdam, 2013

65. Wapengebruik. Van inzicht in modus operandi naar een effectieve aanpak

M.S. de Vries, Universiteit Twente, Enschede, 2013

66. Politieverhalen. Een etnografie van een belangrijk aspect van politieculturen

M.J. van Hulst, Tilburg University, Tilburg, 2013

67. Recherchebazen. Een empirisch onderzoek naar justitieel politieleiderschap

E.J. van der Torre, M.J. van Duin & E. Bervoets, LokaleZaken, Rotterdam, 2013

68. Driehoeken: overleg en verhoudingen. Van lokaal tot nationaal

E.J. van der Torre & T.B.W.M. van der Torre-Eilert, m.m.v. E. Bervoets & D. Keijzer, LokaleZaken, Rotterdam, 2013

69. Overvallen vanuit daderperspectief. Situationele aspecten van gewelddadige, niet-gewelddadige en afgeblazen overvallen

W. Bernasco, M.R. Lindegaard & S. Jacques, NSCR, Amsterdam, 2013

70. Geweld tegen de politie. De rol van mentale processen van de politieambtenaar

L. van Reemst, T. Fischer & B. Zwirs, Erasmus Universiteit, Rotterdam, 2013

71. Vertrouwen in de politie: trends en verklaringen

L. van der Veer, A. van Sluis, S. Van de Walle & A. Ringeling, Erasmus Universiteit, Rotterdam, 2013

72. Mobiel banditisme. Oost- en Centraal-Europese rondtrekkende criminele groepen in Nederland

Siegel, i.s.m. R. Koenraadt, D. Lyubenova, N. Sovre & A. Troscianczuk, Universiteit Utrecht, 2013

73. De ontwikkeling van de criminaliteit van Rotterdamse autochtone en allochtone jongeren van 12 tot 18 jaar. De rol van achterstanden, ouders, normen en vrienden

F.M.H.M. Driessen, F. Duursma & J. Broekhuizen, Bureau Driessen, Utrecht, 2014

74. Speciaal blauw. Verschijningsvormen en overwegingen van specialisatie en despecialisatie binnen de Nederlandse politieorganisatie

R.J. Morée, W. Landman & A.C. Bos, Twynstra Gudde, Amersfoort, 2014

75. Gevangene van het verleden. Crisissituaties na de terugkeer van zedendelinquenten in de samenleving

M.H. Boone, H.G. van de Bunt & D. Spiegel, m.m.v. K. van de Ven, Erasmus Universiteit, Rotterdam, Universiteit Utrecht, 2014

76. Brandstichters onder vuur. Een empirisch onderzoek naar zaken van brandstichting en hun daders

L. Dalhuisen & F. Koenraadt, Universiteit Utrecht, 2014

77. Van stadswacht naar nieuwe gemeentepolitie? Gemeentelijk toezicht en handhaving in de openbare ruimte

T. Eikenaar & B. van Stokkom, Radboud Universiteit, Nijmegen, 2014

78. Politie mensen over het strafrecht

J. Kort, M.I. Fedorova & J.B. Terpstra, Radboud Universiteit, Nijmegen, 2014

79. Kijken, luisteren, lezen. De invloed van beeld, geluid en schrift op het oordeel over verdachtenverhooren

M. Malsch, R. Kranendonk, J. de Keijser, H. Elffers, M. Konter & M. de Boer, NSCR, Amsterdam, 2015

80. De mentale gesteldheid van de familierechercheur. Een onderzoek naar werkgerelateerde stress en secundaire posttraumatische groei binnen een bijzondere groep politieambtenaren

L.J.A. Bollen, M.C. Saan, M.J.J. Kunst, B.W.C. Zwirs & K.F. Kuijpers, Universiteit Leiden, 2015

81. Na de vrijlating. Een exploratieve studie naar recidive en re-integratie van jihadistische exgedetineerden

D.J. Weggemans & B.A. de Graaf, Universiteit Leiden, Universiteit Utrecht, 2015

82. Dat heeft iemand anders gedaan! Een studie naar slachtofferschap en modus operandi van identiteitsfraude in Nederland

L. Paulissen & J. van Wilsem, Universiteit Leiden, 2015

83. Demonstratieve kampementen

Roorda, Rijksuniversiteit Groningen, 2015

84. Private ordebewaarders bij betogingen

Roorda, Rijksuniversiteit Groningen, 2015

85. Spelen met weerbaarheid. Belemmerende patronen en doorbrekende handelingsperspectieven bij het ontwikkelen van basisteams

W. Landman, R. Kouwenhoven & M. Brussen, Twynstra Gudde, Amersfoort, 2015

86. 'Onnodige' bureaucratie binnen het basispolitiewerk. Onderzoek naar de achtergronden van een hardnekkig verschijnsel

