POLITIE & Wetenschap

Cybercriminele jeugdgroepen

Joeri Loggen
Sander Veenstra
Rutger Leukfeldt

DE HAAGSE HOGESCHOOL
RIEC Noord-Nederland

Cybercriminele jeugdgroepen in een gedigitaliseerde samenleving

Cybercriminele jeugdgroepen

Een onderzoek naar het ontstaan, de groei en de aanpak van criminele jeugdgroepen in een gedigitaliseerde samenleving

Joeri Loggen MSc
Sander Veenstra MSc
Prof.dr. Rutger Leukfeldt

Lefebvre Sdu, 2026

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

Omslagontwerp: Imago Mediabuilders
Afbeelding omslag: Joeri Loggen en ChatGPT

ISBN: 9789012411530
NUR: 600, 680, 125

Inhoudsopgave

Voorwoord

Voor je ligt het resultaat van een onderzoek naar jeugdgroepen die betrokken zijn bij cybercrime in Noord-Nederland. In Nederland wordt cybercrime in toenemende mate gepleegd door jongeren en jongvolwassenen die in groepsverband opereren. De schade die zij veroorzaken loopt jaarlijks op tot tientallen miljoenen euro's. Naast financiële schade ervaren slachtoffers ook emotionele gevolgen en bovendien kan cybercrime fungeren als opstap naar delicten met een nog grotere maatschappelijke impact.
Een effectieve identificatie en aanpak van deze groepen is daarom van groot belang. Toch ontbreekt het aan wetenschappelijke kennis over de kenmerken van cybercriminele jeugdgroepen en over hoe deze groepen kunnen worden gesignaleerd en aangepakt. Bovendien blijkt uit de praktijk dat gemeenten, die de regie voeren op de aanpak van (cyber)criminele jeugdgroepen, grote moeite hebben met zowel de identificatie als de aanpak van deze groepen.
Dit onderzoek beoogt vanuit wetenschappelijk perspectief aanknopingspunten te bieden voor beleid en praktijk. Tegelijkertijd is het doel inzicht te krijgen in de praktische invulling van de aanpak, waar knelpunten liggen en waar ruimte is voor verbetering.
Dit onderzoek is tot stand gekomen dankzij een intensieve samenwerking tussen de onderzoekers en professionals uit het werkveld. Wij willen onze consortiumpartners dan ook hartelijk danken voor hun betrokkenheid bij het opstellen van het onderzoeksvoorstel, het meedenken over de richting van het onderzoek en hun inzet bij het werven van respondenten binnen hun netwerk. Specifiek zijn dit het Openbaar Ministerie (OM), arrondissementsparket Noord-Nederland, de politie, eenheid Noord-Nederland, het RIEC Noord-Nederland, de gemeenten Leeuwarden, Groningen en Smallingerland, de Nederlandse Vereniging van Banken en Vereniging COIN.
Ook willen we alle respondenten bedanken die tijd hebben vrijgemaakt om hun expertise op het gebied van (cyber)criminele jeugdgroepen met ons te delen. Daarnaast willen we de politiemedewerkers in Noord-Nederland bedanken voor het extraheren en beschikbaar stellen van relevante registraties, die een belangrijk onderdeel vormen binnen dit onderzoek. En tot slot bedanken we onze collega-onderzoekers van De Haagse Hogeschool voor hun kritische blik, hun inhoudelijke bijdragen en het meedenken gedurende het hele onderzoeksproces.

Joeri Loggen
Sander Veenstra
Rutger Leukfeldt

Samenvatting

Aanleiding

Veiligheidspartners in Noord-Nederland geven aan moeite te hebben met (1) het in kaart brengen en (2) aanpakken van jongeren en jeugdgroepen betrokken bij cybercriminele activiteiten, en (3) behoefte te hebben aan meer kennis over dit onderwerp: zowel over het fenomeen zelf als over de manieren om dergelijke groepen te identificeren en effectief aan te pakken.

Hoewel actuele cijfers over het aantal criminele jeugdgroepen in Nederland ontbreken, lijkt het verkrijgen van zicht op deze groepen de afgelopen jaren lastiger te zijn geworden (NJI, 2023). Het aantal 'problematische jeugdgroepen' in Nederland dat tussen 2009 en 2014 werd gemonitord, daalde in die periode van 1760 naar 623, een daling van 65%. Ook in Noord-Nederland was die trend zichtbaar (Ferwerda & Van Ham, 2014). Deze ontwikkeling kan erop duiden dat jeugdgroepen minder goed in beeld komen, eerder dan dat zij daadwerkelijk verdwijnen.

Mogelijk is er sprake van een verschuiving van traditionele criminaliteit naar cybercrime. Daarvoor zijn aanwijzingen voorhanden. Traditionele criminaliteit onder jongeren neemt af, terwijl zij zich in toenemende mate schuldig maken aan allerlei vormen van cybercrime (Leukfeldt & Roks, 2021; WODC, 2021). Dit is problematisch om drie redenen.

Allereerst is er beperkt zicht op cybercriminele jeugdgroepen; zij staan nog nauwelijks op de radar van lokale veiligheidscoalities – lokale samenwerkingen tussen de politie, het Openbaar Ministerie (OM) en hulp- en zorgorganisaties, onder regie van de gemeente. Dergelijke groepen kunnen niet worden aangepakt als zij niet in beeld zijn. Ten tweede is er nog weinig bekend over het fenomeen van cybercriminele jeugdgroepen zelf, zoals hun kenmerken en met welke delicten ze zich bezighouden. Kennis hierover is essentieel voor de ontwikkeling van effectieve aanpakken en interventies. Ten derde is de bestaande aanpak van jeugdgroepen vooralsnog traditioneel georiënteerd. Een aanpak- en interventiestrategie die specifiek is toegespitst op cybercrime ontbreekt vooralsnog.

Tegelijkertijd blijkt uit eerder onderzoek dat cybercriminele (jeugd)groepen sterk lokaal verankerd zijn, waardoor juist lokale actoren een sleutelrol spelen in de aanpak ervan (Leukfeldt et al., 2020). Diezelfde lokale veiligheidspartners lijken echter minder goed zicht te hebben op cybercriminele jeugdgroepen. Hierdoor wordt in de praktijk sterk geleund op (experts van) de politie, terwijl de politie deze groepen niet alléén kan bestrijden. Een integrale aanpak is noodzakelijk om zicht te krijgen op de aanpak van cybercrime (Jewkes & Yar, 2012; Veenstra et al., 2013).

In dit onderzoek richten we ons specifiek op Noord-Nederland (de provincies Drenthe, Friesland en Groningen), omdat meerdere gemeenten uit deze provincies aangaven moeite te hebben met het in kaart brengen en aanpakken van cybercriminele activiteiten van jeugdgroepen en omdat zij behoefte hadden aan meer kennis op dit gebied.

Onderzoeksvragen
Het onderzoek volgt drie sporen. Allereerst richten we ons op (cyber)criminele jeugdgroepen die bekend zijn bij lokale veiligheidscoalities (spoor 1). Ten tweede onderzoeken we in hoeverre in Noord-Nederland sprake is van bij lokale veiligheidscoalities nog onbekende jeugdgroepen die zich toeleggen op cybercrime (spoor 2). Het daarmee verkregen inzicht in cybercriminele jeugdgroepen is een vereiste voor de aanpak ervan. Nadat er zicht is verkregen op die groepen, rijst dus logischerwijs de vraag wat mogelijkheden zijn voor de (integrale) aanpak daarvan. In spoor 3 staat daarom het ontwikkelen van handreikingen voor een dergelijke integrale aanpak centraal. Per spoor zijn vragen vastgesteld die richting geven aan het onderzoek.

Spoor 1: bekende jeugdgroepen
Het eerste spoor richt zich op (cyber)criminele jeugdgroepen die bekend zijn bij lokale veiligheidscoalities. Binnen spoor 1 staan de volgende onderzoeksvragen centraal:
1.1 Welke (cyber)criminele jeugdgroepen zijn bekend bij lokale veiligheidscoalities binnen Noord-Nederland?
1.2 Wat zijn de kenmerken van bekende (cyber)criminele jeugdgroepen, zoals omvang, rolverdeling, hiërarchie, banden tussen leden, en het gebruik van facilitators en online en offline ontmoetingsplaatsen?
1.3 Wat zijn de demografische kenmerken en criminele carrières van individuele leden van bekende cybercriminele jeugdgroepen?
1.4 Wat zijn de aard en modus operandi van de traditionele en/of cybercriminele delicten waarmee bekende cybercriminele jeugdgroepen zich bezighouden, en hoe ziet de verwevenheid tussen traditionele delicten en cyberdelicten eruit?

Spoor 2: onbekende jeugdgroepen
Binnen het tweede spoor staan cybercriminele jeugdgroepen centraal die bij lokale veiligheidscoalities nog onbekend zijn. De volgende vragen geven richting aan dit onderzoeksspoor:
2.1 In hoeverre zijn er bij lokale veiligheidscoalities onbekende, cybercriminele jeugdgroepen actief binnen Noord-Nederland?
2.2 Wat zijn de kenmerken van nog onbekende cybercriminele jeugdgroepen, zoals omvang, rolverdeling, hiërarchie, banden tussen leden, en gebruik van facilitators en online en offline ontmoetingsplaatsen?
2.3 Wat zijn de demografische kenmerken en criminele carrières van individuele leden van nog onbekende cybercriminele jeugdgroepen?

2.4 Wat zijn de aard en modus operandi van de traditionele en/of cybercriminele delicten waarmee nog onbekende cybercriminele jeugdgroepen zich bezighouden, en hoe ziet de verwevenheid tussen traditionele delicten en cyberdelicten eruit?

Spoor 3: integrale aanpak
Binnen spoor 3 staat het ontwikkelen van handreikingen voor de (integrale) aanpak van cybercriminele jeugdgroepen centraal. Onderstaande onderzoeksvragen vormen voor dit spoor het vertrekpunt:
3.1 In hoeverre hebben actoren die betrokken zijn bij de (integrale) aanpak van criminele jeugdgroepen in Noord-Nederland zicht op de onder onderzoeksvraag 1 en 2 geïdentificeerde cybercriminele groepen?
3.2 In hoeverre en op welke wijze kan de integrale aanpak van cybercriminele jeugdgroepen worden bevorderd?

- Wat houdt de (integrale) aanpak van cybercriminele jeugdgroepen in? Welke actor (mono) of actoren (integraal) zijn betrokken?
- In hoeverre is de (integrale) aanpak delictspecifiek en in welke mate volstaat deze voor de aanpak van cybercriminele jeugdgroepen?
- Wat zijn verbeterpunten in de huidige aanpak van cybercriminele jeugdgroepen?
- Wat zijn best practices uit de (integrale) aanpak van cybercriminele jeugdgroepen?
- In hoeverre kunnen interventies die zich richten op jeugdige cyberdaders bijdragen aan de aanpak van cybercriminele jeugdgroepen (zie bijvoorbeeld Oosterwijk & Fischer, 2017)?

Methoden
In dit onderzoek hebben we vier onderzoeksmethoden toegepast: (1) een literatuurstudie; (2) expertinterviews; (3) zaakreconstructies; en (4) een analyse van politieregistraties.

Literatuurstudie
Allereerst hebben we een non-systematische narratieve literatuurstudie uitgevoerd, waarbij we hebben gezocht naar relevante literatuur in de gangbare wetenschappelijke databases (ACM Digital Library, EBSCOhost, ProQuest, Scopus, Web of Science, Wiley Online Library). Daarbij hebben we ons gericht op zowel kwalitatieve als kwantitatieve Nederlandstalige en Engelstalige academische literatuur. De literatuurstudie diende drie doelen:

1. het krijgen van meer inzicht in de verschillende aspecten van (cyber)criminele groepen, zoals de ontstaans- en groeiprocessen, de structuur en samenstelling van deze groepen, en hun (cyber)criminele activiteiten;
2. het vormen van de inhoudelijke basis voor de ontwikkeling van de topiclijst voor de expertinterviews, en de analyse van deze interviews en die van de zaakreconstructies en politieregistraties;
3. het identificeren van best practices voor de integrale aanpak van cybercriminele jeugdgroepen.

Expertinterviews
Daarnaast hebben we 39 praktijkprofessionals geïnterviewd die betrokken waren bij het onderzoeken en/of de aanpak van (cyber)criminele jeugdgroepen. Deze waren werkzaam bij de Nederlandse politie, gemeenten, het OM, het jongerenwerk, het onderwijs, banken en telecomproviders. De interviews hadden twee doelen:
1. inzicht krijgen in de bij lokale veiligheidscoalities bekende en onbekende cybercriminele jeugdgroepen;
2. inzicht krijgen in de bestaande aanpakken, best practices en verbeterpunten.

De interviews richtten zich op de kenmerken van traditionele en cybercriminele jeugdgroepen die (on)bekend zijn bij lokale veiligheidscoalities en de (integrale) aanpak daarvan.

Zaakreconstructies
Op basis van documentanalyses en verdiepende interviews hebben we vijf casussen rondom cybercriminele jeugdgroepen onderzocht, die we kregen via het Regionaal Informatie- en Expertisecentrum (RIEC), de districtsrecherche en het OM. De RIEC-casus is geanalyseerd aan de hand van een publicatie in het *Tijdschrift voor Veiligheid*, de overige vier via rechterlijke uitspraken, ook wel European Case Law Identifiers (ECLI's) genoemd. De zaakreconstructies zijn gecodeerd aan de hand van thematische analyse, waarbij we ons hebben gericht op de kenmerken van de groepen en hun leden, de gebruikte modus operandi en de (integrale) aanpak. Aanvullend hierop hebben we interviews gehouden met professionals die waren betrokken bij deze opsporingsonderzoeken, om zo informatie te verkrijgen die niet in de ECLI's terug te vinden was.

Politieregistraties
De laatste onderzoeksmethode betrof het analyseren van politieregistraties, om zo verdiepend inzicht te krijgen in de verwevenheid tussen traditionele jeugdgroepen en cybercriminele activiteiten, en in eventuele nieuwe cybercriminele jeugdgroepen. Allereerst hebben we aan alle 40 gemeenten in Noord-Nederland gevraagd of zij jeugdgroepen in beeld hadden en of ze identificerende gegevens konden delen. Van de 40 gemeenten reageerden er 25. Daarvan hadden 10 gemeenten in totaal 13 jeugdgroepen in beeld, waarvan 9 gemeenten de identificerende gegevens deelden. Deze gegevens zijn gekoppeld aan politie-informatie om in kaart te brengen in hoeverre de bij gemeenten bekende jongeren ook bij de politie bekend waren als verdachte van cybercrime.
Daarnaast hebben we cybercrimeregistraties over de periode van één jaar geanalyseerd om te onderzoeken in hoeverre in Noord-Nederland ook 'nieuwe' en bij lokale veiligheidscoalities nog onbekende jeugdige cyberdaders actief waren in groepsverband. De periode waarop de registraties betrekking hadden, was dezelfde periode als waarop de uitvraag onder gemeenten betrekking had.

We hebben 53 politieregistraties geïdentificeerd, waarop we een socialenetwerkanalyse hebben uitgevoerd om groepen te kunnen identificeren. Dit resulteerde in 109 unieke verdachten en 26 groepen. Hieruit hebben we een steekproef getrokken van in totaal 6 groepen, die we verder inhoudelijk hebben geanalyseerd. Daarbij hebben we ons specifiek gericht op kernleden. De analysestrategie kwam overeen met de strategie die is gebruikt bij de zaakreconstructies.

Daderinterviews
Via consortium- en veiligheidspartners hebben we geprobeerd in contact te komen met jongeren die actief waren binnen cybercriminele jeugdgroepen. De reden hiervoor is dat de expertinterviews, zaakreconstructies en politieregistraties als beperking hebben dat ze niet rechtstreeks afkomstig zijn van de jongeren zelf. Dit heeft tot gevolg dat de bronnen waarschijnlijk een vertekend beeld geven; daders en groepen die buiten het zicht van de experts en de politie blijven, hebben mogelijk afwijkende kenmerken ten opzichte van de wél geïdentificeerde leden en groepen. Om die reden is het ook belangrijk om de jongeren zelf te spreken.
We hebben geprobeerd om via Reclassering Nederland en jongerenwerkers in Noord-Nederland in contact te komen met jongeren die betrokken zijn bij cybercriminele activiteiten. Ook hebben we ons aangesloten bij zogenoemde wasstraten[1] in Noord-Nederland. Ondanks deze inspanningen hebben we uiteindelijk slechts één dader kunnen spreken. De voornaamste reden hiervoor was dat bijna alle partners geen kennis hadden van potentiële respondenten relevant voor dit onderzoek. Het interview met deze dader is niet meegenomen in de resultaten van dit onderzoek.

Resultaten

Spoor 1: de bij lokale veiligheidscoalities bekende (cyber)criminele jeugdgroepen
Spoor 1 richtte zich op de jeugdgroepen die in beeld zijn bij lokale veiligheidscoalities. Data hierover hebben we verkregen via expertinterviews en een uitvraag bij de 40 Noord-Nederlandse gemeenten. Op onze vraag werd door 25 gemeenten gereageerd. Daarvan gaven er 10 aan één of meer groepen te kennen, waarvan 9 gemeenten ook de identificerende gegevens hebben aangeleverd. Dit resulteerde in informatie over 13 bij gemeenten bekende groepen en 4 individuen die onderdeel zijn van een groep die bij de gemeente vooralsnog onbekend is. In totaal zijn 207 jeugdigen geïdentificeerd.
In de praktijk waren dit enkel groepen die betrokken waren bij traditionele criminaliteit, voor zover gemeenten hier zicht op hadden. Lokale veiligheidscoalities, onder leiding van gemeenten, hadden geen zicht op jeugdgroepen die zich bezighielden met cybercriminele activiteiten. De primaire reden voor dit gebrek aan zicht is de sterke afhankelijkheid van straatinformatie. Integrale overlegtafels bespreken problematische

1 Dit betreft een aanpak waarbij op één of enkele dagen veel verdachten van cybercrime, specifiek geldezels, versneld worden gehoord (Openbaar Ministerie, 2025).

en criminele jeugdgroepen op basis van waarnemingen op straat, waardoor zij sterk afhankelijk zijn van deze informatiebron. Dit maakt het lastig om te identificeren of jongeren cyberdelicten plegen, en zo ja welke, omdat deze activiteiten zich doorgaans niet op straat afspelen en daardoor buiten het bereik van traditionele observaties blijven. Lokale actoren zien dit dus niet, waardoor deze activiteiten niet worden besproken, en er dus ook geen verdere identificatie van cybercriminele jeugdgroepen plaatsvindt.

Veel respondenten gaven aan slechts beperkt zicht te hebben op de aard van de delicten, structuur, samenstelling, en werkwijze van criminele jeugdgroepen en hun leden. De bevindingen die wij hier presenteren zijn daarom voornamelijk gebaseerd op individuele (beperkte) observaties en ervaringen uit de praktijk. Het beeld dat wij schetsen is daarmee niet noodzakelijk volledig of sluitend, maar weerspiegelt de kennis die door respondenten kon worden aangedragen. Bij de interpretatie van de resultaten dient hiermee rekening te worden gehouden.

Het merendeel van de traditionele criminele jeugdgroepen die bekend zijn bij gemeenten en werden beschreven tijdens de interviews, vertoonde een combinatie van problematisch en crimineel gedrag, waaronder gewelds- en drugsmisdrijven, vernieling en misdrijven tegen de openbare orde. Hoewel uit onze data naar voren kwam dat lokale veiligheidscoalities geen expliciet zicht hebben op jeugdgroepen die betrokken zijn bij cybercrime, bleek wel dat jeugdgroepen gebruikmaken van het internet voor communicatie en dat er vermoedens zijn van betrokkenheid bij cybercrime.

Respondenten hadden een beperkt zicht op de precieze structuur en samenstelling van traditionele criminele jeugdgroepen en op hun ontstaans- en groeiprocessen. Wel was bekend dat de omvang van dergelijke groepen sterk varieerde, tussen de 4 en 40 leden. Binnen sommige groepen was sprake van een vaste kern, die kon bestaan uit 3 tot 15 leden. De vaste kern lijkt stabieler te zijn dan de flexibelere lagen daaromheen. Hoe en wanneer deze groepen gevormd waren, was veelal onbekend, al lijkt een deel te zijn ontstaan vanuit een 'normale' jongerengroep. In eerste instantie gaat het hierbij om jongeren die samen rondhangen, waarbij deze groepen gaandeweg individuen aantrekken die al strafbare feiten hebben gepleegd. Daarnaast kunnen jongeren zich uit eigen initiatief aansluiten bij bestaande jeugdgroepen of actief worden gerekruteerd door groepsleden. In beide gevallen spelen met name offline relaties en fysieke locaties een rol. Jongeren leren elkaar kennen op straat, op school, bij de sportvereniging of doordat ze in dezelfde wijk wonen. Verder hebben jongeren die betrokken zijn bij dezelfde groep vaak familie- en vriendschapsbanden. Ook sociale media kunnen een rol spelen bij het ontstaan, de groei en de fluïditeit van traditionele criminele jeugdgroepen.

De leeftijd van de jongeren en jongvolwassenen die onderdeel waren van traditionele criminele jeugdgroepen lag volgens respondenten tussen de 8 en 29 jaar. De besproken jeugdgroepen lijken op basis van leeftijd te kunnen worden ingedeeld in twee categorieën. Enerzijds zijn er groepen die vrijwel volledig uit minderjarigen bestaan. Anderzijds bestaan er groepen waarin zowel minderjarigen als volwassenen actief zijn. Kijken we naar het geslacht, dan blijkt het grootste deel van deze groepen te bestaan uit

jongens en jonge mannen. De etnische achtergrond was divers. Verder waren veel jongeren binnen deze groepen nog leerplichtig, maar bleek er veelvuldig sprake van schoolverzuim. Qua opleidingsniveau varieerde de groep van laag- tot hoogopgeleide jongeren. Daarnaast hadden sommige jongeren een zorgverleden en werden zij als kwetsbaar beschouwd. De sociaaleconomische status van groepsleden liet eveneens een divers beeld zien. Jongeren konden afkomstig zijn uit verschillende maatschappelijke lagen. Een vergelijkbare diversiteit was zichtbaar in de thuissituatie.
Op basis van hun criminele carrière lijken de jongeren en jongvolwassenen binnen traditionele criminele jeugdgroepen in twee groepen te kunnen worden verdeeld. Enerzijds was een deel van de leden een *first offender*, vooral de jongere leden. Anderzijds konden leden geclassificeerd worden als *recidivist.* Deze groep bestond voornamelijk uit de oudere en vaak meerderjarige leden. Zij waren al eerder in beeld geweest bij politie en justitie voor delicten als mishandeling en winkeldiefstal. Tot slot gaven respondenten aan dat jongeren vooral deelnamen aan traditionele criminele jeugdgroepen vanwege de wens om snel geld te verdienen, evenals statusverwerving en de behoefte om ergens bij te horen.

Spoor 2: de bij lokale veiligheidscoalities onbekende (cyber)criminele jeugdgroepen
In spoor 1 is naar voren gekomen dat lokale veiligheidscoalities onder leiding van gemeenten (die de regie voeren op de aanpak van (criminele) jeugdgroepen) uitsluitend zicht hebben op traditionele criminele jeugdgroepen. Jeugdgroepen die betrokken zijn bij cybercrime blijven buiten beeld, al waren er (soms) wel vermoedens, maar geen concrete aanwijzingen, van de aanwezigheid van cybercriminele (al dan niet hybride) groepen.
Uit de expertinterviews, de zaakreconstructies en de politieregistraties bleek echter dat er talloze (hybride) cybercriminele groepen actief zijn (geweest). Zo leverde de analyse van politieregistraties in totaal 26 groepen op, variërend van 2 tot 23 leden, die zich voornamelijk bezighielden met verschillende vormen van online fraude.Deze groepen zijn veelal bekend bij monodisciplinaire partners, vooral bij de strafrechtelijke actoren (politie, OM) en (gedeeltelijk) bij enkele private partijen, waaronder banken en telecomproviders. Informatie over jeugdgroepen die betrokken zijn bij cybercrime is gefragmenteerd aanwezig bij individuele partners en is niet breed toegankelijk voor lokale veiligheidscoalities.
Ook voor deze bevindingen geldt dat respondenten benadrukten slechts beperkt zicht te hebben op de kenmerken van cybercriminele jeugdnetwerken, waardoor de bevindingen die wij hier presenteren niet noodzakelijk volledig of sluitend zijn, maar de kennis weerspiegelen die door respondenten kon worden aangedragen. Bij de interpretatie van de resultaten dient hiermee rekening te worden gehouden.
Er zijn twee soorten jeugdgroepen te onderscheden op basis van de delicten die zij plegen. Enerzijds kunnen jeugdgroepen betrokken zijn bij zowel traditionele criminaliteit (zoals gewelds-, vermogens- en drugsdelicten, vernieling en misdrijven tegen de openbare orde) als cybercrime (zoals bankhelpdeskfraude, verkoopfraude, phishing, vriend-in-nood-fraude en het witwassen van wederrechtelijk verkregen voordeel). Dit

worden hybride groepen genoemd en deze lijken veelvuldig voor te komen. Ze ontstaan met het doel om traditionele criminaliteit te plegen, maar breiden op een gegeven moment hun criminele activiteiten uit naar cybercrime.
Anderzijds kunnen jeugdgroepen zich exclusief op cybercrime richten (zoals bankhelpdeskfraude, phishing, vriend-in-nood-fraude, online identiteitsfraude en verkoopfraude). Hoewel dit gepaard kan gaan met cybercrime in enge zin (zoals hacken), zijn er niet of nauwelijks Noord-Nederlandse jeugdgroepen bekend die zich hier specifiek op toeleggen.
Cybercrime en traditionele criminaliteit raken steeds vaker met elkaar verweven. Er kan sprake zijn van verwevenheid waarbij cybercrime en traditionele criminaliteit samen worden gepleegd, maar er geen directe relatie is tussen beide: een groep kan zich bijvoorbeeld bezighouden met bankhelpdeskfraude en met het verkopen van drugs. Er zijn echter ook gevallen naar voren gekomen waarbij er een sterkere, meer directe verbinding lijkt te zijn tussen traditionele criminaliteit en cybercrime, waarbij cybercrime veelal voorafgaat aan de traditionele delicten. Zonder cyber zou het traditionele delict niet of veel moeilijker te plegen zijn. Deze meer directe verwevenheid is zichtbaar op drie gebieden: (1) witwassen en ondermijnende criminaliteit; (2) investeren van via cybercrime verkregen wederrechtelijk voordeel in traditionele criminaliteit; en (3) geweld dat gepaard gaat met cybercrime.
Op basis van de politieregistraties, de zaakreconstructies en de expertinterviews is deels zicht verkregen op de structuur, de samenstelling, het ontstaan en de groei van hybride en cybercriminele jeugdgroepen. Daarbij vertoonden beide typen jeugdgroepen veel overeenkomsten. Enerzijds konden groepen dynamisch zijn en ad hoc ontstaan wanneer zich een gelegenheid voordeed om cybercrime te plegen. Ze waren dan fluïde zonder duidelijke hiërarchie en hadden een relatief korte levensduur. Anderzijds konden groepen relatief stabiel zijn. Deze waren doorgaans kleinschalig, met een vaste kerngroep van drie tot vijf leden, en vertoonden een grotere mate van structuur en hiërarchie. Tegelijkertijd bleven de lagen buiten de kern dynamisch van samenstelling. Beide typen groepen hadden doorgaans kernleden, professionele en/of gerekruteerde facilitators en geldezels of andere katvangers. Toetreding tot deze groepen verliep via actieve rekrutering of geleidelijke betrokkenheid, waarbij zowel offline als online relaties en fysieke én virtuele ontmoetingsplaatsen een rol speelden.
De kernleden van de groepen waren doorgaans tussen de 12 en 28 jaar. Geldezels en katvangers waren meestal minderjarig, al konden ook volwassenen worden ingezet. Kernleden waren meestal man, al lijkt geslacht wel samen te hangen met de rol binnen de groep. Vrouwen werden bijvoorbeeld veelal gebruikt als beller. De etnische achtergrond van kernleden was zeer divers en leek eveneens samen te hangen met de rol binnen de groep. Geldezels leken vaker een migratieachtergrond te hebben. Het opleidingsniveau van kernleden varieerde sterk: van niet- of laagopgeleide tot (hoog)opgeleide verdachten. De meeste kernleden en geldezels hadden een relatief lagere sociaaleconomische status en kwamen uit achterstandswijken, waarbij een deel een problematische gezinssituatie had. Sommigen groeiden op in stabiele gezinnen, terwijl

anderen een instabiele achtergrond leken te hebben. Over het algemeen waren de cognitieve vaardigheden beperkt en waren geldezels vaak kwetsbaar en onwetend.
Op basis van de politieregistraties, de zaakreconstructies en de expertinterviews zijn drie typen criminele carrières te onderscheiden onder jongeren en jongvolwassenen die actief zijn binnen hybride en cybercriminele jeugdgroepen: overstappers, hybride plegers en digitale starters. Overstappers beginnen hun criminele carrière met het plegen van traditionele criminaliteit, zoals drugsdelicten, woningovervallen of wapengeweld, en maken op enig moment een duidelijke overstap naar cybercrime. Hierna richten ze zich uitsluitend op cybercrime, voornamelijk online fraude. Hybride plegers combineren traditionele delicten en cybercrime. Digitale starters daarentegen beginnen hun criminele carrière direct met financiële cybercrime en blijven doorgaans weg van traditionele criminaliteit. In de context van cybercrime kunnen zowel overstappers, hybride daders als digitale starters gespecialiseerd zijn in één soort cybercrime of juist generalistisch zijn en dus betrokken zijn bij verschillende typen cyberdelicten.
De belangrijkste motivaties voor zowel jongeren binnen hybride groepen als voor daders die zich uitsluitend richtten op cybercrime waren het verkrijgen van status en financieel gewin. Deze twee motivaties zijn nauw met elkaar verweven: status wordt in belangrijke mate ontleend aan het bezit en het kunnen etaleren van luxe en dure goederen en kleding, die gekocht kunnen worden met de opbrengsten uit cybercrime.

Spoor 3: de (integrale) aanpak van jeugdige (cyber)daders in Noord-Nederland
Spoor 3 richtte zich op de mate waarin partners zicht hebben op jeugdgroepen die betrokken zijn bij cybercrime en hoe de aanpak van deze groepen kan worden versterkt.
Lokale veiligheidscoalities, onder regie van gemeenten, hadden in hun geheel geen zicht op cybercriminele jeugdgroepen. Dit komt enerzijds doordat zij te sterk leunen op straatinformatie en anderzijds over onvoldoende kennis beschikken om cyberdaders te identificeren. Integrale overlegtafels bespreken problematische en criminele jeugdgroepen op basis van waarnemingen op straat, waardoor zij sterk afhankelijk zijn van deze informatiebron. Dit maakt het lastig om te identificeren of jongeren cyberdelicten plegen, en zo ja welke, omdat deze activiteiten zich doorgaans niet op straat afspelen en daardoor buiten het bereik van traditionele observaties blijven. Strafrechtelijke partners, vooral de politie en het OM, hebben meer zicht, mede dankzij de informatie uit aangiftes en data-analyse, terwijl ze minder afhankelijk zijn van straatinformatie. Actoren als banken en telecomproviders verrijken het beeld van de politie en het OM. Jeugdgroepen worden echter ook in de opsporings- en vervolgingspraktijk beperkt in kaart gebracht. Het gaat vooral om het laaghangend fruit, zoals de geldezels. Data om een groep beter in kaart te brengen lijken er echter wel te zijn, zo laten de vijf zaakreconstructies zien. Het betreft hier grote onderzoeken, boven het basisteam-niveau, waarbij meerdere kernleden zijn geïdentificeerd. Dergelijke onderzoeken vergen echter veel capaciteit, iets wat op dit moment beperkt beschikbaar is.
Wat betreft de aanpak van jeugdgroepen die betrokken zijn bij cybercrime, hebben we drie benaderingen geïdentificeerd. De eerste is de integrale aanpak, waarbij meerdere

lokale actoren samenwerken. Deze bleek een zeldzaamheid; slechts één casus voldeed hieraan. Toch biedt een integrale aanpak meerdere voordelen, waaronder een rijker informatiebeeld en complementaire interventiemogelijkheden. Ten tweede kan er sprake zijn van een multidisciplinaire samenwerking bij het in kaart brengen van groepen met een monodisciplinaire uitvoering. Dit gaat veelal over kleinere samenwerkingsverbanden, zoals tussen de politie en de banken en telecomproviders, waarbij voornamelijk sprake is van informatiedeling vanuit de private actoren naar de politie voor een opsporingsonderzoek. De daadwerkelijke aanpak vindt veelal monodisciplinair plaats door de politie en het OM. Tot slot kan er sprake zijn van monodisciplinaire aanpakken, zoals banken die rekeningen blokkeren en telecomproviders die telefoonnummers blokkeren.

Ons onderzoek laat zien dat integrale kansen vaak onbenut blijven, terwijl een integrale aanpak in potentie een rijker informatiebeeld en een breder palet aan interventiemogelijkheden oplevert. Het meer benutten van bestaande integrale samenwerkingsstructuren voor de aanpak van cybercrime lijkt dan ook wenselijk.

De praktijk leunt vooralsnog met name op een strafrechtelijke aanpak. De scope van strafrechtelijk onderzoek is echter vaak beperkt: zowel het aantal subjecten als de delicten waarvoor bewijs wordt verzameld zijn doorgaans afgebakend. Hierdoor wordt meestal slechts naar één of een selectie van subjecten en delicten gekeken, waardoor andere betrokkenen en strafbare feiten buiten beeld blijven. Maar, dergelijke opsporingsonderzoeken leveren veelal (bruikbare) politie-informatie op. Integrale samenwerking biedt de mogelijkheid om zowel de scope van het onderzoek (de informatievergaringsfase) als de interventies te verbreden, mogelijk met politie-informatie als startpunt. Door (onder voorwaarden) informatie te delen, kan het zicht van lokale partners op cybercriminele jeugdgroepen dus worden bevorderd. Dit vormt de kern van de meerwaarde van een integrale samenwerking: de aanpak richt zich op de groep en de activiteiten als geheel, in plaats van een specifiek subject en/of delict, zoals bij de uitsluitend strafrechtelijke aanpak veelal het geval is. Daarnaast neemt het interventiepotentieel toe, doordat iedere organisatie over eigen interventiemogelijkheden beschikt. Hierdoor kunnen interventies van verschillende organisaties gelijktijdig worden ingezet en gecombineerd. Of die mogelijkheden ook inzetbaar en effectiever zijn, is nog voer voor discussie.

Binnen de aanpak van cybercriminele jeugdgroepen zijn meerdere verbeterpunten geïdentificeerd. De kern daarbij is dat meerdere samenwerkingsmogelijkheden onbenut blijven, vooral de meer structurele samenwerkingen, zoals via het RIEC en de jeugdgroepenaanpak. De integratie van cybercrime in bestaande samenwerkingsstructuren vergt dat we eerst beter zicht hebben en dus in staat zijn om te signaleren. Daarnaast vraagt dit om de toepassing en evaluatie van bestaande interventies, zoals het RIEC-interventierepertoire, en waar nodig om de ontwikkeling van nieuwe interventies, zodat ketenpartners handvatten hebben om op te treden tegen deze vorm van (groeps)criminaliteit die voor hen veelal nog onbekend is.

Het verbeteren van het zicht op cybercriminele jeugdgroepen vraagt van praktijkprofessionals dat zij bekwaam zijn in vroegtijdig signaleren en proactief optreden en dat

zij deze signalen efficiënt kunnen delen met lokale actoren. Om de betrokkenheid van jongeren bij cybercrime in een vroeg stadium te kunnen signaleren en om proactief te kunnen optreden, hebben praktijkprofessionals kennis en inzicht nodig op het gebied van cybercrime. Volgens de respondenten lijkt het daar veelal aan te ontbreken. Bovendien verloopt het delen van signalen stroef, waardoor ze niet de juiste partners bereiken en het informatiebeeld over cybercriminele jeugdgroepen beperkt blijft. Daarom is er behoefte aan:

- het vergroten van de kennis van praktijkprofessionals (zoals politieagenten en jongerenwerkers) om cybercrime zowel offline als online te kunnen signaleren. Dit maakt vroegsignalering en proactief optreden mogelijk.
- het verbeteren van de samenwerking tussen lokale actoren, waaronder de politie, gemeenten, basis- en middelbare scholen, jongerenwerkers, banken en telecomproviders. Dit maakt een snellere signaaluitwisseling en betere informatiedeling mogelijk.

Daarnaast is het noodzakelijk om nieuwe interventies te ontwikkelen en deze (net als de bestaande interventies) te evalueren, zodat ketenpartners handvatten hebben om op te treden tegen vormen van (groeps)cybercriminaliteit die zij veelal nog niet kennen. Daarbij is behoefte aan:

- de ontwikkeling van interventies die specifiek gericht zijn op verschillende groepen binnen cybercriminele groepen, zoals kernleden en geldezels;
- het evalueren van deze interventies.

Aanbevelingen

Een van de belangrijkste bevindingen van dit onderzoek is dat gemeenten momenteel onvoldoende zicht hebben op criminele jeugdgroepen, en in het bijzonder op jeugdgroepen die betrokken zijn bij cybercrime. Hierdoor kunnen zij geen regie voeren op de aanpak daarvan. De centrale aanbeveling is daarom om dit zicht op cybercriminele jeugdgroepen te vergroten.

Om de betrokkenheid van jongeren bij cybercrime in een vroeg stadium te kunnen signaleren en om proactief te kunnen optreden, hebben praktijkprofessionals (meer) kennis en inzicht nodig op het gebied van cybercrime. Dit onderzoek laat zien dat zij hier nog onvoldoende over beschikken. De volgende maatregelen worden aanbevolen.

Beter herkennen van cybercrime-gerelateerde signalen

- Scholing en training. Organiseer trainingen waarin professionals in de hele rechtshandhavingsketen leren om (de neiging tot) cybercrime onder jeugdigen te herkennen. De trainingen moeten inzicht bieden in de verschijningsvormen en risico's van cybercrime, maar vooral ook handvatten geven om betrokkenheid bij cybercrime (vroegtijdig) te herkennen.
- Gebruik van vroegsignaleringsindicatoren. Dit onderzoek identificeert een aantal vroegsignaleringsindicatoren, waaronder betrokkenheid bij offline criminaliteit, het bezit van meerdere simkaarten/telefoons en het bezitten van goederen die, ge-

zien iemands financiële positie, niet op een legale manier verkregen kunnen zijn. Deze indicatoren kunnen, aangevuld met inzichten uit ander onderzoek, als basis dienen voor signalering.
- Breder signaleren. Specifiek voor cybercrime geldt dat niet alleen geleund kan worden op signalen 'van de straat'. Ook online surveillance en toezicht zijn nodig, net als het delen van signalen die daaruit voortkomen. Dat is deels een taak van de politie, maar ook jongerenwerkers en andere professionals kunnen hieraan bijdragen.

Structurele en periodieke monitoring
Om structureel meer zicht te krijgen op cybercriminele jeugdgroepen kan periodiek in de politiesystemen de cybercrime-query worden uitgevoerd die voor dit onderzoek is ontwikkeld. Daarmee kunnen groepen in kaart gebracht worden op basis van politieregistraties. Momenteel vinden er al periodieke (jeugd)overleggen plaats tussen gemeenten en de politie. Het advies is om hierbij aan te sluiten en periodiek de resultaten van een dergelijke query in te brengen, bijvoorbeeld in de jeugdgroepenaanpak.
De uitvoering van de query ligt bij de politie. In samenspraak met het OM kan worden besloten om hele groepen en/of sleutelfiguren binnen deze groepen strafrechtelijk aan te pakken, afhankelijk van wat het meest effectief en haalbaar is. Tegelijkertijd is een louter strafrechtelijke aanpak ontoereikend en doet deze onvoldoende recht aan de omvang van de cybercrime-problematiek in de maatschappij. Geïdentificeerde groepen die niet direct leiden tot opsporingsonderzoek, evenals politie-informatie, kunnen daarom worden ingebracht in bestaande samenwerkingsstructuren, zoals de jeugdgroepenaanpak en het RIEC-samenwerkingsverband, en dienen als startpunt voor een integrale aanpak.

Samenwerkingsstructuren beter benutten
Hoewel er al meerdere structurele samenwerkingsverbanden bestaan, waaronder de jeugdgroepenaanpak en het RIEC-samenwerkingsverband, worden deze in de praktijk nog nauwelijks benut voor de aanpak van cybercrime, terwijl ze daar wel geschikt voor lijken.
Om bestaande samenwerkingsstructuren beter te benutten, is meer inzicht nodig in de criteria waaraan casussen moeten voldoen om daarbij ingebracht te kunnen worden. De politie heeft hierin een sleutelrol vanwege haar informatiepositie. Bij de vraag hoe en waar een criminele groep het beste kan worden ingebracht, is het van belang op welke informatiebron de identificatie berust. Het delen van persoonsgegevens in een samenwerkingsstructuur vraagt om een weloverwogen voortraject:
- identificatie op basis van politie-informatie. Is een groep geïdentificeerd via politiegegevens, dan ligt het voor de hand dat de politie en het OM eerst gezamenlijk beoordelen of een strafrechtelijke aanpak haalbaar en opportuun is. Is dit niet het geval, dan kan worden gekeken naar integrale kansen. Voorwaarde is wel dat vooraf helder is welke criteria er gelden om een casus te kunnen inbrengen in de jeugdgroepenaanpak, in het RIEC of in een ander samenwerkingsverband.

- identificatie op basis van lokale partnerinformatie. Komt een groep in beeld via lokale partners, zoals scholen, jongerenwerk of wijkteams, dan verloopt het proces vaak anders. Deze partijen zullen doorgaans eerst zelf afwegen of zij handelingsmogelijkheden hebben binnen hun eigen mandaat en instrumentarium. Pas als zij onvoldoende mogelijkheden zien of als de problematiek groter is dan hun bereik, kan opschaling naar een samenwerkingsstructuur volgen. Dit vraagt om duidelijke afspraken en korte lijnen tussen lokale partners, de politie en gemeenten, zodat een eventuele opschaling efficiënt en zorgvuldig kan plaatsvinden.

Aanbevelingen voor de jeugdgroepenaanpak
Specifiek voor de jeugdgroepenaanpak blijkt dat daarin jongeren voorkomen die bij de politie bekend zijn vanwege traditioneel afwijkend gedrag, maar die soms óók betrokken blijken bij cybercrime. Deze aanwijzingen worden nu vaak gemist. Een aanbeveling is om de resultaten vanuit de query in te brengen in de geschikte bestaande samenwerkingsstructuur. Specifiek voor jeugdgroepen kan dit gedaan worden via het groepsscanonderdeel van het 7-stappenmodel. Dit vraagt om een (landelijke) aanpassing van de groepsscan en de query. Hierbij kan per groepslid een volledig overzicht met antecedenten én verdenkingen worden gegenereerd, met specifieke aandacht voor cybercrime.

Aanpakken en effectiviteit
De aanpak van cybercrime vindt momenteel veelal monodisciplinair plaats. Multidisciplinaire samenwerkingen voor informatievoorziening met een monodisciplinaire uitvoering zijn mogelijk, en bestaande samenwerkingsstructuren worden niet of nauwelijks benut, terwijl ze zich daar (ogenschijnlijk) wel voor lenen. Hoewel er dus aanwijzingen voor bestaan dat het traditionele interventierepertoire ook toegepast kan worden op cybergroepen (zoals de RIEC-casus), is er te weinig bekend over de effectiviteit van deze interventies en aanpakken. Meer onderzoek is nodig om vast te stellen welke aanpakken werken bij cybercriminele jeugdgroepen. Waar nodig kunnen interventies worden ontwikkeld of geoptimaliseerd.
Ondanks die kanttekening, is het advies:
- bekendheid vergroten. Bevorder de bekendheid van beproefde interventies binnen de rechtshandhavingspraktijk. Voorbeelden zijn de Geldezelaanpak en Hack_Right (voor een uitgebreider overzicht, zie CCV, 2023b).
- gerichte inzet. Zet zowel monodisciplinair als in gelegenheidssamenwerkingen zo veel mogelijk in op interventies die kansrijk zijn gebleken.
- nieuwe ontwikkeling**.** Tegelijkertijd is er ruimte en een noodzaak om interventies te blijven ontwikkelen, bij uitstek tegen de opportunistische jonge doelgroep die zich bezighoudt met online fraude. Daar zijn tot op heden weinig op maat gesneden interventies tegen voorhanden.

Bij deze drie aanbevelingen is het essentieel om de processen en uitkomsten systematisch te evalueren.

1 Inleiding

1.1 Achtergrond

Veiligheidspartners in Noord-Nederland geven aan problemen te ondervinden met cybercriminele jeugdgroepen, in dit onderzoek gedefinieerd als samenwerkingsverbanden die bestaan uit ten minste twee personen tussen de 12 en 24 jaar oud (Ferwerda & Van Ham, 2010, 2014; Wasserman & Faust, 1994; WODC, 2021), die betrokken zijn bij criminele activiteiten. Specifiek hebben lokale veiligheidspartners moeite met (1) het in kaart brengen en (2) aanpakken van jongeren en jeugdgroepen betrokken bij cybercriminele activiteiten, en hebben ze (3) behoefte aan meer kennis over dit onderwerp: zowel over het fenomeen zelf als over de manieren om dergelijke groepen te identificeren en effectief aan te pakken (Leukfeldt et al., z.d.; Veenstra, 2023).
Hoewel actuele cijfers over het aantal criminele jeugdgroepen in Nederland ontbreken, lijkt het verkrijgen van zicht op deze groepen de afgelopen jaren lastiger te zijn geworden (NJI, 2023). Het aantal 'problematische jeugdgroepen' in Nederland dat tussen 2009 en 2014 in beeld was, daalde in die periode van 1760 naar 623, een daling van 65%. Ook in Noord-Nederland was die trend zichtbaar (Ferwerda & Van Ham, 2014). Deze ontwikkeling kan erop duiden dat jeugdgroepen minder goed in beeld komen, eerder dan dat zij daadwerkelijk verdwijnen: alhoewel criminele jeugdgroepen de afgelopen jaren steeds minder aanwezig waren in de openbare ruimte, namen hun activiteiten op sociale media juist toe (NJI, 2023; RIEC, 2022; Weerman, 2017). Een mogelijke verklaring voor deze daling is dat jongeren zich in mindere mate bezighouden met traditionele criminaliteit en juist meer cybercriminaliteit zijn gaan plegen (Jansen et al., 2022; Leukfeldt & Roks, 2021; Openbaar Ministerie, 2024; WODC, 2021).
Cybercrime[2] is een steeds groter probleem wereldwijd (Akkermans et al., 2024; ENISA, 2024; Europol, 2024; FBI, 2025; Interpol, 2024). Dit is ook het geval in Nederland (Akkermans et al., 2024), waar het aantal slachtoffers van cybercrime is toegenomen met 22% tussen 2012 en 2021 (Akkermans et al., 2022). Deze toename lijkt te gelden voor

2 Alle criminele activiteiten waarbij internet en communicatietechnologie (ICT) belangrijk zijn bij de uitvoering van het delict (Yar, 2005).

zowel cybercrime in enge zin[3] als gedigitaliseerde criminaliteit.[4] Dit zijn zorgwekkende ontwikkelingen, niet alleen omdat cybercrime als initiatiepunt kan dienen om vervolgens (ernstige vormen van) traditionele criminaliteit te plegen (Schellevis & Van Hulzen, 2022), maar ook omdat slachtofferschap van cybercrime ernstige negatieve gevolgen kan hebben, zoals financiële schade, schuldgevoel, stress, machteloosheid, verdriet en/of angst (Akkermans et al., 2024; Borwell et al., 2022; Leukfeldt et al., 2018). Omdat cybercrime nog (te) vaak niet (h)erkend wordt door bijvoorbeeld opsporingsdiensten, hulporganisaties en de sociale omgeving, kunnen de negatieve gevolgen zich opstapelen en kan er sprake zijn van zogenoemde *double* of zelfs *triple hits*. Daarbij ervaren slachtoffers niet alleen directe gevolgen, maar ook indirecte gevolgen, zoals *victim blaming*, waardoor de impact nog groter kan zijn (Leukfeldt et al., 2018).

Hoewel de dadergroep van cybercrime divers is, komt uit de literatuur naar voren dat er ook vaak jongeren bij betrokken zijn (voor een overzicht, zie Loggen et al., 2024b, 2024a). Dit is in Nederland ook het geval. Zo blijkt uit de Monitor Zelfgerapporteerde Jeugddelinquentie dat in 2023 4,2% van de 10- tot 12-jarigen cybercrime heeft gepleegd. Bij de 12- tot 18- en 18- tot 23-jarigen waren deze percentages respectievelijk 9% en 7,2% (Tollenaar et al., 2024). Verder komt uit een analyse van 300.000 willekeurig geselecteerde BVH-registraties uit de periode 2018-2020 naar voren dat 12% van de verdachten van cybercrime in enge zin minderjarig was. Bij gedigitaliseerde criminaliteit was dit percentage 15%, al liepen de percentages wel uiteen. Zo was het percentage minderjarige verdachten bij vriend-in-nood-fraude en online identiteitsfraude 8%, terwijl dit bij bankhelpdeskfraude 21% was (Ruiter et al., 2023). Hierbij dient wel te worden opgemerkt dat de exacte leeftijd van deze verdachten niet bekend is. Het is goed mogelijk dat het merendeel van de meerderjarige verdachten jonger dan 24 is, en daarmee dus ook kan worden aangemerkt als jeugdige.

Daarbij lijken jongeren zich in toenemende mate schuldig te maken aan het plegen van verschillende vormen van cybercrime (vooral online fraude) (Leukfeldt & Roks, 2021), terwijl hun betrokkenheid bij traditionele criminaliteit afneemt (Openbaar Ministerie, 2024; Schellevis & Van Hulzen, 2022; WODC, 2021). Dit lijkt te worden ondersteund door cijfers van het OM: in 2021 waren jongeren tot en met 21 jaar als verdachte betrokken bij 47% van de cybercrimezaken, tegenover 33% in 2018 (Schellevis & Van Hulzen, 2022). Bovendien was tussen 2012 en 2023 meer dan de helft van de cybercrimeverdachten 25 jaar of jonger (Openbaar Ministerie, 2024).

Ondanks het feit dat het aantal jongeren dat betrokken is bij cybercrime lijkt toe te nemen, is er nog maar weinig bekend over deze specifieke dadergroep (Loggen et al., 2024b, 2024a). Ditzelfde geldt voor effectieve interventies. Wel heeft eerder onderzoek al enig licht geworpen op de volwassen daders die betrokken zijn bij cybercrime. Daarbij kwam naar voren dat daders die zich bezighouden met financiële cybercrime (zoals

3 Delicten waarbij ICT zowel het middel als het doel is (Akkermans et al., 2022; Davidson et al., 2022; Dragos, 2023; McGuire & Dowling, 2013), zoals distributed denial of service (DDoS) aanvallen en hacking.

4 Traditionele delicten gepleegd met behulp van ICT, bijvoorbeeld phishing en koop- en verkoopfraude (Akkermans et al., 2022; APWG, 2025; Davidson et al., 2022; European Union Agency for Law Enforcement Cooperation, 2021; McGuire & Dowling, 2013).

phishing) dergelijke delicten veelal in samenwerkingsverband plegen (Bulanova-Hristova et al., 2016; Hutchings, 2014; Leukfeldt & Holt, 2020; Matthijsse et al., 2023; Odinot et al., 2017; Romagna & Leukfeldt, 2024a). Ook zijn stappen ondernomen om een beter begrip te krijgen van het ontstaan, de groei en de structuur van deze groepen (Leukfeldt et al., 2016; Leukfeldt, Kleemans et al., 2017b, 2017a; Lusthaus et al., 2023), de delicten waarbij deze groepen betrokken zijn en de verwevenheid tussen traditionele criminaliteit en cybercrime (Leukfeldt et al., 2016; Leukfeldt & Roks, 2021; Odinot et al., 2018; Roks & van den Broek, 2018; Storrod & Densley, 2017). Verder komt uit voorgaand onderzoek naar voren dat cybercriminele groepen sterk lokaal verankerd lijken te zijn (Kruisbergen et al., 2018a, 2019; Leukfeldt et al., 2019), wat maakt dat een aanpak door lokale veiligheidspartners mogelijk effectief is.
We weten dus dat er lokaal gewortelde cybercriminele groepen zijn en we weten dat cybercrime ook wordt gepleegd door jongeren, in deze studie gedefinieerd als personen tussen de 12 en 24 jaar. Verder weten we dat een groot deel van de criminele jongeren in groepsverband (traditionele) criminaliteit pleegt (Ferwerda, 2000; Ferwerda & Van Ham, 2017), en dat jongeren in toenemende mate betrokken zijn bij cybercrime. Het is echter onbekend in hoeverre er sprake is van criminele jeugdgroepen die (ook) cybercrime plegen of zelfs cybercriminele jeugdgroepen waarbij de jeugdige daders zich specifiek bezighouden met cybercrime. Onderzoek naar de criminele activiteiten van deze cybercriminele jeugdgroepen en hun ontstaan, groei en structuur ontbreekt. Datzelfde geldt voor de persoonlijkheidskenmerken en criminele carrière van groepsleden. Bovendien zijn de processen van het ontstaan, de groei en de structuur van cybercriminele jeugdgroepen de afgelopen jaren complexer geworden. Dat komt onder andere door de opkomst van nieuwe virtuele *offender convergence settings,* plekken waar (potentiële) criminelen elkaar ontmoeten en informatie uitwisselen (Felson, 2003; Leukfeldt et al., 2016; Soudijn & Zegers, 2012). Daarnaast komt het door de ontwikkeling van nieuwe online communicatiemethoden, zoals Telegram (Bekkers et al., 2023; Garkava et al., 2024; Roks & Monshouwer, 2020; Van Wegberg, 2020), die ook zouden kunnen dienen als offender convergence setting.

1.2 Aanleiding

Cybercrime is dus een steeds groter probleem in Nederland, waar ook jongeren bij betrokken zijn, veelal in groepsverband. Echter, veiligheidspartners in Noord-Nederland geven aan moeite te hebben met (1) het in kaart brengen en (2) aanpakken van jongeren en jeugdnetwerken betrokken bij cybercriminele activiteiten, en (3) behoefte te hebben aan meer kennis over dit onderwerp: zowel over het fenomeen zelf, als over de manieren om dergelijke groepen te identificeren en effectief aan te pakken.
Allereerst is er beperkt zicht op cybercriminele jeugdgroepen; zij staan nog nauwelijks op de radar van lokale veiligheidscoalities – lokale samenwerkingen tussen de politie, het Openbaar Ministerie (OM) en hulp- en zorgorganisaties, onder regie van de gemeente. Dergelijke groepen kunnen niet worden aangepakt wanneer zij niet zichtbaar zijn. Ten tweede is er nog weinig bekend over het fenomeen van cybercriminele jeugd-

groepen zelf, zoals hun kenmerken en met welke delicten ze zich bezighouden. Kennis hierover is essentieel voor de ontwikkeling van effectieve interventies. Ten derde is de bestaande aanpak van jeugdgroepen vooralsnog traditioneel georiënteerd. Een aanpak- of interventiestrategie die specifiek is toegespitst op cybercrime ontbreekt vooralsnog.
Tegelijkertijd blijkt uit eerder onderzoek dat cybercriminele (jeugd)groepen sterk lokaal verankerd zijn, waardoor juist lokale actoren een sleutelrol spelen in de aanpak ervan (Leukfeldt et al., 2020). Diezelfde lokale veiligheidspartners lijken echter minder goed zicht te hebben op cybercriminele jeugdgroepen. Hierdoor wordt in de praktijk sterk geleund op (experts van) de politie, terwijl de politie deze groepen niet alléén kan bestrijden. Een integrale aanpak is noodzakelijk om zicht te krijgen op de aanpak van cybercrime (Jewkes & Yar, 2012; Veenstra et al., 2013).
In dit onderzoek richten we ons specifiek op Noord-Nederland (de provincies Drenthe, Friesland en Groningen), omdat meerdere gemeenten uit deze provincies aangaven moeite te hebben met het in kaart brengen en aanpakken van cybercriminele activiteiten van jeugdgroepen en omdat zij behoefte hadden aan meer kennis op dit gebied.

1.3 Doelstelling en onderzoeksvragen

Samenvattend is er op dit moment nog maar weinig bekend over de kenmerken van cybercriminele jeugdgroepen, terwijl dit juist wel belangrijk is voor een effectieve aanpak. Bovendien is het de vraag of lokale veiligheidscoalities nog wel de juiste methoden en middelen hebben om dergelijke groepen te identificeren en te monitoren. Dit onderzoek heeft daarom tot doel om inzicht te bieden in cybercriminele jeugdgroepen in Noord-Nederland en om handvatten te bieden voor de integrale aanpak daarvan. Het onderzoek is echter nadrukkelijk méér dan een momentopname. Op basis van de inzichten uit het onderzoek wordt in samenwerking met het consortium een methodiek ontwikkeld waarmee ook andere lokale veiligheidscoalities zicht kunnen krijgen op cybercriminele jeugdgroepen.
Het onderzoek volgt drie sporen. Allereerst richten we ons op (cyber)criminele jeugdgroepen die bekend zijn bij lokale veiligheidscoalities (spoor 1). Ten tweede onderzoeken we in hoeverre in Noord-Nederland sprake is van jeugdgroepen die zich toeleggen op cybercrime en die nog onbekend zijn bij lokale veiligheidscoalities (spoor 2). Het daarmee verkregen inzicht in cybercriminele jeugdgroepen is een vereiste voor de aanpak ervan. Nadat we zicht hebben gekregen op die groepen rijst dus logischerwijs de vraag wat mogelijkheden zijn voor de (integrale) aanpak daarvan. In spoor 3 staat daarom het ontwikkelen van handreikingen voor de integrale aanpak centraal. Per spoor zijn vragen vastgesteld die richting geven aan het onderzoek.

1.3.1 *Spoor 1: bekende jeugdgroepen*

Het eerste spoor richt zich op (cyber)criminele jeugdgroepen die bekend zijn bij lokale veiligheidscoalities. Binnen spoor 1 staan de volgende onderzoeksvragen centraal:

1.1 Welke (cyber)criminele jeugdgroepen zijn bekend bij lokale veiligheidscoalities binnen Noord-Nederland?
1.2 Wat zijn de kenmerken van bekende (cyber)criminele jeugdgroepen, zoals omvang, rolverdeling, hiërarchie, banden tussen leden, en het gebruik van facilitators en online en offline ontmoetingsplaatsen?
1.3 Wat zijn de demografische kenmerken en criminele carrières van individuele leden van bekende cybercriminele jeugdgroepen?
1.4 Wat zijn de aard en modus operandi van de traditionele en/of cybercriminele delicten waarmee bekende cybercriminele jeugdgroepen zich bezighouden, en hoe ziet de verwevenheid tussen traditionele delicten en cyberdelicten eruit?

1.3.2 *Spoor 2: onbekende jeugdgroepen*

Binnen het tweede spoor staan cybercriminele jeugdgroepen centraal die bij lokale veiligheidscoalities nog onbekend zijn. De volgende vragen geven richting aan dit onderzoeksspoor:
2.1 In hoeverre zijn er bij lokale veiligheidscoalities onbekende cybercriminele jeugdgroepen actief binnen Noord-Nederland?
2.2 Wat zijn de kenmerken van nog onbekende cybercriminele jeugdgroepen, zoals omvang, rolverdeling, hiërarchie, banden tussen leden, en gebruik van facilitators en online en offline ontmoetingsplaatsen?
2.3 Wat zijn de demografische kenmerken en criminele carrières van individuele leden van nog onbekende cybercriminele jeugdgroepen?
2.4 Wat zijn de aard en modus operandi van de traditionele en/of cybercriminele delicten waarmee nog onbekende cybercriminele jeugdgroepen zich bezighouden, en hoe ziet de verwevenheid tussen traditionele delicten en cyberdelicten eruit?

1.3.3 *Spoor 3: integrale aanpak*

Binnen spoor 3 staat het ontwikkelen van handreikingen voor de (integrale) aanpak van cybercriminele jeugdgroepen centraal. Onderstaande onderzoeksvragen vormen voor dit spoor het vertrekpunt:
3.1 In hoeverre hebben actoren die betrokken zijn bij de (integrale) aanpak van criminele jeugdgroepen in Noord-Nederland zicht op de onder onderzoeksvraag 1 en 2 geïdentificeerde cybercriminele groepen?
3.2 In hoeverre en op welke wijze kan de integrale aanpak van cybercriminele jeugdgroepen worden bevorderd?

- Wat houdt de (integrale) aanpak van cybercriminele jeugdgroepen in? Welke actor (mono) of actoren (integraal) zijn betrokken?
- In hoeverre is de (integrale) aanpak delictspecifiek en in welke mate volstaat deze voor de aanpak van cybercriminele jeugdgroepen?
- Wat zijn verbeterpunten in de huidige aanpak van cybercriminele jeugdgroepen?
- Wat zijn best practices uit de (integrale) aanpak van cybercriminele jeugdgroepen?

- In hoeverre kunnen interventies die zich richten op jeugdige cyberdaders bijdragen aan de aanpak van cybercriminele jeugdgroepen (zie bijvoorbeeld Oosterwijk & Fischer, 2017)?

1.4 Definities en afbakening

In dit onderzoek staan meerdere onderwerpen en begrippen centraal. Om de leesbaarheid en begrijpelijkheid van dit rapport te vergroten, worden hieronder de belangrijkste begrippen gedefinieerd en afgebakend.

1.4.1 *Cybercrime*

Cybercrime kan dienen als paraplubegrip: het omvat dan 'alle misdrijven waarbij ICT van wezenlijk belang is voor de realisatie van het delict'. Daarbinnen worden twee categorieën onderscheiden: misdrijven waarbij ICT uitsluitend het middel is (oude wijn in nieuw zakken, denk aan fraude via internet) en misdrijven waarbij ICT zowel het middel als het doel is (McGuire & Dowling, 2013). De eerste categorie wordt veelal cybercrime in ruime zin of 'gedigitaliseerde criminaliteit' genoemd. De tweede categorie is 'cybercrime in enge zin', maar wordt ook wel 'high tech crime' of 'cybercrime' genoemd (Van der Wagen et al., 2020). In dit rapport gebruiken we cybercrime als paraplubegrip en dus niet als verwijzing naar 'cybercrime in enge zin'. Zowel cybercriminele jeugdgroepen die zich bezighouden met gedigitaliseerde criminaliteit als cybercriminele jeugdgroepen die cybercrime in enge zin plegen, zijn dus onderwerp van dit onderzoek. De keuze om het begrip cybercrime te gebruiken is gemaakt omwille van de leesbaarheid, maar belangrijker nog: vanwege de verwevenheid tussen de delictscategorieën. Bij online oplichting (gedigitaliseerde criminaliteit) kan er bijvoorbeeld ook sprake zijn van hacken of het gebruik van malware (cybercrime in enge zin) om de fraude te kunnen plegen.

1.4.2 *Jeugd en jeugdgroepen*

In dit onderzoek staan jeugdgroepen centraal. Voor de afbakening van dit begrip verdienen twee aspecten nadere aandacht: (1) jeugd en (2) groepen. Voor het begrip jeugd sluiten wij aan bij eerder gehanteerde definities: jongeren en jongvolwassenen van 12 tot 24 jaar (Ferwerda & Van Ham, 2010, 2014; WODC, 2021). Als tijdens het onderzoek echter blijkt dat ook enkele personen buiten deze leeftijdscategorie tot een jeugdgroep behoren, dan worden zij niet buiten beschouwing gelaten.
Het tweede aspect betreft de terminologie die we gebruiken om samenwerkingsverbanden aan te duiden. Dit kan variëren van 'samenwerkingsverband' tot 'netwerk' of 'groep'. In dit onderzoek kiezen we ervoor om de term 'groep' te gebruiken. Daarvoor zijn drie redenen. Vanuit theoretisch perspectief vormt binnen dit onderzoek sociaalnetwerkanalyse een belangrijk onderdeel. Binnen sociaalnetwerkanalyse worden alle samenwerkingsverbanden, ongeacht hun omvang, aangeduid als groepen (*co-offending*

groups in het Engels). Alle groepen samen vormen vervolgens het overkoepelende netwerk (Wasserman & Faust, 1994). Vanuit praktische overwegingen sluit dit onderzoek aan bij de aanpak van jeugd door gemeenten, die de jeugd*groepen*aanpak wordt genoemd (CCV, 2023a). Tot slot, zoals in de resultaten zal blijken, hebben we in dit onderzoek meerdere samenwerkingsverbanden geïdentificeerd die bestaan uit slechts twee leden. Om goed aan te sluiten bij sociaalnetwerkanalyse en de praktijk, kiezen we ervoor om de term 'groep' te hanteren. Deze term houdt nadrukkelijk geen verband met specifieke kenmerken van de groep, zoals de mate van dynamiek.

1.4.3 *Hybride*

Jongeren en groepen die betrokken zijn bij cybercrime kunnen worden ingedeeld in verschillende categorieën, gebaseerd op uiteenlopende criteria. Een belangrijk aspect dat in dit onderzoek veelvuldig zal worden toegepast, is de aard van de delicten die deze jongeren en groepen plegen. Grofweg zijn er drie categorieën te onderscheiden. Ten eerste zijn er jongeren en groepen die zich uitsluitend bezighouden met offline criminaliteit. In dit rapport zullen we deze aanduiden als traditionele criminele (jeugd) groepen. Ten tweede zijn er jongeren en groepen die zich uitsluitend richten op cybercrime. Voor deze categorie hanteren we de term cybercriminele (jeugd)groepen. Tot slot kunnen jongeren en groepen zich bezighouden met zowel offline criminaliteit als met cybercrime. Ze kunnen bijvoorbeeld diefstallen en inbraken plegen, en zich tegelijk bezighouden met phishing (zie bijvoorbeeld Leukfeldt, 2014). Deze jongeren en groepen worden in dit rapport aangeduid als hybride criminele jongeren en hybride netwerken, aangezien ze in beide 'werelden' – fysiek en digitaal – criminele activiteiten plegen.

1.4.4 *Groepsrollen*

Centraal in dit onderzoek staan (cyber)criminele jeugdgroepen. In de literatuur is beschreven dat er binnen dergelijke groepen sprake kan zijn van een rolverdeling (Leukfeldt et al., 2016; Leukfeldt, Lavorgna et al., 2017; Lusthaus et al., 2023; Nguyen & Luong, 2021). Hierbij moet echter wel worden opgemerkt dat deze studies zich niet expliciet richtten op jeugdgroepen. In het vervolg van dit rapport zullen we waar mogelijk onderscheid maken tussen deze groepen, omdat hun kernmerken van elkaar kunnen verschillen.
Kernleden hebben veelal een leidinggevende rol en zijn verantwoordelijk voor de coordinatie en uitvoering van de criminele activiteiten. Zij verkrijgen nagenoeg alle criminele opbrengsten en vormen doorgaans een relatief stabiele groep die lang met elkaar samenwerkt. Facilitators leveren specifieke diensten of goederen die noodzakelijk zijn om de cybercriminele activiteiten succesvol uit te voeren (Leukfeldt et al., 2016; Leukfeldt, Lavorgna et al., 2017; Leukfeldt, 2014; Loggen & Leukfeldt, 2022). Hierbij wordt in de literatuur onderscheid gemaakt tussen professionele en gerekruteerde facilitators. Professionele facilitators bieden uit eigen initiatief hun goederen en/of diensten

aan en werken vaak samen met meerdere groepen. Gerekruteerde facilitators leveren ook goederen en/of diensten, maar worden door kernleden zelf gerekruteerd en opereren meestal binnen één groep. Zij spelen doorgaans een minder belangrijke rol en zijn eenvoudiger te vervangen dan de professionele facilitators (Leukfeldt et al., 2016; Leukfeldt, Lavorgna et al., 2017; Leukfeldt, 2014; Loggen & Leukfeldt, 2022). Tot slot zijn in sommige groepen katvangers en/of geldezels actief. Deze individuen worden door kernleden ingezet voor specifieke taken, zoals het ophalen van producten die gekocht zijn met illegaal verkregen geld (katvangers) of het beschikbaar stellen van hun bankpas en bankrekening (geldezels) (Bekkers et al., 2023; Leukfeldt, Lavorgna et al., 2017; Leukfeldt, 2014; Loggen & Leukfeldt, 2022; Schiks et al., 2021).

1.4.5 *Lokale veiligheidscoalities en monodisciplinaire actoren*

In dit rapport maken we onderscheid tussen lokale veiligheidscoalities en monodisciplinaire actoren. Lokale veiligheidscoalities verwijzen naar een gedeeld beeld van veiligheidspartners (onder regie van gemeenten) over de aanwezigheid van (cyber)criminele jeugdgroepen. Het gaat hierbij dus om een beeld van een jeugdgroep dat gedeeld wordt door *meerdere* lokale partners, waaronder de gemeente.
Daartegenover staat het beeld van monodisciplinaire actoren. Dit is het beeld dat één actor heeft over het bestaan van een (cyber)criminele jeugdgroep, maar dat onbekend is bij de bredere lokale veiligheidscoalitie. Een voorbeeld hiervan is een jeugdgroep die geïdentificeerd is aan de hand van politiedata – deze is veelal onbekend bij bijvoorbeeld de gemeente.

1.4.6 *Aanpakken en interventies*

Binnen dit onderzoek richt spoor 3 zich specifiek op de aanpak van cybercriminele jeugdnetwerken. Met een aanpak wordt een bredere, overkoepelende methode bedoeld, terwijl interventies verwijzen naar specifiekere en kleinschaligere maatregelen. De jeugdgroepenaanpak is bijvoorbeeld een overkoepelende methode voor het aanpakken van jeugdgroepen, waarbinnen verschillende interventies ingezet kunnen worden, zoals waarschuwingsbrieven en gebiedsverboden. Wanneer we in dit onderzoek dus spreken over een 'aanpak', bedoelen we een brede methodiek; de term 'interventies' duidt op meer specifieke maatregelen.

1.4.7 *Geografische afbakening*

Tot slot heeft het onderzoek een geografische afbakening: we richten ons alleen op groepen binnen Noord-Nederland. Enerzijds is dit omdat de vraag naar meer kennis over (cyber)criminele jeugdgroepen kwam vanuit Noord-Nederland. Meerdere lokale actoren, waaronder diverse gemeenten, de politie, het OM en het RIEC Noord-Nederland, hebben met de onderzoekers samengewerkt om te komen tot een praktisch relevant onderzoeksplan en hebben ook hun medewerking aan het onderzoek toegezegd.

Anderzijds biedt een geografische afbakening de mogelijkheid om te kunnen focussen op een select aantal groepen. Aangezien we niet kunnen voortbouwen op eerder onderzoek naar deze specifieke doelgroep, maakt dit het onderzoek behapbaar. De inzichten uit dit onderzoek zijn echter breder toepasbaar dan alleen Noord-Nederland, want ook elders speelt dezelfde problematiek.

1.5 Leeswijzer

In hoofdstuk 2 besteden we aandacht aan de methodologische verantwoording van de onderzoeksmethoden in dit onderzoek. Hoofdstuk 3 omvat de literatuurstudie, waarbij we ingaan op de bestaande literatuur over traditionele criminele groepen en cybercriminele (jeugd)groepen. Hoofdstuk 4 beschrijft de resultaten uit spoor 1, hoofdstuk 5 gaat in op de resultaten uit spoor 2 en hoofdstuk 6 richt zich op spoor 3. In hoofdstuk 7 wordt de conclusie van het onderzoek beschreven, waarbij we de deelvragen beantwoorden. Tot slot vormt hoofdstuk 8 de discussie.

2 Methodologische verantwoording

In dit hoofdstuk beschrijven we de methodologische verantwoording van de onderzoeksmethoden die we in deze studie hebben gebruikt. Om de onderzoeksvragen te beantwoorden (zie paragraaf 1.3) hebben we gebruikgemaakt van vier onderzoeksmethoden: (1) literatuurstudie; (2) expertinterviews; (3) zaakreconstructies; en (4) een analyse van politieregistraties. Daarbij maken we dus gebruik van triangulatie[5] qua databronnen, methoden en datatypen. In Tabel 1 is de methodenmatrix weergegeven, waarin we aangeven welke onderzoeksmethoden worden gebruikt om de verschillende deelvragen te beantwoorden.
Dit hoofdstuk is als volgt opgebouwd. Allereerst staan we stil bij de literatuurstudie. Vervolgens wordt de methodologische verantwoording gegeven voor de expertinterviews. Daarna beschrijven we de zaakreconstructies, gevolgd door de analyse van de politieregistraties. Het hoofdstuk sluit af met de bespreking van de ethische en privacyaspecten en een resumé.

Tabel 1. Methodenmatrix

Spoor	Onderzoeksvraag	Literatuur	Interviews	Zaak-reconstructie	Politie-registraties
1.1	Identificeren bekende jeugdgroepen		X	X	X
1.2	Kenmerken bekende (cyber) criminele jeugdgroepen	X	X	X	X
1.3	Kenmerken leden	X	X	X	X
1.4	Aard van de delicten	X	X	X	X
2.1	Identificeren nieuwe (cyber) criminele jeugdgroepen	X	X	X	X
2.2	Kenmerken onbekende (cyber) criminele jeugdgroepen	X	X	X	X
2.3	Kenmerken leden	X	X	X	X
2.4	Aard van de delicten	X	X	X	X
3.1	Zicht op bestaande (cyber) criminele jeugdgroepen		X	X	
3.2	Verbeteren aanpak	X	X	X	

5 Bij triangulatie worden verschillende databronnen, datatypen en methoden door elkaar aangevuld, wat de validiteit van de bevindingen verhoogt (Lavorgna, 2013; Leung, 2015; Meijer et al., 2002).

2.1 Literatuurstudie

De literatuurstudie wordt inhoudelijk beschreven in hoofdstuk 3. In deze paragraaf wordt de verantwoording gegeven voor de doelstellingen en de gehanteerde methodiek van de literatuurstudie. De literatuurstudie diende drie doelen. Ten eerste vormde zij de start van het onderzoek, waarbij we hebben gezocht naar publicaties om inzicht te krijgen in verschillende aspecten van (cyber)criminele groepen. Hierbij hebben we specifiek gekeken naar de ontstaans- en groeiprocessen, de structuur en de samenstelling van deze groepen en hun (cyber)criminele activiteiten. De focus lag zowel op traditionele als op cybercriminele groepen en beperkte zich niet uitsluitend tot jeugdgroepen. Ook groepen bestaande uit volwassenen zijn in de literatuurstudie meegenomen. Ten tweede vormden de resultaten van de literatuurstudie de inhoudelijke basis voor de ontwikkeling van de *topiclist*, die we hebben gebruikt tijdens de expertinterviews, en voor de analyse van de zaakreconstructies en politieregistraties. Ten derde is in de literatuur gezocht naar best practices voor de integrale aanpak van cybercriminele jeugdgroepen. Kortom, de literatuurstudie droeg bij aan het beantwoorden van onderzoeksvragen binnen alle sporen van deze studie.
Qua literatuurstudie hebben we gekozen voor een non-systematische narratieve literatuurreview. We hebben gezocht naar relevante literatuur in de gangbare wetenschappelijke databases (ACM Digital Library, EBSCOhost, ProQuest, Scopus, Web of Science, Wiley Online Library). Daarbij hebben we ons gericht op zowel kwalitatieve als kwantitatieve Nederlandstalige en Engelstalige academische literatuur over de ontstaans- en groeiprocessen, de structuur en samenstelling, en de (cyber)criminele activiteiten van traditionele en cybercriminele (jeugd)groepen. Gegevens die we hebben geëxtraheerd uit de relevante literatuur waren de methodologie (zoals de onderzoeksvragen, het onderzoeksdesign, de methode van dataverzameling, de deelnemers en het type data), de belangrijkste resultaten, de conclusie en de beperkingen.

2.2 Expertinterviews

De tweede onderzoeksmethode bestond uit interviews met praktijkprofessionals die betrokken waren bij het onderzoeken en/of de aanpak van (cyber)criminele jeugdgroepen. Deze expertinterviews dienden twee doelen. In de eerste plaats is met behulp van deze interviews zicht verkregen op bekende criminele jeugdgroepen en hun (cyber)criminele activiteiten (spoor 1). Tegelijkertijd werd tijdens de interviews ook gevraagd naar aanwijzingen voor het bestaan van 'nieuwe' cybercriminele groepen, die nog niet op de radar stonden van lokale veiligheidscoalities (spoor 2). Het is immers mogelijk dat afzonderlijke praktijkprofessionals, zoals een digitale wijkagent of jongerenwerker, wel weet hebben van cybercriminele activiteiten van jeugdgroepen, maar dat die vooralsnog buiten het zichtveld blijven in de systemen van veiligheidspartners en/of de (integrale) aanpak van jeugdgroepen. Het tweede doel van de interviews was het krijgen van inzicht in de bestaande aanpak van jeugdcriminaliteit, best practices en

verbeterpunten. Op deze manier droegen de interviews ook bij aan het in kaart brengen van mogelijkheden voor de integrale aanpak van cybercriminele groepen (spoor 3).

2.2.1 *Beschrijving experts*

In totaal zijn 39 experts geïnterviewd. We hebben interviews gehouden met politiemedewerkers (n = 8), gemeentemedewerkers (n = 7), officieren van justitie en andere OM-medewerkers (n = 4), jongerenwerkers (n = 4), medewerkers van basis- en middelbare scholen (n = 2), leerplichtambtenaren (n = 2), een fraudespecialist van een bank (n = 1) en een fraudespecialist van een telecomprovider (n = 1). Daarnaast hebben we één focusgroep gehouden met 10 personen (politiemedewerkers = 2, bankwezen = 8, zie Tabel 2). De 29 personen die we via de reguliere interviews hebben gesproken (man = 17, vrouw = 12), hebben we in 21 interviews gesproken. Bij 6 van deze interviews was meer dan één expert aanwezig. De interviews vonden plaats op locatie (n = 12) of online (n = 9), duurden tussen de 38 en 120 minuten (M = 66, SD = 23,14), en werden allemaal opgenomen op een beveiligde audiorecorder (zie ook paragraaf 2.8).
Naast de reguliere interviews hebben we ook een focusgroep gehouden met 10 deelnemers (man = 7, vrouw = 3). Dit was een groepsinterview, omdat de betreffende deelnemers als team wilden worden geïnterviewd. Dit vond op locatie plaats en duurde 68 minuten.

Tabel 2. Beschrijving van de geïnterviewde praktijkprofessionals

Respondent-nummer	Instantie	Aantal respondenten bij het interview	Kennis van cybercriminele jeugdgroepen
R1	Gemeente	1	Nee
R2	Gemeente	1	Nee
R3	Gemeente	2	Nee
R4	Nederlandse Politie	1	Ja
R5	Nederlandse Politie	1	Ja
R6	Nederlandse Politie	1	Ja
R7	Gemeente	3	Ja
R8	Nederlandse Politie	1	Ja
R9	Bank	1	Ja
R10	Telecom	1	Ja
R11	OM	1	Nee
R12	Nederlandse Politie	1	Ja
R13	Middelbare school	1	Nee
R14	Jongerenwerk	2	Nee
R15	OM	1	Ja
R16	Basisschool	1	Nee
R17	Jongerenwerk	2	Ja
R18	OM	1	Nee
R19	Nederlandse Politie	3	Ja
R20	Gemeente (leerplicht)	2	Nee
R21 (focusgroep)	Bank (n = 8) Nederlandse Politie (n = 2)	10	Ja
R22	OM	1	Ja

2.2.2 *Werving van de respondenten*

Voor de werving van de experts is nauw samengewerkt met de consortiumpartners. Aan hen is gevraagd om binnen hun netwerk te zoeken naar professionals die voldeden aan alle vooraf vastgestelde selectiecriteria: (1) betrokkenheid bij (de aanpak van) traditionele en/of cybercriminele jeugdgroepen; (2) kennis en ervaring met traditionele en/of cybercriminele jongeren en/of jeugdgroepen; en (3) werkzaam bij een lokale veiligheidspartner in Drenthe, Groningen en/of Friesland of bij een landelijke partner die actief is in de aanpak van cybercrime. Na toestemming van de potentiële deelnemer werden diens contactgegevens met ons gedeeld.
Daarna zijn zij in eerste instantie benaderd via e-mail. In deze e-mail werd toegelicht hoe wij aan hun contactgegevens waren gekomen, wat het doel was van de studie en het interview, hoe het interview zou verlopen en hoe de anonimiteit en de veilige opslag

van gegevens waren gewaarborgd. Ook was een *informed consent*-formulier toegevoegd als bijlage (zie bijlage A voor de e-mail en bijlage B voor het formulier). Als een potentiële deelnemer op onze e-mail reageerde en aangaf interesse te hebben in een interview, dan planden we een afspraak voor het interview. Wanneer een reactie op de eerste e-mail uitbleef, volgde een herinneringsmail en uiteindelijk een telefonische follow-up, die dezelfde inhoud had als de eerste e-mail. In totaal hebben we 34 personen benaderd. Daarvan hebben 25 personen aangegeven geïnterviewd te willen worden. 3 personen hebben niet gereageerd en 6 personen gaven aan geen interview te willen. Daarmee was de response rate 74%. Omdat in 4 van de interviews ook experts aanwezig waren die we in eerste instantie niet hadden benaderd, maar die waren uitgenodigd door de benaderde collega, kwam het totaal aantal experts dat we uiteindelijk hebben geïnterviewd uit op 39.

2.2.3 *Procedure*

De expertinterviews waren semigestructureerd. Het interviewprotocol dat is gebruikt tijdens de interviews is opgesteld aan de hand van de onderzoeksvragen, de literatuur (beschreven in hoofdstuk 3) en de Monitor Georganiseerde Criminaliteit (Kruisbergen et al., 2018a), en is opgebouwd uit vier onderdelen (zie Bijlage C voor het interviewprotocol).
Allereerst werd gevraagd naar algemene informatie over de deelnemer, zoals diens organisatie, functie en de wijze waarop de deelnemer betrokken was bij het onderzoeken en/of de aanpak van traditionele en/of cybercriminele jeugdgroepen. Vervolgens is ieder spoor afzonderlijk afgelopen. Binnen spoor 1 zijn we dieper ingegaan op de traditionele en cybercriminele jeugdgroepen die bekend waren bij lokale veiligheidscoalities. Als de experts kennis hadden van dergelijke groepen werden vragen gesteld over het ontstaan, de groei, de structuur en de samenstelling van deze groepen. Ook is ingegaan op de aard en modus operandi van de gepleegde delicten en de eventuele verwevenheid van traditionele en cybercriminele delicten. Verder zijn de demografische kenmerken en criminele carrière van groepsleden uitgevraagd en is doorgevraagd naar de manier waarop zicht is verkregen op deze groepen.
Spoor 2 richtte zich op cybercriminele jeugdgroepen die mogelijk nog onbekend waren bij lokale veiligheidspartners. Daarbij werden grotendeels dezelfde vragen gesteld als bij spoor 1, aangevuld met vragen over de mate waarin andere zorg- en veiligheidspartners op de hoogte waren van deze groepen. Tot slot stond in spoor 3 de (integrale) aanpak van criminele jeugdgroepen centraal. Daarbij is stilgestaan bij de bestaande aanpak van traditionele en/of cybercriminele jeugdgroepen, de wijze waarop de groepsaanpak georganiseerd is, in hoeverre er sprake is van een integrale aanpak, welke actoren daarbij betrokken zijn, hoe de aanpak eruitziet, wat de sterke en zwakke punten zijn van deze aanpak en of er nog aanpakken en/of interventies in ontwikkeling zijn.

2.2.4 *Beperkingen van expertinterviews*

Het interviewen van experts heeft enkele beperkingen. Allereerst hebben we respondenten geselecteerd en benaderd op basis van hun kennis, ervaring en beschikbaarheid. Daarmee hebben we gebruikgemaakt van *convenience* en *purposive sampling*. Hierdoor kan er sprake zijn van *selection bias*, waardoor de steekproef mogelijk niet volledig representatief is (Whitley et al., 2013). Experts werden geselecteerd door ons consortium. Daarbij hadden de personen die we geïnterviewd hebben affiniteit met het thema cybercrime. Vermoedelijk hebben ze daardoor een ander perspectief dan andere professionals binnen de veiligheidsketen.
Daarnaast is het mogelijk dat individuen die openstaan voor een interview mogelijk andere informatie hebben dan personen die niet wilden deelnemen aan een interview. Politiemedewerkers die bijvoorbeeld betrokken zijn bij internationale *high profile* opsporingsonderzoeken zouden een interview kunnen weigeren om zo geen gevoelige en vertrouwelijke informatie prijs te geven. Dergelijke internationale opsporingsonderzoeken naar cybercriminele jeugdgroepen kunnen mogelijk andere informatie geven over het ontstaan, de groei en de structuur van deze groepen. Tot slot hebben de geïnterviewde praktijkprofessionals enkel zicht op (cyber)criminele jeugdgroepen die bij hen bekend zijn. Groepen die nog onder de radar opereren zijn daarom niet besproken in de interviews. Mogelijk verschillen deze in kenmerken van de groepen die in dit onderzoek wél aan bod kwamen. De bevindingen dienen daarom met enige terughoudendheid geïnterpreteerd te worden.
Desondanks achten wij de steekproef van geïnterviewde respondenten een goede afspiegeling van het totaal aantal experts op het gebied van problematische en (cyber) criminele jeugd. Dit heeft drie redenen. Allereerst is het onderzoek (grotendeels) afgebakend tot een beperkt geografisch gebied (Noord-Nederland). Ten tweede hebben we bij het benaderen van respondenten ons consortium ingezet. Iedere consortiumpartner beschikt over een eigen netwerk van experts. Door aan al onze partners te vragen om potentiële deelnemers aan te dragen voor een interview, nemen we aan dat we een representatieve groep experts hebben geïnterviewd. Tot slot kwam in de interviews een consistent beeld naar voren, wat suggereert dat er sprake was van saturatie. Dat doet vermoeden dat het verkregen beeld representatief is voor de onderzochte doelgroep. Uiteraard blijft het mogelijk dat de groep geïnterviewde experts selectief is samengesteld, maar gezien de multidisciplinaire samenstelling achten wij dit onwaarschijnlijk (Fusch & Ness, 2015).

2.3 Analysestrategie expertinterviews

De expertinterviews zijn (gedeeltelijk) automatisch getranscribeerd met behulp van Amberscript (zie paragraaf 2.7 voor een uitgebreide beschrijving van deze software). Vervolgens zijn ze geanalyseerd in Atlas.ti aan de hand van een combinatie van deductieve en inductieve thematische analyse.

Voorafgaand aan de analyse is een codeboek opgesteld, gebaseerd op de onderzoeksvragen, de literatuurstudie, het interviewprotocol en de Monitor Georganiseerde Criminaliteit (deductieve aanpak) (Braun & Clarke, 2006). Het codeboek bestond uit drie hoofdcategorieën, corresponderend met de drie sporen die in dit onderzoek centraal staan. Iedere categorie was verdeeld in thema's. Ieder thema bestond uit subthema's, die weer bestonden uit codes (zie bijlage D).
De eerste categorie richtte zich op (cyber)criminele jeugdgroepen die bekend waren bij lokale veiligheidscoalities. Deze categorie omvatte de volgende thema's: (1) algemene informatie over de voor de respondent bekende groepen; (2) structuur; (3) ontstaan en groei; (4) demografische en persoonlijkheidskenmerken leden; (5) criminele carrière individuele leden; en (6) delicten. De tweede categorie betrof cybercriminele jeugdgroepen die nog onbekend waren bij lokale veiligheidscoalities, maar die al wel op de radar stonden bij één of enkele lokale actoren. Deze categorie bevatte, naast dezelfde zes thema's als spoor 1, een extra thema: kennis van zorg- en veiligheidspartners over de bij de respondent bekende groepen. De derde categorie richtte zich op de (integrale) aanpak van (cyber)criminele jeugdgroepen in Noord-Nederland. Deze categorie bestond uit de volgende thema's: (1) zicht op criminele groepen; (2) aanpak en interventies; en (3) preventie.
Naast deze deductieve categorisatie zijn de thema's van dit codeboek tijdens de analyse van de interviews aangevuld met nieuwe codes die uit de data naar voren kwamen (inductieve aanpak) (Braun & Clarke, 2006). Door zowel een inductieve als deductieve methode toe te passen, hebben we gebruikgemaakt van een hybride aanpak bij het analyseren van de interviews. Deze aanpak combineert het voordeel van een theorie-geïnformeerde, deductieve analyse, met de mogelijkheid om nieuwe, relevante inzichten uit de data te integreren via een inductieve aanpak (Fereday & Muir-Cochrane, 2006).
Na de codering zijn de codes per thema systematisch met elkaar vergeleken en zijn ze via een patroonanalyse de onderliggende patronen, verschillen en overeenkomsten tussen codes geïdentificeerd. Binnen het thema 'ontstaan en groei' hebben we bijvoorbeeld alle data die waren gelabeld met de code 'hoe betrokken bij groep' systematisch naast elkaar gelegd om zo de verschillende rekruterings- en toetredingsmechanismes te identificeren. Deze werkwijze hebben we herhaald voor alle codes.

2.4 Zaakreconstructies

Tijdens eerdere bijeenkomsten met de betrokken consortiumpartners bleek dat er in Noord-Nederland enkele cybercriminele jeugdgroepen actief waren. Door een casusgebonden documentenanalyse en verdiepende interviews met betrokkenen hebben we de geleerde lessen in kaart gebracht. Centrale vragen daarbij waren: hoe is de betreffende groep geïdentificeerd en wat zijn best practices voor de (integrale) aanpak ervan?
De interviews voor de zaakreconstructies verschilden van de expertinterviews doordat ze specifiek gericht waren op concrete casussen en de best practices die daaruit gehaald konden worden. Feitelijk hanteerden we hierbij de methode van de Monitor Georgani-

seerde Criminaliteit. Dit is een langlopend project, waarbij opsporingsonderzoeken naar georganiseerde criminaliteit kwalitatief worden geanalyseerd. Al decennialang blijken zaakreconstructies daarin een beproefde methode om vormen van criminaliteit waar nog weinig kennis over is, zoals cybercrime, inzichtelijk te maken (zie Kleemans, 2016; Leukfeldt & Kleemans, 2021). De zaakreconstructies leverden een bijdrage aan de beantwoording van de onderzoeksvragen binnen alle onderzoekssporen.

2.4.1 *Verkrijgen van de zaakreconstructies*

Ook bij de organisatie van de zaakreconstructies speelden consortiumpartners een bemiddelende rol: zij hadden zicht op relevante casuïstiek waarin sprake was van een integrale aanpak van cybercriminele jeugdgroepen in Noord-Nederland. Via hen is de vraag uitgezet om relevante casuïstiek aan te leveren.
We ontvingen één RIEC-casus (die gerelateerd kan worden aan drie opsporingsonderzoeken) en vier separate opsporingsonderzoeken naar cybercriminele samenwerkingsverbanden. Het betrof één onderzoek naar een cybercriminele groep in RIEC-verband in Noord-Nederland, waarvoor geen inzage in persoonsgegevens nodig was (zaakreconstructie C1). Over dat onderzoek is namelijk een artikel verschenen in het *Tijdschrift voor Veiligheid*, dat het vertrekpunt heeft gevormd voor de reconstructie. De overige vier onderzoeken zijn afgeronde opsporingsonderzoeken (zaakreconstructies C2-5). Voor de selectie van die onderzoeken hebben we als criterium gehanteerd dat het moest gaan om onderzoeken waarin sprake was van een groep van jeugdigen (12-24 jaar) die in gezamenlijkheid betrokken waren bij online criminaliteit. Daarbij heeft de districtsrecherche één casus aangedragen (zaakreconstructie C2). De cyber-parketsecretaris van het OM in Noord-Nederland leverde vanwege zijn diepgravende dossierkennis drie geschikte onderzoeken aan (zaakreconstructies C3-5).
Vanwege de proportionaliteit en subsidiariteit van informatiedeling is een gelaagde werkwijze gehanteerd. Proportionaliteit houdt in dat de gedeelde informatie in redelijke verhouding staat tot het doel van dit onderzoek. Subsidiariteit betekent dat steeds de informatiebron met de minste persoonsgegevens wordt ingezet om de onderzoeksvragen te beantwoorden. Concreet hebben we gezocht naar een evenwicht tussen het verkrijgen van alle informatie die noodzakelijk is voor het beantwoorden van de onderzoeksvragen, en het zo veel mogelijk beperken van de toegang tot persoonsgegevens en andere gevoelige informatie. Daarom hebben we bewust gekozen voor afgeronde opsporingsonderzoeken die ook al voor de rechter zijn gebracht. Op die manier kon de documentenanalyse in eerste aanleg worden verricht op basis van de beschikbare ECLI's via rechtspraak.nl. Vervolgens is voor de RIEC-casus een senior analist / themahouder cybercrime van het RIEC geïnterviewd, die betrokken was bij de casus. Voor onderzoek dat we kregen via de districtsrecherche hebben we een interview gehouden met de betrokken teamleider. Voor de onderzoeken die we via het OM kregen, is de cyber-parketsecretaris geïnterviewd die bij alle zaken betrokken is geweest, vanwege diens dossier- en dossieroverstijgende kennis.

2.4.2 *Kenmerken van de zaakreconstructies*

In totaal hebben we vijf zaakreconstructies geanalyseerd: één van het RIEC Noord-Nederland, één van de districtsrecherche en drie van het OM. De districtsrecherche-casus bestond uit één ECLI en de drie door het OM aangeleverde casussen bestonden uit vijf ECLI's. Tabel 3 toont een compleet overzicht van de methodologische kenmerken van de zaakreconstructies.

Tabel 3. Methodologische kenmerken van de zaakreconstructies

Zaakreconstructie ID	Hoe verkregen	Bron	Wie geïnterviewd
C1	RIEC Noord-Nederland	Publicatie *Tijdschrift voor Veiligheid*	Senior analist / thema-houder cybercrime
C2	Districtsrecherche	ECLI	Teamleider
C3	OM	ECLI	Cyber-parketsecretaris
C4	OM	ECLI	Cyber-parketsecretaris
C5	OM	ECLI	Cyber-parketsecretaris

2.4.3 *Analysestrategie*

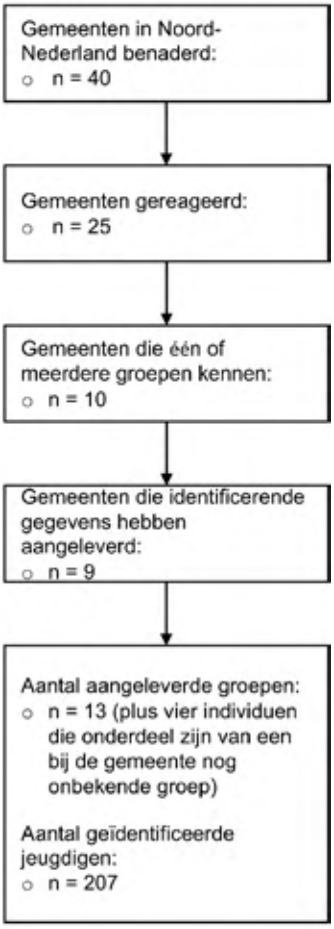
Alle zaakreconstructies en bijbehorende interviews zijn geanalyseerd in Atlas.ti, waarbij we hebben gebruikgemaakt van deductieve en inductieve thematische analyse (Braun & Clarke, 2006). Op basis van de onderzoeksvragen, de literatuur en de Monitor Georganiseerde Criminaliteit hebben we, voorafgaand aan de analyse, een codeboek opgesteld (zij bijlage E). Dit codeboek omvatte de volgende acht thema's: (1) zaakgegevens; (2) overzicht (opsporings)onderzoek; (3) structuur en samenstelling; (4) ontstaan en groei; (5) kenmerken van leden; (6) activiteiten en werkwijze; (7) omvang, verdeling en besteding van het wederrechtelijk verkregen voordeel; en (8) aanpak. Tijdens het analyseren zijn aanvullend nieuwe codes toegevoegd als deze vanuit de data naar voren kwamen en nog niet in het oorspronkelijke codeboek waren opgenomen. Binnen elk thema en subthema hebben we vervolgens de verschillende codes systematisch met elkaar vergeleken om zo patronen, overeenkomsten en verschillen te identificeren.

2.5 Politieregistraties

Om een dieper inzicht te krijgen in de verwevenheid tussen traditionele jeugdgroepen en cybercriminele activiteiten (spoor 1) en om zicht te krijgen op eventuele nieuwe cybercriminele jeugdgroepen (spoor 2), hebben we gebruikgemaakt van registraties uit de systemen van de politie. De werkwijze per spoor wordt hieronder toegelicht.

2.5.1 *Het verzamelen en analyseren van politieregistraties*

Vanwege hun regiefunctie bij de aanpak van criminele jeugdgroepen is aan alle gemeenten in Noord-Nederland (n = 40) gevraagd of er bij hen criminele jeugdgroepen bekend waren (spoor 1). Op onze vraag werd gereageerd door 25 gemeenten. Daarvan gaven er 10 aan dat zij één of meer groepen kenden, waarvan 9 gemeenten ook de identificerende gegevens hebben aangeleverd. Dit resulteerde in informatie over 13 bij gemeenten bekende groepen en 4 individuen die onderdeel zijn van een groep die bij de gemeente vooralsnog onbekend is. In totaal zijn 207 jeugdigen geïdentificeerd. Figuur 1 illustreert dit proces.



Figuur 1. Schematische weergave van het benaderen van gemeenten en het verkrijgen van gegevens van bekende jeugdgroepen

Per gemelde groep is gevraagd naar identificerende gegevens[6] van de groepsleden die bij de gemeente bekend waren. Het verstrekken van de identificerende gegevens door gemeenten aan de politie was juridisch geborgd via het ingerichte handhavingsknelpunt bij het RIEC. Daarmee was gegevensuitwisseling tussen partners mogelijk conform het daarvoor geldende privacyprotocol. In samenwerking met de intelligenceorganisatie van de politie is vervolgens in kaart gebracht in hoeverre in de politiesystemen aanwijzingen bestaan voor de betrokkenheid van de groepen (en hun individuele leden) bij cybercrime.

Daarna hebben we cybercrimeregistraties over de periode van één jaar geanalyseerd, op basis van de Landelijke Cybercrime Query (LCQ), om te onderzoeken in hoeverre in Noord-Nederland ook 'nieuwe' en bij lokale veiligheidscoalities nog onbekende jeugdige cyberdaders actief waren in groepsverband. De periode waarop de registraties betrekking hebben, is dezelfde periode als waarop de uitvraag onder gemeenten betrekking heeft.

Deze data werden gebruikt om in kaart te brengen in hoeverre de bij gemeenten bekende jongeren ook bij de politie bekend waren als verdachte van cybercrime. Daarnaast hebben we deze data gebruikt om te onderzoeken in hoeverre in Noord-Nederland ook 'nieuwe' en bij lokale veiligheidscoalities nog onbekende jeugdige cyberdaders actief waren in groepsverband. Een data-analist van de politie heeft hiervoor de LCQ gebruikt om te zoeken in de registratiedatabase van de politie. Hiermee worden registraties gevonden die een relatie hebben met zowel cybercrime in enge zin als gedigitaliseerde criminaliteit. Registraties over gedigitaliseerde criminaliteit kunnen echter buiten beschouwing zijn gebleven, omdat zij als 'traditioneel delict' zijn gelabeld en daardoor niet in alle gevallen in de 'cyber'-query worden meegenomen. Registraties werden geselecteerd als ze aan vijf criteria voldeden:

1. De registratie betrof cybercrime.
2. De registratie was aangemaakt tussen 1 september 2022 en 30 september 2023. Dit is dezelfde periode waarin gemeenten de gegevens van jongeren aanleverden die zij monitoren omdat die lid zijn van een problematisch of criminele jeugdgroep. Onderdeel van deze studie is het onderzoeken of deze jongeren zich ook bezighouden met cybercrime, en in hoeverre de gemeente daarvan op de hoogte is.
3. De verdachten in de registratie waren tussen de 12 en 24 jaar oud, conform de definitie van het Wetenschappelijk Onderzoeks- en Datacentrum van het ministerie van Justitie en Veiligheid (Ferwerda & Van Ham, 2010, 2014; WODC, 2021).
4. De registratie bevatte minimaal twee verdachten. Daarmee sluiten we aan bij de definitie van problematische en criminele jeugdgroepen van het ministerie van Justitie en Veiligheid (Ministerie van Justitie en Veiligheid et al., 2022).
5. Minimaal één verdachte woonde in Drenthe, Groningen of Friesland, of de registratie was opgemaakt door een politie-eenheid in Noord-Nederland. Dit omdat we ons in dit onderzoek specifiek richten op cybercriminele jeugdgroepen in Noord-Nederland.

6 NAW, geboortedatum, BSN (als unieke identifier).

Vervolgens werden deze gegevens gepseudonimiseerd door de data-analist voordat wij ze ontvingen. Ze bevatten vijf variabelen: (1) BVH-nummer; (2) de cybercrime gekoppeld aan de registratie; (3) gepseudonimiseerd ID van de verdachte; (4) geboortedatum van de verdachte; en (5) de vier cijfers van het postcodenummer waarin de verdachte woont. In totaal bevatte de dataset 110 unieke verdachten en 54 unieke politieregistraties. Eén verdachte en bijbehorende registratie zijn verwijderd, omdat deze verdachte toch geen onderdeel bleek te zijn van een groep. De overgebleven 109 verdachten en 53 registraties vormden 26 groepen. In bijlage F wordt een voorbeeld van de gegevens beschreven.

Daarnaast hebben we deze dataset aangevuld met geografische informatie: de coördinaten van het centroid van iedere postcode. Deze data zijn verkregen via het RIEC. De coördinaten stelden ons in staat om de groepsleden op een privacyvriendelijke manier op een kaart te plotten. Vervolgens hebben we aan de hand van een socialenetwerkanalyse alle groepen uit deze data geïdentificeerd. Dit geeft een overzicht van alle groepen, hun structuur en waar de leden wonen.

Voor alle door de gemeente geïdentificeerde jeugdige verdachten hebben we aan de politie gevraagd om te kijken of die terug te vinden waren in de door hen aangeleverde data. Dit is door de politie gedaan, waarna de politie aangaf voor welke verdachten dit van toepassing was.

Voor de inhoudelijke analyse van de geïdentificeerde groepen was inzage nodig in de politieregistraties over de leden die bij deze groepen betrokken waren. Een verkennende analyse van de Dienst Regionale Intelligence Organisatie (DRIO) van de Nederlandse Politie stelde vast dat het verstrekken van de registraties over de groepen en alle daarbij betrokken personen buitenproportioneel en voor analysedoeleinden bovendien ondoenlijk zou zijn. Per groepslid varieerde het aantal door te nemen politieregistraties (uit BVH) namelijk van enkele honderden tot enkele duizenden pagina's. Het doel van het onderzoek om inzicht te bieden in de aanwezigheid van cybercriminele groepen in de regio is met de gepseudonimiseerde data al behaald. Dat zijn er, verspreid over de regio, immers 26, waarvan de samenstelling varieert van 2 tot 23 groepsleden[7] (zie paragraaf 5.1). Voor het verkrijgen van inzicht in het ontstaan, de structuur, de samenstelling, de criminele activiteiten en de aanpak van de geïdentificeerde groepen kan ook worden volstaan met een analyse van een steekproef van alle data. Vanuit het oogpunt van proportionaliteit, subsidiariteit en (analysetechnische) haalbaarheid hebben we daar dus voor gekozen.

Uiteindelijk is er een gerichte steekproef uit de dataset getrokken. De steekproef is samengesteld op basis van drie selectiecriteria: (1) de omvang van de groep; (2) het type cyberdelict; en (3) de mate van lokale verankering. Hierbij is gekozen voor *purposive sampling;* een steekproefmethode om doelgericht te selecteren en om gedetailleerde inzichten te krijgen in de specifieke groepsstructuren en -leden. Deze methode is na-

7 De omvang van de groepen is gebaseerd op de aangeleverde gepseudonimiseerde politiedata. Uit de inhoudelijke analyse van zes van deze groepen bleek dat het daadwerkelijke aantal verdachten, zoals beschreven in de politieregistraties, groter was dan in eerste instantie gerapporteerd door de politie.

drukkelijk niet bedoeld om tot een generaliseerbaar beeld te komen (Whitley et al., 2013).

Hoewel het genereren van een representatief beeld niet het doel was, hebben we er bij de selectie van groepen wel naar gestreefd om maximale variatie in de drie selectiecriteria te waarborgen. Idealiter bestudeerden we dus groepen die verschillen in omvang, type delict en mate van lokale verankering. Dit resulteerde in de selectie van de groepen N3, N8, N12, N18, N21 en N24 (Tabel 4). Twee van deze groepen (N3 en N24) waren betrokken bij zowel traditionele criminaliteit als cybercrime. Omdat deze groepen criminele activiteiten plegen in zowel de offline als de online wereld, noemen we dit hybride groepen. De overige vier groepen (N8, N12, N18, en N21) hielden zich uitsluitend bezig met cybercrime, voor zover bekend vanuit de politiedossiers. Een belangrijke kanttekening hierbij is dat de LCQ enkel cybercrimeregistraties identificeert. Het is daarom niet verwonderlijk dat vier van de zes groepen exclusief cybercrime plegen. Per geïdentificeerde groep is over alle groepsleden de informatie uit BVH opgevraagd (beperkt tot artikel 8 en 13 van de Wet politiegegevens (Wpg)), waardoor we dus ook (voor zover beschikbaar) inzage hebben gekregen in aanwijzingen voor betrokkenheid bij andere criminele activiteiten. Daarmee is deze bevinding relatief betrouwbaar.

In totaal zijn zes groepen bestudeerd, waarin op basis van de query verspreid over de groepen 42 leden zijn geïdentificeerd die (in gezamenlijkheid) cybercrime plegen. Het betreft hier groepen die zijn geïdentificeerd omdat de daarbij betrokken subjecten gezamenlijk als verdachte voorkomen in één of meer cybercrimeregistraties die vallen binnen het bereik van de LCQ. De analyse is daarmee gebaseerd op in BVH gelabelde en dus gestructureerde informatie. Het kan zo zijn dat ook andere subjecten een rol spelen, dat de aan de groepen gekoppelde verdachten ook anderzijds betrokken zijn bij criminaliteit, bijvoorbeeld bij gedigitaliseerde criminaliteit die buiten het bestek van de LCQ valt, of bij traditionele delicten, zoals drugshandel, of dat rollen wellicht niet goed zijn gelabeld. Om de samenstelling van de groepen goed in kaart te brengen en ook te onderzoeken in hoeverre er aanwijzingen bestaan dat (leden van) de groepen ook anderzijds betrokken zijn bij online dan wel offline criminaliteit, is een deel van de verkregen politieregistraties inhoudelijk geanalyseerd.

Hoewel alle registraties zijn gescand, hebben we binnen de geselecteerde groepen vervolgens opnieuw een selectie gemaakt, met de focus op registraties over kernleden. De belangrijkste reden hiervoor was dat meer inzicht in deze kernleden een belangrijk doel van het onderzoek was. Daarnaast richtte dit onderzoek zich op het verbeteren van de verstoring van groepen. Een van de methoden om dit te doen is door interventies specifiek te richten op kernleden. Kernleden zijn hiervoor de meest geschikte doelgroep, omdat het doorgaans veel moeite kost om hen te vervangen.