J. Kort & J.B. Terpstra, Radboud Universiteit Nijmegen, 2015

87. Politie en GHB-problematiek op het platteland

T. Nabben & D.J. Korf, Universiteit van Amsterdam, 2016

88. Basisteams in de Nationale Politie. Organisatie, taakuitvoering en gebiedsgebonden werk

J. Terpstra, I. van Duijneveldt, T. Eikenaar, T. Havinga & B. van Stokkom, Radboud Universiteit Nijmegen, 2016

89. Samen of apart. De invloed van overleg tussen agenten bij het opstellen van het proces-verbaal

Vredeveldt, L. Kesteloo & P.J. van Koppen, Vrije Universiteit Amsterdam, 2016

90. Overvallen in beeld. Gedrag van daders, slachtoffers en omstanders

M.R. Lindegaard, W. Bernasco & T. de Vries, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, Amsterdam, 2016

91. Boeven vangen. Een onderzoek naar proactief politieoptreden

W. Landman & L. Kleijer-Kool, Twynstra Gudde, Amersfoort, 2016

92. VVC onder de aandacht. Een onderzoek naar ZSM en de gevolgen voor het politiewerk

R. Salet & J. Terpstra, m.m.v. P. Frielink, Radboud Universiteit Nijmegen, 2017

93. De mogelijke meerwaarde van bodycams voor politiewerk. Een internationaal literatuuronderzoek

S. Flight, Sander Flight Onderzoek & Advies, Amsterdam, 2017

93A Focus. Evaluatie pilot bodycams Politie Eenheid Amsterdam 2017-2018

S. Flight, Sander Flight Onderzoek & Advies, Amsterdam, 2019

93b Evaluatie bodycams Landelijke Eenheid; Proeftuin bodycams Dienst Infrastructuur 2018

S. Flight, Sander Flight Onderzoek & Advies, Amsterdam, 2019

94. Criminele families in Noord-Brabant. Een verkenning van generatie-effecten in de georganiseerde misdaad

H. Moors & T. Spapens, EMMA, Den Haag; Tilburg University, Tilburg, 2017

94a. Intervenieren in criminele families

Boer, R. Ceulen, H. Moors, T. Spapens, EMMA/Tilburg University, 2020

95. Effectiviteit van het verdachtenverhoor. Een veldstudie naar de relatie tussen verhoortechnieken, de verklaring van verdachten en de aanwezigheid van de advocaat in zware zaken

W.J. Verhoeven & E. Duinhof, Erasmus Universiteit, Rotterdam, 2017

96. Van meerdere markten thuis? Overlap in markten van zware en georganiseerde misdaad en de consequenties voor de opsporing

T. Spapens, m.m.v. M. Bruinsma, Tilburg University, Tilburg, 2017

97. Horen, zien en zwijgen. Opsporing in dorpen en stadsbuurten met een gesloten leefgemeenschap

Bervoets & M. Bruinsma, Bureau Bervoets, Amersfoort, 2017

98. Geweld tegen hulpverleners in de psychiatrie. Aard, omvang en aangifte bij de politie

J.M. Harte, I. van Houwelingen & M.E. van Leeuwen, Vrije Universiteit, Amsterdam, 2017

99. Geëiste en opgelegde straffen bij de strafrechtelijke afhandeling van georganiseerde criminaliteit. Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit

C.G. van Wingerde & H.G. van de Bunt, Erasmus School of Law, Rotterdam, 2017

100. Doorgroeiers in de misdaad. De criminele carrières en achtergrondkenmerken van jonge daders van een zwaar delict

V. van Koppen, V. van der Geest & E.R. Kleemans, Vrije Universiteit, Amsterdam, 2017

101. Profielen van Nederlandse outlawbikers en Nederlandse outlawbikerclubs

Blokland, W. van der Leest & M. Soudijn (m.m.v. E. Kleinheerenbrink & I. van Die), Leiden Law School, Leiden, 2017

102. Verdachten van terrorisme in beeld. Achtergrondkenmerken, ‘triggers’ en eerdere politiecontacten

Thijs, E. Rodermond & F. Weerman, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, Amsterdam, 2018

103. Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld

W. Bantema, S.M.A. Twickler, S.A.J. Munneke, M. Duchateau & W.Ph. Stol, NHL Stenden Hogeschool, Leeuwarden; Rijksuniversiteit Groningen, Groningen, 2018

104. Een bittere pil. Het fenomeen en de aanpak van illegale medicijnenhandel

van Leiden, A. Lenders & H. Ferwerda, Bureau Beke, Arnhem, 2018

105. Vastzitten zonder straf. Over verzekeringsstellingen en schadevergoedingen op basis van artikel 89 Sv

P. Kruize & P. Gruter, Bureau Ateno, Amsterdam, 2018

106. ‘Ik hou het hier wel uit, hoor’. Mentale weerbaarheid binnen de districtsrecherche

H. Sollie, Twynstra Gudde, Amersfoort, 2018

107. Bestuurlijke bevoegdheden, politie en de lokale aanpak van onveiligheid

R. Salet & H. Sackers, Radboud Universiteit, Nijmegen, 2019

108. Politie en actief burgerschap: een veilig verbond? Een onderzoek naar samenwerking, controle en (neven)effecten

V. Lub & T. de Leeuw, m.m.v. A.S. Leerkes & R.J. Kleinhans, Bureau voor Sociale Argumentatie, Rotterdam; Erasmus Universiteit, Rotterdam; Bureau voor Maatschappij, Veiligheid & Deviantie, Rotterdam, 2019

109. Wijkagenten en veranderingen in hun dagelijks werk. Verslag van een onderzoek

J. Terpstra, m.m.v. A. Evers, Radboud Universiteit, Nijmegen, 2019

110. Naar een efficiëntere noodhulp? Een verkennend actieonderzoek

Scholtens & I. Helsloot, m.m.v. S. Kraaijenbrink, J. Vlagsma, M. Jürgens, D. Mouris & M. Eising, Crisislab, Renswoude, 2019

111. Bestrijding van Outlaw Motorcycle Gangs. Een rechtsvergelijkende studie naar de aanpak van onrechtmatige organisaties in rechtsstatelijk perspectief.

J. Koornstra, B. Roorda, M. Vols & J.G. Brouwer, Rijksuniversiteit Groningen, 2019

112. Politiestraatgezag en (on)gehoorzaam burgergedrag

Scholtens, M. Helsloot, I. Helsloot, Crisislab, Renswoude, 2019

113. Verkeershandhaving op Nederlandse autosnelwegen; Evaluatie van de werkwijze van het Team EVT, de effecten en de acceptatie van politiecontroles

Ch. Goldenbeld, A. Stelling-Kończak, S. van der Kint, SWOV, Den Haag, 2019

114. Virtual reality als onderzoeksmethode om inbrekers te doorgronden

van Sintemaartensdijk, J.L. van Gelder, P.A.M. van Lange, M. Otte, J.W. van Prooijen, Vrije Universiteit Amsterdam, 2019

115. Wanneer blaffende honden bijten. Een vergelijking tussen fataal en niet-fataal huiselijk geweld

P. Aarten, C. Boelema Robertus, L. Alink, M. Liem, Universiteit Leiden, 2020

116. Kijk naar het systeem. Begrijpen en beïnvloeden van opsporingspraktijken

W. Landman, R. Kouwenhoven, M. Brussen, Twynstra Gudde, Amersfoort, 2020

117. Verbeelding in de verhoorkamer. De invloed van het gebruik van beeldmateriaal in het verhoor op verhoortechnieken en proceshouding

W.J. Verhoeven, G. Vanderveen, L. van Dillen, S. Kruit, Erasmus Universiteit, Universiteit Leiden, 2020

118. Met gepast geweld. Politiegeweld in Nederland in 2016

M. Kuin, F. Kriek, J. Timmer, m.m.v. Y. Bleeker en E. Verbeek, Regioplan, Amsterdam en Vrije Universiteit Amsterdam, 2020

119. De rol van bodycambeelden in de opsporing en bewijsvoering

Vredeveltdt, L. Kesteloo, A. Hildebrandt, Vrije Universiteit Amsterdam, 2020

120. Slachtoffer van onlinecriminaliteit, wat nu?

S.G.A. van de Weijer, E.R. Leukfeldt, S. van der Zee, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, Amsterdam, 2020

121. Een alternatief voor jeugdige hackers? Plan- en procesevaluatie van Hack_Right

J.A.M. Schiks, M.S. van 't Hoff-de Goede, E.R. Leukfeldt. De Haagse Hogeschool, Centre of Expertise Cybersecurity, Den Haag; Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, Amsterdam, 2021

122. Criminaliteit en huiselijk geweld: twee kanten van dezelfde medaille? De relatie tussen criminaliteit en huiselijk geweld

S. van Deuren, J. Kroese, M. van Dijk, V. Eichelsheim, A. Blokland, S. van de Weijer. Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, Amsterdam, 2021

123. Oververtegenwoordiging verder ontcijferd. Een kwantitatief onderzoek naar sociale verschillen in verdenkingskans en zelfgerapporteerd crimineel gedrag onder jongeren in Nederland