Tabel 4. Kenmerken van de inhoudelijk geanalyseerde groepen op basis van de politieregistraties

Groep ID	Aantal leden*	Type delict	Geografische spreiding
3	9	Bankhelpdeskfraude, fraude bankgegevens	Verspreid
8	4	Aan- en verkoopfraude	Lokaal verankerd met perifere leden
12	3	Bankhelpdeskfraude	Verspreid
18	2	Bankhelpdeskfraude, fraude bankgegevens	Lokaal verankerd
21	2	Sextortion	Lokaal verankerd
24	2	Stalking	Verspreid

Noot. * De omvang van de groepen is gebaseerd op gepseudonimiseerde politiegegevens. De daadwerkelijke omvang van deze groep bleek na de inhoudelijke analyse groter te zijn

2.5.2 *Analysestrategie*

De data-analyse bestond uit twee stappen. Allereest hebben we een socialenetwerkanalyse uitgevoerd op de gepseudonimiseerde politiegegevens. Hiermee hebben we alle afzonderlijke groepen in de dataset geïdentificeerd en geografisch geplot. Bij het identificeren van groepen hebben we als uitgangspunt genomen dat verdachten die samen in dezelfde registratie voorkomen een onderlinge relatie hebben en daarmee onderdeel zijn van dezelfde groep. In de tweede stap hebben we de unieke registraties op basis waarvan de groepen zijn geïdentificeerd doorgenomen. Per groepslid zijn alle registraties gescand en bij focus op de kernleden uitvoerig geanalyseerd.
De inhoudelijke analyse was nagenoeg identiek aan de analysestrategie bij de zaakreconstructies. Daarbij hebben we geanonimiseerde uitwerkingen van de politieregistraties geanalyseerd in Atlas.ti, aan de hand van deductieve en inductieve thematische analyse (Braun & Clarke, 2006). Het codeboek was hetzelfde als bij de zaakreconstructies en bestond uit: (1) zaakgegevens; (2) overzicht (opsporings)onderzoek; (3) structuur en samenstelling; (4) ontstaan en groei; (5) kenmerken van leden; (6) activiteiten en werkwijze; (7) omvang, verdeling en besteding van het wederrechtelijk verkregen voordeel; en (8) aanpak. Binnen elk thema en subthema hebben we vervolgens de verschillende codes systematisch met elkaar vergeleken om zo patronen, overeenkomsten en verschillen te kunnen identificeren.

2.6 Daderinterviews

De tot nu toe beschreven databronnen bieden een breed perspectief op (cyber)criminele jeugdgroepen en hun leden. Ze hebben echter als belangrijkste beperking dat ze niet rechtstreeks afkomstig zijn van de jongeren zelf. Dit heeft tot gevolg dat de bronnen waarschijnlijk een vertekend beeld geven; daders en groepen die buiten het zicht van de experts en de politie blijven, hebben mogelijk afwijkende kenmerken ten op-

zichte van de wél geïdentificeerde leden en groepen. Om die reden is het ook belangrijk om de jongeren zelf te spreken.
Via consortium- en veiligheidspartners hebben we geprobeerd om in contact te komen met deze jongeren. Zo hebben we het OM, Reclassering Nederland en jongerenwerkers uit Noord-Nederland gevraagd of zij binnen hun eigen netwerk bekend waren met jongeren die betrokken waren bij cybercriminele activiteiten. Ook hebben we ons aangesloten bij wasstraten in Noord-Nederland. Ondanks deze inspanningen hebben we uiteindelijk slechts één dader kunnen spreken. De voornaamste reden hiervoor was dat bijna alle partners geen kennis hadden van potentiële respondenten relevant voor dit onderzoek. Deze ene dader is uiteindelijk niet meegenomen in de resultaten, omdat het maar een enkel interview betrof.

2.7 Software

De kwalitatieve analyses zijn uitgevoerd in Atlas.ti versie 25. De sociaalnetwerkanalyse en geografische analyse zijn uitgevoerd in R versie 4.3.3 (R Core Team, 2024) en R studio versie 2023.12.1+402 (RStudio Team, 2024). Voor data wrangling hebben we gebruikgemaakt van tidyverse (Wickham et al., 2019), here (Müller, 2017) en readxl (Wickham & Bryan, 2015). Het plotten van figuren en kaarten is gedaan met igraph (Csárdi et al., 2024), ggraph (Pedersen, 2017a), ggplot2 (Wickham et al., 2007), patchwork (Pedersen, 2019), gridExtra (Auguie, 2010), scales (Wickham et al., 2011), tidygraph (Pedersen, 2017b), cbsodataR (De Jonge, 2016) en sf (Pebesma & Bivand, 2023).

2.8 Ethiek en privacy

2.8.1 *Samenwerking RIEC en de wetenschap*

Voor dit onderzoek was sprake van een samenwerking tussen het RIEC Noord-Nederland en de wetenschap, vertegenwoordigd door het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving (NSCR) en het lectoraat Cybercrime en Cybersecurity van De Haagse Hogeschool. De achterliggende gedachte was dat het mes aan twee kanten snijdt: het in kaart brengen van cybercriminele jeugdgroepen in Noord-Nederland biedt partners in het RIEC-samenwerkingsverband kansen om adequaat invulling te geven aan de integrale aanpak van cybercrime. Dat thema heeft prioriteit binnen het Noord-Nederlandse RIEC. Tegelijkertijd zijn de inzichten die met het onderzoek worden opgedaan zowel vanuit methodologisch als inhoudelijk perspectief wetenschappelijk relevant: het onderzoek biedt zicht op (structurele) manieren om cybercriminele jeugdgroepen te identificeren en draagt bij aan het verkrijgen van inzicht in kenmerken van (leden binnen) cybercriminele jeugdgroepen, de verwevenheid met traditionele criminaliteit en mogelijkheden voor de aanpak van zulke groepen.

Om de samenwerking vorm te geven, zijn het onderzoek en het voornemen om daarin samen te werken met de wetenschap in december 2021 aangemeld als 'concreet handhavingsknelpunt (HHK)' bij het RIEC Noord-Nederland. Het gremium dat bevoegd is tot het inchecken van signalen binnen het RIEC-samenwerkingsverband, heeft toen aangegeven eerst antwoord te willen op twee vragen:

1. In hoeverre en op welke wijze is de voor het onderzoek beoogde gegevensuitwisseling onder het RIEC-convenant[8] mogelijk *tussen convenantpartners*?
2. In hoeverre en op welke wijze kan een eventuele samenwerking *met de wetenschap* vormgegeven worden, gelet op het verschil van insteek tussen het onderzoek in het kader van een handhavingsknelpunt in RIEC-verband en wetenschappelijk onderzoek dat wordt verricht door een kennisinstelling?

Juristen van de politie, het OM en het RIEC hebben zich over beide vragen gebogen en zijn in oktober 2022 tot het gezamenlijke oordeel gekomen dat de beoogde gegevensuitwisseling onder het RIEC-convenant mogelijk is én dat onder voorwaarden ook de samenwerking met de wetenschap kan worden vormgegeven.
Voor de samenwerking met de wetenschap werden de volgende voorwaarden toegepast:

- De onderzoeker van De Haagse Hogeschool is gedurende de looptijd van het onderzoek gedetacheerd bij het RIEC.
- De onderzoeker overlegt een VOG-P en tekent een geheimhoudingsverklaring.
- De onderzoeker is uitsluitend geautoriseerd voor het inzien van gegevens die strikt voor het onderzoek noodzakelijk zijn.
- Alle data die voor wetenschappelijke doeleinden zijn gebruikt, zijn geanonimiseerd alvorens ze door de wetenschappelijke instelling zijn verwerkt.

Ondanks deze voorwaarden en de goedkeuring van betrokken juristen, bleek deze constructie bij praktijkpartners toch nog (juridische) vragen op te roepen, onder andere bij het delen van (persoons)gegevens. Achteraf gezien zou de traditionele route via het PaG mogelijk sneller en eenvoudiger zijn geweest.

2.8.2 *Juridische grondslag voor inzage in opsporingsonderzoeken en politiedata*

Het aanmelden van het onderzoek als HHK biedt de mogelijkheid tot inzage in politiegegevens. De juristen van het RIEC, het OM en de politie kwamen echter tot de conclusie dat het inrichten van het HHK binnen het RIEC geen juridische grondslag biedt voor het gebruik van politie-informatie voor wetenschappelijke doeleinden (analyse en publicatie). Voor inzage in politiegegevens voor wetenschappelijke doeleinden is toestemming van het Parket-Generaal (PaG) van het OM vereist. In december 2022 heeft

8 Voluit: het Convenant ten behoeve van de Bestuurlijke en Geïntegreerde Aanpak Georganiseerde Criminaliteit, Bestrijding Handhavingsknelpunten en Bevordering Integriteitsbeoordelingen.

het PaG de onderzoekers daarvoor toestemming gegeven op basis van artikel 22 Wpg jo 4:7 lid 1 van het Besluit politiegegevens. Die toestemming is beperkt tot de verwerking van gegevens op grond van de artikelen 8 en 13, lid 1 van de Wpg, en is van toepassing op zowel de zaakreconstructies (analyse van opsporingsonderzoeken) als op de analyse van politieregistraties. De door de politie verstrekte data bevatten conform de reikwijdte van de toestemming van het PaG uitsluitend informatie die valt onder artikel 8 en 13 van de Wpg. Daarmee blijft informatie uit opsporingsonderzoek, anders dan in geanonimiseerde vorm via ECLI's, buiten beschouwing.

2.8.2.1 *Politieregistraties*

De door de politie verstrekte data bevatten conform de reikwijdte van de toestemming van het PaG uitsluitend informatie die valt onder artikel 8 en 13 van de Wpg. Daarmee blijft informatie uit opsporingsonderzoek buiten beschouwing, behalve de informatie die in geanonimiseerde vorm is beschreven in ECLI's. De politie heeft dat waar nodig vooraf steekproefsgewijs gecheckt en geverifieerd, bijvoorbeeld wanneer er ogenschijnlijk sprake was van informatie uit een onderzoek door de aanwezigheid van onderzoekshandelingen in het dossier. Een implicatie van deze werkwijze is dat het aantal geïdentificeerde groepen en in groepsverband bij cybercrime betrokken verdachten in Noord-Nederland feitelijk een onderschatting vormt van het daadwerkelijke aantal. Tegelijkertijd biedt deze informatie wel het juiste vertrekpunt voor het doel van dit onderzoek: het ontwikkelen van een instrument om lokale veiligheidscoalities in de toekomst ook te kunnen voeden met informatie over de aanwezigheid van cybercriminele jeugdgroepen. Bij het opwerken van een signaal binnen bijvoorbeeld de jeugdgroepenaanpak of het RIEC is het aannemelijk dat wordt gebruikgemaakt van politie-informatie die (wegens afbreukrisico) niet afkomstig is uit een lopend strafrechtelijk onderzoek (artikel 9).
De vanuit het OM betrokken professional en DRIO-medewerkers hebben vooraf samen gecheckt of het databestand dat uiteindelijk is gedeeld met de wetenschap en gebruikt voor wetenschappelijke analyses, geanonimiseerd was.

2.8.3 ***Waarborgen van privacy en veilige opslag***

Vanuit de wetenschappelijke kant is dit onderzoek voorgelegd aan de Ethische Commissie van De Haagse Hogeschool. De expertinterviews zijn opgenomen op een 256-bit versleutelde audiorecorder. De audiobestanden hierop zijn alleen toegankelijk met een geavanceerd wachtwoord dat alleen bekend is bij de onderzoeker die de interviews heeft uitgevoerd. Bij diefstal of verlies van deze audiorecorder zijn alle bestanden hierop dus niet toegankelijk voor derden. Na afloop van het interview werden de audiobestanden zo snel mogelijk op een XTS-AES 256-bits versleutelde USB-stick en Research Drive[9] gezet en werd het audiobestand verwijderd van de audiorecorder.

9 Een versleutelde online server van Surf die voldoet aan alle beveiligingseisen voor wetenschappelijk onderzoek.

De interviews werden verbatim (letterlijk) uitgewerkt[10] en gepseudonimiseerd met behulp van de transcriptiesoftware Amberscript. Het bedrijf dat deze service aanbiedt (Amberscript) heeft zijn hoofdkantoor in Nederland, slaat data op in Nederland, valt onder de Nederlandse wet- en regelgeving en voldoet aan de Algemene Verordening Gegevensbescherming (AVG), waarbij de audiobestanden en transcripten automatisch en versleuteld worden verwerkt. Voor het pseudonimiseren van de transcripten zijn de richtlijnen van het NSCR en De Haagse Hogeschool gehanteerd. Transcripten zijn eveneens opgeslagen op de beveiligde USB-stick en Research Drive en zijn alleen toegankelijk voor de onderzoekers. Ditzelfde geldt voor alle overige data die zijn gebruikt in dit onderzoek.

2.9 Resumé

In dit onderzoek hebben we vier onderzoeksmethoden toegepast: (1) literatuurstudie; (2) expertinterviews; (3) zaakreconstructies; en (4) een analyse van politieregistraties.

Literatuurstudie
Allereerst hebben we een non-systematische narratieve literatuurreview uitgevoerd, waarbij we hebben gezocht naar relevante literatuur in de gangbare wetenschappelijke databases (ACM Digital Library, EBSCOhost, ProQuest, Scopus, Web of Science, Wiley Online Library). Daarbij hebben we ons gericht op zowel kwalitatieve als kwantitatieve Nederlandstalige en Engelstalige academische literatuur. De literatuurstudie diende drie doelen:

1. Het krijgen van meer inzicht in de verschillende aspecten van (cyber)criminele groepen, zoals de ontstaans- en groeiprocessen, de structuur en samenstelling van deze groepen, en hun (cyber)criminele activiteiten.
2. Het vormen van de inhoudelijke basis voor de topiclijst voor de expertinterviews, de analyse van deze interviews en die van de zaakreconstructies en politieregistraties.
3. Het identificeren van best practices voor de integrale aanpak van cybercriminele jeugdgroepen.

Expertinterviews
Daarnaast hebben we 39 praktijkprofessionals geïnterviewd die betrokken waren bij het onderzoeken en/of de aanpak van (cyber)criminele jeugdgroepen en die werkzaam waren bij de Nederlandse politie, gemeenten, het OM, het jongerenwerk, het onderwijs, banken en telecomproviders. De interviews hadden twee doelen:

1. Inzicht krijgen in de bij lokale veiligheidscoalities bekende en onbekende cybercriminele jeugdgroepen.
2. Inzicht krijgen in de bestaande aanpakken, best practices en verbeterpunten.

10 De citaten in dit rapport zijn letterlijk overgenomen uit de interviews en zaakreconstructies, en kunnen daardoor grammaticaal niet helemaal juist zijn.

De interviews richtten zich op de kenmerken van traditionele en cybercriminele jeugdgroepen die (on)bekend waren bij lokale veiligheidscoalities en de (integrale) aanpak van deze jeugdgroepen.

Zaakreconstructies
Op basis van documentanalyses en verdiepende interviews hebben we vijf casussen over cybercriminele jeugdgroepen onderzocht. Die kregen we via het RIEC, de districtsrecherche en het OM. De RIEC-casus is geanalyseerd aan de hand van een publicatie in het *Tijdschrift voor Veiligheid*, de overige vier via ECLI's. De zaakreconstructies zijn gecodeerd via thematische analyse, waarbij we ons gericht hebben op de kenmerken van de groepen en hun leden, de gebruikte modus operandi en de (integrale) aanpak.

Politieregistraties
De laatste onderzoeksmethode betrof het analyseren van politieregistraties, om zo meer inzicht te krijgen in de verwevenheid tussen traditionele jeugdgroepen en cybercriminele activiteiten en om eventuele nieuwe cybercriminele jeugdgroepen in beeld te krijgen. Allereerst hebben we aan alle 40 gemeenten in Noord-Nederland gevraagd of zij jeugdgroepen in beeld hadden en of ze identificerende gegevens konden delen. Van de 40 gemeenten reageerden er 25. Daarvan hadden er 10 één of meer groepen in beeld, waarvan 9 gemeenten de identificerende gegevens deelden. Deze gegevens zijn gekoppeld aan politie-informatie om in kaart te brengen in hoeverre de bij gemeenten bekende jongeren ook bij de politie bekend waren als verdachte van cybercrime.
Daarnaast hebben we cybercrimeregistraties over de periode van één jaar geanalyseerd om te onderzoeken in hoeverre in Noord-Nederland ook 'nieuwe' en bij lokale veiligheidscoalities nog onbekende jeugdige cyberdaders actief waren in groepsverband. Hierbij hebben we eerst een socialenetwerkanalyse uitgevoerd om zo groepen te identificeren. Vervolgens hebben we zes groepen verder inhoudelijk geanalyseerd, waarbij we ons specifiek hebben gericht op kernleden. De analysestrategie kwam overeen met de strategie die we gebruikt hebben bij de zaakreconstructies.

Daderinterviews
Via consortium- en veiligheidspartners hebben we contact proberen te leggen met jongeren die actief waren binnen cybercriminele jeugdgroepen. De reden hiervoor is dat de expertinterviews, zaakreconstructies en politieregistraties als beperking hebben dat ze niet rechtstreeks afkomstig zijn van de jongeren zelf. Daardoor geven deze bronnen waarschijnlijk een vertekend beeld; daders en groepen die buiten het zicht van de experts en de politie blijven, hebben mogelijk afwijkende kenmerken ten opzichte van de wél geïdentificeerde leden en groepen. Om die reden is het ook belangrijk om de jongeren zelf te spreken.
We hebben geprobeerd om via Reclassering Nederland en jongerenwerkers uit Noord-Nederland in contact te komen met jongeren die betrokken waren bij cybercriminele activiteiten. Ook hebben we ons aangesloten bij wasstraten in Noord-Nederland. Ondanks deze inspanningen hebben we uiteindelijk slechts één dader kunnen spreken.

3 Literatuurstudie

In dit hoofdstuk bespreken we de relevante literatuur over traditionele en cybercriminele (jeugd)groepen. Verder besteden we aandacht aan de kenmerken van (cyber)criminele jongeren en staan we stil bij de huidige aanpakken en interventies. Alhoewel dit rapport betrekking heeft op (cyber)criminele *jeugd*groepen, besteden we ook aandacht aan traditionele en cybercriminele groepen die *niet* uitsluitend uit jongeren bestaan. Dit heeft twee redenen. Allereerst is er weinig wetenschappelijke literatuur die specifiek is gericht op cybercriminele *jeugd*groepen. Ten tweede is het van belang om het ontstaan, de groei en de structuur van cybercriminele jeugdgroepen en de kenmerken van de individuele leden te vergelijken met die van traditionele (cyber)criminele groepen (al dan niet bestaande uit volwassenen). Lokale veiligheidspartners beschikken namelijk al over enige ervaring met de aanpak van traditioneel georiënteerde groepen. Door ook naar volwassen (cyber)criminele groepen te kijken, kunnen we de mate van overlap tussen beide groepen onderzoeken. Aan de hand hiervan kan er bijvoorbeeld voor worden gekozen om bewezen aanpakken en interventies bij volwassen groepen ook in te zetten bij jeugdgroepen. Omdat het vermoeden bestaat dat er een overlap is in kenmerken tussen cybercriminele jeugdgroepen en cybercriminele groepen die niet uitsluitend bestaan uit jongeren, besteden we daarom ook aandacht aan deze laatste groep.
In dit hoofdstuk bespreken we eerst de structuur en samenstelling van traditionele en cybercrime (jeugd)groepen, gevolgd door hun ontstaan en groeiprocessen. Daarna volgen de kenmerken van de leden die actief zijn binnen deze groepen met aandacht voor demografische gegevens, criminele carrières en motivaties. Vervolgens bespreken we de aanpak van (cyber)criminele jeugdgroepen in Nederland. Het hoofdstuk eindigt met een samenvatting en een conclusie.

3.1 Kenmerken van traditionele en cybercriminele (jeugd)groepen

In deze paragraaf komen de kenmerken van traditionele en cybercriminele (jeugd) groepen aan bod. Daarbij staan we allereerst stil bij de structuur en de samenstelling daarvan, waarna we het ontstaan en de groei bespreken.

3.1.1 *Structuur en samenstelling*

In deze paragraaf beschrijven we de structuur en de samenstelling van (jeugd)groepen die betrokken zijn bij traditionele criminaliteit en cybercrime. Specifiek hebben we

aandacht voor hiërarchie, leiderschap, rolverdeling en de dynamiek binnen deze groepen.

3.1.1.1 *Traditionele criminele (jeugd)groepen*

Traditionele criminele samenwerkingsverbanden (groepen die betrokken zijn bij traditionele vormen van criminaliteit) kunnen sterk variëren in hun structuur en samenstelling. Aan de ene kant van het spectrum bevinden zich bureaucratische of piramidevormige *organisaties*. Dit zijn strikt hiërarchische organisaties met een duidelijke taakverdeling, gedragscodes en een eigen sanctiesysteem (Kleemans et al., 1998). Een voorbeeld hiervan is de Italiaanse maffia (Paoli, 2014). Aan de andere kant staan criminele *groepen*. Deze zijn, in vergelijking met piramidevormige organisaties, dynamischer (ze veranderen vaker van samenstelling), minder duurzaam (groepen zijn maar voor een korte periode actief) en minder hiërarchisch (Kleemans et al., 1998; Kleemans & Van de Bunt, 1999). Toch zijn de onderlinge relaties binnen deze samenwerkingsverbanden zelden volledig horizontaal. Zo beschikken sommige leden over persoonlijk gespecialiseerde kennis, vaardigheden en ervaringen (Bellotti et al., 2020; Duijn et al., 2014), terwijl andere leden juist veel sociale connecties hebben, binnen een criminele groep en in de bredere criminele wereld (Ficara et al., 2023). Dergelijke leden kunnen een prominente of centrale rol binnen de groep innemen (Kleemans et al., 1998; Kruisbergen et al., 2018a) en zijn veelal onderdeel van de kern van de groep.

Naast deze kernleden kunnen binnen traditionele criminele groepen ook facilitators actief zijn. Dit zijn personen die specifieke goederen en/of diensten leveren die leden van de groep zelf niet kunnen of willen verkrijgen of uitvoeren (Kleemans et al., 1998). Daarmee zijn facilitators essentieel voor het succesvol uitvoeren van bepaalde criminele activiteiten (Kleemans, 2007; Kruisbergen et al., 2018a). Facilitators kunnen twee soorten diensten leveren. Enerzijds kunnen ze bepaalde activiteiten uitvoeren die de groep niet zelf wil doen. Anderzijds kunnen ze ondersteuning bieden bij de uitvoering van misdrijven en het witwassen van illegaal verkregen geld (Kleemans et al., 1998; Kruisbergen et al., 2018a).

Een tweede type facilitator – ook wel brokers genoemd – bevindt zich in *structural holes*; plekken waar (delen van) groepen niet goed met elkaar verbonden zijn, bijvoorbeeld door geografische of sociale barrières (Burt, 1992; Kleemans, 2007, 2013). Brokers zijn dus verantwoordelijk voor het verbinden van deze (delen van) groepen (Kleemans, 2007, 2013). Voorbeelden zijn personen die grote sommen geld kunnen witwassen of die drugsgroepen tussen Nederland en bijvoorbeeld Zuid-Amerika met elkaar kunnen verbinden.

De jeugdige traditionele criminele samenwerkingsverbanden die actief zijn in Nederland hebben uiteenlopende vormen. Ze variëren van kleine groepjes tot grote groepen, van ongestructureerd tot sterk georganiseerd en van geïsoleerd tot open (Van Gemert & Weerman, 2013). Afhankelijk van de criminele activiteiten die worden gepleegd, kunnen deze jeugdgroepen zowel kenmerken van een bureaucratische organisatie als van een criminele groep vertonen (Mellor et al., 2005). Uit diverse Nederlandse onder-

zoeken[11] blijkt echter dat de meeste jeugdige samenwerkingsverbanden vooral als fluide groepen functioneren. Ze hebben een dynamisch karakter en hebben doorgaans geen strikte hiërarchie, organisatie of structuur (Beke et al., 2000; Esbensen & Weerman, 2005; Ferwerda & Van Ham, 2011; Peeters & Dongen, 2022; RIEC, 2022).
Hoewel deze groepen geen strikte, piramidale of bureaucratische structuur lijken te hebben, kan er wel sprake zijn van een machtsverdeling met verschillende rollen en taken, en kunnen ze wel uit meerdere lagen bestaan (Peeters & Dongen, 2022; RIEC, 2022; Van Gemert, 2005). Als een jeugdgroep uit meerdere lagen bestaat, kunnen die lagen bestaan uit: kernleden, doorgroeiers en jonge aanwas. Kernleden vormen het hart van de groep en hebben veelal een leidinggevende rol, waarbij ze de andere (minderjarige) leden aansturen en bepaalde klusjes laten uitvoeren (RIEC, 2022). Doorgroeiers zijn jongeren die al enige tijd betrokken zijn bij criminele activiteiten en steeds vaker ernstige delicten plegen, al dan niet in opdracht van hogere groepsleden. Zij hebben vaak de ambitie om verder door te groeien binnen de (georganiseerde) criminaliteit (Programma Straatwaarde(n), 2020; RIEC, 2022). De jonge aanwas maakt nog niet actief deel uit van de groep, maar hangt er al wel omheen en is betrokken bij het uitvoeren van kleine klusjes, zoals op de uitkijk staan (Programma Straatwaarde(n), 2020; RIEC, 2022).

3.1.1.2 *Cybercriminele (jeugd)groepen*

In de afgelopen jaren zijn er meerdere studies uitgevoerd naar cybercriminele samenwerkingsverbanden die zich bezighielden met onder andere phishing, banking malware, hacking en botnets. Deze groepen waren actief in onder andere Nederland, Zweden, Duitsland, het Verenigd Koninkrijk, de Verenigde Staten en Vietnam (Bulanova-Hristova et al., 2016; Kruisbergen et al., 2018a; Leukfeldt et al., 2016; Leukfeldt, Kleemans et al., 2017a, 2017b; Leukfeldt, Lavorgna et al., 2017; Leukfeldt & Holt, 2020; Lusthaus & Varese, 2021; Nguyen & Luong, 2021; Odinot et al., 2018). Uit deze onderzoeken blijkt dat cybercriminele samenwerkingsverbanden grotendeels als criminele groepen opereren en dat ze veel overeenkomsten vertonen met traditionele criminele groepen (Bulanova-Hristova et al., 2016; Kleemans et al., 1998).
In de literatuur worden twee typen cybercriminele groepen onderscheiden: (1) groepen met een stabiele kern; en (2) dynamische groepen. Groepen met een stabiele kern kenmerken zich door een relatief stabiele en vaste groep kernleden, terwijl de samenstelling van de overige lagen regelmatig kan wisselen. Deze groepen hebben doorgaans enige mate van hiërarchie en structuur. Zo bestaat een deel van de financieel gemotiveerde groepen uit kernleden, facilitators en geldezels (Brenner, 2002; Bulanova-Hristova et al., 2016; Leukfeldt et al., 2016; Leukfeldt, Kleemans et al., 2017a, 2017b; Leukfeldt, Lavorgna et al., 2017; Lusthaus et al., 2023; Nguyen & Luong, 2021; Nurse & Bada, 2019; Wall, 2015).

11 Waarbij vragenlijsten zijn afgenomen onder studenten, interviews zijn gehouden met experts en daders, en juridische informatie is geanalyseerd.

Kernleden zijn verantwoordelijk voor de coördinatie van de criminele activiteiten. Vaak vormen zij een relatief stabiele groep en werken ze langdurig samen. Deze stabiliteit lijkt voor een deel gerelateerd te zijn aan offline banden, waarbij kernleden elkaar al uit de fysieke omgeving kennen voordat ze onderdeel werden van de groep. Voorbeelden zijn jeugdvrienden (Veenstra, 2023) of zwagers (Loggen & Leukfeldt, 2022). Maar het kan ook voorkomen dat kernleden die onderdeel zijn van een stabiele groep geen offline banden met elkaar hebben, maar elkaar hebben leren kennen via virtuele *offender convergence settings*, ook wel criminele ontmoetingsplaatsen genoemd (Soudijn & Zegers, 2012). Binnen deze groep kernleden kan sprake zijn van een hiërarchie, waarbij één kernlid andere kernleden aanstuurt, en van een rolverdeling, waarbij ieder kernlid specifieke taken uitvoert (Leukfeldt, Lavorgna et al., 2017).

De tweede laag van statische cybercriminele groepen bestaat vooral uit facilitators, die specifieke diensten of goederen leveren waarmee cybercriminele activiteiten succesvol kunnen worden uitgevoerd. Dit kan variëren van het ontwikkelen van malware of phishing-websites tot het verstrekken van bankgegevens, het rekruteren van geldezels of het witwassen van wederrechtelijk verkregen voordeel (Leukfeldt et al., 2016; Leukfeldt, Lavorgna et al., 2017; Leukfeldt, 2014; Loggen & Leukfeldt, 2022). In de literatuur worden twee soorten facilitators beschreven. Professionele facilitators bieden uit eigen initiatief hun goederen en/of diensten aan en werken vaak samen met meerdere groepen. Gerekruteerde facilitators leveren ook goederen en/of diensten, maar worden door kernleden zelf gerekruteerd en opereren meestal binnen één groep. Zij spelen doorgaans een minder belangrijke rol en zijn eenvoudiger te vervangen dan professionele facilitators (Leukfeldt et al., 2016; Leukfeldt, Lavorgna et al., 2017; Leukfeldt, 2014; Loggen & Leukfeldt, 2022).

De derde laag van statische cybercriminele groepen bestaat uit geldezels en katvangers. Deze individuen worden door kernleden binnen de groep ingezet voor specifieke taken, zoals het ophalen van producten die zijn gekocht met illegaal verkregen geld (katvangers) of het beschikbaar stellen van hun bankpas en bankrekening (geldezels). In dit laatste geval wordt de bankrekening van geldezels gebruikt om illegaal verkregen bedragen op over te maken en vervolgens contant op te nemen (Bekkers et al., 2023; Leukfeldt, Lavorgna et al., 2017; Leukfeldt, 2014; Loggen & Leukfeldt, 2022; Schiks et al., 2021). Deze drie lagen zijn niet in iedere groep aanwezig. Sommige groepen maken geen gebruik van facilitators, bijvoorbeeld wanneer kernleden zelf de benodigde goederen of diensten kunnen leveren. Ook geldezels zijn niet altijd nodig, bijvoorbeeld in groepen die zich bezighouden met de handel in gestolen gegevens of wanneer vanaf de bankrekening van slachtoffers direct goederen worden gekocht via webshops (Leukfeldt, Lavorgna et al., 2017; Loggen & Leukfeldt, 2022).

Naast deze groepen met een meer stabiele kern, worden in de literatuur ook cybercriminele groepen beschreven met een meer dynamisch karakter. Deze groepen lijken grotendeels opportunistisch en ontstaan wanneer zich een gelegenheid voordoet om een delict te plegen. Leden van dergelijke groepen ontmoeten elkaar mogelijk op online plekken, waar ze mededaders zoeken met de juiste vaardigheden voor specifieke cybercrimes. In tegenstelling tot de meer stabielere groepen spelen langdurige relaties

hierbij een relatief onbelangrijke rol. Wel hebben dynamische groepen doorgaans eenzelfde rolverdeling: ze bestaan uit kernleden, facilitators en/of katvangers en geldezels (Brenner, 2002; Bulanova-Hristova et al., 2016; Choo & Smith, 2008; Hutchings, 2014; Leukfeldt, Kleemans et al., 2017b; Leukfeldt, Lavorgna et al., 2017; Odinot et al., 2018).

3.1.2 *Ontstaan en groei*

Bij het ontstaan en de groei van traditionele en cybercriminele (jeugd)groepen spelen verschillende factoren, mechanismen en processen een rol. De twee belangrijkste worden hieronder toegelicht: sociale gelegenheidsstructuren, sociale relaties, en offender convergence settings.

3.1.2.1 *Sociale gelegenheidsstructuur*

Een eerste mechanisme dat van invloed is op het ontstaan en de groei van cybercriminele (jeugd)groepen is de sociale gelegenheidsstructuur. Dit concept verwijst naar de sociale context en waarbinnen individuen toegang krijgen tot criminele kansen – bijvoorbeeld doordat ze via hun sociale omgeving in aanraking komen met personen die criminaliteit kunnen faciliteren (Kleemans & De Poot, 2008). Sociale gelegenheidsstructuren bepalen daarmee wie de mogelijkheid krijgt om betrokken te raken bij criminele activiteiten. Iemand die werkt als vrachtwagenchauffeur kan bijvoorbeeld via zijn werk in contact komen met een collega die bepaalde illegale producten smokkelt.

3.1.2.2 *Sociale relaties*

Ten tweede spelen offline banden een belangrijke rol bij het ontstaan en de groei van criminele groepen, omdat ze een oplossing bieden voor de problemen die ontstaan bij het aangaan van een crimineel samenwerkingsverband. Een voorbeeld van dergelijke problemen is egoïstisch en opportunistisch gedrag door leden, wat kan leiden tot instabiliteit binnen de groep. Wanneer individuen een sociale relatie met elkaar hebben, zoals verwantschap, vriendschap en romantische relaties, kennen ze elkaar al goed, hebben ze beiden in deze relatie geïnvesteerd en is de kans groot dat ze elkaar in de toekomst ook bij niet-criminele aangelegenheden tegenkomen (Kleemans et al., 1998). Dit verlaagt vervolgens de kans op problemen bij de samenwerking. Het verhoogt daarmee de stabiliteit van de groep en leidt ertoe dat de groep goed kan presteren.
Offline relaties ontstaan niet willekeurig; ze worden beïnvloed door de sociale en geografische afstand tussen individuen. Dit betekent dat wanneer mensen sociaal en geografisch dicht bij elkaar staan en regelmatig met elkaar in contact komen in het dagelijks leven, ze een relatief grote kans hebben om een band op te bouwen. Hieruit volgt dat leden van criminele groepen meestal in dezelfde buurt zijn opgegroeid, naar dezelfde school zijn gegaan of dezelfde etniciteit hebben. Dit wijst op relationele en lokale inbedding van deze groepen (Kleemans et al., 1998).

3.1.2.3 *Offender convergence settings*

Ten derde spelen offender convergence settings een belangrijke rol bij de totstandkoming en de groei van criminele samenwerkingsverbanden. Deze fysieke en virtuele plaatsen (Felson, 2003; Soudijn & Zegers, 2012) zijn specifieke locaties waar (potentiële) daders elkaar op bepaalde tijden kunnen ontmoeten, zonder toezicht van de autoriteiten. Daarmee kunnen ze eveneens als sociale gelegenheidsstructuur fungeren. Offender convergence settings zijn essentieel om vertrouwen in mededaders te ontwikkelen, om gedeelde criminele mogelijkheden te identificeren en criminele samenwerkingen aan te gaan. Deze plaatsen spelen dus een belangrijke rol bij het ontwikkelen van offline en online relaties; relaties die voorafgaand aan de criminele samenwerking nog niet bestonden. Een belangrijk kenmerk van deze settings is dat ze variëren in de tijd en in de mate van toezicht. Zo fungeert een speeltuin overdag, wanneer er kinderen en ouders aanwezig zijn, doorgaans niet als ontmoetingsplek voor daders. 's Nachts kan dat echter wel het geval zijn, wanneer de speeltuin donker, leeg en onbewaakt is (Felson, 2003).

Criminele ontmoetingsplaatsen worden gebruikt door zowel aspirant-daders en beginnende daders als door meer ervaren daders die op zoek zijn naar mededaders (Felson, 2003, 2006; Romagna & Leukfeldt, 2024b). Voor nieuwkomers bieden deze settings kansen om nieuwe vaardigheden te ontwikkelen, kennis op te doen en in contact te komen met meer ervaren daders (Felson, 2003, 2006; Maimon & Louderback, 2019). Voor actieve daders bieden dergelijke plaatsen de mogelijkheid om hun netwerk uit te breiden en nieuwe samenwerkingsverbanden aan te gaan met personen buiten hun directe sociale kring. Dit is van belang omdat personen binnen een sociaal netwerk vaak vergelijkbare kennis en vaardigheden delen (Ouellet et al., 2019). Met andere woorden, offender convergence settings maken het mogelijk om samenwerkingen aan te gaan met individuen die beschikken over kennis, vaardigheden en ervaring die noodzakelijk zijn om criminaliteit te plegen (Duijn et al., 2014; Felson, 2003).

3.1.2.4 *Traditionele criminele (jeugd)groepen*

Sociale gelegenheidsstructuren en al bestaande offline relaties spelen een belangrijke rol bij het ontstaan en de groei van veel traditionele criminele groepen (Adamse et al., 2024; De Boer et al., 2022; Kleemans et al., 1998). Zo zijn bij georganiseerde criminaliteit familie- en vriendschapsbanden van belang, zowel voor dynamische (transnationale) groepen als voor meer gestructureerde, maffia-achtige organisaties (Albini, 1971; Kleemans & Van de Bunt, 1999; Sciarrone, 2014). Kinderen van personen die betrokken zijn bij transnationale georganiseerde criminaliteit hebben bijvoorbeeld een grotere kans om in de voetsporen van hun ouders te treden (De Seranno & Colman, 2023; Spapens & Moors, 2020; Van Dijk et al., 2019). Bij maffia-achtige organisaties, zoals de Calabrische 'Ndrangheta, wordt de kerngroep vaak gevormd door familiebanden, die verder worden uitgebreid via gearrangeerde huwelijken (Sciarrone, 2014). Ditzelfde geldt voor (religieuze) terroristische organisaties (Holman, 2016; Magouirk et al., 2008; Schwarzenbach & Jensen, 2024). Bij jeugdbendes raken nieuwe leden veelal betrokken

via al actieve leden, die vaak deel uitmaken van het sociale netwerk van het lid, vooral familie en vrienden (Densley, 2012; Klein & Maxson, 2006; Pyrooz & Densley, 2016).
Jongeren kunnen op meerdere manieren betrokken raken bij traditionele criminele (jeugd)groepen. Allereerst kunnen ze geleidelijk in een groep terechtkomen, vaak door bestaande offline banden met groepsleden. Voorbeelden hiervan zijn vriendschappen, familiebanden, straatcontacten, werk, hobby's of vrijetijdsactiviteiten (Adamse et al., 2024; Beke et al., 2000; CCV, 2022; Densley, 2012; Kleemans & Van Koppen, 2020; Programma Straatwaarde(n), 2020; RIEC, 2022). Daarnaast komt het voor dat jongeren zich op eigen initiatief aansluiten bij een traditionele criminele (jeugd)groep. Dit kan plaatsvinden via geplande rekrutering, waarbij jongeren actief worden benaderd met de vraag of ze bijvoorbeeld bepaalde klusjes willen uitvoeren. Maar rekrutering kan ook ongepland plaatsvinden (Adamse et al., 2024; Beke et al., 2000; CCV, 2022; Programma Straatwaarde(n), 2020; RIEC, 2022). In beide gevallen spelen zowel offline als online contacten een rol (Programma Straatwaarde(n), 2020). Verder komt het voor dat jongeren toetreden tot een traditionele criminele groep omdat ze worden bedreigd of afgeperst door groepsleden (Programma Straatwaarde(n), 2020). Tot slot kunnen jongeren op eigen initiatief contact zoeken met leden van criminele groepen in een poging om onderdeel te worden van een groep (Adamse et al., 2024; Programma Straatwaarde(n), 2020).
Bij de toetreding van jongeren tot traditionele criminele (jeugd)groepen is er sprake een combinatie van offline banden en fysieke offender convergence settings. Toch lijken virtuele settings, in de vorm van online platforms, ook steeds belangrijker te worden. Zo komen jeugdige daders steeds vaker met elkaar in contact via sociale media, zoals Snapchat, Instagram, Telegram en TikTok (Bekkers et al., 2022; Bekkers & Leukfeldt, 2023; RIEC, 2022; Wolsink et al., 2023). Via dergelijke contacten in virtuele settings ontstaan vervolgens relaties die uiteindelijk leiden tot het ontstaan van criminele jeugdgroepen (RIEC, 2022; Wolsink et al., 2023).

3.1.2.5 *Cybercriminele (jeugd)groepen*

Ook bij cybercriminele groepen is bij het ontstaan en de groei een belangrijke rol weggelegd voor zowel offline relaties als fysieke en virtuele offender convergence settings. Volgens Leukfeldt en collega's (2016) kan het ontstaans- en groeiproces van groepen die betrokken zijn bij financiële cybercrime worden opgedeeld in vier groepen, verdeeld over twee categorieën. In de eerste categorie staan offline banden centraal. Cybercriminele groepen kunnen bijvoorbeeld exclusief via offline contacten en fysieke offender convergence settings ontstaan en groeien, waarbij kernleden elkaar kennen via onder andere familiebanden en vriendschappelijke of romantische relaties, omdat ze naar dezelfde school gingen of omdat ze in dezelfde buurt zijn opgegroeid (Bulanova-Hristova et al., 2016; Leukfeldt et al., 2016, 2019; Leukfeldt, 2014; Leukfeldt & Roks, 2021; Loggen & Leukfeldt, 2022; Lusthaus & Varese, 2021; Odinot et al., 2018). Facilitators en geldezels kunnen eveneens gerekruteerd worden via offline banden en fysieke settings. Denk aan: leeftijdsgenoten op school, kennissen of vrienden (Bekkers et al., 2023; Leukfeldt et al., 2019; Leukfeldt & Roks, 2021; Loggen & Leukfeldt, 2022). Een

groep kan daarnaast ook ontstaan en groeien doordat kernleden elkaar leren kennen via offline contacten, terwijl virtuele offender convergence settings, zoals bepaalde online fora, online games en sociale media (zoals Snapchat en Instagram) worden gebruikt om specialisten of geldezels te rekruteren (Bekkers & Leukfeldt, 2023; Bulanova-Hristova et al., 2016; Leukfeldt et al., 2016; Leukfeldt, Lavorgna et al., 2017; Ruiter et al., 2023).
In de tweede categorie staan online contacten centraal. Zo kunnen kernleden met elkaar in contact komen via online kanalen (zoals fora en sociale media), terwijl offline relaties en fysieke offender convergence settings worden gebruikt om lokale criminelen te benaderen. Tot slot kunnen groepen exclusief via online contacten en virtuele settings ontstaan en groeien (Leukfeldt, Lavorgna et al., 2017). Het gebruik van online kanalen om in contact te komen met mededaders biedt meerdere voordelen ten opzichte van offline contacten. Zo kunnen (potentiële) cyberdaders op internet niet alleen anoniem opereren, maar zijn ook de meeste online chatdiensten versleuteld, waardoor ze vrijuit kunnen communiceren zonder bang te hoeven zijn om afgeluisterd te worden. In beide gevallen wordt de drempel voor het aangaan van sociale banden en het plegen van criminaliteit verlaagd (Odinot et al., 2018).
Bij de meeste cybercriminele groepen die in de literatuur onderzocht zijn, lijken offline banden en fysieke offender convergence settings cruciaal te zijn (Leukfeldt, Lavorgna et al., 2017). Traditionele sociale contacten spelen dus, net als bij traditionele criminele groepen, een belangrijke rol (Kleemans et al., 1998; Kleemans & Van de Bunt, 1999; Leukfeldt et al., 2019, 2020; Leukfeldt & Roks, 2021). Datzelfde geldt voor vertrouwen en loyaliteit (Kleemans & Van de Bunt, 1999; Leukfeldt, Lavorgna et al., 2017; Odinot et al., 2018). Daarmee zijn deze cybercriminele groepen, ondanks hun internationale oriëntatie, vaak sterk lokaal ingebed (Kruisbergen et al., 2018a; Leukfeldt et al., 2019). Dat maakt de online component echter niet minder belangrijk. Ook bij de groepen waarbij offline offender convergence settings belangrijk zijn spelen online componenten een rol bij het rekruteren van mededaders, facilitators en geldezels (Leukfeldt et al., 2019; Leukfeldt, Lavorgna et al., 2017; Leukfeldt, 2014; Loggen & Leukfeldt, 2022).

3.2 De kenmerken van leden die actief zijn binnen traditionele en cybercriminele (jeugd)groepen

In deze paragraaf beschrijven we de kenmerken van jongeren en jongvolwassenen die actief zijn binnen traditionele en cybercriminele jeugdgroepen. Daarbij besteden we aandacht aan socio-demografische kenmerken, intrinsieke en persoonlijkheidskenmerken, familiegerelateerde kenmerken, de sociale omgeving en criminele carrières. Er is een gebrek aan wetenschappelijke literatuur die specifiek is gericht op jongeren die actief zijn binnen cybercriminele groepen. Daarom bespreken we ook literatuur over jongeren die niet specifiek actief zijn binnen dergelijke groepen. Allereerst beschrijven we de kenmerken van jongeren die betrokken zijn bij traditionele criminele groepen, gevolgd door de kenmerken van (jeugdige) cyberdaders.

3.2.1 *Traditionele criminele (jeugd)groepen*

Jongeren die actief zijn binnen georganiseerde criminele groepen zijn meestal man – vaker dan bij de meer doorsnee traditionele criminaliteit (Calderoni et al., 2022; De Boer et al., 2022). Deze jongeren lijken relatief vaker schoolproblemen te hebben, waaronder spijbelen, slechte schoolprestaties en een relatief lager opleidingsniveau, in vergelijking met jongeren die niet betrokken zijn bij criminaliteit (Calderoni et al., 2020, 2022; CCV, 2022; Frualdo, 2019; Peeters & Dongen, 2022; Programma Straatwaarde(n), 2020; RIEC, 2022; Weerman, 2014). Het risico op deelname aan georganiseerde criminaliteit wordt verder verhoogd door een relatief lagere sociaaleconomische status, het behoren tot een etnische minderheid of het ervaren van marginalisatie[12] (Calderoni et al., 2022; De Boer et al., 2022; Kleemans & Van Koppen, 2020; Programma Straatwaarde(n), 2020).
Ook antisociale persoonlijkheidskenmerken, zoals impulsiviteit en agressiviteit, lijken positief samen te hangen met rekrutering in de georganiseerde criminaliteit (Frualdo, 2019), net als gedrags- en emotionele problemen (Peeters & Dongen, 2022; Programma Straatwaarde(n), 2020; RIEC, 2022). Ditzelfde geldt voor drugsgebruik, een lichte verstandelijke beperking en een lagere mate van zelfcontrole (Calderoni et al., 2020; Frualdo, 2019; Peeters & Dongen, 2022; Programma Straatwaarde(n), 2020).
Jongeren die actief zijn binnen de georganiseerde criminaliteit lijken vaker op te groeien in eenoudergezinnen of problematische thuissituaties (door bijvoorbeeld psychische problematiek, financiële problemen of verslaving), terwijl niet-criminele jongeren juist vaker uit een 'traditioneel' gezin komen. (Calderoni et al., 2022; Peeters & Dongen, 2022; Programma Straatwaarde(n), 2020; RIEC, 2022). De afwezigheid van een vaderfiguur, een zwakke ouder-kindband, gebrek aan toezicht en gebrek aan emotionele steun lijken ook de kans op betrokkenheid bij georganiseerde criminaliteit te verhogen (Programma Straatwaarde(n), 2020; RIEC, 2022; Weerman, 2014).
Tot slot speelt de sociale omgeving een belangrijke rol in de betrokkenheid bij georganiseerde misdaad. Familieleden, vrienden of partners die al betrokken zijn bij georganiseerde criminaliteit vergroten de kans op rekrutering (Calderoni et al., 2020, 2022; CCV, 2022; Programma Straatwaarde(n), 2020). Ook de wijk waarin jongeren opgroeien lijkt van invloed te zijn. Zo groeien jongeren betrokken bij georganiseerde criminaliteit veelal op in kwetsbare wijken, die gekenmerkt worden door de aanwezigheid van drugs, criminele rolmodellen, armoede, weinig toezicht en verpaupering (Kemp et al., 2020; Programma Straatwaarde(n), 2020). In deze context wordt crimineel gedrag vaak gezien als normaal en de enige manier voor een betere toekomst (RIEC, 2022).

3.2.1.1 *Criminele carrière*

In Nederland lijken jongeren vaak al vroeg in de adolescentie betrokken te raken bij traditionele criminele (jeugd)groepen. Zo plegen ze veelal vóór hun 15e levensjaar

12 Het idee of gevoel systematisch buitengesloten te worden van volwaardige deelname aan belangrijke aspecten van de samenleving.

vooral lichte delicten (zoals winkeldiefstal). Voor jongens geldt dat de frequentie van het aantal gepleegde delicten toeneemt tot het rond hun 15e levensjaar een hoogtepunt bereikt en vervolgens vanaf het 21e levensjaar weer afneemt. Bij meisjes ligt deze piek rond het 18e levensjaar en is de afname van het aantal gepleegde delicten minder sterk in vergelijking met jongens. Een klein deel van de jongeren gaat op oudere leeftijd juist meer en zwaardere delicten plegen en groeit zo door binnen de georganiseerde criminaliteit (Kleemans & Van Koppen, 2020; Moffitt, 2007; RIEC, 2022).
Nederlandse jongeren hebben verschillende motivaties om zich aan te sluiten bij traditionele criminele (jeugd)groepen, zoals status, het vooruitzicht op snel en makkelijk geld verdienen en de behoefte om ergens bij te horen (CCV, 2022; De Boer et al., 2022; Programma Straatwaarde(n), 2020; RIEC, 2022). Het lidmaatschap van een criminele groep biedt een sociale identiteit, waardoor ze onderdeel worden van een subcultuur die een gevoel van verbondenheid geeft (De Boer et al., 2022). Tot slot worden ze gemotiveerd door erkenning of worden ze aangetrokken door sensatiezucht of de opwindende levensstijl (CCV, 2022; Programma Straatwaarde(n), 2020).

3.2.2 *Cybercriminele (jeugd)groepen*

Het aantal studies dat zich specifiek richt op de kenmerken van jongeren binnen cybercriminele groepen is beperkt. Daarom gaan we in deze paragraaf ook in op de kenmerken van de 'algemene' populatie cyberdaders. Het is bekend dat voor een deel sprake is van individueel opererende daders. Hoewel hun kenmerken deels delictafhankelijk zijn, is er een aantal overeenkomsten te ontlenen aan de literatuur die richting geeft voor het beleid. Om die reden, en omwille van de leesbaarheid, bespreken we kenmerken die terugkomen bij beide groepen daders gezamenlijk. Waar verschillen bestaan tussen cybercrime in enge zin en gedigitaliseerde criminaliteit lichten we dat expliciet toe. De resultaten in deze paragraaf zijn grotendeels gebaseerd op de systematische reviews van Loggen en collega's (2024b, 2024a). Wanneer een cyberdelict niet wordt benoemd bij een specifiek daderkenmerk, dan betekent dit dat hierover geen (robuuste) literatuur beschikbaar is.
Over het algemeen wordt cybercrime (waaronder hacking en online fraude) gepleegd door jonge mannen onder de 30 jaar (Bossler, 2021a; Chen et al., 2021; Chua & Holt, 2016; Fox & Holt, 2021). Zowel bij hacking als bij online fraude lijkt de sociale omgeving een belangrijke rol te spelen bij het betrokken raken bij deze delicten. Deviante vrienden kunnen hierbij fungeren als rolmodel en bron van kennisoverdracht, waardoor jongeren de benodigde vaardigheden leren om cybercriminaliteit te plegen en zo een grotere kans hebben om betrokken te raken bij dergelijke delicten (Adou & Kolé, 2020; Bossler, 2021b; Chon, 2016; Fox & Holt, 2021). Ook de gezinssituatie blijkt van invloed: beperkt ouderlijk toezicht en een instabiele gezinssituatie vergroten de kans op cybercrime (Holt & Steinmetz, 2021; Ibrahim, 2016; Kao et al., 2009; Lee & Holt, 2020; Ogunleye et al., 2020).
Hoewel er sprake is van gedeelde risicofactoren, zijn er ook duidelijke verschillen tussen deze typen daders. Hackers lijken doorgaans een relatief hogere sociaaleconomi-

sche status te hebben (Fox & Holt, 2021), terwijl die van online fraudeurs juist relatief lager lijkt te zijn (Chen et al., 2021; Jegede et al., 2016). Ook de motieven verschillen: hackers worden vaak gedreven door sensatiezucht, uitdaging, plezier, erkenning door *peers* en plezier (Cayubit et al., 2017; Chon, 2016; Van der Wagen et al., 2021), terwijl online fraude primair lijkt te worden gepleegd vanwege financieel gewin (Adejoh et al., 2019; Chen et al., 2021; Ogunleye et al., 2020).

Tot slot is er binnen cybercrime een aparte groep jongeren met technische vaardigheden, ook wel cyberbreinen genoemd. Deze jongeren houden zich veelal bezig met de meer complexe technische delicten, zoals hacken en het ontwikkelen en verspreiden van malware. Bij deze groep lijkt sprake te zijn van een unieke set risicofactoren. Specifiek lijkt er een positieve relatie te zijn tussen IT-kennis en betrokkenheid (Chua & Holt, 2016; Morris & Blackburn, 2009; Peersman et al., 2022). Ditzelfde geldt voor een aantal persoonlijkheidskenmerken, waaronder psychopathie, machiavellianisme en narcisme (Seigfried-Spellar et al., 2017; Selzer & Oelrich, 2021), terwijl de relatie met vriendelijkheid en consciëntieusheid negatief is (Seigfried-Spellar & Treadway, 2014). Ook zijn er aanwijzingen van een verband tussen kenmerken van een autismespectrumstoornis en betrokkenheid bij het plegen van technische delicten (Seigfried-Spellar et al., 2015). Tot slot lijkt deze groep relatief vaker betrokken te zijn bij andere vormen van cybercrime, zoals illegaal downloaden en online intimidatie, en bij traditionele delicten, waaronder winkeldiefstal, mishandeling en vandalisme (Holt et al., 2020; Lee & Holt, 2020; Udris, 2016).

3.3 De aanpak van en programma's gericht op (cyber)criminele jeugdgroepen in Nederland

In deze paragraaf gaan we nader in op de aanpak van problematische en (cyber)criminele jeugdgroepen in Nederland, met de nadruk op het voorkómen dat jongeren betrokken raken bij dergelijke groepen. We beginnen met een korte bespreking van hoe de aanpak in theorie geregeld is en welke factoren de effectiviteit hiervan verhogen. Vervolgens bespreken we de belangrijkste aanpakken en interventies en hun effectiviteit.

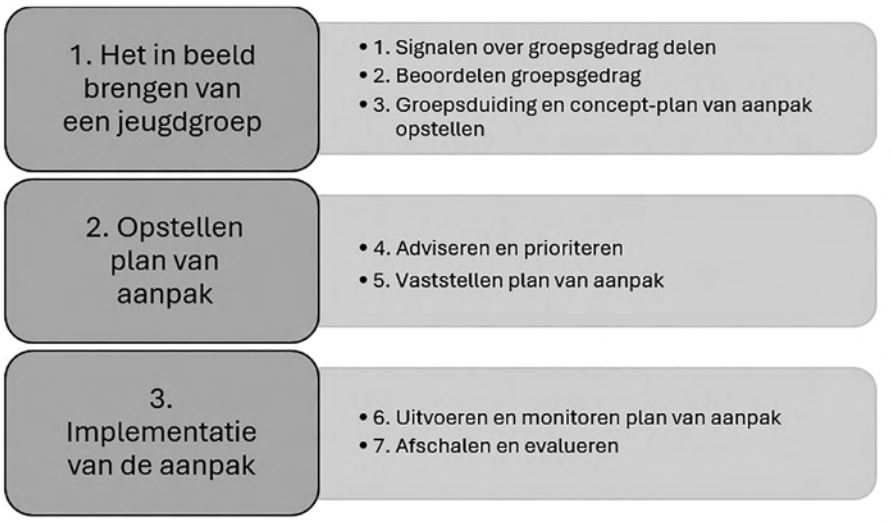
In Nederland speelt de lokale driehoek (burgemeester, officier van justitie en districtschef van de politie), onder leiding van de burgemeester, een centrale rol bij de aanpak van problematische en traditionele criminele jeugdgroepen (CCV, 2023a). De driehoek bepaalt welke jeugdgroepen geprioriteerd worden en waar een integrale aanpak op moet worden ingezet. Vervolgens is de gemeente verantwoordelijk voor de uitvoering. De effectiviteit van dergelijke aanpakken en interventies is afhankelijk van vijf factoren. Allereerst dienen ze contextgericht te zijn: er moet een duidelijk overzicht worden verkregen van de problemen die zich rondom het jeugdgroep voordoen en van de specifieke doelgroep waarop de aanpak en interventie gericht worden. Ten tweede is het belangrijk om het beeld dat is verkregen via systeeminformatie aan te vullen met gegevens van de straat (bijvoorbeeld door praktijkprofessionals te interviewen). Ten derde moet de aanpak en interventie aansluiten bij de beschermende en risicofactoren

die in de betreffende casus een rol spelen. Ten vierde moet de aanpak en interventie tijdens de uitvoering continu worden gemonitord, zodat deze waar nodig kan worden bijgestuurd. Ten vijfde moeten de gestelde doelen haalbaar zijn en moet de voortgang van de aanpak en interventie regelmatig worden gemeten om de effectiviteit te waarborgen. Tot slot blijkt een integrale aanpak het meest effectief, waarbij de gemeente samenwerkt met verschillende partners die de benodigde middelen en expertise hebben om de interventies uit te voeren (CCV, 2022).

3.3.1 *Het 7-stappenmodel*

De aanpak van problematische jeugdgroepen vindt doorgaans plaats via de jeugdgroepenaanpak, waarbij het 7-stappenmodel vaak het vertrekpunt is. Dit model is de opvolger van de shortlistmethodiek, die tot 2015 gebruikt werd (Ferwerda & Kloosterman, 2004). De overstap naar het 7-stappenmodel werd vooral ingegeven door het feit dat jeugdgroepen binnen de shortlistmethodiek een strikte classificatie kregen (hinderlijk, overlastgevend, crimineel), terwijl dergelijke samenwerkingsverbanden tegenwoordig meer dynamisch zijn en daardoor vaak niet meer duidelijk in één categorie passen (Bureau Beke, z.d.; Ferwerda & Van Ham, 2017). Bovendien kunnen jongeren elkaar door de digitalisering van de samenleving zowel offline als online ontmoeten, waardoor de toepassing van de oude categorieën problematisch werd (Bureau Beke, z.d.; Ministerie van Justitie en Veiligheid, z.d.).
In 2023 werd het 7-stappenmodel herzien, omdat het onvoldoende aansloot bij het gedrag en de activiteiten van de hedendaagse problematische jeugdgroepen. Zo neemt het gebruik van sociale media door jongeren toe (CCV, 2023a) en is de fluïditeit van jeugdgroepen groter geworden. Hierdoor lijken dynamische groepen vaker de overhand te hebben dan meer statische samenwerkingsverbanden (CCV, 2023a; RIEC, 2022). Daarnaast is de mobiliteit toegenomen, waardoor problematische jeugdgroepen zich over meerdere gemeenten kunnen uitstrekken (CCV, 2023a).
Het 7-stappenmodel dient als leidraad voor de integrale aanpak van problematische en criminele jeugdgroepen, zowel de meer dynamische als de meer statische groepen (CCV, 2023a; Landelijk projectteam proeftuinen, 2016; Ministerie van Justitie en Veiligheid, z.d.). Het model biedt een overzicht van de taken en verantwoordelijkheden van de betrokken partijen en geeft richtlijnen voor de uitwisseling van informatie tussen de ketenpartners, waaronder de burgemeester, de politie, het OM, jongerenwerkers, leerplichtambtenaren, scholen en woningcorporaties (CCV, 2023a).
Het model is onderverdeeld in zeven stappen, verdeeld over drie fases (zie Figuur 2 voor een schematische weergave). In fase één wordt het jeugdgroep in beeld gebracht. Deze fase bestaat uit drie stappen: (1) signalen over groepsgedrag delen; (2) beoordelen groepsgedrag; en (3) groepsduiding en concept-plan van aanpak opstellen. In fase twee wordt een plan van aanpak opgesteld. Deze fase bestaat uit de stappen: (4) adviseren en prioriteren; en (5) vaststellen plan van aanpak. In fase drie wordt de aanpak geïmplementeerd, gemonitord, afgesloten en geëvalueerd. Deze fase bestaat uit de stappen: (6) uitvoeren en monitoren plan van aanpak; en (7) afschalen en evalueren.

Het model is dynamisch: op basis van nieuwe informatie kan de aanpak, ook tijdens de uitvoering, worden aangepast (CCV, 2023a).



Figuur 2. Schematische weergave van het 7-stappenmodel

In de eerste fase wordt een jeugdgroep verder in beeld gebracht. In stap 1 (signalen over groepsgedrag delen) delen de ketenpartners informatie en signalen over de problematische gedragingen van een jeugdgroep. Dit gebeurt op groepsniveau; persoonlijke gegevens over individuele leden worden niet gedeeld. Vervolgens wordt aan de hand van deze inventarisatie beoordeeld of er sprake lijkt te zijn van een problematisch jeugdgroep. Is dit het geval, dan wordt doorgegaan naar stap 2 (beoordelen groepsgedrag). Daarin wordt gedetailleerde informatie gedeeld om een beter beeld te krijgen van het gedrag van de groep. Dit wordt gebruikt om te bepalen of er inderdaad sprake is van problematisch of crimineel gedrag. Als dit het geval is, worden de individuele leden van de groep geïdentificeerd en voert de politie een groepsscan uit. Tot slot worden in stap 3 (groepsduiding en concept-plan van aanpak opstellen) de groepsdynamiek, de rolverdeling, het type problematiek en de groepscontext in kaart gebracht. Ook wordt het concept-plan van aanpak opgesteld (CCV, 2023a).

De tweede fase van het 7-stappenmodel staat in het teken van het opstellen van een gericht plan van aanpak, dat bedoeld is om het problematische en/of criminele gedrag terug te dringen. In stap 4 (adviseren en prioriteren) wordt een beleidsadvies opgesteld over de noodzaak van de aanpak van de groep. Op basis van dit advies en het concept-plan van aanpak wordt door de lokale driehoek besloten of de groep moet worden geprioriteerd. Stap 5 (vaststellen plan van aanpak) bestaat uit het verder uitwerken van het concept-plan van aanpak, waarin concreet beschreven wordt hoe de jeugdgroep wordt aangepakt. In latere stappen kan dit plan worden aangepast op basis van nieuwe informatie (CCV, 2023a).

In de derde fase wordt het plan van aanpak uitgevoerd en wordt de voortgang gemonitord. Stap 6 (uitvoeren en monitoren plan van aanpak) bestaat uit het implementeren van het plan. Er wordt nauwlettend gekeken naar de mate waarin de ketenpartners de afgesproken interventies daadwerkelijk uitvoeren. Tot slot wordt in stap 7 (afschalen en evalueren) beoordeeld in hoeverre de vooraf gestelde doelen zijn behaald en of de aanpak kan worden afgebouwd of gestopt. Ook vindt in deze stap de eindevaluatie van het hele proces plaats (CCV, 2023a).

De eerste versie van het 7-stappenmodel is inmiddels bij meerdere gemeenten in gebruik. Uit evaluaties hiervan komt naar voren dat de betrokken veiligheidspartners het model als positief beoordelen (Van Loon & Jansen, 2017). Daarbij wordt aangegeven dat het model het vroegtijdig signaleren van problematische jeugdgroepen vergemakkelijkt (stap 1). Dit lijkt vooral het gevolg van een intensievere en meer structurele samenwerking tussen de betrokken veiligheidspartners en leidt ertoe dat deze partijen sneller bij de aanpak betrokken raken. Bovendien zijn de respondenten die in de evaluatie geïnterviewd zijn positief gestemd over de periodieke overleggen tussen de verschillende partners, omdat deze ervoor zorgen dat problematische groepen sneller in kaart gebracht kunnen worden. Tot slot staan de respondenten positief tegenover het kunnen prioriteren van jeugdgroepen door de lokale driehoek, wat ertoe leidt dat partners sneller tot actie kunnen overgaan (Van Loon & Jansen, 2017).

Er zijn meerdere casussen bekend waarbij het 7-stappenmodel heeft bijgedragen aan een afname of het volledig verdwijnen van problematisch en overlastgevend gedrag binnen jeugdgroepen. Zo leidde de implementatie van het model in de regio Parkstad (Zuidoost-Limburg) tot een afname van de overlast die werd veroorzaakt door een jeugdgroep (CCV, 2018). In deze casus hebben veiligheidspartners de jeugdgroep in kaart gebracht aan de hand van systeeminformatie (zoals politiedata) en open bronnen (zoals straatinformatie), waarna verschillende instanties (zoals de gemeente, de politie, het OM, het Veiligheidshuis, Reclassering Nederland, de Raad voor de Kinderbescherming en de leerplichtambtenaar) gezamenlijk het 7-stappenmodel uitvoerden. De aanpak werd vormgegeven met de methodiek PlusMinMee (zie paragraaf 3.3.2). Er werd gekozen voor een aanpak waarbij specifieke interventies verliepen langs drie sporen: (1) interventies door de gemeente, de sociale dienst, maatschappelijk werk en jeugdzorg; (2) interventies door het basisteam van de politie; (3) interventies door de districtsrecherche. De aanpak omvatte hulpverlening bij softdrugsverslaving, stop-gesprekken, extra controles en ondersteuning bij het vinden van een opleiding (CCV, 2018). Vergelijkbare positieve resultaten werden geboekt in Hilversum, Groningen en Purmerend (Polman, 2016; Rozema, 2018).

Ondanks de positieve resultaten heeft het 7-stappenmodel ook enkele knelpunten. Deze hebben vooral betrekking op de informatie-uitwisseling tussen de verschillende partners. Zo is het voor politieagenten niet altijd duidelijk welke informatie wel of niet gedeeld mag worden, wat kan leiden tot terughoudendheid. Ook jongerenwerkers kunnen terughoudend zijn in het delen van informatie, uit vrees dat dit het vertrouwen van de jongeren kan schaden. Daarnaast kan het (grote) aantal betrokken partners het

werkproces vertragen en kan het onduidelijkheid veroorzaken over ieders verantwoordelijkheden (Van Loon & Jansen, 2017)[13].

3.3.2 *PlusMinMee-methodiek*

Binnen de jeugdgroepenaanpak kan, naast gebruikmaking van het 7-stappenmodel, ook de PlusMinMee-methodiek worden toegepast. Die biedt de mogelijkheid om de posities van individuele jongeren binnen een problematische groep in kaart te brengen. De toepassing ervan vindt plaats nadat eerst een grondig overzicht is verkregen van de groepssamenstelling en -dynamiek. Op basis van de uitkomsten kan worden bepaald of de hele groep moet worden aangepakt of slechts specifieke individuen.
Met behulp van de methodiek kunnen jongeren binnen een groep worden opgedeeld in drie categorieën: plus, min en mee. De plus-categorie bestaat uit jongeren die een positieve invloed hebben op de groep en nog op een positieve manier kunnen worden beïnvloed. Voor deze groep kunnen interventies zoals maatschappelijke hulpverlening worden ingezet. De min-categorie omvat jongeren die een negatieve invloed uitoefenen op de groep en die niet meer vatbaar zijn voor positieve gedragsverandering. Voor hen wordt een strafrechtelijke aanpak overwogen. Tot slot bestaat de mee-categorie uit meelopers. Bij deze groep wordt in kaart gebracht in hoeverre zij vatbaar zijn voor positieve (plus) of negatieve (min) invloeden (CCV, 2018; Jeugdboa.nl, z.d.; Wolsink et al., 2023).

3.3.3 *Preventie met Gezag*

Een relatief nieuw programma gericht op de aanpak van (potentiële) jeugdige daders is Preventie met Gezag. Dit programma heeft een integrale insteek, waarbij wordt samengewerkt met diverse ketenpartners (zoals de gemeente, het OM en zorginstanties). De doelstellingen van het programma zijn: (1) het voorkomen of beperken van de betrokkenheid van jongeren tot 27 jaar bij georganiseerde, ondermijnende criminaliteit; (2) het vergroten van de weerbaarheid van jongeren tegen deze vorm van criminaliteit; (3) het verbeteren van de leefbaarheid in kwetsbare wijken; en (4) het bieden van toekomstperspectief voor deze jongeren. Het programma wordt gefinancierd door de Rijksoverheid en loopt meerdere jaren (CCV, z.d.-a; Gemeente Rotterdam, 2023; Gemeente Schiedam, z.d.; Rijksoverheid, z.d.).
Het programma richt zich op wijken waarin jongeren een verhoogd risico lopen om in contact te komen met en betrokken te raken bij georganiseerde criminaliteit. Voorbeelden van interventies zijn het versterken van emotionele vaardigheden, bewustwordingsprogramma's en het bevorderen van een veilige thuissituatie (Gemeente Rotterdam, 2023). Binnen het programma wordt ook aandacht besteed aan cybercrime (zie bijvoorbeeld CCV, 2024) onder de naam 'Jeugd en cyber'. Dit onderdeel richt zich op

13 Inmiddels heeft het CCV een methode (praktijktoets 7-stappenmodel) om periodiek de knelpunten op een rij te zetten (CCV, z.d.-b).

het vergroten van het bewustzijn van jongeren over hun online gedrag en de mogelijke gevolgen daarvan.

3.3.4 *TopX-aanpak*

Een andere aanpak die is gericht op problematische en criminele jongeren, is de TopX-aanpak. In Amsterdam wordt bijvoorbeeld gewerkt met de Top600-aanpak, die zich richt op het integraal aanpakken van 600 jongeren die betrokken zijn bij high impact delicten (zoals straatroven en inbraken). Als deze jongeren ook deel uitmaken van een jeugdgroep, dan krijgen zij prioriteit in de aanpak (Ferwerda et al., 2021; Gemeente Amsterdam, z.d.; Van Gemert & Weerman, 2013). Uit een recente evaluatie van het Wetenschappelijk Onderzoek- en Datacentrum (WODC) blijkt echter dat de Top600-aanpak niet leidt tot een afname van recidive onder de betrokken jongeren (Beijersbergen et al., 2023).

3.3.5 *Strafrechtelijke aanpak*

Naast preventieve en integrale aanpakken kunnen problematische jeugdgroepen ook strafrechtelijk worden vervolgd. De effectiviteit van een repressieve aanpak is echter onderwerp van discussie. Onderzoek suggereert bijvoorbeeld dat een gevangenisstraf voor sommige jongeren juist statusverhogend kan werken (RIEC, 2022; Van Uden, 2019). Wanneer ze dan weer uit de gevangenis komen, kunnen ze binnen hun milieu een hogere status hebben gekregen, wat de toegang tot criminele mogelijkheden juist vergemakkelijkt.

3.3.6 *De RIEC-aanpak*

Hoewel er op landelijk niveau geen specifieke aanpak bestaat voor cybercriminele jeugdgroepen, verdient de RIEC-aanpak hier een vermelding. Deze integrale casusaanpak is gericht op de bestrijding van ondermijnende criminaliteit en wordt landelijk toegepast (RIEC, 2019). In Noord-Nederland is deze aanpak bovendien succesvol ingezet tegen cybercrime (Veenstra, 2023).
De integrale aanpak start met een signaal vanuit een convenantpartner, waarna een casusbeschrijving wordt opgesteld en beoordeeld. Convenantpartners, waaronder gemeenten, provincies, het OM, de nationale politie, de Belastingdienst en de Fiscale Inlichtingen- en Opsporingsdienst (RIEC, 2019) brengen ieder hun eigen informatiepositie en interventiemogelijkheden in. Deze samenwerking leidt tot een breed en gecoördineerd interventiepakket, dat is gericht op meerdere domeinen van verdachten en criminele groepen. Alhoewel de RIEC-aanpak niet specifiek ontwikkeld is voor cybercrime, laat een succesvolle toepassing in Noord-Nederland zien dat deze werkwijze ook potentie heeft voor de aanpak van cybercriminele jeugdgroepen (Veenstra, 2023).

3.3.7 *Integrale aanpak van online fraude*

Sinds 2023 is er één landelijke aanpak voor online fraude: het *Actieplan integrale aanpak online fraude.* Dit is een publiek-private samenwerking, waarin diverse organisaties en overheidsinstanties samenwerken aan een gecoördineerde aanpak van online fraude. Deze aanpak is gericht op zowel (potentiële) daders als op (potentiële) slachtoffers. Partners binnen dit initiatief zijn onder andere VNO-NCW, MKB Nederland, de Nederlandse Vereniging van Banken, de Consumentenbond, de Vereniging Nederlandse Gemeenten (VNG), de politie, het OM, COIN, thuiswinkel.org, het ministerie van Economische Zaken en Klimaat, het ministerie van Financiën en het ministerie van Justitie en Veiligheid. Het actieplan richt zich op vier pijlers: inzicht in online fraude, slachtofferpreventie, daderpreventie, en opsporing en vervolging (Ministerie van Justitie en Veiligheid, 2024).
Het Actieplan 2024 bouwt voort op de basis die in 2023 is gelegd en richt zich op het uitwerken van concrete maatregelen en oplossingen voor uitdagingen die binnen de publiek-private samenwerking zijn geïdentificeerd. Hierbij staan deze vraagstukken centraal: (1) Kennisagenda: het vergroten van de kennis over verschillende vormen van online fraude, inclusief modus operandi, daderprofielen en slachtofferkenmerken; (2) Gegevensdeling: een van de grootste knelpunten bij de integrale aanpak. Dit vraagstuk is gericht op het identificeren van de belemmeringen bij gegevensuitwisseling en het zoeken naar werkbare oplossingen; (3) Technische barrières en interventies: de ontwikkeling van (technische) maatregelen en interventies om het verdienmodel van daders te verstoren en slachtofferschap te voorkomen; (4) Opvolging door de politie en het OM: het ontwikkelen van een brede, schaalbare en innovatieve aanpak voor de opsporing en vervolging van cyberdaders en cybercriminele groepen; (5) Weerbaarheid en preventie: het versterken van de bewustwording en weerbaarheid van (potentiële) slachtoffers en het voorkomen van daderschap; en (6) Hulp aan slachtoffers: het verbeteren van de toegankelijkheid van hulp en handelingsperspectieven voor slachtoffers van online fraude (Ministerie van Justitie en Veiligheid, 2024).

3.3.8 *Interventies voor jeugdige cyberdaders*

Tot slot worden in de literatuur meerdere interventies beschreven die zich richten op jeugdige cyberdaders (voor een overzicht, zie Oosterwijk & Fischer, 2017). Deze interventies zijn veelal gericht op primaire preventie (het voorkomen van daderschap onder de algemene populatie jongeren) en op cyberagressie, sexting en hacking. Uit enkele studies komt naar voren dat interventies die zijn gericht op traditionele criminaliteit ook toegepast kunnen worden op specifieke vormen van cybercrime, zoals cyberagressie. Algemeen blijkt wel dat de effectiviteit van deze interventies onbekend is (Oosterwijk & Fischer, 2017).

3.4 Resumé

In dit hoofdstuk zijn we nader ingegaan op de kenmerken van (cyber)criminele (jeugd) groepen, hun leden en activiteiten. Daarnaast hebben we stilgestaan bij de verschillende aanpakken die worden toegepast op problematische en criminele jongeren en jeugdgroepen.
Samenvattend komt naar voren dat er tot op heden nog maar weinig specifieks bekend is over jeugdige cybercriminele samenwerkingsverbanden. Kijken we breder naar cybercriminele samenwerkingen waarbij niet alleen jongeren betrokken zijn, dan blijkt dat het merendeel in de categorie 'fluïde groepen' geplaatst kan worden: ze zijn veelal dynamisch en hebben in mindere mate een hiërarchie en rolverdeling. Wel lijkt de kerngroep stabieler te zijn. Deze bestaat uit leden uit de bovenste laag van de groep die verantwoordelijk zijn voor de coördinatie van criminele activiteiten. Als groepen gevormd worden door meerdere lagen, dan bestaat de middelste laag uit professionele en gerekruteerde facilitators. Dit zijn personen die bepaalde goederen en/of diensten kunnen leveren die noodzakelijk zijn voor de uitvoering van delicten. De onderste laag omvat veelal geldezels en andere katvangers. Deze personen worden door kernleden gebruikt om zelf zo veel mogelijk anoniem te blijven.
Bij het ontstaan en de groei van cybercriminele groepen is een belangrijke rol weggelegd voor sociale gelegenheidsstructuren (de offline banden die toegang bieden tot gelegenheden waarin criminaliteit gepleegd kan worden) en offender convergence settings (specifieke locaties op bepaalde tijden waar (potentiële) daders elkaar kunnen ontmoeten, zonder toezicht van de autoriteiten). In de literatuur zijn vier combinaties van gelegenheidsstructuren en offender convergence settings beschreven voor de ontstaans- en groeiprocessen van cybercriminele groepen: (1) exclusief via offline banden; (2) met offline banden als basis en met online contacten, veelal verkregen via virtuele offender convergence settings, om facilitators en geldezels te rekruteren; (3) met virtuele offender convergence settings en online relaties als basis en offline banden, al dan niet via fysieke offender convergence settings om lokale criminelen te benaderen; en (4) exclusief via virtuele offender convergence settings. Ondanks het feit dat offline relaties nog steeds een belangrijke rol spelen binnen de ontstaans- en groeiprocessen, komt naar voren dat online contacten, die veelal ontstaan via virtuele offender convergence settings, een steeds belangrijkere rol spelen.
Cybercriminele groepen kunnen op basis van de delicten waarbij ze betrokken zijn, worden opgedeeld in twee categorieën. Enerzijds kan er sprake zijn van groepen die actief zijn binnen zowel traditionele criminaliteit als cybercrime. Dit worden ook wel hybride groepen genoemd. Anderzijds kunnen cybercriminele groepen zich specifiek richten op cybercrime.
Tot op heden is er beperkt onderzoek verricht naar individuen die onderdeel zijn van cybercriminele (jeugd)groepen. Door het gebrek aan wetenschappelijke literatuur die specifiek is gericht op jongeren die actief zijn binnen cybercriminele groepen, hebben we ook literatuur besproken over jongeren die niet specifiek actief zijn binnen dergelijke groepen. Over het algemeen wordt cybercrime gepleegd door jonge mannen onder

de 30 jaar. Zowel bij hacking als bij online fraude lijkt de sociale omgeving een belangrijke rol te spelen bij het betrokken raken bij deze delicten. Ook de gezinssituatie blijkt van invloed: beperkt ouderlijk toezicht en een instabiele gezinssituatie vergroten de kans op cybercrime. Hackers lijken doorgaans een relatief hogere sociaaleconomische status te hebben, terwijl die van online fraudeurs juist relatief lager lijkt te zijn. Bovendien worden hackers vaak gedreven door sensatiezucht, uitdaging, plezier, erkenning van leeftijdsgenoten en plezier, terwijl online fraude primair lijkt te worden gepleegd vanwege financieel gewin. Tot slot is er binnen cybercrime een aparte groep jongeren met technische vaardigheden, ook wel cyberbreinen genoemd. Deze jongeren houden zich veelal bezig met de meer complexe technische delicten, zoals hacken. Bij deze groep lijkt sprake te zijn van een unieke set risicofactoren. Specifiek lijkt er een positieve relatie te zijn tussen IT-kennis en betrokkenheid. Ook zijn er aanwijzingen van een verband tussen kenmerken van autismespectrumstoornissen en betrokkenheid bij en het plegen van technische delicten.

Voor zover bekend is er nog geen methode ontwikkeld die zich specifiek richt op de aanpak van jeugdgroepen die betrokken zijn bij cybercrime. Binnen de algemene jeugdgroepenaanpak wordt gebruikgemaakt van het 7-stappenmodel. Het primaire doel van dit model is het optimaliseren van de integrale aanpak van deze groepen. Dit model heeft inmiddels wel een cyber-component. De zeven stappen uit het model zijn verdeeld in drie categorieën: 'in beeld brengen jeugdgroep', 'bepalen of en hoe jeugdgroep aangepakt wordt' en 'jeugdgroep aanpakken'. Het model wordt al enkele jaren in de praktijk toegepast en wordt overwegend positief beoordeeld door de betrokken veiligheidspartners. Daarbij is het model voor zover bekend alleen toegepast op jeugdgroepen die zijn betrokken bij traditionele, fysieke criminaliteit. Ook hebben aanpakken en interventies die gebaseerd zijn op het 7-stappenmodel al tot meerdere successen geleid. Andere methoden die worden toegepast om problematische en criminele jeugdgroepen terug te dringen, zijn de PlusMinMee-methodiek, Preventie met Gezag, de TopX-aanpak en repressieve maatregelen. Op landelijk niveau zijn twee aanpakken relevant voor cybercriminele jeugdgroepen: de RIEC-aanpak, die is gericht op criminele groepen in het algemeen, en het Actieplan integrale aanpak online fraude. De RIEC-aanpak is een integrale casusaanpak die is gericht op de bestrijding van ondermijnende criminaliteit en die landelijk wordt toegepast. Hoewel de RIEC-aanpak niet specifiek ontwikkeld is voor cybercrime, laat een succesvolle toepassing in Noord-Nederland zien dat de werkwijze ook potentie heeft voor de aanpak van cybercriminele jeugdgroepen. Het Actieplan omvat een integrale samenwerking die is gericht op vier pijlers: inzicht in online fraude, slachtofferpreventie, daderpreventie, en opsporing en vervolging. Hoewel het Actieplan niet specifiek gericht is op de aanpak van cybercriminele (jeugd)groepen, biedt het wel mogelijkheden voor uitbreiding, waar ook specifiek naar gekeken kan worden.

Concluderend stellen we vast dat cybercriminele jeugdgroepen nog nauwelijks zijn onderzocht. De kennis die er is over dit onderwerp is vooral afkomstig van studies naar cybercriminele groepen van volwassenen. Of de resultaten van deze studies ook van toepassing zijn op jeugdgroepen is niet duidelijk. Daarnaast hebben deze studies meer-

dere beperkingen. Zo zijn ze gebaseerd op opsporingsonderzoeken en hebben ze vooral betrekking op cybercriminele groepen die betrokken zijn bij financieel gemotiveerde cybercrime. Tot op heden weten we nog weinig over de structuur, de samenstelling en de ontstaans- en groeiprocessen van cybercriminele groepen die nog niet bekend zijn bij politie en justitie, en groepen die zich bezighouden met andere delicten dan financieel gemotiveerde cybercrime. Bovendien is er tot nu toe geen specifieke methodiek om dergelijke cybercriminele jeugdgroepen in kaart te brengen en vervolgens aan te pakken.

4 Resultaten spoor 1: de bij lokale veiligheidscoalities bekende (cyber) criminele jeugdgroepen

In de komende drie hoofdstukken presenteren we de resultaten van dit onderzoek. In dit hoofdstuk staat spoor 1 centraal, waarbij we ingaan op de kenmerken van (cyber) criminele jeugdgroepen die bij een volledige lokale veiligheidscoalitie in beeld zijn. Gemeenten hebben de regiefunctie bij de aanpak van criminele jeugdgroepen. Daarom gaan we ervan uit dat jeugdgroepen die in beeld zijn bij de gemeente, in beeld zijn bij de volledige lokale veiligheidscoalitie. Zijn jeugdgroepen in beeld bij andere lokale actoren dan gemeenten (zoals de politie en jongerenwerkers), dan beschouwen we die als groepen die onbekend zijn bij lokale veiligheidscoalities. In hoofdstuk 5 komt spoor 2 aan bod, waarbij de jeugdgroepen centraal staan die nog onbekend zijn bij lokale veiligheidscoalities. Tot slot staat in hoofdstuk 6 spoor 3 centraal, waarbij we ingaan op de inzichten die we hebben opgedaan over de (integrale) aanpak van (cyber)criminele jeugdgroepen.
Het huidige hoofdstuk bestaat uit vier delen die corresponderen met de vier deelvragen van spoor 1. Allereerst beschrijven we in hoeverre lokale veiligheidscoalities bekend zijn met traditionele en/of cybercriminele jeugdgroepen. Daarna komt de aard van de delicten aan bod waar deze jeugdgroepen zich mee bezighouden. Dit wordt gevolgd door een uiteenzetting over de structuur, de samenstelling, het ontstaan en de groei van deze groepen, waarna we een beschrijving geven van de kenmerken van de leden van deze jeugdgroepen. Het hoofdstuk eindigt met een resumé.

4.1 De (cyber)criminele jeugdgroepen die bekend zijn bij lokale veiligheidscoalities in Noord-Nederland

We wilden een overzicht krijgen van alle problematische en (cyber)criminele jongeren en jeugdgroepen die actief waren in Noord-Nederland. Daarom hebben we in de periode van 5 december 2022 tot medio 2023 alle 40 gemeenten in Drenthe, Groningen en Friesland gevraagd in hoeverre zij een beeld hadden van problematische en/of criminele jeugdgroepen, en of deze ook betrokken waren bij cybercrime. Van deze 40 gemeenten hebben er 25 gereageerd. Daarvan gaven 10 gemeenten aan dat ze bekend waren met actieve problematische en/of criminele jeugdgroepen. Deze waren volgens de gemeenten echter uitsluitend betrokken bij traditioneel overlastgevend en crimineel

gedrag. Geen van de gemeenten had een groep in beeld dat voor zover bekend (ook) betrokken was bij cybercrime.
Dit beeld werd ondersteund door de geïnterviewde praktijkprofessionals: lokale veiligheidscoalities (onder leiding van gemeenten) hadden geen zicht op jeugdgroepen die zich bezighielden met cybercriminele activiteiten. Toch bestond er wel zicht op traditionele criminele jeugdgroepen (R1, R2, R3, R7) en waren er bij twee gemeenten vermoedens van betrokkenheid van deze jeugdgroepen bij cybercrime, al ontbrak hier concreet bewijs voor (R1, R2). Ook in de overige interviews met een basisschoolmedewerker (R16), een medewerker van een middelbare school (R13), jongerenwerkers (R14, R17) en leerplichtambtenaren (R20) kwam naar voren dat lokale veiligheidscoalities enkel zicht hebben op jeugdgroepen die betrokken waren bij traditionele criminaliteit. In één gemeente (R7) bleek wel zicht te zijn op een cybercrimineel jeugdgroep, maar liep hier geen aanpak op, wat betekent dat de lokale veiligheidscoalitie hier niet van op de hoogte was.
Als reden voor het gebrek aan zicht op cybercriminele jeugdgroepen gaven zeven respondenten (R1, R2, R3, R7, R8, R11, R17) aan dat bij het in kaart brengen van deze groepen vooral wordt geleund op straatinformatie en signalen uit de wijk. Het inwinnen van informatie gebeurt daarbij dus nog op traditionele wijze. In de beleving van deze respondenten opereren cyberdaders vaak niet op straat, wat leidt tot een beperkt beeld. In paragraaf 6.1 gaan we hier verder op in.

4.2 De aard van de delicten waarmee bekende (cyber)criminele jeugdgroepen zich bezighouden

In deze paragraaf besteden we aandacht aan de aard van de delicten waarmee traditionele criminele jeugdgroepen zich bezighouden. Spoor 1 richt zich op jeugdgroepen die bekend zijn bij lokale veiligheidscoalities. Aanvankelijk was het de bedoeling om in dit hoofdstuk uitsluitend informatie uit de interviews met gemeentemedewerkers op te nemen. Zij weten immers wat de kenmerken zijn van de jeugdgroepen die bekend zijn bij de lokale veiligheidscoalities. Zoals we in paragraaf 4.1 al schreven, bleek dit uitsluitend te gaan over jeugdgroepen die betrokken waren bij traditionele criminaliteit.
Een belangrijke kanttekening betreft de mate van zicht die respondenten hebben op deze groepen. Veel respondenten gaven aan slechts beperkt zicht te hebben op de aard van de delicten, structuur, samenstelling, en werkwijze van criminele jeugdgroepen en hun leden. De bevindingen die wij hier presenteren zijn daarom voornamelijk gebaseerd op individuele (beperkte) observaties en ervaringen uit de praktijk. Daarbij is het mogelijk dat respondenten eveneens invullingen, interpretaties of aannames hebben gedaan die niet volledig overeenkomen met de feitelijke situatie. Het beeld dat wij schetsen is daarmee niet noodzakelijk volledig of sluitend, maar weerspiegelt de kennis die door respondenten kon worden aangedragen. Bij de interpretatie van de resultaten dient hiermee rekening te worden gehouden.

Tijdens de interviews met andere praktijkprofessionals werd echter ook gesproken over problematische[14] en traditionele criminele jeugdgroepen die nog onbekend waren bij lokale veiligheidscoalities. In eerste instantie zou deze informatie worden behandeld in spoor 2. Maar doordat er geen duidelijke verschillen bestonden tussen de jeugdgroepen die bekend zijn bij de volledige lokale veiligheidscoalities en de jeugdgroepen die uitsluitend bekend zijn bij monopartners, hebben we ervoor gekozen om alle informatie in dit hoofdstuk te behandelen. Dit voorkomt herhaling en draagt bij aan een sterkere onderbouwing van de geïdentificeerde kenmerken van deze groepen.
Tabel 5 geeft een overzicht van de delicten die worden gepleegd door traditionele criminele jeugdgroepen. Daaruit komt naar voren dat deze jeugdgroepen een combinatie van problematisch en crimineel gedrag vertonen (R1, R2, R3, R7, R8, R12, R17, R19), zoals: 'dat ze ondernemers lastigvallen, ramen besmeuren met eieren, vuurwerkoverlast, dat soort dingen' (R1) en 'overlast (…) vooral richting winkeliers of omwonenden (…) die daar best veel last van hebben' (R1). R7 beschreef een groep waarbij leden zich schuldig maakten aan overlastgevend gedrag, het overtreden van de APV en iemand van zijn fiets trappen.
Daarnaast kunnen deze groepen zich volgens de experts ook bezighouden met gewelds- en drugsmisdrijven, vernieling en misdrijven tegen de openbare orde. Geweldsmisdrijven omvatten onder andere intimidatie, afpersing, mishandeling, berovingen (zoals straatroven), bedreiging en aanranding (R2, R3, R7, R8, R11, R12, R14, R17, R19). Ook kunnen individuele leden betrokken zijn bij ernstige (gewelds)incidenten (R11)
Vermogensdelicten, zoals diefstal (scooterdiefstal en fietsendiefstal, al dan niet in opdracht van anderen), worden ook gepleegd door traditionele criminele jeugdgroepen (R8, R20). Dit geldt ook voor drugsdelicten (R5, R11, R13, R14, R16, R17, R20). In sommige gevallen is de groep actief betrokken bij de handel in drugs, maar er zijn ook gevallen bekend waarin leden van een jeugdgroep worden aangemoedigd door personen die niet direct onderdeel zijn van de groep om voor hen drugs te dealen: 'jongens die [zich] wat met straatdealen bezighielden, met koerieren' (R3). Een andere expert beschreef een casus waarin jongeren, terwijl ze op school waren, het bericht kregen dat ze een pakketje (met daarin vermoedelijk drugs) moesten bezorgen (R20). Tot slot kunnen jeugdgroepen betrokken zijn bij vernieling en misdrijven tegen de openbare orde (R3, R7). Voorbeelden hiervan zijn het ingooien van ruiten, het overtreden van de APV, het halen en brengen van pakketjes (vermoedelijk met messen), mensenhandel en overige ondermijnende activiteiten.
Alhoewel uit onze data naar voren kwam dat lokale veiligheidscoalities geen expliciet zicht hebben op jeugdgroepen die betrokken zijn bij cybercrime, bleek wel dat jeugdgroepen gebruikmaken van internet voor communicatie en het faciliteren van traditionele criminaliteit. Zo bleek uit zeven interviews (R1, R2, R5, R7, R12, R14, R19) dat respondenten het vermoeden hadden dat een deel van de bekende jeugdgroepen zich

14 De groepen die enkel betrokken waren bij problematisch en overlastgevend gedrag, maar geen daadwerkelijke criminaliteit pleegden worden verder niet besproken, omdat dit geen *criminele* jeugdgroepen zijn.

ook bezighield met dergelijke online gefaciliteerde traditionele criminele activiteiten, zoals online drugshandel, opruiing, afpersing en uitbuiting. Hier was echter geen concreet bewijs voor. Een andere expert noemde een groep die zich, voor zover bekend, uitsluitend met traditionele criminaliteit bezighield, maar een onverklaarbaar verdienmodel had:

> *'Er is een verdienmodel dat we niet kunnen uitleggen. (…) Die groep waar ik het nu over heb, die gaat op vakantie naar Spanje en daar huren ze een hotelkamer en leven als God in Frankrijk. Ze doen echt alles wat ze maar kunnen. (…) En we hebben (…) gezien dat ze in [verschillende] landen verschillende (…) B&B's afhuren. Nou, de laatste was in <naam stad>, hebben ze daar voor 50.000 euro vernield. En dat wordt gewoon afgetikt (…). En we hebben wel een van de vriendinnen, die heeft 12.000 euro op [haar] rekening gehad van een marktplaatsfraude.' (R19)*

Bovendien gaven enkele experts aan te vermoeden dat sommige jeugdgroepen zich bezighielden met het (al dan niet onder dwang) rekruteren van geldezels. Ook gaven ze aan dat ze soms zagen dat leden uit een jeugdgroep contact hadden met personen die verdacht werden van betrokkenheid bij cybercrime.

Tabel 5. Delicten waarbij traditionele criminele jeugdgroepen betrokken zijn die bekend zijn bij lokale veiligheidscoalities

Hoofdcategorie delict	Specifieke delicten
Geweldsmisdrijven	Intimidatie, afpersing, voetbalgeweld, mishandeling (zoals een voorbijganger van zijn fiets trappen of mishandeling in de horeca), berovingen (zoals straatroven), wapenbezit (zoals het op zak hebben van messen) en aanranding
Vermogensdelicten	Diefstal (scooterdiefstal en fietsendiefstal, al dan niet in opdracht van een ander) en drugshandel
Vernieling en misdrijven tegen de openbare orde	Het ingooien van ruiten, het overtreden van de APV, het halen en brengen van pakketjes (vermoedelijk met messen), mensenhandel en overige ondermijnende activiteiten
Vermoedens van online gefaciliteerde traditionele delicten	Online drugshandel, online opruiing, online afpersing, uitbuiting en het rekruteren van geldezels

4.3 De kenmerken van de bekende (cyber)criminele jeugdgroepen

In deze paragraaf beschrijven we de kenmerken van traditionele criminele jeugdgroepen. Experts beschreven specifieke traditionele criminele jeugdgroepen, maar spraken ook over traditionele criminele jeugdgroepen in algemene zin. Beide perspectieven worden in deze paragraaf geïntegreerd. Daarbij gaan we eerst in op de structuur en de samenstelling van de groepen, gevolgd door hun ontstaans- en groeiproces.

4.3.1 *Structuur en samenstelling*

Traditionele criminele jeugdgroepen werden besproken in 15 interviews (R1, R2, R3, R5, R7, R8, R11, R12, R13, R14, R16, R17, R18, R19, R20). Tegelijkertijd werd duidelijk dat respondenten slechts beperkt zicht hebben op de precieze structuur en samenstelling van deze jeugdgroepen. Wat tijdens de interviews naar voren kwam, is dat de omvang van traditionele jeugdgroepen sterk varieert en dynamisch is. De groepsgrootte lijkt te schommelen tussen de 4 en 40 leden, waarbij de samenstelling van dag tot dag kan verschillen. Zo antwoordde R3 op de vraag wat de omvang van jeugdgroepen is: 'Dat verschilt wel per dag. (…) dat zijn niet elke keer (…) dezelfde mensen die daar nog staan' (R3).

Binnen sommige groepen is sprake van een vaste kern, die kan bestaan uit 3 tot 15 leden (R1, R3, R7, R8, R11, R14): 'Die [groep] kent (…) een vaste kern van zeven, acht personen' (R3). Deze kerngroep wordt doorgaans gevormd door meerderjarige leden die de leiding hebben binnen de groep: 'En wat we bij een aantal van die groepen zien, is dat degene die het uiteindelijk aan zou moeten sturen, dat dat de meerderjarigen zijn' (R11). De vaste kern lijkt stabieler te zijn dan de flexibelere lagen daaromheen. Binnen de groepen is daarnaast sprake van enige rolverdeling (R7, R13, R14, R17). Zo zijn er binnen de meeste groepen één of meer kernleden met een leidinggevende rol die de overige leden aansturen. Ook bestaat een deel van de groepen uit meelopers. Deze veelal minderjarigen moeten in opdracht van de leiders bepaalde activiteiten uitvoeren, zoals het dealen van drugs. Naarmate deze jongeren ouder worden, groeien ze vaak verder door binnen de groep.

Tot slot werd het gebruik van geweld binnen traditionele criminele jeugdgroepen slechts door één expert (R11) benoemd. Hij beschreef een casus waarin leidinggevende leden straffen oplegden aan ondergeschikte leden, bijvoorbeeld als zij vertrouwelijke informatie deelden.

4.3.2 *Ontstaan en groei*

De ontstaans- en groeiprocessen van traditionele criminele jeugdgroepen bleken lastig zichtbaar voor experts, zo kwam naar voren uit de 15 interviews (R1, R2, R3, R5, R7, R8, R11, R12, R13, R14, R16, R17, R18, R19, R20). Over hoe en wanneer deze groepen ontstaan is weinig bekend, al ontstaat een deel van de traditionele criminele jeugdgroepen vanuit een 'normale' jongerengroep (R11). In eerste instantie gaat het hierbij om jongeren die samen rondhangen, waarbij deze groepen gaandeweg individuen aantrekken die al strafbare feiten hebben gepleegd. Daarnaast kunnen jongeren zich uit eigen initiatief aansluiten bij bestaande jeugdgroepen (R16) of actief worden gerekruteerd door groepsleden (R13, R17).

In beide gevallen spelen met name offline relaties en fysieke locaties een rol. Jongeren leren elkaar kennen op straat, op school, bij de sportvereniging of doordat ze in dezelfde wijk wonen (R1, R2, R3, R7, R8, R11, R14, R16, R17): 'De wijk is leidend. Ze kennen elkaar dan her en der ook wel van school, maar we zien toch vaak dat het een wijk is

waar het [contact] ontstaat' (R2). De wijk lijkt echter een steeds minder belangrijke rol te gaan spelen: 'En die jeugd heeft allemaal scootertjes of [een] elektrische fiets, het verplaatst zich ook net zo makkelijk, net zo snel. Het is niet meer zo wijkgebonden' (R3). In hoeverre deze locaties ook dienen als offender convergence settings, is onbekend.
Daarnaast hebben jongeren die betrokken zijn bij dezelfde groep vaak familie- en vriendschapsbanden. Dergelijke banden kunnen ook online verdergaan, zoals op Telegram, WhatsApp en Snapchat (R5, R11, R14). Dit is eveneens terug te zien in de ontmoetingsplekken die gebruikt worden; dit kan zowel in de fysieke wereld zijn, zoals op straat (R1, R7, R13, R14, R17) als online (R5, R7, R11).

4.4 De kenmerken van individuele leden van bekende (cyber)criminele jeugdgroepen

In deze paragraaf gaan we nader in op de kenmerken van individuele leden van de traditionele jeugdgroepen, zoals deze naar voren kwamen in de expertinterviews. Achtereenvolgens staan we stil bij de demografische kenmerken, de criminele carrières en de motivaties van jongeren om deel te nemen aan traditionele criminaliteit.

4.4.1 *Demografische kenmerken*

De leeftijd van jongeren en jongvolwassenen die onderdeel zijn van traditionele criminele jeugdgroepen varieerde tussen de 8 en 29 jaar (R1, R2, R3, R7, R8, R13, R17), al bestond het merendeel uit leden tussen de 12 en 24 jaar. Daders buiten deze leeftijdsgroep lijken minder vaak voor te komen: 'In principe is het vanaf een jaar of 12, maar we hebben zelfs laatst een jeugdgroep gehad waar nog jongere kinderen in zaten, maar in principe van 12 tot (…) 23.' (R18)

De besproken jeugdgroepen lijken op basis van leeftijd te kunnen worden ingedeeld in twee categorieën. Enerzijds zijn er groepen die vrijwel volledig uit minderjarigen bestaan, waarbij de kernleden doorgaans ouder zijn (15-17 jaar) en de overige leden jonger (R3, R7, R11). Anderzijds bestaan er groepen waarin zowel minderjarigen als volwassenen actief zijn, met leeftijden tussen de 12 en 24 jaar en hier en daar een uitschieter. In deze gemengde groepen bevinden de oudere, vaak volwassen leden zich meestal hoger in de hiërarchie, terwijl minderjarigen lagere posities bekleden.
Gekeken naar geslacht blijkt het grootste deel van de jongeren en jongvolwassenen man te zijn (R1, R2, R7), alhoewel een klein deel ook bestond uit meisjes en jonge vrouwen (R1, R2, R3): 'Maar meestal is twintig procent een meisje, tien, twintig [procent]' (R2) en 'Er zijn met name jongens. Ik heb één groep gehad waar vijf, zes meiden bij zaten. (…). Maar over het algemeen zijn het inderdaad (…) jongens' (R11).
De etnische achtergrond lijkt divers. Zowel jongeren met een Nederlandse (R7, R8, R13) als met een migratieachtergrond (R1, R7, R14) – die veelal wel in Nederland geboren zijn – kunnen deel uitmaken van traditionele criminele jeugdgroepen. Veel jon-

geren binnen deze groepen zijn nog leerplichtig, maar vertonen vaak significant schoolverzuim (R1, R3, R11, R13, R14). Op de vraag of deze jongeren ook naar school gaan, antwoordde een respondent:

> *'Je hebt van die jongelui die je zowel voor strafrechtzaken krijgt, maar ook wel voor de leerplicht. Bij sommigen lijkt het verband met elkaar te houden, maar ik kan niet een-op-een zeggen dat al die gasten, omdat ze niet naar school gaan, of dat een reden zou zijn geweest [dat ze deelnamen aan een criminele groep].' (R11)*

Qua opleidingsniveau varieerde de groep van laag- tot hoogopgeleide jongeren (R3). Als jongeren nog onderwijs volgden, behaalden ze doorgaans slechte cijfers (R14). Daarnaast hadden sommige jongeren een zorgverleden en werden zij als kwetsbaar beschouwd (R1, R20). Tegelijkertijd is het belangrijk te benadrukken dat dit beeld mede wordt bepaald door de jongeren die het snelst bij professionals in beeld komen. De perspectieven van de experts zijn mogelijk vooral gebaseerd op jongeren met problemen, waardoor bepaalde kenmerken mogelijk oververtegenwoordigd zijn in hun waarnemingen. Het is daarom niet uitgesloten dat jeugdgroepen ook kunnen bestaan uit jongeren die wel goede cijfers halen of geen zorgverleden hebben.
De sociaaleconomische status (SES) van groepsleden liet eveneens een divers beeld zien. Jongeren kunnen afkomstig zijn uit verschillende maatschappelijke lagen (R3, R11, R20). Sommigen groeien op in achterstandswijken en komen uit gezinnen met een relatief lage SES (R1, R2, R3, R8, R16), terwijl anderen een meer gemiddelde SES hebben (R17). Een vergelijkbare diversiteit was zichtbaar in de thuissituatie. Enerzijds kunnen jongeren opgroeien in problematische gezinnen (R1, R2, R3, R7, R8, R13, R16, R17, R20), waarbij sprake is van uiteenlopende problematiek: '(…) gebroken gezinnen, uitkeringen van ouders (…). Alcohol, huiselijk geweld. Het klassieke plaatje kon je er eigenlijk wel op loslaten' (R8). En:

> *'Door de thuissituatie, omdat er trauma's zijn, omdat het huiselijk geweld is, omdat er schulden zijn. Armoede (…) speelt een grote rol. De plek waar je woont. Als je in deze huizen kijkt, zijn het ook vaak huizen die heel klein zijn, te weinig ruimte voor alle kinderen. Kinderen zoeken vaak ook wel [hun] heil elders.' (R2)*

> *'De kwetsbare gezinnen waar financiële problemen zijn, waar misschien sprake is van huiselijk geweld, waar [het] gewoon niet veilig is, waar ze [zich] (…) op straat waarschijnlijk veiliger voelen dan thuis. Drankgebruik in die gezinnen, waar het gewoon minder stabiel is, ruzies gemaakt worden, gezinnen die uit elkaar zijn, of samengestelde gezinnen.' (R16)*

Problematische thuissituaties hoeven niet altijd samen te hangen met een lage SES. Ook jongeren uit welvarender gezinnen kunnen betrokken raken bij cybercrime:

'Uit alle wijken, waar ze ook vandaan komen, bij alle jongeren die zorgelijk in beeld blijven, speelt (…) de thuissituatie (…). En dat heeft niet altijd met laag- of hoogopgeleid te maken. Of ouders van goede komaf. (…) Vaak [zijn] ouders veel aan het werk, [hebben] geen tijd [voor hun kinderen]. De binding tussen ouders en kinderen is dan minder. Of juist dat ze te veel verantwoordelijkheid en vrijheid krijgen en daar niet mee om weten te gaan, dat ze daardoor wat ontsporen.' (R3)

Anderzijds konden jongeren binnen deze groepen ook opgroeien in een doorsnee gezin (R13, R17, R20): *'Ze zijn eigenlijk wel in een heel normaal gezin (…) opgegroeid'* (R17).

4.4.1.1 *Criminele carrière*

Binnen traditionele criminele jeugdgroepen lijken de jongeren en jongvolwassenen qua criminele carrière in twee groepen te kunnen worden verdeeld. Enerzijds bestaat een deel van de leden uit first offenders, vooral de jongere leden (R3, R11). Daarbij lijkt het instapdelict dat deze jongeren plegen wel in ernst te zijn toegenomen ten opzichte van eerdere generaties (R7, R11):

'Tot (…) een aantal jaren geleden, als je een first offender minderjarige had, had [hij] een keer iets gejat in een winkel. Maar je ziet steeds meer dat ook die first offenders, zeker vanuit die [traditionele criminele jeugd]groepen, dat dat snel gaat om echte gewelddelicten, met vermogen, het kan over diefstal met geweld of afpersing of iets dergelijks gaan.' (R11)

Anderzijds is een deel van de leden recidivist (R1, R8). Deze groep bestond vooral uit de oudere en vaak meerderjarige leden. Zij waren al eerder in beeld geweest bij politie en justitie voor delicten als mishandeling en winkeldiefstal (R8). Een belangrijke factor die beïnvloedt of een jongere als first offender wordt geregistreerd, is het moment waarop de gemeente signaleert dat een jongere betrokken raakt bij criminaliteit. Wordt er vroeg ingegrepen, dan zijn jongeren vaak nog first offender (R2).

4.4.1.2 *Motivaties*

Voor veel jongeren leek de wens om snel geld te verdienen een belangrijke motivatie voor deelname aan traditionele criminele jeugdgroepen (R13, R14, R16, R17): *'Jongeren gaan niet een bijbaantje [nemen], gaan geen kranten meer lopen voor een luttele [vergoeding], terwijl ze weten dat [ze] verderop [met] (…) een pakketje rondbrengen [veel geld kunnen verdienen].'* (R17)

Daarnaast speelden statusverwerving en de behoefte om ergens bij te horen een belangrijke rol in de motivatie van jongeren om zich aan te sluiten bij deze groepen (R14, R16): 'Ik moet die dure kleding hebben, want dan hoor ik erbij' (R14) en 'dat ze [basisschoolleerlingen] zich gaan aansluiten [bij een jeugdgroep], want ze willen graag bij groepen horen' (R16). Ook hierbij is het van belang om te benadrukken dat deze mo-

tivaties vooral gebaseerd zijn op jongeren die bij de geïnterviewde experts in beeld zijn. Het is goed mogelijk dat andere, minder zichtbare motivaties eveneens een rol spelen, maar dat respondenten daar geen zicht op hadden. De bevindingen bieden daarmee een indicatie van de meest voorkomende waarnemingen, eerder dan een uitputtend of volledig beeld van de motivaties van alle jongeren binnen dergelijke groepen.

4.5 Resumé

In dit hoofdstuk hebben we de kenmerken van jeugdgroepen en hun leden besproken die in beeld zijn bij lokale veiligheidscoalities. In de praktijk waren dit enkel groepen die betrokken waren bij traditionele criminaliteit. Lokale veiligheidscoalities (onder leiding van gemeenten) hadden geen zicht op jeugdgroepen die zich bezighielden met cybercriminele activiteiten. De primaire reden voor dit gebrek aan zicht lijkt te zijn dat er vooral wordt geleund op straatinformatie en signalen uit de wijk bij het in kaart brengen van deze groepen. Het inwinnen van informatie gebeurt daarbij dus nog op traditionele wijze. In de beleving van de respondenten opereren cyberdaders vaak niet op straat, wat leidt tot een beperkt beeld.