W. Bezemer, A. Leerkes. Erasmus Universiteit, Rotterdam, 2021

124. Gebiedsgebonden politiewerk in ontwikkeling. Onderzoek naar basisteams in een digitale en superdiverse samenleving

J. Terpstra, R. Salet, I. van Duijneveldt, T. Havinga, Radboud Universiteit 2021

125. Slimme(re) opsporing, Een verslag van de ontwikkeling en pogingen tot implementatie van een handreiking voor efficiënte opsporing door de politie

Helsloot, P. van Lochem, C. Kijne, Crisislab, Renswoude 2022

126. Politiewerk op het web. Een verkennend onderzoek naar online gegevensvergaring door de politie

Wouter Landman, Sanne Groothuis, Twijnstra Gudde, Amersfoort, 2022

127. Living apart together? Publiek-private relaties in de bestrijding van interne financieel-economische criminaliteit

Dr. C.A. Meerts, Prof. dr. mr. W. Huisman, Prof. dr. E.R. Kleemans, m.m.v. M. van Straten, MSc, VU-Universiteit, Amsterdam, 2022

128. Politiestraatwerk onder corona. Verbinding tussen landelijk beleid en lokale gemeenschap

Wouter Stol, Litska Strikwerda, Saskia Westers, Wendy Schreurs, NHL Stenden Hogeschool, 2023

129. Moreel kompas

Anton van Wijk, Marjan Olfers, Mark van Vugt, Ard Barends, Juno van Esseveldt, Den Haag, 2023

130. Liquidaties in Nederland. Ontwikkelingen & achtergronden van schutters en andere betrokkenen

Sheila Adjiembaks, Frank Boerman, Robby Roks, Ewout Stoffers, RIEC Midden-Nederland, onderzoeksbureau ESSA Research, Erasmus Universiteit Rotterdam, Landelijke Eenheid Nationale Politie, 2023

131. Goed-fout. Criminele verdringing in legale (ketens)processen; een verkennend onderzoek met voorbeelden uit de hout-, afval- en fruitketen

Bureau Bervoets, Eric Bervoets, Mirjam Corsel, Tim Boekhout van Solinge, m.m.v. Sabine Hellemons, maart 2024

132. Van opsporing tot bewijsvoering. Plaats delict-onderzoek voor de hele strafrechtketen

M. de Gruijter, A.J. Loeve, C.J. de Poot en M. Zuidberg, april 2024

133. Ongekend. Een onderzoek naar de impact van dreiging vanuit georganiseerde criminaliteit op politiewerk

S. Mehlbaum, J. Broekhuizen, K. van den Akker, m.m.v. S. van Ruiten, T. te Beest en J. de Boer, Halfweg, mei 2024

134. Criminele familienetwerken. Subculturele factoren en clan-achtige kenmerken

T. Spapens, H. Moors, L. de Veen, S. van Nimwegen, R. Bredo, S. Vriends, C. Jacobs, Tilburg University, EMMA (Experts in Media en Maatschappij, Nationale politie), oktober 2024

135. Polarisation, escalatie en alledaagse vrede. Aandachtswijken onder een vergrootglas

L.A. Slooter, Universiteit Utrecht, Politie & Wetenschap, januari 2025

136. Gerichtte invitatie tijdens het kindverhoor. De meerwaarde en timing van gerichtte invitatie in het verkrijgen van een uitgebreide verklaring van kinderen

D.J.H. Smeets, L.R.A. Alink, m.m.v. K. Dekens, R. Haak, I. Rispens en J. van der Sleen, Universiteit Leiden, 2025

137. Politiestraatwerk en informatiegebruik. Een longitudinale studie (1991-2023) over gevolgen van digitalisering

W. Stol, L. Strikwerda, J. Jansen, W. Schreurs, mei 2025

138. Herinneringen aan misbruik van langer geleden. De betrouwbaarheid van (hervonden) herinneringen aan misbruik

M. ter Beek, H. Otgaar, B. Verschuere, september 2025

139. Politieagent worden. Socialiseren in de wereld van de politie

W. Landman, H. Solle, m.m.v. V. König, maart 2026

140. Van mens tot mens. De 'soevereinen-beweging' in Nederland

L. de Veen, M. van Rees-van Bakkum, H. Moors, juli 2026

141. Versterking van de politiecapaciteit in de Europese modellen voor de handhaving van milieudelicten. Strategische lessen voor de Nederlandse politie

A. Matczak, juli 2026

141. Police Capacity Building in European Models of Environmental Crime Enforcement. Strategic Lessons for the Dutch Police

A. Matczak, juli 2026