Het merendeel van de traditionele criminele jeugdgroepen vertoonde een combinatie van problematisch en crimineel gedrag, waaronder gewelds- en drugsmisdrijven, vernieling en misdrijven tegen de openbare orde. Alhoewel uit onze data naar voren kwam dat lokale veiligheidscoalities geen expliciet zicht hebben op jeugdgroepen die betrokken zijn bij cybercrime, bleek wel dat jeugdgroepen gebruikmaken van internet voor communicatie en dat er vermoedens zijn van betrokkenheid bij cybercrime.

Respondenten hadden slechts beperkt zicht op de precieze structuur en samenstelling van traditionele criminele jeugdgroepen en op hun ontstaans- en groeiprocessen. Een belangrijke kanttekening betreft de mate van zicht die respondenten hebben op deze groepen. Veel respondenten gaven aan slechts beperkt zicht op de aard van de delicten, structuur, samenstelling, en werkwijze van criminele jeugdgroepen en hun leden. De bevindingen die wij hier presenteren zijn daarom voornamelijk gebaseerd op individuele (beperkte) observaties en ervaringen uit de praktijk. Daarbij is het mogelijk dat respondenten eveneens invullingen, interpretaties, of aannames hebben gedaan die niet volledig overeenkomen met de feitelijke situatie. Het beeld dat wij schetsen is daarmee niet noodzakelijk volledig of sluitend, maar weerspiegelt de kennis die door respondenten kon worden aangedragen. Bij de interpretatie van de resultaten dient hiermee rekening te worden gehouden.

Wel was bekend dat de omvang van dergelijke groepen sterk varieerde, tussen de 4 en 40 leden. Binnen sommige groepen is sprake van een vaste kern, die kan bestaan uit 3 tot 15 leden. De vaste kern lijkt stabieler te zijn dan de flexibelere lagen daaromheen. Hoe en wanneer deze groepen ontstaan, is nauwelijks bekend, al ontstaat een deel van de traditionele criminele jeugdgroepen vanuit een 'normale' jongerengroep. In eerste instantie gaat het hierbij om jongeren die samen rondhangen, waarbij deze groepen gaandeweg individuen aantrekken die al strafbare feiten hebben gepleegd. Daarnaast kunnen jongeren zich uit eigen initiatief aansluiten bij bestaande jeugdgroepen of ac-

tief worden gerekruteerd door groepsleden. In beide gevallen spelen met name offline relaties en fysieke locaties een rol. Jongeren leren elkaar kennen op straat, op school, bij de sportvereniging of doordat ze in dezelfde wijk wonen. Daarnaast hebben jongeren die betrokken zijn bij dezelfde groep vaak familie- en vriendschapsbanden.
Wat betreft demografische gegevens ligt de leeftijd van jongeren en jongvolwassenen die onderdeel zijn van traditionele criminele jeugdgroepen tussen de 8 en 29 jaar. De besproken jeugdgroepen lijken op basis van leeftijd te kunnen worden ingedeeld in twee categorieën. Enerzijds zijn er groepen die vrijwel volledig uit minderjarigen bestaan. Anderzijds bestaan er groepen waarin zowel minderjarigen als volwassenen actief zijn. Gekeken naar geslacht blijkt het grootste deel van de jongeren en jongvolwassenen man te zijn. De etnische achtergrond lijkt divers. Verder zijn veel jongeren binnen deze groepen nog leerplichtig, maar vertonen zij vaak significant schoolverzuim. Qua opleidingsniveau varieerde de groep van laag- tot hoogopgeleide jongeren. Daarnaast hadden sommige jongeren een zorgverleden en werden zij als kwetsbaar beschouwd. De sociaaleconomische status van groepsleden liet eveneens een divers beeld zien. Jongeren kunnen afkomstig zijn uit verschillende maatschappelijke lagen. Een vergelijkbare diversiteit was zichtbaar in de thuissituatie.
Binnen traditionele criminele jeugdgroepen lijken de jongeren en jongvolwassenen in twee groepen te kunnen worden verdeeld qua criminele carrière. Enerzijds bestaat een deel van de leden uit first offenders, vooral de jongere leden. Anderzijds is een deel van de leden recidivist. Deze groep bestond vooral uit de oudere en vaak meerderjarige leden. Zij waren al eerder in beeld geweest bij politie en justitie voor delicten zoals mishandeling en winkeldiefstal. Tot slot leek voor veel jongeren de wens om snel geld te verdienen een belangrijke motivatie voor deelname aan traditionele criminele jeugdgroepen. Daarnaast speelden statusverwerving en de behoefte om ergens bij te horen een belangrijke rol.

5 Resultaten spoor 2: de bij lokale veiligheidscoalities onbekende (cyber) criminele jeugdgroepen

In dit hoofdstuk staan jeugdgroepen centraal die betrokken zijn bij cybercriminele activiteiten en die bij één of een beperkt aantal actoren in beeld zijn, maar (nog) onbekend zijn bij de bredere lokale veiligheidscoalitie. De resultaten zijn gebaseerd op de expertinterviews, de zaakreconstructies en de politieregistraties.
Het hoofdstuk is als volgt opgebouwd. Eerst gaan we in op de cybercriminele jeugdgroepen die we hebben geïdentificeerd in de systeeminformatie van de politie. Verder bekijken we in hoeverre de jongeren die bij gemeenten bekend zijn vanwege betrokkenheid bij problematische of traditionele criminele jeugdgroepen ook voorkomen in de systeeminformatie van de politie op het gebied van cybercrime. Vervolgens bespreken we de mate waarin de verschillende actoren zicht hebben op cybercriminele jeugdgroepen. Tot slot komen de kenmerken aan bod van cybercriminele jeugdgroepen en hun leden die bij lokale veiligheidscoalities onbekend zijn.

5.1 Cybercriminele jeugdgroepen die bij lokale veiligheidscoalities onbekend zijn

In hoofdstuk 4 schreven we dat lokale veiligheidscoalities geen zicht hebben op cybercriminele jeugdgroepen. We weten echter op basis van systeeminformatie van de politie en uit gesprekken met lokale actoren dat deze groepen er wel degelijk zijn. De belangrijkste conclusie hierbij is dat informatie over jongeren en cybercriminele jeugdgroepen gefragmenteerd is en alleen beschikbaar is voor strafrechtpartners en/of bij een aantal private partijen, maar niet toegankelijk is voor bredere lokale veiligheidscoalities.

5.1.1 *Politieregistraties: geïdentificeerde groepen*

Om te onderzoeken in hoeverre er in Noord-Nederland cybercriminele jeugdgroepen actief zijn, hebben we allereerst de systeeminformatie van de politie geraadpleegd. Dit leverde 53 cybercrime-gerelateerde politieregistraties op, waarin 109 verdachten werden genoemd. De leeftijd van deze verdachten varieerde van 12 tot 24 jaar (M = 20,23; SD = 2,00, zie Figuur 3). Verdachten kwamen voor in één tot zes registraties (M = 1,72; SD = 1,00), waarbij de meerderheid (52,3%) slechts in één registratie werd genoemd

(Figuur 4). Ruim de helft van de verdachten werd in de periode 1 september 2022 tot 30 september 2023 verdacht van betrokkenheid bij maar één cyberdelict. Tegelijkertijd was dus iets minder dan de helft van de verdachten betrokken bij meerdere cybercrimes.

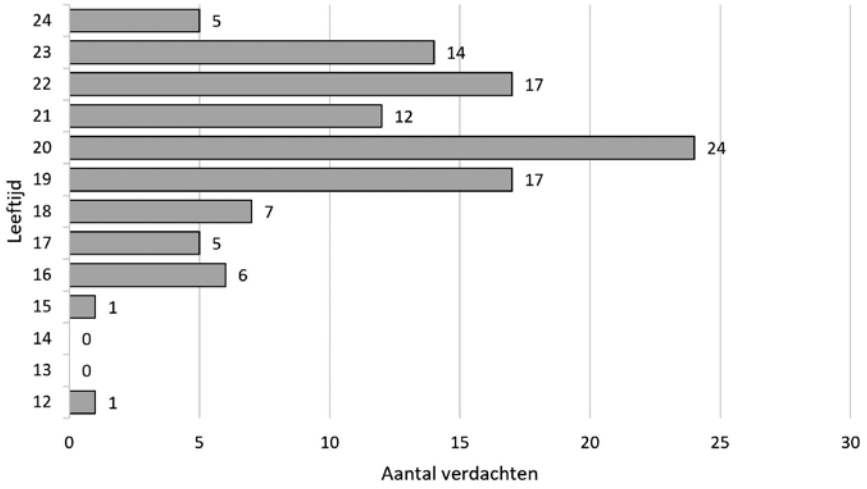
Bij de 109 verdachten die we in de politieregistraties hebben geïdentificeerd, vonden we in totaal 352 onderliggende connecties. Er is sprake van een connectie tussen twee verdachten wanneer ze samen in één registratie voorkomen. In sommige gevallen werden twee dezelfde verdachten geïdentificeerd in verschillende registraties, waardoor er sprake was van dubbele relaties. Als we alleen kijken naar het aantal unieke relaties tussen verdachten, blijven er 249 over. Het gezamenlijk voorkomen van twee personen in dezelfde registratie kan berusten op toeval. Hoewel zij dan samen bij een delict betrokken zijn, duidt dit niet automatisch op een structureel samenwerkingsverband. De inhoudelijke analyse van zes nader onderzochte groepen laat echter zien dat het aantal door de politie officieel aangedragen verdachten een onderschatting vormt van het werkelijke aantal betrokken personen. Dit ondersteunt de keuze om individuen toch als groep de classificeren wanneer zij volgens de officiële politiedata slechts in één registratie voorkomen: sommige personen worden wel in de registraties genoemd, maar ontbreken in de officieel aangedragen data.

Door verdachten met elkaar te verbinden hebben we 26 unieke groepen geïdentificeerd. Deze groepen waren betrokken bij verschillende soorten cybercrime: bankhelpdeskfraude (n = 36), fraude bankgegevens/internetbankieren (n = 6), aan- en verkoopfraude (n = 3), vriend-in-noodfraude (n = 2), sextortion (n = 1), stalking (n = 1) en overige afpersing (n = 2) (Figuur 5). Daarnaast was in twee registraties het type cybercrime onbekend.

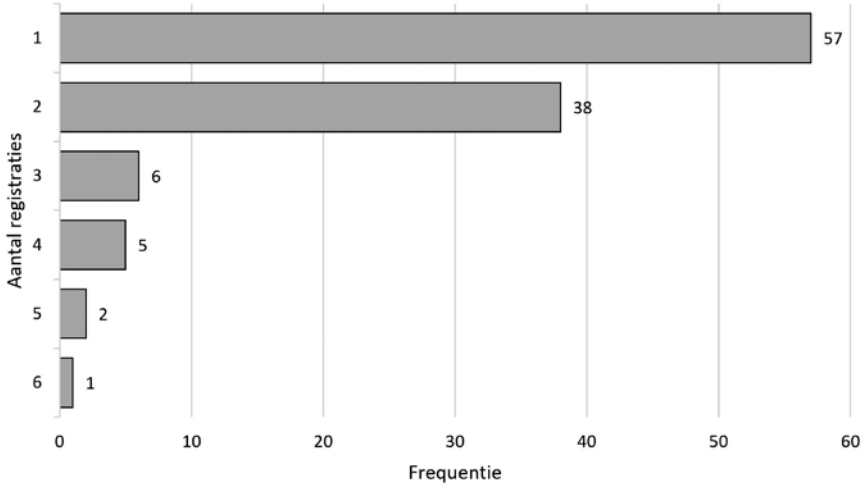
De grootte van de groepen varieerde van 2 tot 23 verdachten (M = 8,63; SD = 7,89) (Figuur 6). De meeste groepen bestonden uit twee verdachten (46,2%). De grootste groep bestond uit 23 verdachten (21,1% van het totale aantal verdachten) en 109 unieke relaties (31,0% van het totale aantal relaties).

We hebben er bewust voor gekozen om in de analyse van de politieregistraties ook samenwerkingsverbanden mee te nemen die bestaan uit slechts twee verdachten, ondanks het feit dat de omvang van deze groepen mogelijk onvoldoende is om te spreken van een structureel samenwerkingsverband. Voor deze keuze zijn twee redenen. Allereerst vormt sociaalnetwerkanalyse een belangrijk onderdeel van dit onderzoek. Binnen sociaalnetwerkanalyse worden alle samenwerkingsverbanden – ongeacht hun omvang – als groepen beschouwd (*co-offending groups* in het Engels). Alle groepen samen vormen vervolgens het overkoepelende netwerk (Wasserman & Faust, 1994).

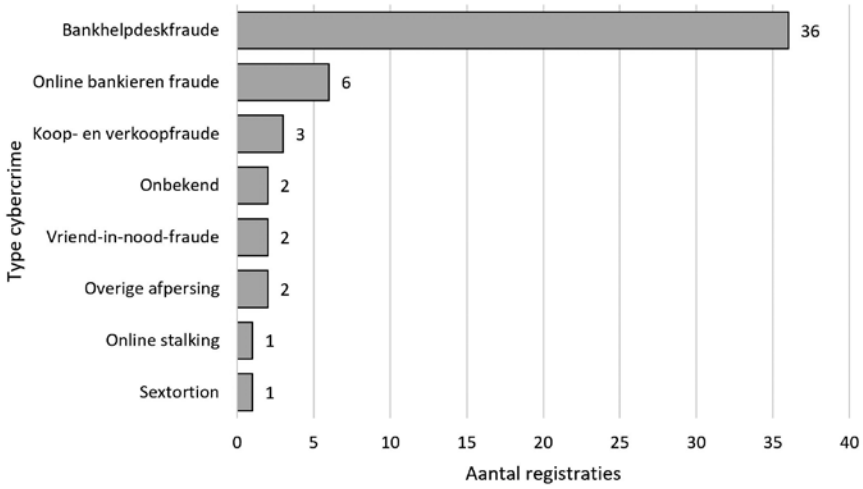
Ten tweede laat de inhoudelijke analyse van de zes nader onderzochte groepen zien – waarvan er drie aanvankelijk bestonden uit slechts twee leden – dat het door de politie aangedragen aantal verdachten waarop de sociaalnetwerkanalyse is gebaseerd, een onderschatting vormt van het werkelijke aantal betrokken personen. Dit ondersteunt de keuze om ook de groepen bestaande uit twee leden, zoals afgeleid uit de officiële gedeelde informatie, in de analyse op te nemen.



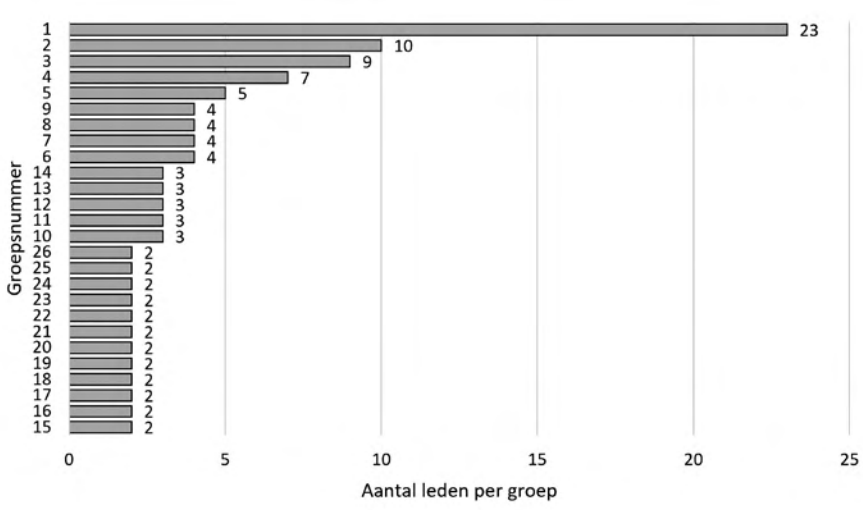
Figuur 3. Verdeling van de leeftijd van de verdachten



Figuur 4. Totaal aantal registraties waar een verdachte in voorkomt



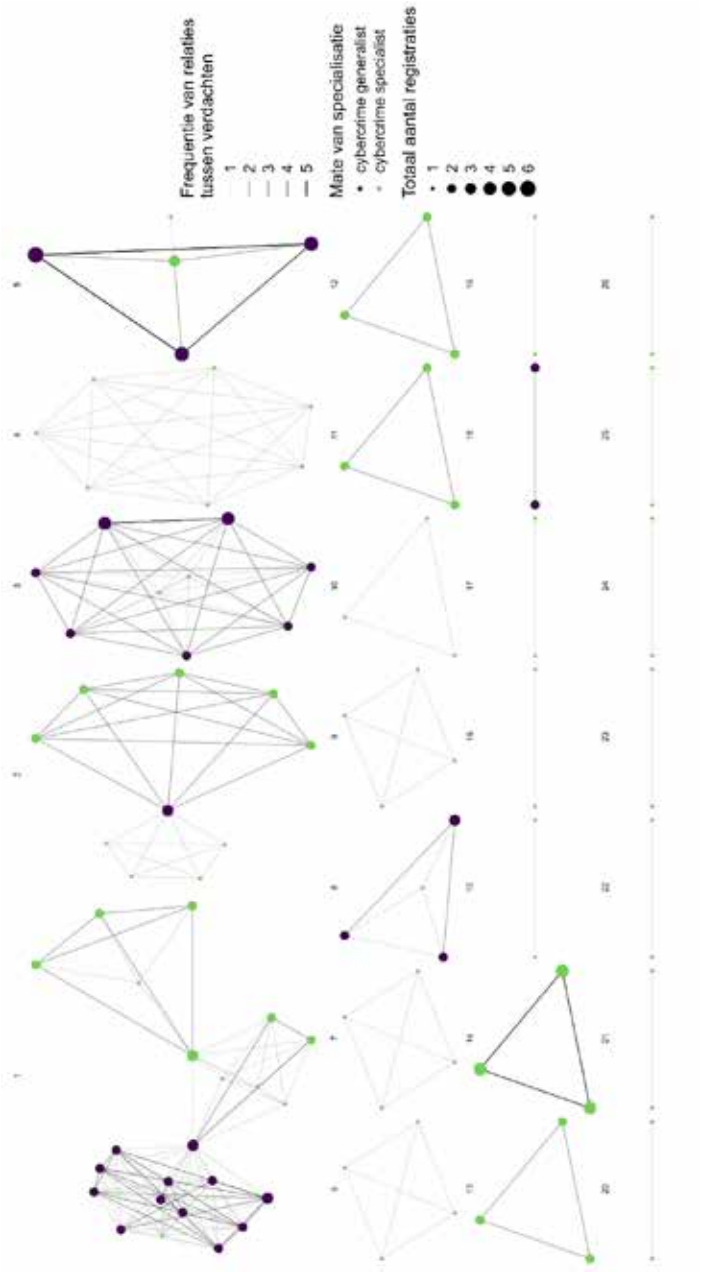
Figuur 5. Het aantal registraties per type cybercrime



Figuur 6. Aantal leden per groep

In Figuur 7 zijn alle groepen grafisch weergegeven. Iedere cirkel representeert een unieke verdachte. Hoe groter de cirkel, hoe vaker de verdachte voorkwam in verschillende unieke politieregistraties. De lijnen geven aan of er sprake is van een relatie tussen twee verdachten. Hoe dikker de lijn, hoe vaker de specifieke twee verdachten samen in verschillende unieke registraties werden genoemd.[15] Tot slot hebben de kleuren van de verdachten betrekking op het aantal gepleegde unieke typen delicten. Groene verdachten hebben één type cybercrime gepleegd (bijvoorbeeld bankhelpdeskfraude), terwijl paarse verdachten twee of meer unieke typen cyberdelicten hebben gepleegd (bijvoorbeeld bankhelpdeskfraude én aan- en verkoopfraude).
In Figuur 7 is te zien dat groepen 1, 2 en 5 bestaan uit meerdere componenten. De grotere groep bestaat dus uit twee of meerdere kleinere groepen, die met elkaar verbonden zijn door één verdachte. Wat verder opvalt is dat het merendeel van de groepen (n = 20) in de periode 1 september 2022 tot 30 september 2023 in de politiesystemen voorkwam voor het plegen van slechts één type cybercrime en daarmee kan worden geclassificeerd als cybercrimespecialist. Bovendien waren 16 groepen maar bij één delict betrokken.

15 Op basis van het type data dat we hebben gekregen, was niet vast te stellen welke specifieke verdachten met elkaar een relatie hadden. Als verdachten A, B en C samen in een registratie worden genoemd, is het mogelijk dat A-B, A-C en B-C een relatie met elkaar hebben, of alleen A-B en A-C. Dit was op basis van de aangeleverde data echter niet vast te stellen. Om die reden zijn we ervan uitgegaan dat wanneer verdachten samen in een registratie worden genoemd, ze een relatie met elkaar hebben. Hiermee wordt het aantal relaties tussen verdachten, en daarmee ook de dichtheid van het netwerk, overschat.



Figuur 7. Schematische weergave van de 26 groepen die we hebben geïdentificeerd in de politiedata

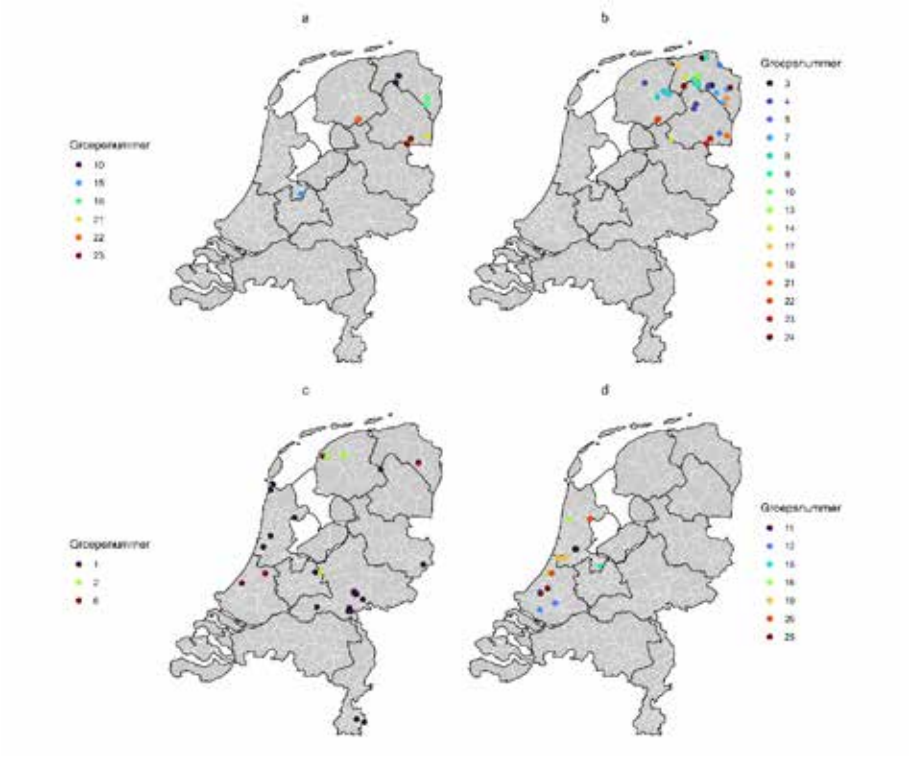
In Figuur 8 en Figuur 9 zijn alle verdachten weergegeven op een kaart van Nederland waarin de gemeentegrenzen zijn aangegeven. Figuur 8 bevat alle groepen van 3 of meer leden, Figuur 9 alle groepen van 2 leden. Iedere cirkel correspondeert met een unieke verdachte en is weergegeven in het viercijferige postcodegebied waar de verdachte woonde. Iedere unieke kleur geeft een specifieke groep weerIn beide figuren corresponderen de groepsnummers met de nummers in Figuur 7.

Figuur 8. Geografische weergave van de woonplaats per verdachte en groep met 3 of meer leden

Figuur 9. Geografische weergave van de woonplaats per verdachte en groep met 2 leden

De systeeminformatie van de politie heeft betrekking op verdachten die óf in Noord-Nederland wonen óf genoemd worden in politieregistraties die zijn aangemaakt door politie-eenheden in Noord-Nederland. In het laatste geval hoeven de verdachten niet per se in Noord-Nederland te wonen.
Bij enkele groepen wonen alle leden in dezelfde gemeente. Dit geldt voor de groepen 10, 15, 18, 21, 22 en 23 (Figuur 10a). Van al deze groepen bevinden de verdachten zich in een gemeente binnen Noord-Nederland, met uitzondering van groep 15. Daarnaast zijn er groepen waarvan de leden verspreid wonen over meerdere gemeenten binnen

Noord-Nederland en niet in een van de provincies buiten Noord-Nederland wonen. Dit betreft de groepen 3, 4, 5, 7, 8, 9, 10, 13, 14, 17, 18, 21, 22, 23 en 24 (Figuur 10b).
Er zijn ook groepen waarbij een deel van de verdachten in Noord-Nederland woont, terwijl anderen in andere provincies wonen. Dit is het geval bij de groepen 1, 2 en 6 (Figuur 10c). Tot slot zijn er meerdere groepen waarvan alle leden buiten Noord-Nederland wonen. Dit betreft de groepen 11, 12, 15, 16, 19, 20 en 25 (Figuur 10d).
Samenvattend blijkt dat 57,7% van de geïdentificeerde groepen bestond uit leden die woonachtig waren in dezelfde of nabijgelegen gemeenten, allen in Noord-Nederland. Van deze 15 groepen woonden alle leden van 5 groepen (33,3%) in dezelfde Noord-Nederlandse gemeente; 4 van deze 5 groepen bestonden uit 2 individuen. Hieruit kunnen twee conclusies worden getrokken. Allereerst zijn de meeste groepen die in Noord-Nederland zijn geïdentificeerd lokaal verankerd, omdat hun leden dicht bij elkaar wonen. Ten tweede kan dit aangeven dat de meest lokaal ingebedde groepen mogelijk kleinschalig van omvang zijn. Echter bestaat ook de mogelijkheid dat deze groepen uit 3 of meer leden bestaan.
Daarnaast waren 3 groepen (1, 2, 6) geografisch verspreid, en hadden 7 andere groepen leden die allemaal buiten Noord-Nederland woonden. Omdat deze laatste 7 groepen toch geïdentificeerd zijn in de politieregistraties, is het waarschijnlijk dat de registratie is aangemaakt door een politie-eenheid in Noord-Nederland, waarbij het slachtoffer dus mogelijk ook daar woonachtig was. Dit kan betekenen dat deze groepen willekeurige slachtoffers targeten, doelbewust slachtoffers buiten hun eigen woonomgeving kiezen, of dat er nog onbekende leden woonachtig in Noord-Nederland betrokken zijn. Gezien de fysieke component die bij de online fraudeactiviteiten van deze groepen meespeelt, lijkt het laatste scenario het meest aannemelijk. Dit ondersteunt bovendien de veronderstelling dat groepen waarin slechts 2 leden zijn geïdentificeerd, in werkelijkheid vaak uit ten minste 3 leden bestaan.



Figuur 10. Verdeling van groepsleden over de verschillende gemeenten

5.1.2 *Zijn leden die bij veiligheidscoalities bekend zijn ook betrokken bij cybergroepen?*

Uit de uitvraag onder de 40 gemeenten in Noord-Nederland en de interviews met gemeentemedewerkers bleek dat geen van de lokale veiligheidscoalities in Noord-Nederland op dat moment jeugdgroepen in beeld had die ook betrokken waren bij cybercriminele activiteiten. Van de 25 gemeenten die reageerden, gaven er 10 aan dat zij jeugdgroepen in beeld hadden. Van deze gemeenten leverden er 9 de identificerende gegevens aan van in totaal 207 groepsleden, verspreid over 13 groepen. Daarnaast werden 4 individuen genoemd die behoorden tot een groep die voor de gemeente op dat moment nog onbekend was.
Per groep is gevraagd om identificerende gegevens[16] van de groepsleden die bij de gemeente bekend waren. In samenwerking met de intelligence-organisatie van de politie is vervolgens in kaart gebracht in hoeverre in de politiesystemen aanwijzingen beston-

16 NAW-gegevens, geboortedatum en BSN (als unieke identifier).

den voor de betrokkenheid van deze groepen (en hun individuele leden) bij cybercrime. Van de 207 door gemeenten geïdentificeerde jeugdigen konden 4 jongeren direct gekoppeld worden aan 3 van de 26 groepen die op basis van de politieregistraties waren geïdentificeerd (groep 3 = 2 individuen, groep 4 = 1 individu, groep 8 = 1 individu). Voor deze 4 jongeren bestaan er dus aanwijzingen voor betrokkenheid bij cybercrime, terwijl dit bij de gemeenten niet bekend was. De overige 9 personen lijken niet direct verdacht te worden van betrokkenheid bij cybercrime, maar hebben wel een relatie met een persoon die verdacht wordt van het plegen van cybercrime.
Deze bevindingen wijzen erop dat de jeugdgroepen die bij gemeenten bekend zijn overwegend betrokken zijn bij overlast en traditionele vormen van criminaliteit. Toch blijkt dat een klein deel van deze jongeren (6,3% van het totaal aantal bij gemeenten bekende groepsleden) ook in verband kan worden gebracht met cybercrime, terwijl dit bij de lokale veiligheidscoalities onbekend is. Bovendien laat de netwerkanalyse van politieregistraties zien dat er in Noord-Nederland wel degelijk cybercriminele jeugdgroepen actief zijn, maar dat deze volledig buiten beeld blijven van de lokale veiligheidscoalities. Cybercrime blijft daardoor vooralsnog volledig buiten beschouwing in de jeugdgroepenaanpak.

5.1.3 *Aanvullend beeld interviews en zaakreconstructies*

Het beeld dat er vanuit lokale veiligheidscoalities geen zicht is op cybercriminele jeugdgroepen, maar dat deze door individuele actoren wél worden gesignaleerd, is ook naar voren gekomen uit de expertinterviews. De belangrijkste conclusie hierbij is dat informatie daarover gefragmenteerd is en alleen beschikbaar is voor strafrechtpartners en/of bij enkele private partijen, maar niet toegankelijk is voor bredere lokale veiligheidscoalities.
Zo kwam uit vijf interviews met politiemedewerkers (R4, R5, R8, R12, R19) naar voren dat zij zicht hebben op cybercriminele jeugdgroepen en groepen die betrokken zijn bij traditionele criminaliteit. Dit werd ook tijdens de focusgroep benadrukt (R21). In één interview met politiemedewerkers (R19) werd aangegeven dat zij geen specifieke kennis hadden van een cybercriminele jeugdgroep, al waren er wel vermoedens van cybercriminele activiteiten binnen een bekend traditionele jeugdgroep.
De cybercriminele jeugdgroepen die bij de politie bekend zijn, kunnen via twee wegen in beeld komen: (1) aangiftes; en (2) de analyse van politiedata. Aangiftes dienen veelal als startpunt voor opsporingsonderzoeken, waarmee vervolgens informatie wordt verzameld om het zicht op een groep te vergroten. Dit was ook het geval voor de groepen uit de vijf zaakreconstructies en de zes groepen (N3, N8, N12, N18, N21 en N24) die op basis van de politieregistraties zijn geïdentificeerd en vervolgens nader onderzocht zijn. In alle gevallen zijn groepsleden geïdentificeerd door één of meer aangiftes. Daarnaast wordt eerder verzamelde politiedata gebruikt om cybercriminele jeugdgroepen te identificeren, bijvoorbeeld aan de hand van socialenetwerkanalyse. Dit werd ook ondersteund door een interview met een OM-medewerker (R22).

Van de vier geïnterviewde OM-medewerkers gaven er drie aan dat zij bekend waren met cybercriminele jeugdgroepen (R11, R15, R22). De vierde respondent had geen specifieke kennis van deze groepen, wat verklaard kan worden door het feit dat deze persoon zich vooral bezighield met jeugdproblematiek in bredere zin en niet specifiek met cybercrime. Ook kwam uit de interviews naar voren dat het OM momenteel geen specifieke informatiestructuur heeft om cybercriminele jeugdgroepen in kaart te brengen. Bovendien wordt het verkrijgen van een beeld van dergelijke groepen niet als kerntaak van het OM beschouwd. Voor informatie is het OM grotendeels afhankelijk van partners.

Tot slot kwam uit de focusgroep (R21) en de interviews met een fraudespecialist van een bank (R9) en een telecomprovider (R10) naar voren dat banken en telecomproviders vooral zicht hebben op cybercriminele activiteiten en in mindere mate op traditionele criminaliteit. De daders hierbij zijn jongvolwassenen. Zo benadrukte de fraudespecialist van de telecomprovider dat zij vooral zicht hebben op delicten die gerelateerd zijn aan de diensten die zij leveren. Een voorbeeld van zo'n delict is het misbruiken van telefoonnummers voor smishing.[17] In de focusgroep werd aangegeven dat banken moeite hebben om groepen in hun eentje in kaart te brengen, omdat (cyber)criminele groepen zich vaak niet beperken tot één bank, maar verspreid zitten over meerdere banken. Bovendien hebben banken vooral zicht op geldezels, terwijl de kernleden buiten schot blijven. Om cybercriminele (jeugd)groepen toch (gedeeltelijk) te kunnen identificeren, koppelen banken aangiftes (onder andere binnen de Electronic Crimes Task Force) en sturen zij die door naar de politie, die deze gegevens meeneemt in het onderzoek naar de groepen.

Vier van de vijf zaakreconstructies versterken het beeld dat de politie en het OM zicht hebben op (een beperkt aantal) cybercriminele jeugdgroepen. De groep in de RIEC-casus was wel in beeld bij meerdere instanties, maar wel pas na politieonderzoek. Voor de groepen die werden geïdentificeerd op basis van de politieregistraties werd in de data niet beschreven in hoeverre andere veiligheidspartners bekend waren met de betreffende groepen. Wel kwam naar voren dat enkele individuen onder bewindvoering stonden. Daarnaast liep voor één lid van groep N3 een persoonsgerichte aanpak.

5.2 Zaakreconstructies en politieregistraties: een samenvatting van de nog niet bekende groepen

In deze paragraaf staan de groepen centraal die we hebben geïdentificeerd in de zaakreconstructies (C1-C5) en de politieregistraties (N3, N8, N12, N18, N21 en N24), waarbij we uit de 26 groepen een steekproef hebben getrokken. Dit zijn groepen die voor lokale veiligheidscoalities nog onbekend waren. In paragraaf 5.2.1 geven we een beschrijving van de groepen die zijn geïdentificeerd in de politieregistraties, en paragraaf 5.2.2 biedt inzicht in de groepen uit de zaakreconstructies. Per bron beschrijven we eerst de hybride groepen (die zowel cybercrime als traditionele criminaliteit ple-

17 Het gebruik van sms om phishingberichten te verspreiden (Mishra & Soni, 2020).

gen), gevolgd door de cybercriminele groepen, die zich uitsluitend met cybercrime bezighouden. De beschrijving van iedere groep volgt dezelfde opbouw: het aantal leden, de gepleegde delicten, de structuur en samenstelling van de groep en de ontstaans- en groeiprocessen.
Deze groepen vormen de basis voor de thematische analyse in dit hoofdstuk. In de paragrafen 5.3, 5.4 en 5.5 wordt de kern van het hoofdstuk weergegeven, waarbij we de informatie van de afzonderlijke groepen overkoepelend samenvatten en aanvullen met data uit de expertinterviews. Het is daarom niet nodig om de paragrafen 5.2.1 en 5.2.2 uitvoerig te bestuderen.

5.2.1 *Groepen die zijn geïdentificeerd in de politiedata*

Tabel 6 geeft een beknopt overzicht van de kenmerken van de groepen die zijn geselecteerd op basis van de politieregistraties. Dit zijn de groepen N3, N8, N12, N18, N21 en N24. Daarbij hebben we onderscheid gemaakt tussen hybride groepen (N3, N24) en cybercriminele groepen (N8, N12, N18, N21).

5.2.1.1 *Hybride groep N3*

Groep N3 bestond uit ten minste 14 leden en pleegde zowel cybercrime als traditionele criminaliteit. De groep was primair betrokken bij bankhelpdeskfraude, maar ook bij witwassen, wapenbezit en wapenhandel. Bij de uitvoering van bankhelpdeskfraude werden meerdere werkwijzen gehanteerd. In één geval werd een slachtoffer telefonisch benaderd door iemand die zich voordeed als bankmedewerker en mededeelde dat er een probleem was met de bankrekening van het slachtoffer, wat verholpen kon worden door het afgeven van haar bankpas. Opvallend was dat in ten minste één geval de 'bankmedewerker' met een Gronings dialect sprak, waarbij het slachtoffer ook in Groningen woonde. In deze casus werd met de bankpassen van het slachtoffer € 6.700 buitgemaakt, evenals de inhoud van een kluis buitgemaakt, ter waarde van € 5.500.

In een tweede geval werden naar een slachtoffer betaalverzoeken verstuurd onder het voorwendsel dat hij hiermee zijn geld veilig kon stellen. In werkelijkheid werden deze betalingen gebruikt voor de aanschaf van goederen.
Daarnaast was de groep actief bij het witwassen van het wederrechtelijk verkregen voordeel, veelal via het contant pinnen van geld, het kopen van luxe goederen met de bankpassen van slachtoffers en het via de bankrekening van slachtoffers bestellen van goederen:

> *'Ik [verbalisant] zag dat er een Mantale Starry Nights Eau de Parfum ter waarde van 125 euro, DIOR Sauvage Eau de Parfum ter waarde van 90,50 euro en een Canada Goose Macmillan (sic) gewatteerde jas met donsvulling en capuchon ter waarde van 995 euro was besteld.'*

En:

'Ik [verbalisant] zag dat er op [een doordeweekse dag 's avonds] met het accountnummer [nummer] een Apple iPhone 14, 128GB, paars, was besteld voor een totaalbedrag van 1.019 euro.'

Daarnaast werd het geld besteed aan cadeaukaarten en loterijloten (N3 en N12): 'En zou bij de [supermarkt] in [een stad], diezelfde middag omstreeks [het tijdstip] getracht zijn om Lotto-loten te kopen voor een bedrag [boven de € 900].'
Bij de bankhelpdeskfraude én het witwassen was een duidelijke rolverdeling en hiërarchie te zien. Slachtoffers werden telefonisch benaderd door een 'beller', die de slachtoffers overhaalde hun bankpassen te overhandigen aan een 'pasophaler'. De bankpassen werden vervolgens gebruikt door katvangers ('pinners') om contant geld te pinnen of goederen te kopen, zoals dure kleding. Daarnaast gebruikten kernleden de naam en adresgegevens van katvangers om online goederen te bestellen (zoals iPhones en parfums) en te laten bezorgen. Deze werden betaald via betaalverzoeken die naar slachtoffers werden gestuurd. Katvangers kregen soms een financiële vergoeding in ruil voor het ter beschikking stellen van hun adres. Zo kreeg een van de leden bijvoorbeeld in één geval € 20.
Ook was er sprake van een duidelijke hiërarchie. Het enige kernlid had een leidinggevende rol en stuurde de overige leden van de groep aan. Twee andere leden hadden een actieve rol bij het bestellen van goederen. De overige leden fungeerden vooral als katvanger: hun adressen werden gebruikt voor het ontvangen van pakketten die waren gekocht met het wederrechtelijk verkregen voordeel. Verder was het onduidelijk of er sprake was van een vaste kern en of de groep dynamisch was, al doet het gebruik van meerdere geldezels vermoeden dat de groep in enige mate dynamisch was.
Binnen de groep werd geweld naar elkaar gebruikt. Daarvan is één incident bekend. Hierbij hadden meerdere leden vuurwapens bij zich, en werd een van de lagere leden van de groep bedreigd en bang gemaakt met een vuurwapen, omdat hij niet wilde meewerken.
Door de groep werden verschillende middelen gebruikt om bankhelpdeskfraude te plegen, zoals een scanner voor internetbankieren en simkaarten. Daarnaast leek de groep ook gebruik te maken van *leads*: de benaderde slachtoffers waren allemaal op hoge leeftijd en woonden in Groningen, waarbij de 'bankmedewerker' sprak met een Gronings dialect. Hoewel er geen directe aanwijzingen voor zijn, doet dit vermoeden dat er een facilitator betrokken was bij de groep.

5.2.1.2 *Hybride groep N24*

Groep N24 bestond, voor zover bekend, uit slechts 2 leden en was betrokken bij zowel online als offline stalking en vernieling. In deze casus werd een familielid van een van de verdachten gestalkt. Dit werd gedaan in de offline wereld door diegene te achtervolgen. Bovendien werden meerdere goederen vernield en werd gedreigd met brandstichting. De stalking vond ook online plaats, onder andere via sociale media: 'Laat me je niet tegen komen (sic) en het boeit me niet als ik jou straks heb neer gestoken (sic) dat ik vast kom te zitten. Heb ik voor mijn familie wel over.'

Uit de politieregistraties komt naar voren dat er binnen de groep sprake was van een duidelijke rolverdeling en hiërarchie: de ene verdachte was een kernlid, vervulde een leidinggevende rol en was direct verantwoordelijk voor het stalken van het slachtoffer. De andere verdachte had een ondergeschikte rol en fungeerde als katvanger: haar account op sociale media werd gebruikt om bedreigende berichten te sturen, die vermoedelijk door het kernlid werden verstuurd. Tot slot is onduidelijk hoe de groep exact is ontstaan, al hadden beide leden elkaar in de fysieke wereld ontmoet.

5.2.1.3 *Cybercrimineel groep N8*

Groep N8 bestond uit ten minste 12 leden en hield zich bezig met verkoopfraude en witwassen. De modus operandi bestond uit het aanbieden van goederen via een socialemediaplatform. Nadat slachtoffers de betaling hadden voltooid, werd het product niet geleverd. Een voorbeeld van een aangifte:

> *'Op Marketplace (van Facebook) heb ik een [product] gezien die ik wilde kopen. Daartoe heb ik contact opgenomen met de verkoper via Messenger. De verkoper heeft een betaalverzoek gestuurd en ik heb voor aankoop plus verzending 80 euro betaald op [datum]. Ik heb de [product] niet ontvangen. Omdat ik onraad rook (advertentie is op Marketplace blijven staan; de accountnaam kwam niet overeen met de naam van de bankrekening) heb ik de verkoper gevraagd om een kopie van het verzendbewijs te sturen. Het antwoord was een duimpje.'*

Voor het witwassen van het wederrechtelijk verkregen voordeel werd gebruikgemaakt van geldezels:

> *'Ik [de geldezel] stuurde het betaalverzoek naar de koper. Ik kreeg van V7 te horen dat er geld op zijn rekening was gezet. En dan spraken we af bij een pinautomaat om het geld te pinnen. Ik kreeg dan het geld contant.'*

Het wederrechtelijk verkregen voordeel was € 6.100. Dit werd verdeeld onder het kernlid en de geldezels, waarbij het kernlid de hoogte van de vergoeding bepaalde. Uit het verhoor kwam naar voren dat de verdeling als volgt verliep:[18]

> *V: 'Kun je vertellen wat V4 dan moest doen?'*
> *A: 'Hij moest het geld pinnen. We hadden van tevoren de afspraak 50/50. Hij kreeg dan de helft van het bedrag.'*

En:

> *V: 'Hoeveel geld kreeg V7 dan elke keer?'*

18 V = vraag van verbalisant; A = antwoord van verdachte.

A: 'Ik bepaalde het bedrag van de betaalverzoeken. Ik nam ook de beslissing hoeveel V7 ervan mocht hebben. De ene keer was het meer als (sic) de andere keer. Ik kreeg het geld elke keer contant en volgens mij heeft hij ook geld overgemaakt naar Paypal (sic). Dat was een keer.'

Binnen deze groep was sprake van een strikte rolverdeling. Eén kernlid had de leiding. Hij was verantwoordelijk voor het benaderen van slachtoffers en het rekruteren van geldezels en stuurde hen ook aan. De overige elf leden fungeerden allemaal als geldezel. Uit het verhoor met een van de geldezels kwam naar voren hoe het kernlid te werk ging:

V: 'Hoe ging het als V5 aangaf dat er geld op zijn rekening stond?'
A: 'Ik kreeg een appje. Elke keer gaf hij aan dat het geld op mijn rekening werd gestort.'
V: 'Wat moest je dan doen?'
A: 'Hij vroeg aan mij of ik het geld dan wilde pinnen. Ik vond dat prima. Wij maakten dan een afspraak om het geld te gaan pinnen. Hij [een] keer in [een stad] en de rest gewoon in [een andere stad].'

De vaste kern van de groep bestond uit het ene leidinggevende kernlid. De groep geldezels was zeer dynamisch, waarbij het kernlid voortdurend nieuwe rekruteerde. Dit was nodig om het wederrechtelijk verkregen voordeel wit te kunnen wassen. Bij deze rekrutering speelden offline contacten een belangrijke rol; het kernlid was bevriend met enkele geldezels en had ook zijn ex-vriendin gerekruteerd. Nadat het geld was overgemaakt naar de geldezelrekeningen, verliep het contact tussen het kernlid en de geldezels veelal telefonisch en via WhatsApp en sms.

5.2.1.4 *Cybercrimineel groep N12*

Groep N12 bestond uit ten minste 3 leden en was betrokken bij bankhelpdeskfraude en witwassen. De gehanteerde werkwijze voor bankhelpdeskfraude was nagenoeg hetzelfde als bij N3. Opvallend was dat in zeker één geval de 'bankmedewerker' Fries sprak, waarbij het slachtoffer in Friesland woonde. Het witwassen vond plaats door met de bankpassen van het slachtoffer contant geld te pinnen. Het wederrechtelijk verkregen voordeel bedroeg uiteindelijk meer dan € 2.000.
Alhoewel er beperkt zicht was op de structuur en de samenstelling van de groep, lijkt er wel sprake te zijn van een taakverdeling. De casus had betrekking op drie groepsleden (katvangers) die naar Friesland reisden om daar bankpassen van slachtoffers op te halen als onderdeel van de bankhelpdeskfraude. Eén persoon vervulde de rol van bestuurder, terwijl een tweede als 'pasophaler' fungeerde. Groepslid drie vervulde, samen met de pasophaler, ook de rol van 'pinner' en gebruikte de gestolen bankpassen om contant geld te pinnen. De drie groepsleden functioneerden als katvangers en werden vermoedelijk aangestuurd door een hoger, onbekend gebleven kernlid.
Naast deze drie groepsleden waar de politieregistraties zich op toespitsten, werden in dezelfde dossiers nog drie andere personen genoemd die mogelijk onderdeel waren

van de groep. Eén van hen had zijn auto uitgeleend aan de drie leden nadat de bestuurder hier via WhatsApp om had gevraagd. De precieze rol van de overige twee leden hebben we niet vast kunnen stellen.
De manier waarop groepsleden gerekruteerd werden is ook onbekend gebleven, al was wel duidelijk dat twee leden elkaar kenden uit de buurt. Verder werden online platforms zoals Snapchat en WhatsApp gebruikt om te communiceren. Alle drie de leden waren bijvoorbeeld onderdeel van dezelfde Snapchat-groep, waarin ze onder andere de adressen van slachtoffers deelden. Verder was er contact via WhatsApp tussen een van de drie leden (V2) en weer iemand anders (V6), waarbij V2 vroeg of hij de auto van V6 kon lenen.

5.2.1.5 *Cybercrimineel groep N18*

Afgezien van de modus operandi bevatten de politieregistraties zeer weinig informatie over groep N18. De groep was primair betrokken bij bankhelpdeskfraude. Opvallend in deze casus was dat de verdachte zich voordeed als bankmedewerker en daarbij gebruikmaakte van de naam van een bestaande customer due diligence (CDD)[19]-analist van de betreffende bank.

5.2.1.6 *Cybercrimineel groep N21*

Groep N21 bestond uit ten minste 2 leden. In de politieregistraties werd ook een derde persoon genoemd, maar in hoeverre zij ook actief was binnen de groep, is onduidelijk gebleven. De criminele activiteiten van de groep waren vooral gericht op sextortion. In de casus die in de politieregistraties werd beschreven, werd het slachtoffer benaderd via een website, waarbij de dader zich voordeed als jonge vrouw. Vervolgens werd het contact voortgezet via WhatsApp, waar zowel de verdachte als het slachtoffer seksueel getinte berichten en foto's uitwisselden. Na enige tijd werd het slachtoffer telefonisch benaderd door iemand die zich voordeed als de vader van de vermeende jonge vrouw. In werkelijkheid waren de jonge vrouw en de vader één en dezelfde persoon. Deze 'vader' beweerde dat het om zijn 16-jarige dochter ging en zette het slachtoffer onder druk om een geldbedrag te betalen: 'Vervolgens wordt de aangever onder druk gezet en moet hij geld betalen. Als het bedrag betaald zou worden, zou er geen politie of de werkgever worden ingeschakeld.' Het slachtoffer werd gedwongen om € 15.000 te betalen om te voorkomen dat de zaak werd gemeld bij de politie. Of er daadwerkelijk geld is buitgemaakt en waar dat dan aan is uitgegeven, is niet terug te vinden in de politiedossiers.
Verder bleek uit het politieonderzoek dat het enige kernlid van de groep (dat zich had voorgedaan als jonge vrouw en haar vader) ook in het bezit was van kinderpornografisch beeldmateriaal: 'Door mij verbalisant werd de telefoon van verdachte uitgelezen. Hierin kwam ik een appgroep tegen waarbinnen kinderpornografische afbeeldingen

19 Customer due diligence is het proces waarbij een organisatie de identiteit, de achtergrond en de risico's van een klant controleert om te voorkomen dat die klant criminaliteit pleegt via de organisatie.

werden gedeeld. Binnen deze groep lijkt het te gaan om een klas, er wordt ook namelijk regelmatig gesproken over school.'

Bij deze groep was sprake van een duidelijke rolverdeling, waarbij het kernlid de leiding had en de andere twee functioneerden als katvangers. Het kernlid benaderde de slachtoffers, deed zich voor als een vrouw en later als de 'vader' van deze fictieve persoon, waarna hij degene was die het slachtoffer onder druk zette om geld te betalen. Uit het onderzoek bleek dat op de telefoon van dit leidinggevende groepslid de website was bezocht waar het initiële contact met het slachtoffer was ontstaan. Op zijn telefoon stonden meerdere telefoonnummers die vermoedelijk toebehoorden aan andere slachtoffers.

Voor de twee andere personen geldt dat hun telefoonnummers werden gebruikt om contact op te nemen met het slachtoffer. Zij fungeerden dus vermoedelijk als katvanger. Ook werd de bankrekening van een van de twee katvangers gebruikt om het afpersingsgeld van het slachtoffer op over te maken. Daarbij werd overigens ook de bankrekening van het kernlid gebruikt.

De exacte manier van rekrutering is onbekend gebleven. Wel is bekend dat het kernlid en één katvanger in hetzelfde dorp woonden en vrienden van elkaar waren. Daarnaast werd gebruikgemaakt van het telefoonnummer van de vriendin van de katvanger om het slachtoffer te benaderen.

Tabel 6. Kenmerken van de groepen die werden geïdentificeerd in de politieregistraties en die nader zijn onderzocht

Groep nr.	Mate van zicht op groep	Structuur en samenstelling					Ontstaan en groei			Delicten		
		Aantal leden	Rollen	Hiërarchie	Dynamiek	Facilitators	Hoe betrokken	Ontmoetingsplaatsen	Banden tussen leden	Traditioneel	Cyber	Verwevenheid
N3	Beperkt	14+	1. Beller 2. Pasophaler 3. Koper goederen 4. Pinnen (katvanger) 5. Naam gebruikt om bestellingen te plaatsen (katvanger) 6. Adres gebruikt om bestellingen te laten bezorgen (katvanger) 7. Op adres laten bezorgen van goederen (katvanger)	Duidelijke hiërarchie: - er zijn meerdere verdachten die een hogere plek in de groep lijken te hebben; - er is een duidelijke leidersfiguur; - onduidelijk of er een vaste kern is.		Onbekend	1. Rekrutering - een groot deel van de leden is gerekruteerd voor het uitvoeren van specifieke taken. 2. Offline contacten: - alle leden zijn gerekruteerd via offline contacten.	1. Snapchat 2. Coffeeshop 3. Woning	1. Vrienden 2. Dorpsgenoten 3. Kennissen	1. Voorhanden hebben van vuurwapens 2. Wapenhandel	1. Bankhelpdeskfraude 2. Witwassen	Mogelijke verwevenheid

Groep nr.	Mate van zicht op groep	Structuur en samenstelling					Ontstaan en groei			Delicten		
		Aantal leden	Rollen	Hiërarchie	Dynamiek	Facilitators	Hoe betrokken	Ontmoetingsplaatsen	Banden tussen leden	Traditioneel	Cyber	Verwevenheid
N8	Beperkt	12+	1. Geldezel 2. Benaderen slachtoffers	Duidelijke hiërarchie: - er was een zeer sterke hiërarchie. Eén kernlid had de leiding, de overige leden waren geldezels; - duidelijke vaste kern, met één kernlid.	Duidelijk dynamisch: één lid is de vaste kern, de overige leden zijn geldezels die elkaar snel opvolgen.	Onbekend	1. Rekrutering: - alle geldezels zijn gerekruteerd door V5. 2. Offline contacten: - V5 had offline contact met alle overige leden die hij heeft gerekruteerd.	1. WhatsApp 2. Bellen / sms'en	1. Vrienden 2. Zorginstelling 3. Kennissen 4. Romantische relaties	Niet	1. Verkoopfraude 2. Witwassen	Geen verwevenheid
N12	Beperkt	3+	1. Autobestuurder 2. Pinner 3. Facilitator	Mogelijke hiërarchie. Deel van de leden haalt in opdracht van anderen bankpasjes op en pint ermee.	Onbekend	Geen	1. Rekrutering: onbekend. Niet duidelijk of en hoe ze gerekruteerd worden. 2. Offline contacten: - twee leden kennen elkaar uit de buurt.	1. Snapchat 2. WhatsApp	Buurt. Twee leden kennen elkaar uit de buurt.	Niet van toepassing	1. Bankhelpdeskfraude 2. Witwassen	Niet van toepassing
N18	Beperkt	4+	Onbekend	Onbekend	Onbekend	Onbekend	Onbekend	Onbekend	Onbekend	Niet van toepassing	Bankhelpdeskfraude	Niet van toepassing

Groep nr.	Mate van zicht op groep	Structuur en samenstelling					Ontstaan en groei			Delicten		
		Aantal leden	Rollen	Hiërarchie	Dynamiek	Facilitators	Hoe betrokken	Ontmoetingsplaatsen	Banden tussen leden	Traditioneel	Cyber	Verwevenheid
N21	Beperkt	2+	1. Kernlid/ benaderen slachtoffers 2. Geldezel	Duidelijke hiërarchie: - er is een kernlid dat duidelijk de leiding heeft en het andere lid aanstuurt.	Onbekend	Onbekend	1. Rekrutering onbekend: - het is onbekend of er binnen deze groep sprake is van rekrutering. 2. Offline contacten: - beide verdachten wonen in hetzelfde dorp en telefoonnummer vriendin verdachte is gebruikt voor het plegen van delicten.	Snapchat. Beide verdachten hebben hier contact.	1. Dorp 2. Romantische relatie	Niet	1. Sextortion 2. Bezitten pornografisch beeldmateriaal	Geen verwevenheid
N24	Beperkt	2	1. Kernlid 2. Katvanger	Duidelijke hiërarchie: - het ene kernlid is duidelijk de leidinggevende en het andere lid is ondergeschikt.	Niet	Niet	1. Rekrutering onbekend. 2. Offline contacten: - beide verdachten zijn vrienden van elkaar.	Woning	Vrienden	Fysieke stalking Vernieling	Online stalking	Duidelijke verwevenheid

5.2.2 *Groepen die zijn geïdentificeerd in de zaakreconstructies*

Tabel 7 biedt een overzicht van de kenmerken van de groepen die zijn geïdentificeerd in de zaakreconstructies. Daarbij hebben we onderscheid gemaakt tussen hybride groepen (C1, C2, C3 en C5) en een cybercriminele groep (C4).

5.2.2.1 *Hybride groep C1*

Groep C1 bestond uit 21 kernleden en tientallen katvangers en was actief binnen zowel de cybercrime als de traditionele criminaliteit. Zo was de groep betrokken bij verkoopfraude via Marktplaats, phishing, bankhelpdeskfraude, de handel in verdovende middelen, geweldsdelicten, wapenbezit, witwassen en diverse economische delicten.
Bij de verkoopfraude werden advertenties op Marktplaats geplaatst, waarbij slachtoffers betaalden voor producten die vervolgens niet werden geleverd. Phishing vond plaats via betaalverzoeken die leidden naar frauduleuze websites, waarmee toegang verkregen werd tot de bankrekeningen van slachtoffers.
Ook was de groep actief op het gebied van traditionele criminaliteit. Eén lid fungeerde als lachgaskoerier en er waren aanwijzingen voor de betrokkenheid van meerdere leden bij drugstransporten. Daarnaast werden 7 kernleden gelinkt aan ernstige geweldsdelicten met (vuur)wapens, waaronder een ripdeal, een kogelbrief en een schietpartij. Dit geweld zou vermoedelijk gerelateerd zijn aan conflicten binnen het (cyber)criminele milieu. Verder werd wederrechtelijk verkregen voordeel witgewassen door het kopen van dure schoenen en kleding zonder dat er bij deze leden een legale bron van inkomsten tegenover stond. Tot slot bestonden de economische delicten uit valsheid in geschifte, zwartwerken en kinderarbeid.
De groep lijkt te zijn doorgegroeid van een traditionele criminele groep naar een groep waarin ook cybercrime gepleegd werd – een hybride groep. Zo waren 8 van de 15 kernleden betrokken bij traditionele criminaliteit (zoals scooterdiefstal en drugshandel) voordat ze zich met cybercrime gingen bezighouden.
De structuur van de groep had meerdere lagen: een vaste kern van 15 leden, 2 facilitators en tientallen geldezels; 4 kernleden vervulden een sleutelrol, waarvan er één een duidelijke leidende rol had. De groep leek in enige mate dynamisch te zijn, waarbij de kernleden in verschillende samenstellingen gezamenlijk cybercrimes pleegden. Bovendien verlieten enkele prominente leden de groep en werden zij vervangen door nieuwe individuen.
De groep maakte gebruik van 2 facilitators, beiden moeders van kernleden. Eén van hen waste geld wit door luxe voertuigen aan te schaffen, die ze gezien haar financiële positie niet kon financieren. De ander trad op als gevolmachtigde van een bedrijf dat werd ingezet voor witwaspraktijken.
Wat betreft hun ontstaan en groei waren de onderlinge relaties binnen de groep divers: familiebanden, vriendschappen, een gedeelde woonomgeving en een gezamenlijke schoolachtergrond; 4 leden waren familie van elkaar (2 moeders en hun zonen), één lid was een jeugdvriend en 13 van de 14 leden die in dezelfde stad woonden, kwamen uit dezelfde buurten. Tot slot hadden 8 leden gezamenlijk onderwijs gevolgd. Dit alles

wijst erop dat de groep sterk lokaal verankerd was. Tot slot maakte de groep gebruik van tientallen geldezels die werden gerekruteerd onder valse voorwendselen, tegen betaling of onder dwang.

5.2.2.2 *Hybride groep C2*

Groep C2 bestond uit 3 leden en was primair betrokken bij bankhelpdeskfraude, het dealen van drugs en geweldsdelicten. Zo was deze groep vermoedelijk betrokken bij een ripdeal waarbij het slachtoffer werd neergeschoten. Het gestolen geld was afkomstig van bankhelpdeskfraude. Daarbij lijkt sprake te zijn van een duidelijke verwevenheid tussen cybercrime en traditionele criminaliteit. Meerdere leden waren actief in beide domeinen. De ripdeal en het schietincident stonden in directe relatie tot de opbrengsten uit bankhelpdeskfraude. Bovendien werd het uit cybercrime verkregen wederrechtelijk voordeel geïnvesteerd in drugs en vuurwapens, wat mogelijk heeft geleid tot verdere betrokkenheid van de groepsleden bij wapenhandel.
De groep lijkt zich ontwikkeld te hebben van een traditionele criminele groep naar een hybride groep. Verder was er binnen de groep sprake van een hiërarchie, waarbij kernleden een leidinggevende functie hadden en onder andere katvangers aanstuurden. Daarnaast was deze kleinere bankhelpdeskfraudegroep onderdeel van een grotere groep die betrokken was bij drugshandel. De mate van dynamiek van de groep was onduidelijk. Als we kijken naar het ontstaan en de groei, kenden 2 leden elkaar via school en woonden zij bij elkaar in de buurt, maar of er sprake was van rekrutering of snowballing was onbekend.

5.2.2.3 *Hybride groep C3*

Groep C3 bestond uit ten minste 4 leden en was betrokken bij bankhelpdeskfraude, waarbij de modus operandi overeenkwam met de eerder beschreven werkwijzen: slachtoffers werden telefonisch benaderd en misleid om toegang tot hun bankgegevens te verschaffen. Daarnaast was één lid betrokken bij de heling van een elektrische fiets. Een ander bezat ongeveer 100 kilo lachgas.
Groep C3 was zeer actief en heeft vermoedelijk tientallen slachtoffers gemaakt, met naar schatting meer dan € 300.000 schade. Slechts een deel hiervan kwam terecht bij de groepsleden en er waren aanwijzingen voor hogere, niet-geïdentificeerde leden binnen de groep. Het wederrechtelijk verkregen voordeel werd besteed aan luxegoederen, waaronder merkkleding en auto's.
De groep lijkt zich ontwikkeld te hebben van een traditionele criminele groep naar een hybride groep. Een van de groepsleden was eerder actief in een criminele jeugdgroep en heeft zich later toegespitst op cybercrime.
Binnen de groep was sprake van een duidelijke rolverdeling. Eén verdachte fungeerde als kernlid, had een leidinggevende rol en ontving vermoedelijk het grootste deel van de opbrengsten. Een tweede lid was verantwoordelijk voor het regelen van adressen waar pakketjes naartoe gestuurd konden worden die werden betaald met het wederrechtelijk verkregen voordeel. Lid drie benaderde slachtoffers telefonisch. Het vierde lid fungeerde als katvanger en nam meerdere pakketjes in ontvangst.

Er lijkt ook sprake van enige mate van hiërarchie, waarbij het kernlid de overige leden aanstuurde. Het kernlid werkte ook samen met kernleden uit andere groepen, wat enige dynamiek binnen de groep doet vermoeden. Het is onduidelijk of er facilitators betrokken waren bij de groep, al was het kernlid wel actief binnen Telegramgroepen waarin werd gehandeld in merkkleding, creditcards, pinpassen en phishingpanels. Vermoedelijk heeft het kernlid via deze groepen meerdere benodigdheden voor het plegen van bankhelpdeskfraude verkregen, waaronder leads.
Wat betreft het ontstaan en de groei van de groep waren de pakketjesregelaar en katvanger buren en kenden zij elkaar persoonlijk. Ook tussen het kernlid en de pakketjesregelaar bestond een nauwe band, al is niet duidelijk hoe ze elkaar ontmoet hebben.

5.2.2.4 *Hybride groep C5*

Groep C5 bestond uit ten minste 4 leden, maar er waren vermoedens dat de groep bestond uit een grotere groep. De groep was betrokken bij bankhelpdeskfraude, vriend-in-nood-fraude, diefstal, drugshandel en geweld. Voor de bankhelpdeskfraude werd dezelfde werkwijze gebruikt als eerder beschreven. Wat hierbij wel opvallend was, was dat bij het ophalen van bankpassen ook andere waardevolle goederen werden meegenomen, waaronder sieraden, een antieke klok, telefoons en laptops.

> *'Een mannelijke stem vraagt aan de vrouw of zij nog contanten of sieraden thuis heeft liggen. De man geeft aan dat dit naar een depot moet en dat één van de collega's dit voor de verwerking bij haar zou kunnen komen ophalen.' (ECLI:NL:RBNNE:2024:51, 2024, p. 19)*

Een van de groepsleden was eveneens betrokken bij geweldsdelicten, waarbij hij explosieven (samengesteld uit zwaar vuurwerk en benzine) naar woningen van concurrenten binnen het cybercriminele milieu gooide. Dit illustreert de duidelijke verwevenheid tussen online en traditionele criminaliteit.
De groep was zeer actief en heeft meer dan 50 slachtoffers gemaakt. Het totale wederrechtelijk verkregen voordeel wordt geschat op € 800.000. Niet alle opbrengsten kwamen terecht bij de geïdentificeerde verdachten, wat doet vermoeden dat hogere, niet-geïdentificeerde leden ook betrokken waren bij deze groep. Een deel van het wederrechtelijk verkregen voordeel werd geïnvesteerd in cryptovaluta.

> *'Verbalisant vond vijf wallets dan wel Bitcoin-adressen die aan de gebruiker van de telefoon toebehoorden. Vier wallets konden worden gekoppeld aan de applicaties op de telefoon. Verdachte had aldus de beschikking over een OKX (voormalig Okex) wallet, Bitvavo wallet, Bitcoin wallet en een Blockchain.info wallet. Op deze wallets is te zien dat er voor meer dan tienduizend euro aan Bitcoin wordt ontvangen.' (ECLI:NL:RBNNE:2024:52, 2024, p. 6).*

Binnen de groep was sprake van een duidelijke rolverdeling. Eén verdachte belde met slachtoffers, terwijl een tweede verdachte bezig was om op afstand in te loggen op

bankrekeningen en een derde lid de bankpassen ophaalde. Daarnaast werd er met de bankpassen van geldezels contant geld gepind. Er was dus een duidelijke structuur te zien:

> *'Deze werkwijze impliceert een zekere mate van organisatie, structuur en taakverdeling. Verschillende verdachten verrichten verschillende handelingen, die elkaar opvolgen of simultaan plaatsvinden en die moeten zijn afgestemd om het gemeenschappelijke doel te bereiken. Het is aannemelijk dat, terwijl de ene verdachte met de aangever belde en [diegene] aan de praat hield, een ander tegelijkertijd bezig was om op afstand de internetbankierenomgeving te manipuleren.' (ECLI:NL:RBNNE:2024:52, 2024, p. 9).*

Ook was er sprake van enige mate van dynamiek binnen de groep. Ten minste één lid van C5 pleegde samen met leden van andere groepen cybercrime. Verder waren er facilitators betrokken bij de groep. Via Telegram ontving een van de groepsleden leads en werd er gebruikgemaakt van software om telefoonnummers te kunnen spoofen en van een belscript.
Wat betreft het ontstaan en de groei kenden twee verdachten elkaar van de straat. Communicatie tussen de groepsleden vond vooral plaats via Snapchat, WhatsApp en Telegram:

> *'Daarnaast was er een Telegram-chat aanwezig. De gebruiker geeft aan dat hij een grote beller is in Nederland. Hij geeft aan dat zijn F-naam in Nederland [naam] is. Hij zegt vervolgens: 'Oke i am eritrean ER boy in Netherlands'.' (ECLI:NL:RBNNE:2024:51, 2024, p. 18)*

5.2.2.5 *Cybercrimineel groep C4*

Groep C4 bestond uit ten minste 5 leden en lijkt specifiek te zijn ontstaan met het doel om online criminaliteit te plegen. De groep was betrokken bij sim-swaps,[20] bankhelpdeskfraude, phishing, smishing, de verkoop van gestolen gegevens op Telegram, online identiteitsfraude en witwassen. Bij de sim-swaps werden telefoongegevens van slachtoffers bemachtigd via een corrupte telecommedewerker. Hierdoor konden de daders tweefactorauthenticatieverzoeken goedkeuren, waarna ze konden inloggen op cryptovaluta-accounts van de slachtoffers. Ook was een van de leden in het bezit van een vuurwapen. Hoewel er geen sprake lijkt te zijn van directe verwevenheid tussen online en traditionele criminaliteit, werd vermoed dat het bezit van het vuurwapen mogelijk verband hield met de cybercriminele activiteiten van het lid.
De groep was zeer actief en heeft tienduizenden euro's buitgemaakt. Bijna alle opbrengsten werden geïnvesteerd in cryptovaluta: 'De hierbij weggenomen geldbedragen wer-

20 Bij sim-swapping hebben kwaadwillenden een eigen simkaart en zorgen zij ervoor, bijvoorbeeld door een telecomprovider te overtuigen, dat een bepaald telefoonnummer – in dit geval van een slachtoffer – wordt overgezet op deze nieuwe simkaart. Zo krijgen daders toegang tot telefoonnummers van slachtoffers (Europol, 2020).

den in meerdere gevallen gebruikt om verschillende cryptovaluta aan te schaffen.' (ECLI:NL:RBNNE:2022:5360, 2022, p. 15).

Binnen de groep was sprake van een duidelijke rolverdeling en hiërarchie. Eén kernlid stuurde de overige groepsleden aan. Een tweede lid was betrokken bij het opzetten van ten minste één Bitcoinaccount. Verdachte drie (de vriendin van het kernlid) gaf instructies aan zijn broertje om een cryptowallet te openen en hier wederrechtelijk verkregen voordeel op over te maken. Tot slot fungeerden verdachten vier en vijf (het broertje en het zusje van het kernlid) als katvangers.

> *'De cryptovaluta die verdachte ten tijde van zijn aanhouding nog in zijn wallet had, heeft hij, terwijl hij zich in beperking in een justitiële jeugdinrichting (hierna: JJI) bevond, met zijn vriendin en broertje naar een andere wallet overgeboekt om deze buiten het bereik van politie en justitie te houden.' (ECLI:NL:RBNNE:2022:5360, 2022, p. 15).*

De mate van dynamiek binnen de groep is onbekend.
Het kernlid heeft meerdere benodigdheden voor het plegen van cybercrime (zoals gestolen accounts, software om grote hoeveelheden sms-berichten te versturen, smsscripts en phishingpanels) verkregen via twee facilitators, die hij beiden contacteerde op Telegram.
Wat betreft het ontstaan en de groei van de groep lijkt het erop dat vrienden van de vriendin van het kernlid hem hebben geïntroduceerd in cybercrime. Ook zijn vriendin, broertje en zusje raakten betrokken bij de groep.

5.3 De aard van de delicten waar cybercriminele jeugdgroepen die bij lokale veiligheidscoalities onbekend zijn zich mee bezighouden

In paragraaf 5.2 zijn de groepen besproken die terug te vinden waren in de politieregistraties en de zaakreconstructies. Naast deze concrete groepen werden tijdens de expertinterviews ook meer algemene kenmerken besproken van de cybercriminele jeugdgroepen die bij lokale veiligheidscoalities onbekend waren. In deze paragraaf en de paragrafen daarna voegen we alle geïdentificeerde kenmerken samen: die uit de politieregistraties en de zaakreconstructies én die uit de expertinterviews.
Deze paragraaf behandelt de aard van de delicten waarmee cybercriminele jeugdgroepen zich bezighouden, de werkwijze bij het plegen van deze delicten en de verwevenheid tussen traditionele criminaliteit en cybercrime. Daarbij maken we weer onderscheid tussen hybride criminele jeugdgroepen en cybercriminele jeugdgroepen.
Ook hier is het belangrijk om te benadrukken dat veel respondenten slechts beperkt zicht hadden op de aard van de delicten, structuur, samenstelling, en werkwijze van cybercriminele jeugdgroepen en hun leden. De bevindingen die wij hier presenteren zijn daarom voornamelijk gebaseerd op individuele (beperkte) observaties en ervaringen uit de praktijk. Daarbij is het mogelijk dat respondenten eveneens invullingen,

interpretaties, of aannames hebben gedaan die niet volledig overeenkomen met de feitelijke situatie. Het beeld dat wij schetsen is daarmee niet noodzakelijk volledig of sluitend, maar weerspiegelt de kennis die door respondenten kon worden aangedragen. Bij de interpretatie van de resultaten dient hiermee rekening te worden gehouden.

Tabel 7. Kenmerken van de groepen die werden geïdentificeerd in de zaakreconstructies

Zaak ID	Mate van zicht op groep	Structuur en samenstelling					Ontstaan en groei			Delicten		
		Aantal leden	Rollen	Hiërarchie	Dynamiek	Facilitators	Hoe betrokken	Ontmoetingsplaatsen	Banden tussen leden	Traditioneel	Cyber	Verwevenheid
C1	Goed	21	1. Kernlid 2. Facilitator 3. Geldezel/ katvanger	Duidelijke hiërarchie	Duidelijke dynamiek	Gebruik van gemaakt. Diensten: - witwassen	Onbekend	Onduidelijk	1. Vrienden 2. Familie 3. Wijk School	1. Handel in verdovende middelen 2. Geweldsdelicten 3. Wapenbezit Witwassen Economische delicten	1. Verkoopfraude via Marktplaats 2. Phishing 3. Bankhelpdeskfraude	Ja
C2	Beperkt	3+	1. Kernlid 2. Katvanger	Duidelijke hiërarchie	Onduidelijk	Onduidelijk	Onduidelijk	Onduidelijk	1. School 2. Wijk	1. Drugs Geweldsdelicten	Bankhelpdeskfraude	Ja
C3	Beperkt	4+	1. Kernlid 2. Facilitators 3. Katvanger	Duidelijke hiërarchie	Onduidelijk	Onduidelijk	Rekrutering	Onduidelijk	Wijk	1. Heling 2. Drugsdelicten	Bankhelpdeskfraude	Onduidelijk
C4	Beperkt	5+	1. Kernlid 2. Facilitators 3. Katvangers	Duidelijke hiërarchie	Onduidelijk	Gebruik van gemaakt. Diensten: - leveren van gestolen accounts, spamsoftware, smsscripts en phishingpanels	Rekrutering	Online	1. Familie 2. Romantische relatie 3. Vrienden		1. Sim-swaps 2. Bankhelpdeskfraude 3. Phishing, smishing 4. Verkoop van gestolen gegevens op Telegram 5. Online identiteitsfraude 6. Witwassen	

Zaak ID	Mate van zicht op groep	Structuur en samenstelling				Ontstaan en groei			Delicten		
		Aantal leden	Rollen	Hierarchie	Dynamiek	Facilitators	Hoe betrokken	Ontmoetingsplaatsen	Banden tussen leden	Traditioneel	Cyber	Verwevenheid
C5	Beperkt	4+	1. Beller 2. Inlogger 3. Bankpassen ophalen 4. Pinners	Duidelijke hiërarchie	Duidelijke dynamiek	Telegram: leads, belscript, spamsoftware	Onduidelijk	Online	Wijk	1. Diefstal 2. Drugshandel 3. Geweld	Bankhelpdesk-fraude- Vriend-in-nood-fraude	Ja

5.3.1 *Hybride criminele jeugdgroepen*

Hybride criminele jeugdgroepen werden besproken tijdens acht expertinterviews (R2, R4, R7, R8, R12, R15, R19, R22, C1, C2, C3, C5, N3, N24). Volgens experts komen dergelijke groepen veelvuldig voor. In de politieregistraties en zaakreconstructies werden deze hybride groepen ook geïdentificeerd (6 van de 11). Deze groepen lijken doorgaans te ontstaan met het primaire doel om geld te verdienen. In eerste instantie doen ze dit door traditionele criminaliteit te plegen. Op een later moment breiden ze hun criminele activiteiten echter uit naar cybercrime:

> *'Wat ons ook opvalt en die dan dus het wapengeweld ook niet schuwen, is dat zij ook altijd al wel bekend zijn binnen de traditionele criminaliteit. Dus die komen vanuit de drugswereld, die komen vanuit de wereld van inbraken, woningovervallen. Die hebben, voor zover wij daar zicht op hebben, nu gewoon een veel lucratievere manier gevonden om geld te verdienen. (…). phishingcampagne zetten ze op, bankhelpdeskfraude doen ze ook, ja meer [van] die vormen.' (R8)*

Ook kunnen leden van dergelijke groepen in het verleden in beeld zijn geweest door het plegen van traditionele criminaliteit en zijn ze nu ook betrokken bij cybercrime (R12, R15, C1, C2, C3, C5): 'Dat was echt een oud[e], klassiek[e] crimineel, [een] jeugdcrimineel (…) totdat wij hem konden linken aan (…) bankhelpdeskfraude. Hij had allemaal money mules [geldezels] geregeld' (R15)

Een andere respondent over hoe het strafblad van dergelijke cybercrime-verdachten eruitzag:

> *'Noem maar op: afpersing, drugsdelict[en], vermogensdelicten, geweld, heel veel geweld, dat soort dingen. En dan zie [je] (…) sommige mensen die (…) dertig antecedenten [hebben]. En dan zie je [dat] de laatste drie [antecedenten] cyberoplichting [zijn].' (R12)*

5.3.1.1 *Traditionele criminaliteit*

Hybride criminele jeugdgroepen zijn dus betrokken bij zowel traditionele criminaliteit als cybercrime. Overkoepelend over de expertinterviews, de zaakreconstructies en de inhoudelijke analyse van de politieregistraties lijken deze jeugdgroepen betrokken te zijn bij gewelds-, vermogens- en drugsdelicten en bij vernieling en misdrijven tegen de openbare orde. Het merendeel van deze delicten lijkt financieel gemotiveerd te zijn.
Geweldsdelicten omvatten onder andere mishandelingen, bedreigingen, openlijke geweldpleging, intimidatie, afpersing, roof- en woningovervallen en wapengeweld (het voorhanden hebben van vuurwapens, zwaar vuurwerk en schietincidenten) (R2, R4, R7, R8, R12, R15, R22, C1, C2, C5). De relatie met geweld lijkt bij deze groepen groter te zijn dan bij de groepen die zich uitsluitend bezighouden met cybercrime. Daarnaast

lijken groepsleden zich in enkele gevallen ook bezig te houden met loverboypraktijken en zedendelicten (R12).
Verder kunnen hybride criminele jeugdgroepen betrokken zijn bij vermogensdelicten (R7, R8, C2, C3, C5), zoals inbraken en diefstallen, en spelen ze een rol binnen de drugshandel (R4, R8, R12, R22, C1, C2, C4, C5). Daarnaast plegen ze vernielingen en misdrijven tegen de openbare orde (R4, R7, R12, C1), waaronder mensenhandel, andere vormen van ondermijnende criminaliteit en het rekruteren van geldezels.

5.3.1.2 *Cybercrime*

Hybride criminele jeugdgroepen zijn eveneens betrokken bij cybercrime. Daarbij kunnen ze zich ten eerste toeleggen op delicten waarbij cyber-elementen een rol spelen (R7, R12, R19, R22), zoals het verkopen van drugs via Telegram en heling via online platforms. Ten tweede kunnen deze groepen actief zijn binnen de gedigitaliseerde criminaliteit (R2, R4, R8, R12, R15, R22). Hoewel dit gepaard kan gaan met cybercrime in enge zin, zoals hacken, zijn er niet of nauwelijks jeugdgroepen bekend die zich hier specifiek op toeleggen.[21]
Qua gedigitaliseerde criminaliteit lijken jeugdgroepen vooral betrokken te zijn bij meerdere vormen van online fraude, zoals bankhelpdeskfraude, verkoopfraude, phishing, vriend-in-nood-fraude en het witwassen van wederrechtelijk verkregen voordeel. Bij al deze vormen speelt *social engineering* een cruciale rol. In de focusgroep (R21) werd daarover het volgende opgemerkt: 'Social engineering, dat is en blijft (…) de gemeenschappelijke deler [van online fraude]. Dus hierna is het ook wel weer iets wat daar denk ik op gaat lijken' (R21). Verder werd tijdens de focusgroep benadrukt dat ICT juist een steeds kleinere rol lijkt te spelen bij de uitvoering van online fraude. Met andere woorden: waar ICT steeds beter en sterker wordt, blijft social engineering een tijdloze techniek die altijd van belang zal blijven bij de modus operandi van online fraude.
De afname van het gebruik van ICT in de modus operandi van online fraude (R21) is terug te zien in de frequentie van verschillende cybercrimes. Zo lijkt phishing, waarbij ICT een essentieel onderdeel is van de modus operandi, de afgelopen jaren te zijn afgenomen. 'We zien al een paar maanden helemaal geen phishing meer' (R9). In de focusgroep (R21) werd aangegeven dat deze afname vooral betrekking heeft op de klassieke vormen van phishing, waarbij phishingmails worden verstuurd uit naam van een bank. Phishing uit naam van bijvoorbeeld postbezorgdiensten of via Marktplaats wordt echter nog wel gepleegd: 'Wat je nog wel ziet, is phishing via Marktplaats. Maar dan gaat [het] vaak toch [om] kleinere bedragen en dat ze dan beltegoed aankopen of bij Bol.com iets bestellen' (R21).

21 Juridisch gezien wordt bij bijvoorbeeld phishing ook computervredebreuk gepleegd (artikel 138ab Sr., dus hacking). Bij phishing gaat het hier echter om het inloggen op een bankrekening met inloggegevens die veelal verkregen zijn via een phishingwebsite. Omdat het hierbij gaat om een 'simpele' vorm van hacking, terwijl het hoofddelict oplichting is, hebben we ervoor gekozen om dit onder gedigitaliseerde criminaliteit te laten vallen, in plaats van cybercrime in enge zin.

Hoewel phishing de afgelopen jaren is afgenomen, werd tijdens de interviews (R5, R8, R9, R21) gemeld dat bankhelpdeskfraude momenteel juist veel vaker voorkomt. De politieregistraties en zaakreconstructies ondersteunen dit beeld. Cyberdaders lijken hierbij zeer professioneel en geloofwaardig te werk te gaan: 'En ook wel de professionaliteit van die bellers. Die hebben vaak goede belscripts. Die weten precies welk antwoord ze moeten geven wanneer een slachtoffer twijfelt' (R21).

> *'En een geloofwaardig verhaal hebben [ze] ook. Dus dat (…) de klant eerst een mailtje krijgt van de KvK. Daarop reageren en daarna meteen worden gebeld door de bank. Tijdens het gesprek krijg je nog een bevestigingsmailtje van wat er besproken is. En zo lijkt het heel erg op een scenario zoals een bank zelf zou kunnen doen. De klant wordt gebeld om uit voorzorg te vragen wat er aan de hand is, of hij niet het slachtoffer van fraude [is]. En daarnaast sturen ze ook natuurlijk communicatie om in de toekomst het te voorkomen.' (R21)*

Uit de focusgroep bleek ook dat cyberdaders hun criminele activiteiten gedeeltelijk lijken te verplaatsen naar het buitenland: 'Dat zie je ook wel dat [er] (…) echt overlap is in die MO en ik krijg wel de indruk dat phishing dus meer op België gericht is. Vriend-in-nood Duitsland, bankhelpdeskfraude Nederland' (R21) en 'Ook wel bankhelpdeskfraude in Duitsland. Dat ze Duits gaan proberen te praten' (R21).

5.3.2 *Cybercriminele jeugdgroepen*

Tot slot kunnen jeugdgroepen zich uitsluitend bezighouden met cybercrime (R4, R5, R6, R8, R9, R10, R11, R15, R19, R21, R22, C4, N8, N12, N18, N21). Cybercriminele jeugdgroepen kunnen zijn ontstaan met het doel om traditionele criminaliteit te plegen, maar hebben op een gegeven moment de overstap gemaakt naar cybercrime: 'Die [dader] zat echt in de klassieke criminaliteit, maar was overgestapt [naar cybercrime]' (R15). Daarnaast lijken er groepen te bestaan die vanaf hun formatie uitsluitend cybercrime plegen en (voor zover bekend) niet betrokken zijn (geweest) bij traditionele vormen van criminaliteit.
Ook deze groepen hebben zich toegespitst op het plegen van online fraude, voornamelijk bankhelpdeskfraude, maar ook phishing, vriend-in-nood-fraude, online identiteitsfraude en verkoopfraude. In sommige gevallen worden ook *account take-overs* gepleegd. Hierbij worden phishingberichten gebruikt om persoonsgegevens van slachtoffers te bemachtigen, waarna ingelogd wordt op het telecomaccount van het slachtoffer. Vanuit deze accounts worden vervolgens abonnementen verlengd, sim-only-abonnementen afgesloten en telefoontoestellen besteld. Ook kunnen VoIP-nummers (Voice over Internet Protocol) worden aangevraagd, die vervolgens worden doorgeschakeld naar 06-nummers en worden gebruikt voor het plegen van bankhelpdeskfraude. Het overnemen van een telecomaccount kan daarmee gezien worden als de eerste stap in het plegen van andere vormen van cybercrime. Daarnaast

houden deze groepen zich bezig met het witwassen van hun wederrechtelijk verkregen voordeel.
Nederlandse cybercriminele jeugdgroepen lijken zich nauwelijks bezig te houden met cybercrime in enge zin: 'En als je kijkt naar ransomware of naar malware, (…) daar is Rusland, de Oost-Europese landen, die komen daar het meest voor in aanmerking' (R6). Hierbij is wel enige nuancering vereist. Veel online fraudedelicten bevatten juridisch gezien vormen van cybercrime in enge zin. Zo is het inloggen op de bankrekening van een slachtoffer met gestolen gegevens juridisch gezien inloggen met een valse sleutel en dus computervredebreuk (artikel 138ab Sr.). Computervredebreuk is een vorm van hacking. Hacken is echter een basisdelict om andere vormen van gedigitaliseerde criminaliteit te plegen, in dit geval online fraude. In dit rapport beschouwen we online fraude als het hoofddelict. Bovendien zijn de vormen van 'hacken' die gebruikt worden in de modus operandi van online fraude niet technisch van aard. Het gaat namelijk gewoon om inloggen met gestolen gegevens of het gebruik van Anydesk, in tegenstelling tot het technisch hacken door bijvoorbeeld gebruik te maken van geavanceerde technieken om in te breken in een bankrekening. Om deze redenen beschouwen we hacken als onderdeel van de modus operandi van online fraude dus als gedigitaliseerde criminaliteit.

5.3.3 *De verwevenheid tussen traditionele criminaliteit en cybercrime*

Uit de politieregistraties, de zaakreconstructies en de expertinterviews is het beeld ontstaan dat cybercrime en traditionele criminaliteit steeds vaker met elkaar verweven zijn. Er kan sprake zijn van verwevenheid waarbij cybercrime en traditionele criminaliteit samen worden gepleegd, maar er geen directe relatie is tussen beide: een groep kan zich bijvoorbeeld bezighouden met bankhelpdeskfraude en met het verkopen van drugs (zoals in C2 het geval was). Er zijn echter ook gevallen naar voren gekomen waarbij er een sterkere, meer directe verbinding lijkt te zijn tussen traditionele criminaliteit en cybercrime, waar cybercrime veelal voorafgaat aan de traditionele delicten. Zonder cyber zou het traditionele delict niet gepleegd zijn, zoals drugshandel gefinancierd met via cybercrime verkregen geld.
Deze meer directe verwevenheid is zichtbaar op drie gebieden: (1) het investeren van via cybercrime verkregen wederrechtelijk voordeel in traditionele criminaliteit; (2) geweld dat gepaard gaat met cybercrime; en (3) witwassen en ondermijnende criminaliteit.

5.3.3.1 *Het investeren van wederrechtelijk verkregen voordeel in traditionele criminaliteit*

Allereerst kan het wederrechtelijk verkregen voordeel (vooral in de vorm van geld) worden geïnvesteerd in traditionele criminaliteit (R5, R8, R12, R21, R22, C1, C2), voornamelijk drugshandel:

'Voor de traditionele groepen die nu ook cybercrime plegen geldt dat cybercriminele verdiensten vaak de basis vormen voor iets groters, zoals drugshandel. Als ze met online criminaliteit snel een ton kunnen verdienen, kunnen ze dat investeren in blokken coke. Dat zou zonder de cybercriminele verdiensten niet zo snel kunnen. Het biedt dus groeipotentieel en status.' (R5)

Ook wapens worden aangeschaft met cybercrimineel geld: '[cyberdaders] gebruiken het [met cybercrime verkregen geld] voor drugs, vuurwapens' (C2). Volgens R12 leidt de toestroom van cybergeld in de drugswereld tot nieuwe spanningen:

'Heel veel geld wordt weer geïnvesteerd in drugshandel. Dus waar nog veel meer snel geld verdiend kan worden. Dus ook in die [drugs]wereld, waardoor er opeens ook andere spelers komen die ook veel geld hebben, (…) krijg je ook weer gedoe mee.' (R12)

5.3.3.2 *Geweld dat gepaard gaat met cybercrime*

Ten tweede lijkt cybercrime regelmatig gepaard te gaan met geweldsincidenten (R4, R5, R7, R12, R15, R21, R22, C1, C2, C5). R4 beschreef de verwevenheid als volgt: 'Wij hebben hier schietincidenten waar op elkaar echt geschoten is, gericht, steekincidenten. En daar ligt deze vorm van fraude [online fraude] aan ten grondslag'. Soms lijken deze schiet- en steekincidenten direct samen te hangen met ripdeals. In C2 werd een jongere bijvoorbeeld beroofd van geld dat afkomstig was van bankhelpdeskfraude, met ernstige gevolgen:

'Wat er toen eigenlijk gebeurd is en dat maakt de boel wel heel verrassend, is dat er een situatie plaatsvindt in een ander incident, waarin een jongen beroofd wordt van bankfraudegeld. En daar is een schot door het hoofd heen gegaan.' (C2)

Daarnaast komt bedrog tussen mededaders voor, wat kan leiden tot geweld wanneer een van hen verhaal probeert te halen:

'Het [kan] best zijn dat ik gisteren met jou een mooie deal heb gemaakt doordat we iemand hebben opgelicht via bankhelpdeskfraude, maar morgen kan ik je ook in je rug steken, omdat ik het geld van je nodig heb.' (R4)

Daders – al dan niet betrokken bij cybercrime – zetten bovendien geweld en bedreiging in om personen onder druk te zetten of af te persen:

'Ze zijn [het] gewend om mensen af te persen. Dus als je niet mee wil, of je wil je bankpasje niet afgeven of [ze] staan bij school en zien [er] wat zwakke broeders en zussen tussen staan. Dat wordt gewoon met dwang gedaan. En je ziet ook met sommige oplichtingszaken dat ze gewoon eerst [de] social media van iemand uitpluizen die ze gaan oplichten. Ja, doen ze misschien ook met een geldezel, zeg maar. 'We weten

gewoon waar je woont', 'We weten wat je vader of moeder doet', of 'We doen je zusje wat aan, die zit hier ook op school'.' (R12)

Cybercrime lijkt deze (ernstige) vormen van geweld aan te trekken vanwege de grote financiële belangen (R21).

5.3.3.3 *Witwassen en ondermijnende criminaliteit*

Tot slot zijn zowel hybride groepen als cybercriminele groepen betrokken bij het witwassen van hun wederrechtelijk verkregen voordeel (R4, R9, R12, C2, C4), waarbij er sprake lijkt te zijn van een verwevenheid tussen de boven- en onderwereld (R4, R9, R8). Witwassen is een belangrijk onderdeel van de financiële modus operandi bij cybercrime. In de interviews en zaakreconstructies werden vier methoden van witwassen genoemd: (1) geldezels; (2) cadeaukaarten en goederen; (3) cryptovaluta; en (4) ondernemingen (zoals winkels).

Ten eerste worden geldezels en geldezelrekeningen ingezet bij bepaalde delicten. Zo kunnen jongeren worden gerekruteerd als geldezel, waarbij hun bankrekening wordt gebruikt om wederrechtelijk verkregen voordeel weg te sluizen (R4, R12, R15, R21). Daarnaast lijken cyberdaders steeds vaker bankrekeningen te openen met behulp van (online) identiteitsfraude. Slachtoffers weten vaak niet dat er een bankrekening op hun naam is geopend (R21). Ook worden slachtoffers soms overgehaald om zelf een bankrekening te openen, die vervolgens als geldezelrekening wordt gebruikt. Dit lijkt vaak te gebeuren bij oudere slachtoffers (R21). Geld dat op deze geldezelrekeningen wordt gestort, kan contant worden opgenomen of besteed aan goederen: 'Dus gewoon dat de money mule [geldezel] met het verkregen geld naar de MediaMarkt gaat, Bijenkorf, Coolblue, dat soort winkels' (R9).

De afgelopen jaren lijkt er een verschuiving te hebben plaatsgevonden in het gebruik van geldezels: klassieke Nederlandse geldezels worden minder vaak ingezet (R21), mogelijk omdat Nederlandse banken relatief snel verdachte rekeningen detecteren en blokkeren:

'Ze [cyberdaders] hebben te weinig bankrekeningen voor het geld dat ze [hebben]. Want ja, [een] bankrekening wordt snel geblokkeerd. Dus een money mule [geldezel] kun je maar één of twee keer gebruiken, dan heeft de bank het door en dan komt zo iemand op een fraudelijst. Dus dan zie je dat ze andere middelen gaan gebruiken [om geld wit te wassen].' (R6)

Om die reden worden mogelijk steeds vaker buitenlandse bankrekeningen geopend en gebruikt. Het voordeel hiervan is dat één geldezel bij meerdere online banken eenvoudig een bankrekening kan openen:

'Dus het is niet dat er helemaal geen geldezels zijn. Ze bestaan nog wel. Maar een aantal [met] buitenlandse rekeningen (…). Litouwen, Spanje. Want je kan tegenwoordig via een appje via verschillende partijen een Spaanse rekening openen, terwijl

je in Nederland [bent]. (…) Je kan dus inderdaad nog steeds Nederlandse money mules [geldezels] hebben. Alleen die zijn dan niet als zodanig zichtbaar, omdat ze inderdaad buitenlandse rekening[en] hebben.' (R21)

Een tweede witwasmethode is het omzetten van wederrechtelijk verkregen voordeel naar waardevolle producten (zoals elektronica en sieraden), cadeaukaarten, Paysafe-kaarten en beltegoed (R9, R21). Hierbij kan het voorkomen dat cyberdaders zelf webshopaccounts aanmaken. Vervolgens sturen zij betaallinks naar slachtoffers, met de mededeling dat zij via deze link hun geld kunnen 'veiligstellen'. In werkelijkheid betalen slachtoffers hiermee het product dat door de dader is besteld.
Ten derde wordt cryptovaluta gebruikt als witwasmiddel: 'En steeds meer de toename in de betalingen richting Bitcoins, crypto' (R9) en 'Het gaat gewoon veel sneller om het (…) rechtstreeks, van de bron naar crypto, naar waar dan ook [over te maken]' (R21). Experts (R9, R21) benadrukten dat het opsporen van verdachte cryptowallets en hun eigenaren aanzienlijk ingewikkelder is dan het traceren van geldezelrekeningen bij banken. Waar banken verdachte rekeningen snel blokkeren, willen cryptobedrijven de benodigde informatie niet altijd delen met onder andere de opsporingsdiensten. Bovendien kunnen cryptowallets in gebruik zijn bij de eindgebruiker zelf, waarbij de sleutel om de wallet te kunnen openen ook niet beheerd wordt door cryptobedrijven. Omdat geldezels op deze manier moeilijker geïdentificeerd kunnen worden, blijven ze langer buiten beeld en kunnen ze herhaaldelijk ingezet worden. Daarnaast komt het voor dat slachtoffers worden misleid om zelf cryptowallets te openen en daar geld op te storten. De benodigde gegevens om gebruik te maken van de wallet worden dan gedeeld met de daders.
Tot slot kunnen ondernemingen worden ingezet om wederrechtelijk verkregen voordeel wit te wassen. Hierbij kan er sprake is van een verwevenheid tussen de criminele wereld en legitieme structuren, zoals ondernemingen, die voor criminele doeleindes worden gebruikt. Dit fenomeen staat ook wel bekend als ondermijnende criminaliteit (R4, R8, R9, R10):

'Waar ze vier, vijf jaar geleden nog met hun eigen gezicht op de camera's stonden bij een MediaMarkt (…) [hebben ze] nu een supermarkt (…) om dingen wit te wassen. (…) Dat er een kapper is die ze kunnen gebruiken om hun Bitcoins te gelde te maken.' (R4)

En:

'We zien soms wel van die juweliers. In [een stad] hebben we [er] nu twee gehad, die hebben gewoon een lopend bedrijf, maar (…) via hun betaalautomaten (…) wordt dan heel veel gecasht met frauduleus verkregen pinpassen bijvoorbeeld. (…) Je ziet inderdaad soms ook wel van die vage groente- of fruitwinkeltjes soms voorbijkomen. (…) Vooral de juweliers en de buitenlandse fruitwinkeltjes.' (R9)

5.4 De kenmerken van cybercriminele jeugdgroepen die bij lokale veiligheidscoalities onbekend zijn

In deze paragraaf beschrijven we de kenmerken van criminele jeugdgroepen die betrokken zijn bij cybercrime en (nog) niet in beeld zijn bij lokale veiligheidscoalities. Daarbij gaan we eerst in op de structuur en de samenstelling van de groepen, gevolgd door hun ontstaans- en groeiproces.

5.4.1 *Structuur en samenstelling*

Op basis van de politieregistraties, de zaakreconstructies en de expertinterviews is slechts een beperkt beeld ontstaan van de structuur en de samenstelling van hybride en cybercriminele jeugdgroepen. Dit beperkte zicht had meerdere oorzaken. In de politieregistraties waren vaak alleen de geldezels en katvangers geïdentificeerd, terwijl details over de kernleden ontbraken. Daarnaast bevatten de geanalyseerde politieregistraties doorgaans alleen verhoren en enkele processen-verbaal, waardoor het zicht op de interne structuur van de groepen beperkt bleef. Hier is het belangrijk om op te merken dat de politieregistraties geen informatie uit opsporingsonderzoeken bevatten. In de zaakreconstructies en tijdens de expertinterviews kwamen kernleden wel meer aan bod, maar bleef het zicht op hen eveneens beperkt.
De hybride en cybercriminele jeugdgroepen vertoonden qua structuur en samenstelling aanzienlijke overeenkomsten. Om herhaling te voorkomen, bespreken we beide typen groepen hier gezamenlijk, waarbij eventuele verschillen expliciet worden benoemd.
Op basis van de beschikbare bronnen kunnen de jeugdgroepen globaal worden onderverdeeld in twee typen: (1) dynamische groepen; en (2) meer stabiele groepen (R2, R4, R5, R6, R7, R8, R9, R10, R11, R12, R15, R19, R21, R22, C1, C2, C3, C4, C5, N3, N8, N12, N24). In de focusgroep werd dit onderscheid als volgt verwoord:

> *'Je hebt de één en je hebt de ander. Je hebt clubjes die echt hecht zijn en samenwerken (…) En je hebt de clubjes waar dat meer flexibel [is]. (…) De aansturing is vaak vanuit de bellers of vanuit iemand die dat organiseert.' (R21)*

Cybercriminele jeugdgroepen lijken doorgaans relatief klein van omvang en bestaan veelal uit 3 tot 5 leden (R5, R6, C4). In enkele gevallen opereren jongeren aanvankelijk alleen en ontstaat pas een groep wanneer het wederrechtelijk verkregen voordeel moet worden witgewassen (R6, R22).
Dynamische groepen worden gekenmerkt door een hoge mate van fluïditeit en dynamiek (R4, R12, R22, C3, C5, N3, N8). Zoals R5 opmerkte: 'Waar het vroeger meer vaste 'groepen' betrof, zijn het tegenwoordig vooral fluïde en dynamische groepen met steeds wisselende samenstellingen. De groepen zijn eigenlijk eerder te betitelen als samengestelde clubjes van individuen, geheel in lijn met onze geïndividualiseerde netwerksamenleving.' In de focusgroep werd dit beeld bevestigd: 'Over het algemeen heb

ik niet het idee dat het echt vaste groepen zijn' (R21). Deze fluïditeit werd verder benadrukt door R19. Hij beschreef bijvoorbeeld de vervangbaarheid van leden: 'Wat we zien is dat die wordt aangehouden, dat de volgende weer [staat] te trap[pelen] om te beginnen' (R19).

Dynamische groepen lijken veelal ad hoc te ontstaan wanneer zich een gelegenheid voordoet om cybercrime te plegen. Drie experts (R4, R12, R22) gebruikten expliciet de term 'gelegenheidsgroepen' om deze dynamische samenwerkingsverbanden te beschrijven. Binnen een groter sociaal netwerk van daders worden dan snel kleinere groepen gevormd. Er '(…) wordt gewoon gekeken wie beschikbaar is en wie ze willen hebben (…) en dan gaan ze hun ding doen [cybercrime]' (R12).

Ook kan het voorkomen dat leden van meerdere stabielere groepen tijdelijk samenwerken in dergelijke gelegenheidsgroepen. R22 beschreef bijvoorbeeld een casus waarin verdachte A samenwerkte met B voor het ene slachtoffer en met C voor het andere slachtoffer, terwijl A ook banden had met D uit een andere zaak. Tegelijkertijd bestond er een stabielere groep van E, F en G dat langdurig samenwerkte, maar ook deelnam aan gelegenheidsgroepen.

Dynamische groepen kenmerken zich door het ontbreken van een duidelijke hiërarchie en een relatief korte levensduur. Toch zijn ook hier vaak kernleden, facilitators en geldezels of katvangers te onderscheiden (R8, R12, R15, C3, C5, N3, N8, N21, N24).

Naast dynamische groepen hebben we ook stabielere groepen geïdentificeerd die door experts als 'hechter' werden omschreven (R8, R12, R15, R21, R22, C1, C2). Deze groepen zijn doorgaans kleinschalig met een vaste kerngroep van 3 tot 5 leden en ze vertonen een grotere mate van structuur en hiërarchie. Tegelijkertijd blijven de lagen buiten de kern dynamisch van samenstelling.

Volgens meerdere experts kunnen deze stabielere groepen onderdeel zijn van een grotere, achterliggende groep. Het zicht hierop was echter beperkt (R5, R6), mede doordat politieteams zich vooral richten op de lagere niveaus binnen de groep (zoals de geldezels en pinners), die weinig informatie prijsgeven over hogergeplaatste (kern)leden (R9). Daarnaast beschikken sommige basisteams mogelijk niet over voldoende expertise om hybride en cybercriminele (jeugd)groepen in kaart te brengen (R19).

Zowel dynamische als stabielere groepen hebben doorgaans een zekere mate van hierarchie en bestaan uit kernleden, professionele en/of gerekruteerde facilitators en geldezels of andere katvangers (R5, R8, R12, R15, R19, R21, C1, C2, C3, C4, C5, N3, N8, N12, N21, N24). Ook kennen beide typen groepen veelal een taakverdeling, waarbij leden verschillende specialismes vervullen (R4, R5, R15, R19, R21, C1, C3, C4, C5, N3, N8, N12, N21). Zoals in de focusgroep werd opgemerkt: 'Specialismes die heb je zeker, of in ieder geval een rolverdeling' (R21). De exacte rollen en taken verschillen per type delict. Over het algemeen vervullen kernleden een leidinggevende en coördinerende rol: 'Dus je ziet wel de mensen die bovenaan hangen. (…). Die regelen de leads, die regelen dit dat en dan zetten ze het weer uit. En zelf doen ze eigenlijk niet eens zoveel meer' (R12).

Binnen cybercriminele jeugdgroepen kan de leidinggevende rol ook worden vervuld door degene met de meeste kennis van het cybercriminele pleegproces (R5) of juist met de sterkste persoonlijkheid:

> *'Vaak zie je dat dat gewoon sterke persoonlijkheden [zijn]. (…) degene met de grootste bek, die op straat ook altijd al de grootste bek had, dat die ook (…) degene is die misschien niet echt een groep leidt, maar wel meer (…) de lakens uitdeelt. Dus (...) bepaalt, de verdeling van de buit bijvoorbeeld.' (R6)*

Veel hybride en cybercriminele jeugdgroepen maken gebruik van facilitators (R4, R6, R10, R15, R22, C1, C4, C5, N12). Deze kunnen onderdeel zijn van de groep zelf (gerekruteerde facilitators), maar zij kunnen ook meer op zichzelf opereren en hun diensten aan meerdere groepen aanbieden (professionele facilitators). Voorbeelden zijn malafide autoverhuurders, makers en beheerders van phishingpanels, personen die slachtoffers telefonisch benaderen, medewerkers van callcenters en ronselaars van geldezels.
Tot slot zijn binnen de jeugdgroepen veelal geldezels en/of katvangers actief. Beide vervullen een cruciale rol in het afschermen van de kernleden voor de autoriteiten. Geldezels worden ingezet wanneer bankrekeningen nodig zijn om wederrechtelijk verkregen voordeel op over te maken. Taken die katvangers uitvoeren, zijn onder andere: bankpassen ophalen, pinnen met de bankpas van slachtoffers, goederen kopen met gestolen geld en bestelde pakketjes ontvangen of ophalen.
Zowel dynamische als stabiele jeugdgroepen zijn vooral betrokken bij online fraude. Hybride groepen combineren dit met traditionele delicten, waarbij de groepen in dit onderzoek veelal betrokken waren bij geweldsdelicten, vermogensdelicten en drugsdelicten (R4, R12, R22, C1, C2, C3, C4, C5, N3, N8, N12, N21).
Een verschil tussen hybride en cybercriminele jeugdgroepen is de mate van geweld tussen mededaders. Geweld lijkt binnen dynamische groepen vaker voor te komen dan binnen statielere groepen (R22). R12 beschreef een casus waarin een lid vermoedelijk door een mededader was neergestoken: 'Geweld is denk ik wel [een] middel dat veel gebruikt wordt door deze jongens, naar elkaar toe ook. Want ze doen wel dingen samen, maar ze hebben ook samen weer ruzie' (R12). Volgens R12 speelt geweld vermoedelijk een grotere rol binnen deze groepen dan waar opsporingsdiensten zicht op hebben.
Tot slot bleek uit de politieregistraties, de zaakreconstructies en de interviews dat het wederrechtelijk verkregen voordeel op verschillende manieren kan worden verdeeld (R22, C3, C5, N3, N8). In sommige groepen werd de buit gelijk verdeeld, zoals in een casus beschreven door R22, waarin de vier groepsleden ieder 25% van de opbrengst ontvingen. In andere groepen moesten leden een deel van hun opbrengsten afstaan aan hogergeplaatste leden (C3, C5).

5.4.2 *Ontstaan en groei*

Uit de politieregistraties, de zaakreconstructies en de expertinterviews is het beeld ontstaan dat de betrokken actoren beperkt zicht hebben op de ontstaans- en groeiprocessen van hybride en cybercriminele jeugdgroepen.
Voor zowel de hybride (R2, R4, R7, R8, R12, R15, R19, R22, C1, C2, C3, C5, N3, N24) als de cybercriminele jeugdgroepen (R4, R5, R6, R7, R8, R9, R10, R11, R15, R19, R21, R22, C4, N8, N12, N18, N21) en voor de dynamische en meer stabiele groepen hebben we dezelfde ontstaans- en groeiprocessen geïdentificeerd. Om herhaling te voorkomen bespreken we beide typen groepen daarom gezamenlijk; waar dat relevant is, benoemen we de verschillen expliciet.
Hybride groepen lijken te ontstaan vanuit traditionele criminaliteit en ze breiden hun activiteiten later uit naar cybercrime, vermoedelijk vanwege de hogere opbrengsten en lagere risico's (R4, R8, R12, R15, R22, C1, C2, C3). Deze groepen worden ook wel 'doorgroeigroepen' genoemd. Cybercriminele jeugdgroepen lijken daarentegen exclusief betrokken bij cybercrime en gaan niet op een bepaald moment ook traditionele criminaliteit plegen.
De toetreding tot jeugdgroepen kan op twee manieren verlopen: (1) via actieve rekrutering; of (2) via geleidelijke betrokkenheid. Bij actieve rekrutering zoeken bestaande leden bewust naar nieuwe jongeren om de groep te vormen of uit te breiden. In andere gevallen kunnen personen geleidelijk onderdeel worden van een groep, veelal vanuit informele sociale verbanden, zoals vriendengroepen in de wijk of klasgenoten op school. Deze contacten kunnen zowel offline als online plaatsvinden en via fysieke of virtuele criminele ontmoetingsplaatsen. De wijze van toetreding en het type relatie lijken samen te hangen met de uiteindelijke rol van het individu binnen de groep. Om die reden hebben we hieronder onderscheid gemaakt tussen kernleden, facilitators, en geldezels en katvangers. Dit onderscheid hebben we in paragraaf 4.3.2 niet gemaakt, omdat de beschikbare informatie over de ontstaans- en groeiprocessen van traditionele criminele jeugdgroepen veelal enkel betrekking had op kernleden.

5.4.2.1 *Kernleden*

Kernleden kunnen zowel actief gerekruteerd worden als geleidelijk onderdeel worden van een groep. In beide gevallen spelen offline contacten een belangrijke rol, zoals vriendschaps-, familie- en romantische relaties (R4, R6, R8, R9, R11, R12, R15, R19, R22, C1, C2, C3, C4, C5, N3, N8, N12, N21, N24). Deze offline relaties lijken essentieel vanwege het vertrouwen dat nodig is bij het delen van criminele opbrengsten. Wanneer mededaders een samenwerking aangaan en elkaar al via offline banden kennen, hebben ze doorgaans vertrouwen in elkaar: 'Groepen zijn deels lokaal verankerd en maken nog steeds gebruik van traditionele sociale banden, onder andere om [het] probleem van vertrouwen op te lossen' (R5). Ook in de politieregistraties en de zaakreconstructies kwam deze lokale verankering sterk naar voren, zowel voor de hybride als voor de cybercriminele jeugdgroepen (N3, N8, N21, N24, C1, C2, C3, C4, C5).

Online relaties tussen kernleden lijken nauwelijks voor te komen. Alleen in casus C4 werd een online connectie vastgesteld tussen twee verdachten, die elkaar via Telegram ontmoetten nadat ze al actief waren in cybercrime. Later ontmoetten ze elkaar ook fysiek en ontwikkelden ze een vriendschap.
Naast dergelijke relaties zijn criminele ontmoetingsplekken, zowel fysiek (R12, C2, C3, C5, N12, N21) als virtueel (R4, R5, R9, R15, R19, R22), ook belangrijk voor het vinden en rekruteren van kernleden. Fysieke ontmoetingsplekken zijn bijvoorbeeld wijken en onderwijsinstellingen: 'Die jongens waar wij op zaten, die komen dan ook bij elkaar uit de wijk' (R12). En:

> *'Wat we ook hebben gezien, is dat er bijvoorbeeld een mbo-instelling is waar studenten van die school met elkaar in aanraking komen op zo'n ICT-opleiding. Dat er dan in zo'n klas vier of vijf verdachten ineens oppoppen. Dus kennelijk proberen ze daar ook dingen met elkaar, waardoor daar ook een netwerkje ontstaat.' (R12)*

Virtuele ontmoetingsplekken omvatten vooral sociale media, zoals Telegram, Snapchat en WhatsApp. Bij het zoeken naar mededaders lijkt sprake te zijn van vraag en aanbod:

> *'Maar het is een kwestie van vraag en aanbod online. (…) En zo vinden ze elkaar. En ik zie dat er gebruik wordt gemaakt van social media en dan met name Snapchat. (…) Ja, waar mensen met elkaar in contact komen.' (R4)*

Volgens meerdere experts maken online platforms het eenvoudiger voor jongeren uit verschillende regio's om met elkaar in contact kunnen komen (R5, R6, R9, R15). Daarbij werd Telegram vaak genoemd als belangrijkste plek. Op dit platform zijn veel groepen actief die zich bezighouden met phishing en bankhelpdeskfraude (R4, R15). Deze groepen kunnen worden gebruikt om actief mededaders te rekruteren, maar ook om online relaties aan te gaan.
Het (toenemende) gebruik van online communicatie, zoals via Telegram en Snapchat, lijkt ertoe te leiden dat sommige jeugdgroepen minder lokaal verankerd zijn. Zo benoemden experts (R5, R15) casussen waarin mededaders in verschillende steden in dezelfde provincie woonden of zelfs in verschillende provincies. Dit beeld werd ondersteund door de analyse van de politieregistraties: een deel van de jeugdgroepen had leden die verspreid over Nederland woonden.

5.4.2.2 *Facilitators*

Facilitators lijken vooral actief gerekruteerd te worden, veelal via virtuele offender convergence settings (R4, R10, R15, C2, C3, C4, C5, N12). Op deze platforms adverteren zij hun producten en diensten: 'Via bijvoorbeeld Telegram worden phishingkits en belscripts gekocht' (R4), 'Ik heb ook [gezien] dat hij [de facilitator] zichzelf filmt en dan is hij een soort helpdesk op Telegram voor anderen' (R15).

'Zo hebben we nog wel een aantal anderen, [een] echte facilitator kunnen pakken. (…) Dat was de maker van [naam phishingpanel] (…) Hij was een bouwer, maar ik heb hem niet in een jeugdnetwerk gezien, maar dat was de echte grote facilitator. Hij verkocht dat [phishingkits].' (R15)

Offline banden tussen facilitators en groepsleden lijken weinig voor te komen (R15, C1, C4). In C1 vervulde de moeder van een kernlid een faciliterende rol door als gevolmachtigde van een bedrijf op te treden. In sommige gevallen worden facilitators gerekruteerd uit het sociale netwerk van een groepslid, zoals een ex-vriendin die bij een bank of callcenter werkt. Via deze facilitator kan toegang worden verkregen tot persoonsgegevens van potentiële slachtoffers (leads):

'Ook een telecombedrijf. En [toen] bleek dus [dat] (…) zijn [de cyberdader] ex-vriendinnetje (…) werkte als callcentermedewerker voor het callcenterbedrijf die ook de salesafdeling deed voor een telecombedrijf. En zij heeft [de bestanden] verkocht op [aan]vraag [van hem].' (R15).

5.4.2.3 *Geldezels*

Geldezels worden ook vaak actief gerekruteerd, waarbij offline relaties en fysieke en virtuele ontmoetingsplaatsen een rol spelen (R4, R7, R11, R12, R15, R21, R22, C3, C4, N8, N12, N21). Hoewel zowel de offline als online omgeving belangrijk is, is uit de interviews, zaakreconstructies en politiedata het beeld ontstaan dat de fysieke wereld het vaakst gebruikt wordt. Geldezels kunnen worden benaderd door familieleden, vrienden of collega's. Voorbeelden van fysieke ontmoetingsplaatsen zijn zorginstellingen, scholen ('En soms is het gewoon op het schoolplein' (R11)) en de straat (zoals bij daklozen en drugsverslaafden).

Uiteindelijk zijn daders 'gewoon op zoek naar kwetsbare mensen' (R21), zoals seizoenarbeiders of asielzoekers (R21). Daarbij kunnen ze inspelen op de actualiteit om geldezels te rekruteren (R21). Als voorbeeld werd de oorlog tussen Rusland en Oekraïne genoemd, waarbij Oekraïense vluchtelingen in Nederland snel een Nederlandse bankrekening nodig hadden. Er zijn gevallen bekend waarbij Oekraïense vluchtelingen onder druk werden gezet of zelfs werden gedwongen om een dergelijke bankrekening te openen. Dit gebruik van druk en/of (dreigen met) geweld lijkt ook in andere gevallen voor te komen.

Rekrutering en het zoeken naar geschikte mededaders via virtuele ontmoetingsplaatsen vindt plaats via sociale media zoals Instagram, Snapchat en Telegram (R4, R6, R9, R21). Cyberdaders plaatsen daarop berichten: 'Je ziet ook wel vaak van die advertenties van 'nou wil je snel geld verdienen' en wij zien ook dat ze daarmee adverteren op Snapchat en dan in bepaalde groepen van bepaalde wijken waarin ze [cyberdaders] actief zijn' (R4) en 'We horen dat dan wel soms van verklaringen van money mules [geldezels] dat ze via Snapchat of iets dergelijks iemand hebben leren kennen en dat ze op die manier geronseld worden' (R21).

Hoewel online rekrutering voorkomt, is er vrijwel altijd een offline component aanwezig, vooral vanwege de noodzaak om fysieke bankpassen te verkrijgen:

> *'Als ik even [in] mijn herinnering graaf, zit er altijd wel (…) een offline contact, in ieder geval omheen. Dus ik zie (…) ze niet zo snel echt alleen maar online spullen ter beschikking stellen. (…) wel verklaarbaar [dat er altijd een offline component is] omdat (…) het ook wel (…) vaak gaat over het afgeven van een bankpas.' (R11)*

5.5 De kenmerken van individuele leden

In deze paragraaf beschrijven we de kenmerken, criminele carrières en motivaties van jongeren die betrokken zijn bij cybercrime, gebaseerd op de politieregistraties, de zaakreconstructies en de expertinterviews. We bespreken de leden van hybride en cybercriminele jeugdgroepen gezamenlijk, omdat beide groepen veel overeenkomsten vertonen. Verschillen worden expliciet benoemd.

5.5.1 *Demografische kenmerken*

In deze paragraaf maken we onderscheid tussen kernleden en geldezels/katvangers, omdat hun demografische kenmerken kunnen verschillen. Dit onderscheid hebben we niet gemaakt in paragraaf 4.4.1 bij de bespreking van de traditionele criminele jeugdgroepen, omdat we daar alleen beschikten over de informatie van kernleden.
De leeftijd van leden binnen hybride en cybercriminele jeugdgroepen ligt doorgaans tussen de 12 en 28 jaar (R4, R5, R6, R8, R11, R12, R15, R19, R22, C1-5, N8, N21, N24). Hoe hoger de positie binnen de groep, hoe ouder het lid meestal is (R22). Zo zijn de kernleden vaak meerderjarig en tussen de 20 en 24 jaar. De doorgroeiers (die een actievere rol hebben dan nieuwe leden, maar in mindere mate betrokken zijn bij de uitvoering van cyberdelicten) zijn doorgaans 16 tot 20 jaar oud. Geldezels en katvangers zijn meestal minderjarig, tussen de 15 en 17 jaar (R4, R8, R11, R22, N3, N8, N12):

> *'[Het] zijn vaak jongeren van een jaar of vijftien, zestien, zeventien. Jonger kom je ze eigenlijk niet tegen. Ik denk dat dat ook wel lastig is, omdat (…) als je zestien, zeventien bent, dan hebben je ouders minder zicht op je [bank]rekening dan als je dertien, veertien, vijftien bent. Dus dat zal er ongetwijfeld iets mee te maken hebben.' (R11)*

Volwassen geldezels komen echter ook voor (R15, N3, N8): 'Vroeger was het een beetje veertien [jaar], maar ze [de cyberdaders] willen tegenwoordig alleen maar mensen hebben die hun eigen rekening kunnen open[en], dus achttien plus' (R15).
Wat betreft geslacht lijken kernleden binnen hybride en cybercriminele jeugdgroepen overwegend man (R4, R8, R10, R12, R19, C1-5, N3, N8, N21, N24), al lijkt geslacht wel samen te hangen met de rol binnen de groep: 'We zien weleens wat meisjes die handen spandiensten doen of meeprofiteren. Bij bankhelpdesk[fraude] worden bewust meisjes ingezet [om slachtoffers op te bellen], want die komen betrouwbaar over'

(R15). Geldezels en katvangers zijn zowel man als vrouw, hoewel mannen vaker voorkomen (R4, R8, R11, R12, R21, N3, N8, N12, N21, N24).
De etnische achtergrond van kernleden is zeer divers (R4, R5, R8, R19, R22, C1-5, N3, N8, N21, N24) en lijkt gedeeltelijk samen te hangen met de rol binnen de groep: 'Etnische achtergrond is wisselend en afhankelijk van rol: de beller moet bijvoorbeeld een goede Nederlandse stem hebben' (R5). Geldezels lijken vaker een migratieachtergrond te hebben (R21, N3, N8), hoewel dit vooral in de focusgroep werd benoemd: '[Het] zijn vaak mensen van buitenlandse afkomst. (…). Mensen die de landstaal ook niet machtig zijn, die de Nederlandse cultuur ook niet kennen, die denken dat het heel normaal is [om je bankpas af te geven]' (R21).
Ook het opleidingsniveau van kernleden lijkt sterk te variëren. Enerzijds betreft het niet- of laagopgeleide jongeren (R5, R6, C2, C3, C5): 'Verder zijn het veelal probleemjongeren die niet zijn geschoold en niet goed kunnen functioneren op school en dus ook niet meer mee kunnen doen in de maatschappij' (R5). Anderzijds zijn er ook voorbeelden van (hoog)opgeleide verdachten (R11, C4, N21). In C4 zat de hoofdverdachte ten tijde van het plegen van de strafbare feiten bijvoorbeeld op het vwo. Geldezels lijken over het algemeen (vervolg)onderwijs te volgen (R11, N3, N8, N12).
Bij de SES van kernleden is ook enige mate van variatie te zien, al lijkt het grootste deel een relatief lagere SES te hebben en uit achterstandswijken te komen (R4, R5, R6, R8, R10, R12, R19, N8). Sommigen staan onder bewindvoering (N8). In enkele gevallen echter kwamen verdachten juist uit welgestelde gezinnen, zoals in C4. Voor geldezels is er eveneens geen eenduidig beeld te zien (R11, N3, N8), al kwam uit de politieregistraties (N3, N8) naar voren dat vijf van de geïdentificeerde geldezels een relatief lage SES hadden, gekenmerkt door financiële problemen (schulden), het ontbreken van inkomen of leefgeld, onder bewindvoering staan, een Wajong-uitkering ontvangen of begeleid wonen. Eén persoon had een relatief gemiddelde SES, waarbij hij als zzp'er werkte en geen schulden had.
Daarnaast groeit een deel van de kernleden die actief is binnen hybride jeugdgroepen op in een problematische gezinssituatie (R4, R8, C5, N3, N24): 'Alcohol, huiselijk geweld, het klassieke plaatje kon je er eigenlijk wel op loslaten' (R8). Voor jongeren die enkel bij cybercrime betrokken zijn, kan de thuissituatie sterk uiteenlopen (R5, R11, C4, N8, N21). Sommigen groeien op in stabiele gezinnen, terwijl anderen een instabiele achtergrond lijken te hebben. Tot slot hangt de thuissituatie mogelijk samen met de rol van de dader binnen de groep (R5). Wat betreft geldezels kwam uit de politieregistraties naar voren dat drie geldezels bij hun alleenstaande moeder of vader woonden (N3, N8). Drie andere geldezels woonden ook nog thuis en hadden allen een stabiele thuissituatie (N12). Verder hadden twee leden uit N3 een relatie en woonden ze samen. Een andere geldezel die betrokken was bij N3 woonde samen met zijn vriendin en pasgeboren kind.
De cognitieve vaardigheden van jongeren die betrokken zijn bij hybride en cybercriminele groepen lijken over het algemeen relatief beperkt (R8, R10, R12): 'Ja, zo slim hoef je er niet voor te zijn [om cyberfraude te plegen]' (R12), al bestaan er ook uitzonderingen. Geldezels zijn vaak kwetsbaar en onwetend (R4, R15, R21) en beschikken

vermoedelijk over relatief beperkte cognitieve vaardigheden (R8, R12, R19). 'Je zag wel kwetsbare jongeren, maar je zag ook jongeren die onwetend waren en gewoon een zakcentje wilden bijverdienen' (R4), 'kwetsbare moeders, de alleenstaanden die geld nodig hebben, verslaafden' (R15) en 'dat is het, eigenlijk zijn [het] allemaal kwetsbare personen' (R21). Dit lijkt ook te gelden voor de pasophalers en andere katvangers. Een belangrijke kanttekening hierbij is dat deze bevindingen grotendeels gebaseerd zijn op de interpretatie van de respondenten, die niet altijd opgeleid zijn om dergelijke conclusies te trekken of cognitieve vaardigheden te beoordelen.
Tot slot kunnen kernleden regelmatig impulsief gedrag vertonen (R12), nemen ze lang niet altijd verantwoordelijkheid voor hun daden (C4) en lijken ze weinig spijt en moreel besef te tonen (R4, R6):

> *'Ze zijn echt super gehaaid, super gewetenloos (…). Dus we hebben hier ook met de jongens gezeten en [tijdens hun verhoor] gevraagd van, vind je dat dan niet erg (…) dat je zoiets doet? En dan zeggen ze: ja, maar de bank vergoedt het toch? Dus dat is de denkwijze van dat soort jongeren van: ja, wat maak je je druk om? De bank heeft het toch vergoed?' (R6)*

5.5.2 *Criminele carrière*

Op basis van de politieregistraties, de zaakreconstructies en de expertinterviews zijn drie typen criminele carrières te onderscheiden onder jongeren en jongvolwassenen die actief zijn binnen hybride en cybercriminele jeugdgroepen: 'overstappers', 'hybride plegers' en 'digitale starters'. Deze categorieën lijken op basis van de beschikbare informatie toepasbaar op zowel kernleden als geldezels en katvangers.
Overstappers en hybride plegers (beiden veelal onderdeel van hybride groepen) beginnen hun criminele carrière met het plegen van traditionele criminaliteit, zoals drugsdelicten, inbraken, afpersing, woningovervallen en wapengeweld (R6, R8, R12, R15, R22, C1, C2, C3, C5). Ze zijn recidivisten wanneer ze beginnen met het plegen van cybercrime. Overstappers maken op enig moment een duidelijke overstap naar cybercrime en richten zich vervolgens uitsluitend op cybercriminele activiteiten, vooral online fraude. Hybride plegers gaan het plegen van traditionele delicten op een gegeven moment combineren met cybercriminele activiteiten en online fraude. Het uitbreiden van criminele activiteiten naar online fraude lijkt veelvuldig plaats te vinden (R12):

> *'Wat ons ook opvalt (…) is dat zij ook altijd al wel bekend zijn binnen de traditionele criminaliteit. Dus die komen vanuit de drugswereld, vanuit de wereld van inbraken, woningovervallen en die hebben, voor zover wij daar zicht op hebben, nu gewoon een veel lucratievere manier gevonden om geld te verdienen.' (R8)*

De aantrekkelijkheid van online fraude werd door een expert verklaard door de combinatie van hoge opbrengsten en relatief beperkte risico's:

'Je ziet wel dat sommige jongens inderdaad [betrokken zijn bij] vuurwapengeweld, [en] ook in de handel in verdovende middelen. Eigenlijk alles aanpakken om veel geld te verdienen. Dus wat ze daarvoor moeten doen, dat maakt niet zoveel uit, als het maar geld oplevert (…). Cybercrime is heel lucratief, dus daarom zie je ook die verschuivingen [van het plegen van traditionele delicten naar cybercrime].' (R6)

Een illustratief voorbeeld is een dader die begon met het plegen van traditionele delicten, waaronder winkeldiefstal (R15). Op een gegeven moment maakte hij de overstap naar het plegen van cybercriminaliteit. Na eerst als geldezel te hebben gefungeerd, was hij vervolgens betrokken bij het ronselen van andere geldezels en klom hij uiteindelijk op tot kernlid. Als kernlid pleegde hij vriend-in-nood-fraude, phishing, verkoopfraude en bankhelpdeskfraude. Voor deze delicten is hij uiteindelijk opgepakt en veroordeeld.
De derde groep jongeren start hun criminele carrière direct met het plegen van cybercrime, zonder eerdere betrokkenheid bij traditionele delicten. Deze jongeren zijn vooral actief binnen groepen die zich exclusief richten op cybercrime en blijven doorgaans weg van traditionele delicten:

'Ik denk dat het wel zo is dat de daders van klassieke delicten phishing kunnen plegen. Dat hebben we al gezien. Maar je hebt ook een hele nieuwe groep die wel cyberdelicten durft te plegen, maar zich nooit zal inlaten met klassieke delict[en]. Van de een naar de ander overstappen, van klassiek naar digitaal, dat gaat prima. Maar je hebt ook gewoon mensen die alleen maar digitaal doen en die ook het profiel niet zouden hebben om klassieke delicten [te] plegen.' (R15)

Volgens experts zijn er twee verklaringen voor dat deze nieuwe groep zich uitsluitend richt op cybercrime. Allereerst bezitten ze mogelijk niet de persoonlijkheidskenmerken om traditionele delicten te plegen: 'Want je [hebt] best wel lef nodig om een pizzeria te overvallen of een tankstation. Dat durven deze gasten echt allemaal niet' (R15). Ten tweede is cybercrime vermoedelijk lucratiever dan andere vormen van criminaliteit: 'Ik denk dat wel door velen nu cybercrime als super lucratief wordt gezien, als ik zie in hoe korte tijd hoeveel geld gemaakt kan worden' (R4).
Daarnaast kan affiniteit met technologie en gamen mogelijk een rol spelen bij het beginnen met cybercrime (R6). Dit is mogelijk het geval bij jongeren die bijvoorbeeld DDoS-aanvallen uitvoeren, maar ook bij daders van online fraude. Vooral jongeren met ervaring in de online gamewereld (zoals het hosten van een gameserver of TeamSpeak) ervaren mogelijk een lagere drempel om te beginnen met cybercrime. Daarnaast kunnen ze tijdens het gamen in contact komen met cybercrime, bijvoorbeeld als de server waarop ze gamen wordt bestookt met DDoS-aanvallen. Zij kunnen zich dan gaan afvragen wat er aan de hand is, hier op internet naar gaan zoeken en zo leren van het bestaan van cybercrime.
In de context van cybercrime kunnen zowel overstappers, hybride daders als digitale starters gespecialiseerd zijn in één soort cybercrime of juist generalistisch werken en

betrokken zijn bij verschillende cyberdelicten[22] (R10, R15, R21, C1-5, N3, N8, N12, N21, N24). Generalisten zijn betrokken bij verschillende vormen van cybercrime, vooral online fraude, waarbij ze opportunistisch te werk gaan: 'Kijk maar wat er allemaal op die telefoons staat. Bankhelpdeskfraude, Marktplaatsfraude, phishing. (…). [Ze zijn] opportunistisch. Wat je pakt, dat pak je. (…) En anderen die zijn ook specifiek met één MO bezig' (R21) en: 'Het is ook niet alleen bankhelpdeskfraude, want als het even lastig is met bankhelpdeskfraude, dan schakelen ze ook voor een deel over naar vriend-in-nood-fraude. (…) Dat zie je ook wel, dat er echt overlap is in die MO' (R21). Daders kunnen verschillende delicten uitproberen met het doel zo veel mogelijk geld te verdienen (R21). Ze beginnen bijvoorbeeld met betaalverzoekfraude, maar veranderen op een gegeven moment naar bankhelpdeskfraude:

> *'[Ik ben een] tijdje terug naar een zitting [geweest van] een jongen, 24 jaar, [die] veroordeeld [was] voor phishing. Maar die had ook bankhelpdeskfraude geprobeerd om te kijken of dat succesvol was. Hij probeerde gewoon zo veel mogelijk geld bij elkaar te harken en daar een leuk leven van te leiden. Maar daar was [hij] niet zo succesvol mee, dus daar was hij gauw weer mee gekapt.' (R21)*

5.5.3 *Motivaties*

Uit de interviews, zaakreconstructies en politieregistraties komt naar voren dat zowel jongeren in hybride groepen als onder daders die zich uitsluitend richten op cybercrime, het verkrijgen van status en financieel gewin de belangrijkste motivaties lijken te zijn (R4, R5, R6, R8, R10, R11, R12, R15, R19, R21, R22, C1-5, N8, N12, N18, N21). Deze bevindingen zijn echter grotendeels gebaseerd op de interpretaties van de respondenten; andere motivaties kunnen daarom niet worden uitgesloten.
Financieel gewin en status zijn nauw met elkaar verweven: status wordt in belangrijke mate ontleend aan het bezit en het kunnen etaleren van dure kleding en luxegoederen, die gekocht kunnen worden met de opbrengsten uit cybercrime. Een veelgenoemd voorbeeld is de rol van merkkleding als statussymbool: 'Merkkleding is gewoon de ziekelijke trigger voor dit soort delicten. Het gaat nu om truien van € 1.500. Dan heb je het probleem dat dat status verhoogt en dat een ander dat ook wil.' (R15)

Daarnaast kan het wederrechtelijk verkregen voordeel besteed worden aan andere luxegoederen, waaronder auto's, parfum en elektronica (zoals iPhones).
Deze behoefte aan status uit zich ook in het streven naar een luxueuze levensstijl, waarin materiële rijkdom een centrale rol speelt:

22 Binnen de academische literatuur lopen de definities van specialisatie en generalisatie uiteen, zowel in typen delicten die worden gepleegd als in de tijdsperiode waarnaar gekeken moet worden. In dit onderzoek richten we ons uitsluitend op cybercriminele activiteiten gedurende hun hele cybercriminele carrière.

'Ik zie het als status. (…) Je hebt dat geld [van cybercrime] nodig om die status te verkrijgen. Ik zie dat zij zich wanen in luxe: luxegoederen, luxevervoertuigen, luxevakanties. Dat er gebruik gemaakt wordt van dure hotels, prostituees, veel drank.' (R4)

Een andere expert bevestigt hoe jongeren hun identiteit en aanzien ontlenen aan uiterlijke kenmerken, zoals kleding: 'dan zie je die jongens, die halen al hun status uit die kleding' (R6). Het plegen van online fraude vormt voor deze jongeren het middel om deze levensstijl te financieren.

5.6 Resumé

Uit hoofdstuk 4 is naar voren gekomen dat lokale veiligheidscoalities onder leiding van gemeenten, die de regie voeren op de aanpak van (criminele) jeugdgroepen, uitsluitend zicht hebben op traditionele groepen. Jeugdgroepen die betrokken zijn bij cybercrime blijven buiten beeld, al zijn er (soms) wel vermoedens maar geen concrete aanwijzingen van cybercriminele (al dan niet hybride) groepen.
Uit de gesprekken met experts en uit de zaakreconstructies en politieregistraties blijkt echter dat er talloze cybercriminele groepen actief zijn (geweest), al dan niet hybride. Deze groepen zijn bekend bij monodisciplinaire partners, vooral bij strafrechtelijke actoren (de politie en het OM) en (gedeeltelijk) bij enkele private partijen, waaronder banken en telecomproviders. Informatie over jeugdgroepen die betrokken zijn bij cybercrime is gefragmenteerd aanwezig bij individuele partners en niet breed toegankelijk voor lokale veiligheidscoalities.
Er zijn twee soorten jeugdgroepen te onderscheden. Enerzijds zijn er hybride criminele jeugdgroepen actief, die betrokken zijn bij zowel traditionele criminaliteit als cybercrime – voornamelijk online fraude. Deze groepen lijken veelvuldig voor te komen. Anderzijds kunnen jeugdgroepen zich exclusief op cybercrime richten, wederom veelal online fraude.
Cybercrime en traditionele criminaliteit raken steeds vaker met elkaar verweven. Soms worden beide typen naast elkaar gepleegd, zonder directe relatie. In andere gevallen is er een sterkere, meer directe verbinding tussen traditionele criminaliteit en cybercrime, waarbij cybercrime veelal voorafgaat aan de traditionele delicten.
Op basis van de politieregistraties, de zaakreconstructies en de expertinterviews hebben we slechts een beperkt beeld gekregen van de structuur, de samenstelling, het ontstaan en de groei van hybride en cybercriminele jeugdgroepen. Daarbij vertonen hybride en cybercriminele jeugdgroepen veel overeenkomsten. Zo kunnen ze enerzijds dynamisch zijn en ad hoc ontstaan wanneer zich een gelegenheid voordoet om cybercrime te plegen, en anderzijds relatief stabiel zijn. Beide typen groepen hebben doorgaans kernleden, professionele en/of gerekruteerde facilitators en geldezels of andere katvangers. Toetreding tot deze groepen verloopt via actieve rekrutering of geleidelijke betrokkenheid, waarbij zowel offline als online relaties, en fysieke en virtuele ontmoetingsplaatsen een rol spelen.

De demografische kenmerken van leden van hybride en cybercriminele groepen laten zien dat kernleden doorgaans volwassen en overwegend man zijn. Geldezels en katvangers zijn meestal minderjarig, kwetsbaar en onwetend. De etnische achtergrond en het opleidingsniveau van kernleden variëren sterk en lijken samen te hangen met hun rol binnen de groep. De meeste kernleden en geldezels hebben een relatief lagere SES, komen uit achterstandswijken en hebben deels een problematische gezinssituatie. Over het algemeen lijken de cognitieve vaardigheden beperkt. Als belangrijkste motivaties komen het verkrijgen van status en financieel gewin naar voren.

6 Resultaten spoor 3: de (integrale) aanpak van jeugdige (cyber)daders in Noord-Nederland

In dit hoofdstuk gaan we in op de aanpak van (cyber)criminele jeugdgroepen. Dat doen we op basis van de bevindingen uit de politieregistraties, de zaakreconstructies en de expertinterviews. Eerst besteden we aandacht aan de mate waarin er bij de (integrale) aanpak van cybercriminele jeugdgroepen in Noord-Nederland zicht is op de groepen die in spoor 1 en 2 zijn geïdentificeerd. Daarna bespreken we in hoeverre en op welke wijze de (integrale) aanpak van cybercriminele jeugdgroepen kan worden bevorderd. Het hoofdstuk eindigt met een resumé.

6.1 De mate van zicht op de cybercriminele jeugdgroepen die in spoor 1 en 2 zijn geïdentificeerd

In hoofdstuk 4 (spoor 1) is gebleken dat lokale veiligheidscoalities geen zicht hebben op cybercriminele jeugdgroepen. Uit de expertinterviews komt het beeld naar voren dat dit vooral wordt veroorzaakt doordat veel lokale partners geen signalen ontvangen over jongeren die betrokken zijn bij cybercrime. Enerzijds lijkt dit gebrek aan signalen te ontstaan doordat veiligheidspartners nog (te) veel leunen op straatinformatie voor het identificeren van deze groep. Anderzijds lijken deze partners te weinig kennis en expertise te hebben om cyberdaders te kunnen identificeren.
In hoofdstuk 5 (spoor 2) bleek dat er in Noord-Nederland meerdere jeugdgroepen betrokken zijn bij cybercrime. Zij zijn bij enkele actoren in beeld (vooral bij de politie en het OM), terwijl actoren als banken en telecomproviders het (mono)strafrechtelijke beeld van de politie en het OM verrijken. Op beide conclusies gaan we nu verder in.
Wat betreft spoor 1 (identificatie van problematische en traditionele criminele jeugdgroepen) bleek uit de expertinterviews (R1, R2, R3, R7, R8, R11, R14, R16, R17, R18, R20) dat gemeenten problematische en criminele jeugdgroepen veelal signaleren vanwege hun gedrag in de openbare ruimte. Hierbij zijn zij sterk afhankelijk van straatinformatie die wordt opgevangen door lokale partners, zoals wijkagenten, jeugdboa's, jongerenwerkers, medewerkers van de jeugdreclassering en verslavingszorg, leerkrachten en buurtbewoners (R1, R2, R7, R8, R11, R14, R16, R17).
Leerkrachten staan bijvoorbeeld in direct contact met leerlingen en hun ouders, waardoor ze signalen over de betrokkenheid van leerlingen bij jeugdgroepen vroegtijdig kunnen opvangen (R16). Ook jongerenwerkers kunnen signalen of informatie over

problematische en criminele jeugdgroepen opvangen, omdat ze aanwezig zijn op straat en op scholen en omdat zij betrokken zijn bij bepaalde maatschappelijke projecten (R14). Daarnaast zijn jongerenwerkers ook online actief. Zo kunnen ze zelf bijvoorbeeld een Instagram-account beheren waar berichten op worden geplaatst, en ze kunnen privéaccounts van jongeren volgen. Hier worden echter nauwelijks signalen van de betrokkenheid van deze jongeren bij (cyber)criminaliteit geïdentificeerd. Enerzijds lijkt dit te komen doordat jongeren hierover niets delen; anderzijds hebben jongerenwerkers niet de kennis om dergelijke signalen te herkennen (R14, R17).
Bovendien lijkt het tegenwoordig lastiger te zijn om traditionele criminele jeugdgroepen goed in kaart te brengen (R3, R14). Enerzijds komt dit doordat jongeren steeds meer gebruik lijken te maken van online kanalen om met elkaar te communiceren en ze elkaar steeds minder vaak op straat ontmoeten: 'Dik 80 procent gaat allemaal via appgroepen (…). En 20 procent is nog fysiek' (R3). Dit is problematisch, omdat deze groepen veelal gesloten zijn, terwijl gemeenten niet de juiste juridische bevoegdheden hebben om toegang te krijgen tot dergelijke groepen:

> *'Ook is [het] (…) naast het fysieke contact moeilijk [om] in contact te komen met jongeren. (…) We [zien] ook in de afgelopen jaren een toename van steeds meer gesloten [online] groepen, groepen, waar wij niet tot nauwelijks, volgens onze bevoegdheden, toegang tot hebben.' (R3)*

Een andere mogelijk verklaring is dat de digitale informatiepositie van gemeenten tekortschiet, of – meer algemeen – dat de verbinding met jongeren onvoldoende is.
Anderzijds hebben hedendaagse problematische jeugdgroepen en criminele jeugdgroepen een hoge mate van dynamiek en fluïditeit, waarbij hun samenstelling per dag verschilt. Dit bemoeilijkt het in kaart brengen van deze groepen en het inzetten van interventies:

> *'En nu hebben we wel een paar keer gehad dat we met elkaar die groep gewoon niet helemaal duidelijk kregen, omdat er elke dag weer een compleet andere groep was (…). En dan blijf je ook een beetje hangen van ja, wat is nou precies die (…) groep? Omdat je hem niet zo duidelijk kan afbakenen (…) blijft inzet soms ook (…) hangen.' (R14)*

De afhankelijkheid van straatinformatie geeft direct de kern weer van het probleem van het gebrekkige zicht op cybercriminele jeugdgroepen (R3, R7, R18). Integrale overlegtafels bespreken problematische en criminele jeugdgroepen op basis van waarnemingen op straat, waardoor zij sterk afhankelijk zijn van deze informatiebron. Dit maakt het lastig om vast te stellen of jongeren cyberdelicten plegen, en zo ja welke, omdat deze activiteiten zich doorgaans niet op straat afspelen en daardoor buiten het bereik van traditionele observaties blijven. Lokale actoren zien deze activiteiten dus niet, waardoor ze niet worden besproken en er dus ook geen verdere identificatie van

cybercriminele jeugdgroepen plaatsvindt. Dit is problematisch, omdat jeugdige cyberdaders doorgaans niet op straat te vinden zijn.
Bovendien lijkt binnen de huidige jeugdgroepenaanpak (alsook het 7-stappenmodel) nog onvoldoende aandacht te zijn voor cybercrime. Als onderdeel van het 7-stappenmodel wordt bijvoorbeeld standaard een groepsscan van de jeugdgroep uitgevoerd, maar de vraag is of daarbij voldoende aandacht is voor cybercrime (R3).
Op basis van spoor 2 (jeugdgroepen die betrokken zijn bij cybercrime) komt het beeld naar voren dat monopartners (en specifiek de politie en het OM) zicht hebben op enkele cybercriminele jeugdgroepen. Andere actoren, zoals banken en telecomproviders, verrijken dit mono-strafrechtelijke beeld, waardoor een completer beeld van deze groepen ontstaat. Dit suggereert dat het (onder voorwaarden) delen van informatie bevorderlijk kan zijn voor het zicht van lokale partners op cybercriminele jeugdgroepen.
Dat de strafrechtelijke actoren een beter zicht hebben op cybercriminele jeugdgroepen lijkt samen te hangen met hun lagere afhankelijkheid van straatinformatie. Zij kunnen onder meer gebruikmaken van meldingen, aangiftes, verklaringen van verdachten, bestaande politiedata en lopende opsporingsonderzoeken (R5, R6, R11, R15, R22, C1-5). Zo beschrijft R6 dat het in kaart brengen van groepen vaak begint bij gegevensdragers en financiële gegevens: 'Vaak loop (…) je het aan vanaf de gegevensdragers (…) en dan zie je inderdaad (…) dat daar cybercrime-gerelateerde feiten mee worden gepleegd, [een telefoon] of een laptop, enzovoort' (R6).
Ondanks deze bredere informatiepositie brengen de politie en het OM veelal slechts een beperkt deel van een jeugdgroep in kaart, vooral het laaghangend fruit, zoals de geldezels of de pinners. Zij krijgen vaak geen inzicht in volledige groepen, waarbij vooral de kernleden buiten beeld blijven (R5, R11, R19): 'Wanneer loopjongen één wordt aangehouden, staat de volgende alweer in de rij. (…) Dat maakt het ontzettend lastig om een volledig beeld te krijgen (…). Dus we krijgen (…) niet echt zicht [op] (…) het netwerk.' (R19)

Er lijkt echter wel voldoende politiedata beschikbaar te zijn om dergelijke groepen verder uit te diepen. De RIEC-casus (C1) heeft dit laten zien. Dit vergt extra investeringen en capaciteit, waar de strafrechtelijke actoren op dit moment beperkt over kunnen beschikken.
Uit hoofdstuk 5 kwam verder naar voren dat private partijen (banken en telecomproviders) eveneens (beperkt) zicht hebben op cybercriminele jeugdgroepen en dat ze de beschikbare informatie delen met de strafrechtelijke actoren voor de strafrechtelijke vervolging.
Dat banken een beperkt beeld hebben, lijkt deels te worden veroorzaakt doordat deze groepen over meerdere banken verspreid kunnen zijn (R21). Als groepen gebruikmaken van geldezels, lukt het banken vaak wel om hen te identificeren (R9, R21). Zo antwoordde een respondent op de vraag hoeveel geldezels kunnen worden geïdentificeerd door banken: 'Ja, 90 procent, eigenlijk allemaal wel' (R9).

Na de identificatie voeren banken vaak aanvullend digitaal onderzoek uit (R9), bijvoorbeeld door te achterhalen of er vanaf een vast IP-adres of vanaf een bepaald toestel is ingelogd op de bankrekeningen van meerdere geldezels. Dit zou er een aanwijzing voor kunnen zijn dat de geldezels hun bankgegevens hebben afgestaan aan iemand hoger in de groep. In sommige gevallen kan dit leiden tot de identificatie van één of een beperkt aantal kernleden. Daarnaast worden geldezels soms geïnterviewd door de bank om zo meer inzicht te krijgen in het rekruteringsproces. Dit blijft vaak zonder resultaat, omdat geldezels hun mond houden. Als geldezels wél informatie prijsgeven, wordt die veelal gedeeld met de politie.
Cybercriminele jeugdgroepen kunnen mogelijk vollediger in kaart worden gebracht door een betere samenwerking tussen banken onderling en tussen de banken en de politie (R21). Een voorbeeld van een dergelijke samenwerking is de Electronic Crimes Task Force. Hierbij worden werkwijzen besproken, maar wordt geen persoonlijke informatie van verdachten uitgewisseld; dat mag niet volgens de AVG. Daarnaast kunnen banken meldingen van slachtoffers bundelen en deze via aangiftes delen met de politie. Hierdoor ontstaat de mogelijkheid om verschillende losse datapunten van de banken aan elkaar te koppelen, waarmee een groep vollediger in kaart kan worden gebracht.
Tot slot proberen telecomproviders om telefoonnummers die gebruikt zijn om cybercrime te plegen te koppelen aan potentiële verdachten (R10). Door onderzoek te doen naar de zendmasten die de telefoon aanstraalde, kunnen locaties van waaruit veel wordt gebeld worden geïdentificeerd, waardoor enigszins zicht kan worden verkregen op cybercriminele jeugdgroepen. Maar ook hier geldt dat het voor telecomproviders nagenoeg onmogelijk is om een geheel cybercriminele jeugdgroep in kaart te brengen.
Samenvattend is de informatievoorziening voor het identificeren en in kaart brengen van problematische en (cyber)criminele jeugdgroepen vanuit gemeenten, jongerenwerkers en scholen nog veelal traditioneel ingericht en gericht op straatinformatie. Jongeren zijn tegenwoordig echter minder actief op straat, wat tot gevolg heeft dat gemeenten maar (zeer) beperkt zicht kunnen krijgen op deze groepen. De politie en het OM, banken en telecomproviders beschikken over meer relevante data, maar hun zicht blijft veelal beperkt tot de lagere leden in de groep, zoals geldezels. Vooral de politie en het OM lijken meer informatie te hebben waarmee cybercriminele jeugdgroepen geïdentificeerd kunnen worden. De vijf zaakreconstructies zijn hier een goed voorbeeld van; het betreft grote onderzoeken, boven het basisteam-niveau, waarbij meerdere kernleden zijn geïdentificeerd. Dergelijke onderzoeken vergen echter veel capaciteit, iets wat op dit moment beperkt beschikbaar is.

6.2 Het bevorderen van de (integrale) aanpak van cybercriminele jeugdgroepen

In deze paragraaf bespreken we de (integrale) aanpak van jeugdgroepen die betrokken zijn bij online criminaliteit. Daarbij beschrijven we eerst hoe de (integrale) aanpak er in de praktijk uitziet. Vervolgens bekijken we in hoeverre deze aanpak delictspecifiek

is. Daarna komen de verbeterpunten en best practices van de (integrale) aanpak aan bod. Tot slot beschrijven we in hoeverre interventies bij jeugdige cyberdaders kunnen bijdragen aan de aanpak van cybercriminele jeugdgroepen.

6.2.1 *Wat houdt de (integrale) aanpak van cybercriminele jeugdgroepen in? En welke actor (mono) of actoren (integraal) zijn hierbij betrokken?*

In dit onderzoek hebben we drie benaderingen geïdentificeerd die momenteel worden gebruikt bij de aanpak van jeugdgroepen die betrokken zijn bij cybercrime. Allereerst kan er sprake zijn van een integrale aanpak, waarbij meerdere lokale actoren samenwerken. Een dergelijke benadering lijkt echter een zeldzaamheid; in dit onderzoek hebben we maar één casus met een integrale aanpak geïdentificeerd: zaakreconstructie C1. Ten tweede kan een beperkt aantal actoren samenwerken bij de identificatie van jeugdgroepen, terwijl interventies veelal door één actor worden uitgevoerd. Ten derde kan er sprake zijn van een monodisciplinaire aanpak, waarbij lokale actoren afzonderlijke jeugdgroepen aanpakken die betrokken zijn bij cybercrime. In de praktijk lijkt deze aanpak het vaakst voor te komen.
Ons onderzoek laat zien dat integrale kansen vaak onbenut blijven, terwijl een integrale aanpak in potentie een rijker informatiebeeld en een breder palet aan interventiemogelijkheden oplevert. Het meer benutten van bestaande integrale samenwerkingsstructuren voor de aanpak van cybercrime lijkt dan ook wenselijk.
Daarnaast wordt in de praktijk veelvuldig gekozen voor een strafrechtelijke aanpak. Hierbij is de scope van het onderzoek vaak beperkt: het aantal subjecten en de delicten waarvoor bewijs wordt verzameld, zijn doorgaans afgebakend. Hierdoor wordt meestal slechts gekeken naar één of enkele subjecten en delicten, waardoor andere betrokkenen en strafbare feiten buiten beeld blijven. Dergelijke opsporingsonderzoeken kunnen echter ook (bruikbare) politie-informatie opleveren, die als startpunt kan dienen voor een integrale aanpak. Zo'n integrale aanpak biedt de mogelijkheid om zowel de scope van het onderzoek (de informatievergaringsfase) als de interventies te verbreden. Integrale samenwerking biedt de mogelijkheid om de scope van het onderzoek (de informatievergaringsfase) én de interventies te verbreden.
De aanpakken en interventies die we in deze paragraaf beschrijven, kunnen worden toegepast op hybride en op uitsluitend cybercriminele jeugdgroepen. Daarom hebben we geen expliciet onderscheid gemaakt tussen beide typen groepen. Wel hebben we onderscheid gemaakt tussen volwaardige integrale aanpakken[23] en monodisciplinaire aanpakken. Bij de aanpakken en interventies die we hieronder beschrijven, is een kanttekening nodig: ons beeld is gebaseerd op wat er tijdens de interviews is aangedragen en op wat er tijdens de zaakreconstructies is geïdentificeerd. Daarmee geven we hieronder dus geen limitatief overzicht van alle aanpakken en interventies.

23 Dit zijn multidisciplinaire samenwerkingen waarbij veelal één actor interventies toepast, gevoed met informatie van anderen.

Een volwaardige integrale aanpak

In dit onderzoek hebben we één casus geïdentificeerd waarin sprake was van een volwaardige, grootschalige integrale aanpak van een cybercriminele jeugdgroep: zaakreconstructie C1 (zie paragraaf 5.2.2). In deze zaak werkten meerdere publieke partners nauw samen bij de analyse van de groep en de uitvoering van de interventies.

De samenwerking verliep langs twee sporen. Enerzijds coördineerde het RIEC het informatiebeeld door gegevens over de groep te verzamelen van diverse partners. Daarmee kon een totaaloverzicht van de groep worden verkregen. Hoewel de groep zich primair richtte op cybercrime, bood de samenwerking ook zicht op andere criminele activiteiten. Anderzijds werkte een beperkt aantal partners (gemeenten, de politie, het OM, de Belastingdienst en de Arbeidsinspectie) intensief samen bij de uitvoering van de interventies. Iedere partner zette daarbij zijn eigen bevoegdheden in. Gemeenten legden dwangsommen op vanwege illegale bewoning en beëindigden een bijstandsuitkering vanwege illegale inkomsten. De politie voerde onder gezag van het OM een strafrechtelijk onderzoek uit en controleerde het wegtransport van gevaarlijke stoffen. Tegelijkertijd vorderde de Belastingdienst onrechtmatig verkregen coronasteun terug en werd belasting geheven over het illegaal verkregen inkomen. Tot slot legde de Arbeidsinspectie boetes op wegens kinderarbeid en zwartwerken.

Deze breed gedragen en gecoördineerde maatregelen maakten het mogelijk om de groep op verschillende fronten aan te pakken. Door (onder voorwaarden) informatie te delen, kunnen lokale partners dus beter zicht krijgen op cybercriminele jeugdgroepen. Dit vormt de kern van de meerwaarde van een integrale samenwerking: de aanpak richt zich op de groep en zijn activiteiten als geheel – en niet op een specifiek subject en/of delict, zoals bij de uitsluitend strafrechtelijke aanpak veelal het geval is.

In algemene zin is deze aanpak niet ontworpen voor cybercrime; de inzet van het RIEC voor de aanpak van cybercrime is zelfs zeldzaam. Doorgaans wordt het RIEC ingezet voor traditionele subjecten of (jeugd)groepen waarvoor aanwijzingen bestaan dat zij ondermijnende criminaliteit plegen. Tegelijkertijd was deze specifieke aanpak opgezet met het doel om een groep aan te pakken die betrokken was bij cybercrime, waarbij de aanpak zich in de breedte richtte op de groep en de misstanden waarbij de groep en de leden betrokken waren.

Hoewel een integrale aanpak in de praktijk beperkt toegepast lijkt te worden, werd tijdens meerdere expertinterviews de waarde van een dergelijke interdisciplinaire aanpak benadrukt. Verschillende partners beschikken over complementaire informatie. Het koppelen van deze informatie vergroot de gezamenlijke informatiepositie en geeft daarmee een rijker informatiebeeld. Daarnaast neemt het interventiepotentieel toe omdat iedere organisatie over eigen interventiemogelijkheden beschikt. Hierdoor kunnen interventies van verschillende organisaties gelijktijdig worden ingezet en gecombineerd. Of die mogelijkheden ook inzetbaar en effectiever zijn, is nog voer voor discussie:

> *'(…) En iedereen heeft z'n eigen schat aan informatie, (…) zijn eigen systemen en zijn eigen blik op de werkelijkheid, en inderdaad zijn eigen gereedschapskist waar die uit*

kan putten. Dus dat is sowieso sterker. Plus, in het kader van het RIEC-onderzoek is gewoon gebleken dat zo'n onderzoek naar die jongens [via] een traditioneel (…) rechercheonderzoek (…) monnikenwerk [is].' (R8)

Ondanks de voordelen lijkt deze integrale aanpak vooralsnog uitzonderlijk te zijn en worden in de praktijk vooral kleinschaligere samenwerkingen en monodisciplinaire interventies toegepast.

Multidisciplinaire samenwerking met een monodisciplinaire uitvoering
Een tweede benadering die in dit onderzoek naar voren kwam, betreft een aanpak waarbij meerdere partijen informatie uitwisselen om een groep in kaart te brengen, maar waarbij de uitvoering van de interventies uiteindelijk bij één actor ligt. Dit is een tweedelige aanpak: multidisciplinair in de informatie-uitwisseling, en monodisciplinair in de interventies. Daarmee onderscheidt deze aanpak zich van zowel de volwaardige integrale aanpak als de strikt monodisciplinaire benadering.
Een eerste samenwerking vindt plaats tussen de politie, het OM en de gemeenten. Deze samenwerking blijkt in de praktijk wisselend te verlopen (R1, R2, R4, R7, R8, R12). In sommige gemeenten deelt de politie actief informatie over traditionele criminele jeugdgroepen met de gemeente, terwijl dit in andere gemeenten juist niet het geval is. Zo beschreven R1 en R2 dat binnen hun gemeenten nauwelijks informatie vanuit de politie wordt gedeeld, terwijl R4, R8 en R12 juist voorbeelden noemden van actieve informatiedeling door de politie. Vanuit de politie lijkt wat betreft cybercriminele jeugdgroepen vooralsnog geen informatie gedeeld te worden. Ook vanuit het OM werd aangegeven dat er weinig informatie wordt gedeeld met gemeenten en veiligheidshuizen over cybercriminele jeugdgroepen (R22). Wel kwam naar voren dat de politie een geanonimiseerde analyse heeft gemaakt van de kenmerken en ronsellocaties van geldezels in een stad in Noord-Nederland. Die analyse is gedeeld met de gemeente (binnen de driehoek), waarna een gezamenlijk plan is gemaakt om doelgroep- en locatiespecifieke interventies in te zetten voor deze geldezels.
Daarnaast werken de politie en het OM samen met banken en telecomproviders (R6, R9, R21). Het OM kan informatie delen met banken om hen te ondersteunen bij een betere detectie van verdachte transacties (R22). Vanuit de banken is de samenwerking met de politie en het OM primair gericht op informatiedeling voor opsporingsonderzoeken (R6). Deze samenwerking bestaat uit twee delen. Ten eerste kan er sprake zijn van het delen van identificerende persoonsgegevens van banken met de politie. Dit is uitsluitend toegestaan op basis van een aangifte door de bank of een vordering door de politie. Banken kunnen bijvoorbeeld aangifte doen en informatie verstrekken, wat vervolgens kan leiden tot een opsporingsonderzoek. Via vorderingen kan vervolgens eventuele extra informatie worden opgevraagd (R9). Dergelijke aangiftes worden vooral gedaan wanneer er een daderindicatie is. Daarnaast kan er aangifte worden gedaan van een fenomeen. Als een bank bijvoorbeeld opmerkt dat er in een bepaalde stad plotseling veel geldezels worden gerekruteerd, kan hiervan aangifte worden gedaan. Banken hebben geen juridische grondslag om (identificerende) gegevens met gemeen-

ten te delen, dus voor het identificeren van (cyber)criminele jeugdgroepen wordt niet rechtstreeks met gemeenten samengewerkt.
Ten tweede worden er niet-herleidbare persoonsgegevens uitgewisseld (R21). Dit wordt onder andere gedaan binnen het structurele samenwerkingsverband Electronic Crimes Task Force. Daarin worden vooral de modus operandi van groepen en de gebruikte methoden rond de cash-outs besproken (R21). Dergelijke algemene informatie is eenvoudiger te delen dan persoonsgegevens, waarvoor striktere voorwaarden gelden.
De politie en het OM werken ook samen met telecomproviders (R10). Ook daarbij is vooral sprake van informatiedeling vanuit de telecomproviders naar de politie en het OM via aangiftes en vorderingen. Zo kan bijvoorbeeld aangifte worden gedaan van verdachte telefoonnummers. In dergelijke gevallen verloopt de informatie-uitwisseling doorgaans soepel en zijn er geen problemen met betrekking tot de AVG. De gegevensuitwisseling met andere partijen is echter complexer.
Banken en telecomproviders werken in de praktijk ook samen met andere private partijen (R9, R10, R21). De banken hadden bijvoorbeeld een samenwerking opgezet met een private partij die accounts voor het rekruteren van geldezels offline haalt (R21). Deze samenwerking verliep echter moeizaam, omdat de betrokken partij traag handelde. Verder kunnen banken samenwerken met bedrijven die worden gebruikt bij de cash-out van wederrechtelijk verkregen voordeel, zoals elektronicazaken of winkels die tegoedbonnen verkopen. Gezamenlijk wordt onderzocht welke maatregelen mogelijk zijn om deze cash-outs te bemoeilijken. Voorbeelden zijn: het trainen van medewerkers om signalen van geldezels te herkennen (zoals het massaal kopen van cadeaukaarten) en het instrueren van medewerkers om bij verdachte situaties in te grijpen of de politie te waarschuwen. Een terugkerend obstakel in deze samenwerkingen betreft de privacywetgeving, met name de AVG. Deze beperkt de mogelijkheden tot informatie-uitwisseling.Samenvattend zien we dat in deze samenwerkingen de uitvoering van de interventies veelal bij de politie of het OM ligt. Zij gaan over tot strafrechtelijke opsporing en vervolging (R4, R5, R8, R11, R12, R15, R18). De rol van de andere partijen blijft voornamelijk beperkt tot het actief delen van informatie, op eigen initiatief of op verzoek. Bij het op verzoek delen van informatie geldt dat daarbij veelal sprake is van vorderingen binnen een strafrechtelijk onderzoek. Een samenwerkingsverband dat specifiek is gericht op het delen van cybercrime-gerelateerde informatie is de Electronic Crime Task Force, waarin de politie en de banken vertegenwoordigd zijn. Door (onder voorwaarden) informatie te delen, krijgen andere lokale partners beter zicht op cybercriminele jeugdgroepen.

Monodisciplinaire aanpak
In veel gevallen wordt de aanpak van cybercriminele jeugdgroepen uitgevoerd door één actor of sector (zoals de politie, het OM, gemeenten, banken, telecomproviders en jongerenwerkers) zonder duidelijke samenwerking met andere partijen. Deze gefragmenteerde aanpak richt zich op zachte maatregelen (zoals voorlichting, weerbaarheidstraining en het bieden van vrijetijdsbesteding) en harde technische maatregelen

om barrières op te werpen tegen cybercrime. Deze interventies richten zich niet specifiek op groepen, maar zijn 'generiek'. Geconstateerd is dat deze mono-aanpak voor verbetering vatbaar is: het effect van interventies is veelal onduidelijk en er is behoefte aan betere samenwerking.
Gemeenten geven voorlichting om cybercrime te voorkomen. Zij zijn bijvoorbeeld betrokken bij het ontwikkelen en stimuleren van lesprogramma's op scholen. Ook wordt er aangesloten bij landelijke initiatieven, zoals HackShield en de MKB Cyber Campus (R3).
De politie en het OM hanteren een strafrechtelijke benadering, die is gericht op individuele daders, zoals kernleden, facilitators en geldezels. Deze aanpak richt zich primair op vrijheidsstraffen, geldboetes en/of het afnemen van het wederrechtelijk verkregen voordeel (R4, R5, R8, R11, R12, R15, R18). De hoogte en aard van de straf hangt af van de rol en de betrokkenheid van de verdachte. Zo benadrukte een respondent: '(…) een geldezel moet je misschien anders aanpakken dan een harde crimineel. (…) Een harde crimineel moet je misschien alleen maar repressief [aanpakken]. Misschien kan je een rising star nog een andere kant op drukken.' (R12)

Hoewel strafrechtelijke vervolging meerdere doelen dient en verschillende effecten kan hebben, kwam uit de expertinterviews het beeld naar voren dat het over het algemeen maar in beperkte mate leidt tot het verminderen van recidive (R4, R6, R8, R19). Met andere woorden: de speciale preventie van gevangenisstraffen lijkt beperkt te zijn. Zo zijn er gevallen bekend waarin cyberdaders veroordeeld waren tot een gevangenisstraf en vanuit hun schorsing of detentie hun criminele activiteiten voortzetten (R6, R8, R21). Bovendien benoemden respondenten (R19) dat het ouderwetse politiewerk (reactief en repressief) mogelijk weinig effect heeft op het terugdringen van cybercrime:

> *'En ook of de (..) straffen opwegen tegen het gewin (..) dat ze ermee verdienen, want als de straf relatief laag is en daarna (…) kunnen ze in één keer weer mega cashen. Ja, dan (..) maakt [dat] het (…) heel, heel aantrekkelijk (…) Sterker nog, ik denk dat straffen niet eens meer nut heeft.' (R19)*

Toch worden er momenteel forse gevangenisstraffen opgelegd voor cybercrime, al is het effect hiervan op recidive nog onduidelijk.
Naast vrijheidsstraffen richt het OM zich nadrukkelijk op het afpakken van het wederrechtelijk verkregen voordeel. Hierbij wordt geprobeerd beslag te leggen op alles van waarde, zoals dure kleding en andere luxegoederen. Dit afpakken wordt gedaan om twee redenen. Allereerst levert het geld op, waardoor de daders minder terug hoeven te betalen. Ten tweede wordt hiermee aangetoond dat misdaad niet loont. Hoewel dit cyberdaders meer pijn lijkt te doen dan een vrijheidsstraf (R6), is het daadwerkelijke effect op bijvoorbeeld recidive nog onduidelijk: 'Toen we [dure kleding] afpakte[n], greep [dat] hem [een verdachte van online fraude] echt aan' (R6). Daarnaast beschreef respondent R6 een casus waarin een verdachte tijdens een verhoor aangaf al rekening

te hebben gehouden met een langdurige gevangenisstraf. Maar toen hem werd medegedeeld dat al zijn wederrechtelijk verkregen voordeel werd afgepakt, reageerde hij zeer emotioneel. Dit werd bevestigd door een andere respondent:

> *'Ze willen geld verdienen en status en aanzien. Kijk, als je ze dat afpakt (…), dat je (…) de Rolex (…) [van hun pols] vandaan haalt, of hun Balenciaga's van hun voeten trek[t], zeg maar. Dat (…) doet wat met ze.' (R8)*

Tot slot werd opgemerkt dat de toepassing van strafrechtelijke maatregelen wordt bemoeilijkt door een aantal factoren (R12). Het primaire probleem hierbij lijkt – bij uitstek bij cybercrime – het moeizame en trage strafrechtproces te zijn (zie ook Ruiter et al., 2023).
Daarnaast verzorgt de politie voorlichting over specifieke thema's, zoals het fenomeen geldezels, hoewel dit vooral incidenteel lijkt plaats te vinden (R4). De effectiviteit van deze voorlichting is echter nog onderwerp van discussie. Respondenten betwijfelen of voorlichting daadwerkelijk een preventief effect heeft (R8).[24] Voorlichting wordt dan ook als nuttig gezien en als onderdeel van een bredere aanpak, maar niet als dé oplossing: 'Er zijn altijd jongeren die daar toch voor kiezen [het plegen van cybercrime] (…). Dus dat dat niet de oplossing is, nee, dat lijkt me helder, maar het is wel onderdeel van een brede aanpak, denk ik.' (R8)

Banken voeren zelfstandig maatregelen uit, die veelal gericht zijn op geldezels (R9, R21). Zo worden bankrekeningen van geldezels geblokkeerd en worden zij geregistreerd in het Intern VerwijzingsRegister en eventueel ook in het Extern VerwijzingsRegister. Opname in het Intern VerwijzingsRegister heeft een relatief lage drempel, terwijl voor het Extern VerwijzingsRegister sprake moet zijn van aangiftewaardig gedrag dat concreet kan worden aangetoond. Opname in het Extern VerwijzingsRegister leidt tot een waarschuwing richting andere financiële instellingen om het financiële systeem te beschermen. Hierbij wordt maatwerk geleverd (R9), zoals het bepalen van de duur van de registratie (vier jaar in plaats van acht jaar) of het beperken tot alleen het Intern VerwijzingsRegister, dat niet gedeeld wordt met andere banken.
Ook banken zetten in op voorlichting (R9, R21), net als gemeenten en de politie. Banken plaatsen bijvoorbeeld waarschuwingen op sociale media en sturen via hun bankieren-app gerichte berichten naar klanten die binnen de leeftijdscategorie van geldezels vallen. Dat doen ze ook bij de groep klanten die in de leeftijdscategorie valt van de ouders van geldezels. In deze berichten wordt gewezen op de risico's van het worden van een geldezel. Verder wordt er preventiemateriaal naar scholen gestuurd en verzorgen banken daar voorlichtingssessies. De effectiviteit van deze aanpak voor algemene preventie wordt ter discussie gesteld (R9). (Potentiële) geldezels volgen doorgaans niet

24 Recent onderzoek wijst uit dat voorlichtingscampagnes en educatieprogramma's vaak niet het gewenste effect hebben, en soms zelfs het tegenovergestelde effect kunnen veroorzaken, waarbij risicogedrag juist wordt versterkt (zie Kruisbergen & De Jonge, 2023).

de sociale kanalen van banken en kunnen meldingen in de bankieren-apps eenvoudig wegklikken zonder de inhoud te lezen.
De voorlichting vanuit banken richt zich niet alleen op het voorkómen van daderschap, maar ook op slachtofferpreventie (R21). Via hun website bieden banken informatie aan om potentiële slachtoffers te waarschuwen voor de verschillende vormen van cybercrime. Daarnaast organiseert De Nederlandse Vereniging van Banken voorlichtingscampagnes, bijvoorbeeld op de 50PlusBeurs.
Ook worden technische preventiemaatregelen ingezet om (cyber)criminaliteit en slachtofferschap te voorkomen. Banken maken bijvoorbeeld gebruik van gespecialiseerde software voor het detecteren van verdachte transacties (R9). Deze software richt zich vooral op uitgaande betalingen van mensen, om zo slachtofferschap te voorkomen. Een belangrijke uitdaging hierbij is het vinden van de juiste balans in de afstelling van deze software: de detectie moet effectief zijn, maar tegelijkertijd moet worden voorkomen dat een groot aantal onschuldige transacties als verdacht worden aangemerkt.
Een tweede technische maatregel betreft het beperken van de geldigheidsduur van de signeercodes die nodig zijn om transacties te bevestigen (R21). Daarnaast hebben banken een zogenaamd spaarslot ontwikkeld. Wanneer het spaarslot wordt geactiveerd, kan er geen geld meer worden overgeboekt van de spaarrekening naar de betaalrekening. Wil een rekeninghouder tóch geld overmaken, dan moet het spaarslot eerst worden uitgeschakeld, waarna een wachttijd van 24 uur ingaat voordat de transactie kan worden uitgevoerd. Deze maatregel is bedoeld om de druk tegen te gaan die daders uitoefenen op slachtoffers. Toch zijn er twee problemen. Ten eerste moet de klant het spaarslot zelf activeren. Daarnaast hebben daders dit soort maatregelen vrij snel door en passen zij hun modus operandi hier vervolgens op aan. In het geval van het spaargeldslot kunnen zij slachtoffers bijvoorbeeld 24 uur aan het lijntje houden of na het verstrijken van deze periode opnieuw contact opnemen. Verder blijkt dat preventieve mogelijkheden, zoals het spaarslot, vaak onvoldoende worden benut door klanten. Dit komt mede doordat klanten zelf de noodzaak ervan niet inzien of de maatregelen als onnodig ervaren.
Tijdens de focusgroep (R21) werd bovendien opgemerkt dat bij vrijwel alle vormen van online fraude social engineering een cruciale rol speelt. Hiertegen is in de optiek van de respondenten weinig te doen: 'Echt effectieve interventies zijn heel lastig' (R21). De delicten zijn vaak zeer geraffineerd en de opbrengsten zijn zo hoog dat daders bereid zijn om veel tijd en moeite te investeren in het manipuleren en overhalen van slachtoffers. Technische interventies kunnen hier vaak weinig tegen doen. Ook preventief zijn er beperkte mogelijkheden, aangezien een enkele waarschuwing veel minder impact heeft dan een fraudeur die vele uren de tijd neemt om het slachtoffer te manipuleren en zijn of haar vertrouwen te winnen:

> *'[Het] gaat gewoon zo geraffineerd en de opbrengsten zijn [zo] hoog, dat ze [cyberdaders] gewoon bereid zijn om [er] heel veel tijd in te steken om zo'n slachtoffer helemaal te hersenspoelen. En daar kun je technisch eigenlijk bijna niks tegen doen. Je kunt er*

preventief heel weinig tegen doen, want een paar keer een slachtoffer waarschuwen is natuurlijk veel minder sterk dan een fraudeur die uren de tijd neemt om zo'n slachtoffer helemaal te hersenspoelen en om te praten en [diens] vertrouwen te winnen.' (R21)

Zelfs wanneer banken vermoeden dat er sprake is van fraude, blijkt het lastig om slachtoffers te overtuigen. In sommige gevallen blijven slachtoffers ontkennen dat zij worden opgelicht – al dan niet in opdracht van de dader – waardoor het voorkómen van schade extra complex wordt.
Interventies die worden toegepast door telecomproviders variëren, afhankelijk van het type delict (R10). Zo wordt het blokkeren van een telefoonnummer als weinig effectief gezien tegen bankhelpdeskfraude, terwijl deze maatregel bij smishing juist wel effectief kan zijn. Bovendien hebben telecomproviders technische maatregelen genomen die het nagenoeg onmogelijk maken om smishing-bommen te versturen (een zeer grote hoeveelheid sms'jes in korte tijd). Personen en telefoonnummers die zijn betrokken bij (cyber)criminaliteit worden geregistreerd op een blocklist, die niet altijd wordt gedeeld met andere telecomproviders. Hoewel het blokkeren van bepaalde personen en telefoonnummers enigszins effectief lijkt te zijn in het verminderen van de hoeveelheid cybercrime, heeft deze maatregel beperkingen. Ten eerste kan de blocklist worden omzeild. Bovendien bestaat het risico dat de verkeerde personen of telefoonnummers worden geblokkeerd, bijvoorbeeld als deze van katvangers of slachtoffers van phishing zijn.
Tot slot wordt ook vanuit de telecomsector voorlichting gegeven met de nadruk op het voorkómen van slachtofferschap (R10). Zo bieden providers via hun website informatie aan over verschillende vormen van cybercrime. De respondenten gaven aan niet te weten of dergelijke preventiemaatregelen effectief zijn, mede doordat cyberdaders hun werkwijze voortdurend kunnen aanpassen. Kleine wijzigingen in deze werkwijze kunnen ertoe leiden dat bestaande voorlichtingscampagnes snel verouderd raken en daardoor minder effectief zijn.
Samenvattend zijn verscheidene actoren monodisciplinair betrokken bij de aanpak van cybercriminele jongeren en jeugdgroepen, variërend van voorlichting en strafrechtelijke vervolging tot het blokkeren van bankrekeningen. Deze interventies zijn doorgaans gericht op individuen en niet delictspecifiek.

Resumé
In dit onderzoek hebben we drie benaderingen geïdentificeerd die momenteel worden gebruikt bij de aanpak van jeugdgroepen die betrokken zijn bij cybercrime. Allereerst een volwaardige integrale aanpak, die we maar in één casus (C1) tegenkwamen: via het RIEC en in samenwerking met de gemeente, de politie, het OM, de Belastingdienst en de Arbeidsinspectie. Ten tweede kan er sprake zijn van een multidisciplinaire samenwerking bij het in kaart brengen van groepen, met een monodisciplinaire uitvoering. Veelal gaat het hierbij om kleinere samenwerkingsverbanden, zoals tussen de politie en de banken en telecomproviders, waarbij vooral sprake is van informatiedeling vanuit

de private actoren naar de politie voor een opsporingsonderzoek. De daadwerkelijke aanpak vindt veelal monodisciplinair plaats door de politie en het OM. Tot slot kan er sprake zijn van monodisciplinaire aanpakken, zoals banken die rekeningen blokkeren en telecomproviders die telefoonnummers blokkeren.
Ons onderzoek laat zien dat integrale kansen vaak onbenut blijven, terwijl een integrale aanpak in potentie een rijker informatiebeeld en een breder palet aan interventiemogelijkheden oplevert. Het meer benutten van bestaande integrale samenwerkingsstructuren voor de aanpak van cybercrime lijkt dan ook wenselijk.
Door (onder voorwaarden) informatie te delen, kan het zicht van lokale partners op cybercriminele jeugdgroepen worden bevorderd. Dit vormt de kern van de meerwaarde van een integrale samenwerking: de aanpak richt zich op de groep en op de activiteiten daarvan als geheel, in plaats van op een specifiek subject en/of delict, zoals bij de uitsluitend strafrechtelijke aanpak veelal het geval is. Daarnaast neemt het interventiepotentieel toe, omdat iedere organisatie over eigen interventiemogelijkheden beschikt. Hierdoor kunnen interventies van verschillende organisaties gelijktijdig worden ingezet en gecombineerd. Of die mogelijkheden ook inzetbaar en effectiever zijn, is nog voer voor discussie.

6.2.2 *Wat zijn verbeterpunten voor de huidige aanpak van cybercriminele jeugdgroepen?*

Op basis van de politieregistraties, de zaakreconstructies en de expertinterviews hebben we meerdere verbeterpunten geïdentificeerd voor de huidige aanpak van cybercriminele jeugdgroepen. Die bespreken we in deze paragraaf.
De kern daarbij is dat meerdere samenwerkingsmogelijkheden onbenut blijven; vooral de meer structurele samenwerkingsverbanden, zoals het RIEC en de jeugdgroepenaanpak. Een mogelijk startpunt van een integrale samenwerking betreft een analyse van politie-informatie. De jeudggroepenaanpak, waarbij gemeenten formeel de regie hebben, vormt de basis van een nauwe en integrale samenwerking met lokale ketenpartners, variërend van zorg- en hulpverleningsinstanties tot toezichthouders en justitiële partijen (R2, R7, R17, R18, R20). In de praktijk maken meerdere gemeenten gebruik van dit model (R1, R2, R3, R7, R18) en meldden experts dat de problematiek rond traditionele criminele jeugdgroepen veelal afnam na de inzet van deze aanpak. De toepassing van de jeugdgroepenaanpak – evenals het daarbij behorende 7-stappenmodel – op cybercriminele jeugdgroepen is niet naar voren gekomen.
De integratie van cybercrime in bestaande samenwerkingsstructuren vergt dat we eerst beter zicht hebben en dus in staat zijn om te signaleren. Daarnaast vraagt het om de ontwikkeling en evaluatie van (beproefde) interventies, zodat ketenpartners handvatten hebben om op te treden tegen deze vorm van (groeps)criminaliteit die voor hen veelal nog onbekend is. Hierbij nemen we de interventies in acht die al bekend zijn vanuit de literatuur, maar die in de praktijk nog niet of nauwelijks bekend zijn of worden ingezet.

Herkennen en delen van cybercrime-gerelateerde signalen

Om het zicht op cybercriminele jeugdgroepen te verbeteren, moeten praktijkprofessionals bekwaam zijn in vroegtijdig signaleren en proactief optreden (R1, R4, R5, R12, R20). Vroegsignalering richt zich op het tijdig identificeren van jongeren die een verhoogd risico lopen op betrokkenheid bij cybercrime. Een proactieve aanpak betekent dat ketenpartners niet wachten tot jongeren daadwerkelijk in aanraking komen met justitie, waarbij de nadruk ligt op het voorkómen van cybercrime. Vooral binnen de politie en de gemeenten ligt hier een belangrijke taak.

Op dit moment is de aanpak vaak nog reactief: pas wanneer jongeren strafbare feiten plegen, worden er interventies ingezet. Volgens de respondenten is deze werkwijze onvoldoende effectief bij cybercrime. Zij hebben de hoop dat de aanpak in de toekomst verschuift naar een proactieve strategie, waarbij niet alleen cybercrime wordt verminderd, maar ook gerelateerde feiten en problemen worden aangepakt.

Om de betrokkenheid van jongeren bij cybercrime in een vroeg stadium te kunnen signaleren en om proactief op te kunnen treden, hebben praktijkprofessionals kennis en inzicht nodig op het gebied van cybercrime. Beide lijken volgens de respondenten echter veelal te ontbreken. Het is daarom van belang dat de kennis van praktijkprofessionals (zoals politieagenten en jongerenwerkers) over het signaleren van cybercrime wordt vergroot (R8, R19).

Dergelijke scholing kan bestaan uit het delen van een lijst met indicatoren voor een mogelijke betrokkenheid bij cybercrime. Een voorbeeld hiervan is het dragen van dure merkkleding door jongeren die zich dit ogenschijnlijk niet kunnen veroorloven gezien hun financiële situatie (R15, R22). Tijdens doorzoekingen zouden politieagenten bijvoorbeeld niet alleen moeten letten op drugs of wapens, maar ook op materiële zaken die niet passen bij de financiële situatie van de verdachte én op de aanwezigheid van meerdere pinpassen, simkaarten of apparaten voor internetbankieren (zoals een Raboscanner). Omdat binnen deze context ook sprake kan zijn van nepkleding, is kennis hierover eveneens noodzakelijk.

Naast deze fysieke signalen moet er ook meer aandacht worden besteed aan signalen die te identificeren zijn op sociale media. Jongerenwerkers mogen bijvoorbeeld de online accounts van jongeren volgen, inclusief privéaccounts (R17). Hun rol hierbij is vooral signalerend, zonder dat er sprake is (systematische) monitoring. Met aanvullende trainingen voor het gebruik van sociale media (zoals Snapchat en TikTok) en het leren herkennen van signalen van (cyber)criminaliteit zouden zij deze media gerichter kunnen raadplegen. Ook bestaat de behoefte aan een extra inzet van digitale jongerenwerkers en digitale wijkagenten (R3, R8, R15, R17, R19, R22):

> *'We zijn wel bezig geweest (…) met het opleiden van digitale jongerenwerkers of de digitale wijkagent (…). Nou ja, dus hij is hier op zoek bij de politie naar een nieuwe, echt goede digitale wijkagent. Daar is wel grote behoefte aan.' (R3)*

Signalen moeten niet alleen worden herkend, maar ook efficiënt worden gedeeld tussen de lokale actoren (R4, R5, R7, R8, R9, R12, R14, R18). Een betere samenwerking

tussen gemeenten, banken en telecomproviders, waarbij signalen sneller kunnen worden gedeeld, kan bijvoorbeeld helpen om cybercriminele jongeren en jeugdgroepen te identificeren en aan te pakken.
Ook de samenwerking en uitwisseling van signalen tussen de politie en de gemeenten kan worden verbeterd (R12). Een concreet probleem is de bureaucratische werkwijze, waarbij een politierapport eerst via het OM naar de gemeente gaat. Dit proces kost tijd en zorgt ervoor dat de gemeente niet altijd direct kan handelen op basis van signalen uit het veld. Deze vertragingen belemmeren de effectiviteit van de aanpak en dat vraagt om betere afstemming en snellere informatiedeling.
Daarnaast kan de samenwerking tussen basisscholen, middelbare scholen, jongerenwerkers, de politie en gemeenten worden versterkt. Op scholen signaleren docenten problematisch en crimineel gedrag bij leerlingen, maar zij weten vaak niet goed bij welke instantie zij deze signalen kunnen melden. Door een nauwere samenwerking en door signalen sneller en gerichter te delen, kunnen problematische situaties eerder worden gemeld, waardoor de betrokken partijen sneller kunnen handelen. Dit kan mogelijk worden gerealiseerd door het aanstellen van laagdrempelige, centrale aanspreekpunten binnen bijvoorbeeld de gemeente of de politie. Hierdoor wordt het voor scholen en andere partijen eenvoudiger om zorgen te melden, en ontstaat er sneller een compleet beeld van de situatie rondom een jongere of groep jongeren.
Ook banken benadrukken de noodzaak van betere samenwerking en signaaluitwisseling, met name om jongeren te beschermen tegen de ronseling als geldezel (R9). Een concreet voorstel is om nauwer samen te werken met sociale wijkteams. Die hebben beter zicht op jongeren die mogelijk kwetsbaar zijn voor of al betrokken zijn bij geldezelactiviteiten. Door samen te werken en informatie uit te wisselen, kan gerichter worden ingezet op het voorkómen dat bijvoorbeeld (potentiële) geldezels onderdeel worden van een cybercriminele groep. Een belangrijke kanttekening hierbij is dat de uitwisseling van gegevens tussen banken en sociale wijkteams op dit moment juridisch niet is toegestaan. Dit vormt een belemmering voor een effectievere gezamenlijke aanpak.

Ontwikkelen, verbeteren en evalueren van interventies
Ten tweede is het noodzakelijk om nieuwe interventies te ontwikkelen en deze (net als al bestaande interventies) te evalueren, zodat ketenpartners handvatten hebben om op te treden tegen vormen van (groeps)cybercriminaliteit die voor hen veelal nog onbekend zijn.
Allereerst is er behoefte aan interventies die specifiek gericht zijn op verschillende groepen binnen cybercriminele groepen, zoals kernleden en geldezels (R18). Deze groepen vragen om maatwerk in de aanpak. Op dit moment wordt daar nog onvoldoende onderscheid in gemaakt, terwijl een gerichte benadering per type lid mogelijk effectiever kan zijn. Bovendien bestaat er bij zowel de mono- als multidisciplinaire aanpak een gebrek aan handelingsperspectief: actoren weten niet in hoeverre traditionele interventies toepasbaar zijn. Daarnaast zijn specifieke interventies onbekend of niet voorhanden en is er (daardoor) sprake van handelingsverlegenheid.

Daarnaast is het van belang om het resocialisatieproces te verbeteren van jongeren die zich schuldig hebben gemaakt aan cybercrime (R6). Deze jongeren plegen vaak ernstige, strafbare feiten, waaronder diefstal met een valse sleutel, computervredebreuk, witwassen en het bezit van phishingsoftware en leads. Om te voorkomen dat deze jongeren na hun vrijlating opnieuw vervallen in (cyber)criminaliteit, is het van belang om tijdens de detentie al te investeren in hun toekomstperspectief (speciale preventie). Zo zouden gedetineerde cyberdaders de mogelijkheid moeten krijgen om opleidingen te volgen die aansluiten bij hun vaardigheden. Een deel van deze jongeren beschikt al over digitale vaardigheden, zoals het schrijven van codes. Door deze vaardigheden op een positieve manier in te zetten, kan hun talent worden benut en kan de kans op recidive worden verkleind. Dit is mogelijk niet voor iedere jongere effectief. Het aanleren van ICT-gerelateerde kennis en vaardigheden zou juist tot een hogere kans op recidive kunnen leiden. Dergelijke interventies blijven daardoor altijd maatwerk.
Ook moeten interventies (beter) worden geëvalueerd (R18). Enerzijds is er behoefte aan meer inzicht in de effectiviteit van individuele interventies, anderzijds aan de evaluatie van de jeugdgroepenaanpak om zicht te houden op de groep én om die te ontmantelen. Door systematisch te evalueren welke maatregelen zijn toegepast en wat het effect daarvan was op een (cyber)criminele jeugdgroep, kan een beter beeld worden verkregen van de effectiviteit van een aanpak. Een goede evaluatie maakt zichtbaar welke jongeren nog steeds deel uitmaken van de jeugdgroep en welke jongeren succesvol zijn uitgestroomd. Op basis hiervan kunnen ketenpartners bepalen of aanvullende maatregelen nodig zijn. Daarnaast biedt een grondige evaluatie de mogelijkheid om te onderzoeken in hoeverre iedere instantie de juiste maatregelen heeft geïmplementeerd.

6.2.3 *Wat zijn de best practices uit de (integrale) aanpak van cybercriminele jeugdgroepen?*

Naast de eerder benoemde verbeterpunten zijn binnen de (integrale) aanpakken van cybercriminele jeugdgroepen ook best practices te identificeren.
Uit zaakreconstructie C1 komt naar voren dat de samenwerking met verschillende partners aanzienlijke voordelen biedt. Ten eerste beschikt iedere partner over unieke informatiebronnen. Door deze te combineren, ontstaat een vollediger beeld van de groep dan wanneer actoren afzonderlijk opereren. Ten tweede vergemakkelijkte het onderbrengen van deze specifieke casus bij het RIEC de uitwisseling van persoonsgegevens, wat cruciaal is om de groep in kaart te brengen. Tot slot beschikt elke partner over eigen bevoegdheden en instrumenten. Door deze gecoördineerd in te zetten, kunnen verschillende onderdelen van de groep worden aangepakt, wat de kans op verstoren vergroot. Het opzetten van structurele samenwerkingsverbanden op basis van bijvoorbeeld convenanten zou dus van (grote) meerwaarde kunnen zijn bij het effectief aanpakken van cybercriminele jeugdgroepen.
De drie hierboven beschreven voordelen zijn ook zichtbaar in de samenwerkingen die zijn gericht op traditionele criminaliteit. Respondenten die bij gemeenten werken, benadrukten het belang van een intensieve en structurele samenwerking tussen keten-

partners (R2). Elke partner brengt zijn eigen perspectief, observaties en informatie in, wat bijdraagt aan een completer beeld van de jeugdgroep en het individuele gedrag van jongeren. Zo signaleren de politie en de jeugdboa's ander gedrag dan bijvoorbeeld de schoolmaatschappelijk werkers. Een concreet voorbeeld van deze samenwerking werd genoemd in het interview met het OM:

> *'En andersom, als er een zittingsdatum bekend is, dan (…) willen [we] net voor of juist net na zo'n zittingsdatum (…) [dat] iemand van het jongerenwerk even checkt bij die jongeren (…) lukt het om daar alleen heen te gaan, (…) kan ik je ondersteunen?' (R18)*

Een ander voorbeeld van een structurele samenwerking is een maandelijks overleg waarin meldingen van de politie, scholen, jongerenwerkers en handhaving worden besproken (R1, R3). In deze overleggen wordt stilgestaan bij actuele overlastlocaties en overlastgevende jeugd, zonder direct identificerende persoonsgegevens te delen. Aan deze overleggen kunnen onder andere gemeenten, handhaving, de politie, jongerenwerkers, verslavingszorg, noodhulpverlening en eventueel ook leerplichtambtenaren deelnemen. Daarnaast had één gemeente een 'convenant Jeugd' opgesteld, waarin werd samengewerkt met verschillende partners. Hierdoor was het mogelijk om niet-identificerende gegevens vrij tussen partners uit te wisselen (R3).
Een samenwerking tussen een gemeente en leerplichtambtenaren werd besproken in het interview met R2:

> *'We hadden een tijdje geleden een jongere, die werd de hele tijd ziekgemeld door z'n moeder. Dat is natuurlijk altijd ingewikkeld, dat is luxeverzuim. Leerplicht zag vervolgens dat deze jongere op straat was, want we hebben met z'n allen [een] straatcontact-app, waarin dat werd gedeeld. (…) En dan kan [de] leerplicht zeggen 'dit is dus niet oké (…) hij hoort ziek te zijn'. [Vervolgens hebben we] direct hem en zijn moeder gebeld (…). We mogen dat dan ook met elkaar delen, omdat je dat ook kenbaar hebt gemaakt aan de jongeren en aan ouders.' (R2)*

Het 7-stappenmodel, dat voor zover bekend nog niet is toegepast op een cybercriminele jeugdgroep, werd door respondenten een waardevolle leidraad genoemd (R2, R18). Zij ervaren dat het model effectief lijkt te zijn in het verminderen van de problematiek rond problematische en criminele jeugdgroepen. Verder wordt het model gezien als logisch en biedt het helderheid over de privacy, de voortgang van de stappen en de voorwaarden voor het delen van informatie. Ook ervaren respondenten het model als flexibel door de mogelijkheid om (indien nodig) van het model af te wijken. Tot slot bleek dat er, als een specifieke groep is geprioriteerd door de lokale driehoek, een juridische grondslag is[25] om de persoonsgegevens van individuele groepsleden snel en eenvoudig te delen tussen de partners binnen de jeugdgroepenaanpak. Hoewel deze

25 Door samenwerkingsconvenanten en de Wet gegevensverwerking door samenwerkingsverbanden (WGS).

best practices terug te zien zijn binnen de aanpak van jeugdgroepen die betrokken zijn bij traditionele criminaliteit, kunnen deze maatregelen ook voordelig zijn bij de aanpak van cybercriminele jeugdgroepen.

6.2.4 *In hoeverre kunnen interventies die zich richten op jeugdige cyberdaders bijdragen aan de aanpak van cybercriminele jeugdgroepen?*

In de praktijk richten interventies bij cybercrime zich veelal op individuele (jeugdige) cyberdaders. Ook in de integrale RIEC-aanpak lag de focus grotendeels op individuele groepsleden, ondanks de samenwerking tussen verschillende actoren. Een belangrijk voordeel van deze aanpak is dat de groep vanuit meerdere kanten wordt aangepakt en dat interventies zich richten op meerdere leden tegelijk. Dit zou een verstoring van de groep als geheel kunnen hebben veroorzaakt, maar dit effect is niet onderzocht en blijft daarmee onduidelijk.
Naast deze integrale aanpak zijn meerdere monodisciplinaire aanpakken geïdentificeerd. De meest voorkomende waren (1) strafrechtelijke vervolging door de politie en het OM; (2) het blokkeren van bankrekeningen door banken; en (3) het blokkeren van telefoonnummers door telecomproviders. Hoewel deze interventies primair gericht zijn op individuen, is het mogelijk dat ze indirect invloed hebben op het functioneren van de groep als geheel (R11).
Het vervolgen van leden kan bijvoorbeeld verstorend werken en heeft mogelijk een afschrikkend effect op andere leden (generale preventie). Tegelijkertijd lijkt het effect beperkt. Niet alle leden zijn gevoelig voor afschrikking, groepen zijn fluïde en dynamisch, waardoor groepsleden eenvoudig vervangen kunnen worden, en er zijn meerdere casussen gevonden waarin verdachten na (of zelfs tijdens) het uitzitten van hun vrijheidsstraf actief bleven in de (cyber)criminaliteit, wat wijst op een beperkt effect van speciale preventie (R4, R6, R8, R19).
De interventies vanuit banken en telecomproviders richten zich veelal op geldezels en katvangers. Alhoewel dit op korte termijn mogelijk een verstorend effect heeft op het functioneren van een groep (het witwassen van wederrechtelijk verkregen voordeel wordt immers bemoeilijkt), lijkt het langetermijneffect beperkt te zijn. Door de dynamiek van groepen kunnen individuele leden eenvoudig worden vervangen en worden voortdurend nieuwe geldezels en katvangers gerekruteerd. Bovendien maken groepen steeds vaker gebruik van buitenlandse bankrekeningen en cryptowallets, waarmee blokkades worden omzeild.
In de literatuurstudie zijn meerdere aanpakken aan bod gekomen, waaronder het 7-stappenmodel, de PlusMinMee-methodiek (beide onderdeel van de jeugdgroepenaanpak), Preventie met Gezag, de TopX-aanpak, repressieve maatregelen, de RIEC-aanpak en de integrale aanpak online fraude. In dit onderzoek hebben we één casus beschreven die gebaseerd is op de RIEC-aanpak. Daarnaast zijn meerdere situaties geïdentificeerd waarin repressieve maatregelen zijn toegepast. De overige interventies zijn niet of nauwelijks bekend en worden daardoor ook niet toegepast. Dit maakt het

ingewikkeld om aan te geven in hoeverre interventies bij jeugdige cyberdaders bijdragen aan de aanpak van cybercriminele jeugdgroepen.
Samenvattend kunnen interventies bij individuele jeugdige cyberdaders bijdragen aan het verstoren van de groep als geheel, maar dit lijkt beperkt te blijven tot de korte termijn. Door de dynamiek van groepen en de vervangbaarheid van individuele leden lijkt het effect op de lange termijn beperkt te blijven. Structurele en groepsgerichte aanpakken en interventies (zoals in zaakreconstructie C1) lijken meer potentie te hebben, maar vereisen wel een verdere evaluatie om hun effectiviteit nader vast te stellen.

6.3 Resumé

In dit hoofdstuk hebben we beschreven in hoeverre partners zicht hebben op jeugdgroepen die betrokken zijn bij cybercrime en hoe de aanpak van deze groepen kan worden versterkt. Lokale veiligheidscoalities, onder regie van gemeenten, hebben geen zicht op cybercriminele jeugdgroepen. Dit komt enerzijds doordat zij te sterk leunen op straatinformatie en anderzijds doordat ze over onvoldoende kennis beschikken om cyberdaders te identificeren. Strafrechtelijke partners (vooral de politie en het OM) hebben meer zicht, mede dankzij de informatie uit aangiftes en data-analyses, terwijl ze minder afhankelijk zijn van straatinformatie. Actoren zoals banken en telecomproviders verrijken het beeld van de politie en het OM. Jeugdgroepen worden veelal echter beperkt in kaart gebracht – het blijft vooral bij het laaghangend fruit, zoals geldezels of pinners. Data om een groep beter in kaart te brengen lijken er echter wel te zijn, zo laten de vijf zaakreconstructies zien. Het betreft hier grote onderzoeken, boven het basisteam-niveau, waarbij meerdere kernleden geïdentificeerd zijn. Dergelijke onderzoeken vergen echter veel capaciteit, die op dit moment beperkt voorhanden is.
Wat betreft de aanpak van jeugdgroepen die betrokken zijn bij cybercrime, hebben we drie benaderingen geïdentificeerd. De eerste is de integrale aanpak, waarbij meerdere lokale actoren samenwerken. Ondanks het feit dat dit beperkt lijkt voor te komen, lijken dergelijke structurele en groepsgerichte aanpakken potentie te hebben, maar vereisen ze wel een verdere evaluatie om hun effectiviteit nader vast te stellen. De tweede benadering is tweedelig: een beperkt aantal actoren werkt samen bij informatie-uitwisseling en de identificatie van jeugdgroepen, terwijl interventies veelal door één actor worden geïmplementeerd. De derde en meest voorkomende benadering is monodisciplinair: actoren opereren afzonderlijk, zonder structurele samenwerking. Deze aanpak is gefragmenteerd en richt zich vooral op generieke maatregelen, zoals strafrechtelijke vervolging door de politie en het OM, het blokkeren van bankrekeningen door banken en het blokkeren van telefoonnummers door telecomproviders. Hoewel deze interventies primair gericht zijn op individuen en niet delictspecifiek zijn, kunnen ze de groep (tijdelijk) verstoren en een afschrikwerkend effect hebben. Dit effect lijkt echter beperkt tot de korte termijn, en lijkt een beperkte impact te hebben op de hele groep door de fluïditeit en dynamiek van deze groepen en door de vervangbaarheid van groepsleden.

Binnen de aanpak van cybercriminele jeugdgroepen zijn meerdere verbeterpunten gevonden. Dit betreft de integratie van cybercrime aanpakken in bestaande samenwerkingsconstructies, zoals het RIEC en de jeugdgroepenaanpak. Integrale samenwerking biedt de mogelijkheid om zowel de scope van het onderzoek (de informatievergaringsfase) als de interventies te verbreden, mogelijk met politie-informatie als startpunt. Omdat praktijkprofessionals onvoldoende kennis en inzicht hebben op het gebied van cybercrime, is het belangrijk om scholing aan te bieden, zoals het delen van een lijst met indicatoren die kunnen wijzen op betrokkenheid bij cybercrime. Daarnaast is het essentieel om interventies te ontwikkelen en te evalueren die zich specifiek richten op cybercrime én op cybercriminele jeugdgroepen. Daarbij is er enerzijds behoefte aan meer inzicht in de effectiviteit van individuele interventies; anderzijds aan de evaluatie van de jeugdgroepenaanpak voor wat betreft het zicht houden op de groep en de ontmanteling daarvan.

7 Conclusie en discussie

In dit hoofdstuk presenteren we de conclusie en de discussie van het onderzoek. Het hoofdstuk volgt de drie verschillende sporen: jeugdgroepen die bij lokale veiligheidscoalities bekend zijn (spoor 1), cybercriminele jeugdgroepen die bij lokale veiligheidscoalities onbekend zijn (spoor 2) en de integrale aanpak van (cyber)criminele jeugdgroepen (spoor 3). Waar relevant, worden onze conclusies geduid aan de hand van theoretische implicaties. Zo kunnen de resultaten in de context van voorgaande literatuur worden geplaatst en deels worden geïnterpreteerd.
Op basis van dit onderzoek kunnen we concluderen dat gemeenten de spil zijn in de aanpak van criminele jeugdgroepen. Hun zicht op traditionele groepen neemt af, en zicht op hybride of cybercriminele jeugdgroepen hebben ze niet. Dat is problematisch, want zonder zicht op zulke groepen kunnen zij geen invulling geven aan de (integrale) aanpak ervan.
Tegelijkertijd zijn er in de regio talloze cybercriminele jeugdgroepen actief. Daarin zijn twee varianten te onderscheiden: hybride groepen (die zowel traditionele criminaliteit als cybercrime plegen) en groepen die zich uitsluitend bezighouden met cybercrime. Opvallend is dat deze groepen, net als traditionele groepen, voor hun ontstaan en groei nog steeds sterk afhankelijk zijn van lokaal verankerde traditionele relaties. Kernleden kennen elkaar bijvoorbeeld van school of uit de buurt. Hun activiteiten hebben bovendien hun uitwerking op de lokale openbare orde en veiligheid. Denk aan geweldsincidenten en het etaleren van status en macht. Kortom, we zien mogelijkheden en een noodzaak om het zicht van gemeenten op cybercriminele jeugdgroepen te verbeteren. Zij zijn immers de regievoerders in de aanpak daarvan.
In de huidige rechtshandhavingspraktijk is integraal samenwerken bij de aanpak van cybercriminele jeugdgroepen echter een zeldzaamheid. Actoren voeren monodisciplinair interventies uit of richten gelegenheidssamenwerkingen op. Structurele samenwerkingsverbanden zoals het RIEC of de jeugdgroepenaanpak blijven grotendeels onbenut. In de wetenschap dat de strafrechtelijke aanpak van cybercrime vooralsnog voor verbetering vatbaar is en per definitie onvoldoende recht doet aan de omvang van de problematiek in de samenleving, is het beter benutten van samenwerkingskansen wenselijk.

7.1 Spoor 1: jeugdgroepen die bekend zijn bij lokale veiligheidscoalities

Het eerste spoor richt zich op de (cyber)criminele jeugdgroepen die bekend zijn bij lokale veiligheidscoalities. We bespreken achtereenvolgens welke groepen dit precies

zijn, wat hun structuur en samenstelling is, hoe zij ontstaan en groeien, wat de kenmerken van individuele leden zijn en wat de aard is van de delicten waar deze groepen zich mee bezighouden.

7.1.1 *Welke (cyber)criminele jeugdgroepen zijn bekend bij lokale veiligheidscoalities binnen Noord-Nederland?*

De jeugdgroepen die bekend zijn bij lokale veiligheidscoalities hebben we in kaart gebracht, dit aan de hand van expertinterviews met gemeentemedewerkers. Ook hebben we een uitvraag gedaan bij de 40 gemeenten in Noord-Nederland met de vraag of zij jeugdgroepen in beeld hebben. Op onze vraag werd gereageerd door 25 gemeenten. Daarvan gaven er 10 aan dat zij één of meer groepen kennen, waarvan 9 gemeenten ook de identificerende gegevens hebben aangeleverd. Dit resulteerde in informatie over 13 bij gemeenten bekende groepen en 4 individuen die onderdeel zijn van een groep die vooralsnog onbekend is bij de gemeente. In totaal zijn 207 jeugdigen geïdentificeerd.
Uit de interviews en de uitvraag bij de gemeenten is gebleken dat lokale veiligheidscoalities (onder regie van gemeenten) vooral zicht hebben op jeugdgroepen die betrokken zijn bij traditioneel problematisch en/of crimineel gedrag. Geen enkele Noord-Nederlandse gemeente heeft expliciet zicht op een cybercriminele jeugdgroep. Dit lijkt vooral te komen doordat de informatieverzameling in de lokale veiligheidspraktijk nog sterk leunt op straatinformatie en signalen uit de wijk, terwijl aanwijzingen voor cybercrimineel handelen niet of nauwelijks te constateren zijn in het fysieke domein. In enkele gevallen waren er vermoedens van cybercriminele activiteiten binnen jeugdgroepen, maar concreet bewijs hiervoor ontbrak.

7.1.2 *Wat zijn de kenmerken van bekende (cyber)criminele jeugdgroepen?*

De data om deze deelvraag te beantwoorden zijn verkregen via de expertinterviews. Omdat experts vaak slechts beperkt zicht hadden op de kenmerken van groepen en mogelijk invullingen, interpretaties, of aannames hebben gedaan die niet volledig overeenkomen met de feitelijke situatie, is het geschetste beeld niet noodzakelijk volledig of sluitend. Het weerspiegelt enkel de kennis die door respondenten kon worden aangedragen. Bij de interpretatie van de resultaten dient hiermee rekening te worden gehouden.
De kenmerken van de jeugdgroepen die bij lokale veiligheidscoalities bekend zijn, hebben we opgedeeld in ‘structuur en samenstelling’ (aantal leden, rollen binnen de groep, mate van hiërarchie, gebruik van facilitators) en ‘ontstaan en groei’ (online en offline ontmoetingsplaatsen, banden tussen leden). Binnen iedere sectie beginnen we met een beschrijving van de empirische resultaten, gevolgd door een koppeling naar de literatuur om zo een vollediger beeld te geven.

7.1.2.1 *Structuur en samenstelling*

Uit de expertinterviews komt naar voren dat er slechts beperkt zicht was op de precieze structuur en samenstelling van traditionele criminele jeugdgroepen. Deze variëren in grootte van 4 tot 40 leden en zijn dynamisch van aard, waarbij de omvang per dag kan verschillen. De kern, die relatief stabiel is, bestaat doorgaans uit 3 tot 15 kernleden. Deze hebben veelal een leidinggevende rol en sturen ondergeschikte leden aan. De buitenste lagen van traditionele criminele jeugdgroepen zijn meer fluïde en bestaan vooral uit meelopers. Dit zijn nagenoeg altijd minderjarigen die taken uitvoeren in opdracht van kernleden. Naarmate zij ouder worden, kunnen ze doorgroeien binnen de groep. Hoewel de resultaten van dit onderzoek (deels) gebaseerd zijn op de beperkte kennis van de respondenten, sluiten ze aan bij eerdere literatuur over zowel traditionele (jeugd)groepen als cybercriminele groepen (Beke et al., 2000; Esbensen & Weerman, 2005; Ferwerda et al., 2017; Ferwerda & Van Ham, 2011; Peeters & Dongen, 2022; RIEC, 2022; Van Gemert, 2005).

7.1.2.2 *Ontstaan en groei*

Uit de expertinterviews blijkt ook dat de ontstaans- en groeiprocessen beperkt zichtbaar waren voor respondenten. Over hoe en wanneer deze groepen ontstaan is weinig bekend. Op basis van de empirische resultaten lijkt een deel van de traditionele criminele jeugdgroepen te ontstaan vanuit een 'normale' jongerengroep. In eerste instantie gaat het hierbij om jongeren die samen rondhangen, maar gaandeweg sluiten daarbij jongeren aan die al strafbare feiten hebben gepleegd. Naast deze langzame 'overname' van een jeugdgroep, kunnen jongeren zich ook uit eigen initiatief aansluiten bij bestaande jeugdgroepen of actief worden gerekruteerd door groepsleden.

Deze bevindingen sluiten aan bij eerder onderzoek, waarin eveneens wordt beschreven dat jongeren veelal geleidelijk toetreden tot criminele groepen, al dan niet via geplande rekrutering, ongeplande rekrutering, en uit eigen initiatief (Adamse et al., 2024; CCV, 2022; Programma Straatwaarde(n), 2020; RIEC, 2022). In de literatuur wordt eveneens beschreven dat in sommige gevallen jongeren onder druk worden gezet, of worden bedreigd of afgeperst om zich bij een groep aan te sluiten (Programma Straatwaarde(n), 2020)

Offline relaties (zoals vriendschaps- en familiebanden) en fysieke ontmoetingsplekken (waaronder de straat, scholen, sportverenigingen en buurten) spelen bij het betrokken raken bij criminele jeugdgroepen een belangrijke rol (Ferwerda et al., 2017). Tegelijkertijd lijken de ontstaans- en groeiprocessen van traditionele criminele jeugdgroepen meer hybride te zijn geworden, waarbij naast offline relaties ook online ontmoetingsplekken een rol lijken te spelen. De literatuur besteedt hier ook aandacht aan: virtuele settings (in de vorm van online platforms, zoals Telegram, Snapchat, Instagram, en TikTok) worden een steeds belangrijkere ontmoetingsplaats (Bekkers et al., 2022; Bekkers & Leukfeldt, 2023; RIEC, 2022; Wolsink et al., 2023). Via deze contacten ontstaan vervolgens relaties die uiteindelijk leiden tot het ontstaan van criminele jeugdgroepen (RIEC, 2022; Wolsink et al., 2023).

In dit onderzoek blijft de rol van virtuele settings bij traditionele criminele jeugdgroepen echter beperkt. Op basis van de expertinterviews lijken offline banden en fysieke ontmoetingsplekken, zoals vriendschapsrelaties en school, verreweg het belangrijkst te zijn bij de vorming van traditionele criminele jeugdgroepen.

7.1.2.3 *Demografische kenmerken*

Uit de expertinterviews komt naar voren dat traditionele criminele jeugdgroepen vooral bestaan uit jongeren en jongvolwassenen tussen de 8 en 29 jaar. Deze groepen kunnen worden ingedeeld in twee categorieën, op basis van leeftijd:

1. Groepen die uitsluitend uit minderjarigen bestaan.
2. Groepen met zowel minderjarigen als volwassenen.

In beide groepen is de meerderheid van de leden man, maar ook meisjes en vrouwen kunnen betrokken zijn. Leden komen uit alle lagen van de samenleving; hun etnische achtergrond is divers, evenals hun opleiding, thuissituatie en sociaaleconomische status. Tot slot hebben sommige jongeren een zorgachtergrond.

Deze bevindingen wijken enigszins af van het beeld dat uit de literatuur naar voren komt. Daarin wordt een meer eenduidig profiel geschetst: jongeren die betrokken zijn bij georganiseerde criminaliteit zijn relatief vaak man (Calderoni et al., 2022; De Boer et al., 2022), hebben vaker schoolproblemen en een lager opleidingsniveau (Beke et al., 2013; Calderoni et al., 2020, 2022; CCV, 2022; Frualdo, 2019; Peeters & Dongen, 2022; Programma Straatwaarde(n), 2020; RIEC, 2022; Weerman, 2014) en hebben relatief vaak een lagere sociaaleconomische status of behoren tot een etnische minderheid (Beke et al., 2000, 2013; Calderoni et al., 2022; De Boer et al., 2022; Kleemans & Van Koppen, 2020; Programma Straatwaarde(n), 2020). Kortom, waar de literatuur een meer geconcentreerd risicoprofiel schetst, komt uit de empirische resultaten van dit onderzoek naar voren dat er een bredere variatie is in achtergrondkenmerken. Hierbij is het wel belangrijk om op te merken dat deze bredere variatie mogelijk het gevolg is van invullingen, interpretaties, en aannames van de respondenten.

7.1.2.4 *Criminele carrière*

Op basis van de expertinterviews kunnen leden grofweg in twee groepen worden verdeeld als het gaat om hun criminele carrière:

1. First offenders: vooral de jongere leden.
2. Recidivisten: vaak oudere, meerderjarige leden die al eerder in beeld zijn geweest bij politie en justitie voor delicten als mishandeling en winkeldiefstal.

Deze bevindingen sluiten aan bij eerder onderzoek door het RIEC, waaruit naar voren komt dat jongeren in Nederland vaak al op jonge leeftijd betrokken raken bij traditionele criminele (jeugd)groepen. Veel jongeren plegen al vóór hun 15e levensjaar lichte delicten, zoals winkeldiefstal. Voor een klein deel van de jongeren geldt dat ze, naarmate ze ouder worden, juist zwaardere delicten gaan plegen en geleidelijk doorgroeien binnen de georganiseerde criminaliteit (RIEC, 2022).

7.1.2.5 *Motivaties*

Volgens de geïnterviewde experts is een van de belangrijkste motivaties voor jongeren betrokken bij traditionele criminele jeugdgroepen het snel willen verdienen van geld. Dit is ook gevonden in eerder onderzoek naar jongeren betrokken bij traditionele criminele (jeugd)groepen in Nederland.
Daarnaast speelden statusverwerving en de behoefte om ergens bij te horen een belangrijke rol volgens de respondenten. Deze drie motivaties worden ook beschreven in eerder onderzoek naar jongeren betrokken bij traditionele criminele (jeugd)groepen in Nederland (CCV, 2022; De Boer et al., 2022; Programma Straatwaarde(n), 2020; RIEC, 2022). Daarbij is het mogelijk dat ook andere motivaties een rol spelen waar respondenten geen zicht op hebben.

7.1.3 *De aard van de delicten waarmee bekende (cyber)criminele jeugdgroepen zich bezighouden*

Uit de expertinterviews blijkt dat traditionele criminele jeugdgroepen die in beeld zijn bij lokale veiligheidscoalities zich voor zover bekend uitsluitend bezighouden met traditionele criminaliteit. Ze vertonen een combinatie van problematisch en crimineel gedrag en zijn betrokken bij diverse delicten:

1. Overlastgevend gedrag: rondhangen, geluidsoverlast, vuurwerkoverlast.
2. Geweldsmisdrijven: intimidatie, afpersing, mishandeling, berovingen, wapenbezit.
3. Vermogensdelicten, zoals scooterdiefstal.
4. Drugsdelicten, zoals het dealen van verdovende middelen.
5. Vernielingen en misdrijven tegen de openbare orde: ruiten ingooien, mensenhandel.

Deze bevindingen sluiten aan bij de resultaten van de Monitor Zelfgerapporteerde Jeugddelinquentie. De monitor biedt bovendien inzicht in de frequentie van het delictgedrag: geweldsdelicten lijken het vaakst voor te komen onder jongeren en jongvolwassenen, gevolgd door vermogensdelicten, vandalisme, wapenbezit, en ten slot drugsverkoop (Tollenaar et al., 2024). Daarnaast bevestigen onze resultaten eerder onderzoek naar Nederlandse criminele jeugdgroepen, waarin ook wordt gerapporteerd dat deze groepen betrokken zijn bij overlast, drugshandel, geweldsdelicten, en vermogensdelicten (Beke et al., 2000, 2013; Beke & Van Wijk, 2001).

7.2 Spoor 2: cybercriminele jeugdgroepen die onbekend zijn bij lokale veiligheidscoalities

Het tweede spoor richt zich op cybercriminele jeugdgroepen die nog onbekend zijn bij lokale veiligheidscoalities. De resultaten zijn gebaseerd op de expertinterviews (n = 13), de zaakreconstructies (n = 5) en de analyse van politieregistraties, waarin we 109 cybercrime-verdachten en 26 cybercriminele jeugdgroepen hebben geïdentificeerd. We bespreken achtereenvolgens welke groepen dit zijn, wat hun structuur en

samenstelling is, hoe ze zijn ontstaan en groeien, wat de kenmerken van individuele leden zijn en wat de aard is van de delicten waar deze groepen zich mee bezighouden. Het is belangrijk om hier te benadrukken dat alle groepen die we in dit onderzoek hebben beschreven betrokken zijn bij financiële cybercrime, zoals phishing, bankhelpdeskfraude, aan- en verkoopfraude, smishing en sextortion. De hier beschreven groepen daderkenmerken hebben dan ook specifiek betrekking op deze groep.

7.2.1 *Zijn er nieuwe cybercriminele jeugdgroepen actief binnen Noord-Nederland die onbekend zijn bij lokale veiligheidscoalities?*

Uit de expertinterviews en de uitvraag onder 40 Noord-Nederlandse gemeenten blijkt dat geen enkele gemeente zicht heeft op cybercriminele jeugdgroepen. Hoewel er soms wel vermoedens zijn van betrokkenheid bij cybercrime, ontbreekt het vooralsnog aan concrete aanwijzingen.
De analyse van politieregistraties laat zien dat er in de periode van 1 september 2022 tot 30 september 2023 in totaal 109 verdachten en 26 groepen zijn geïdentificeerd die betrokken zijn bij cybercrime in Noord-Nederland. Van deze 109 verdachten waren er 4 ook bij gemeenten in beeld vanwege betrokkenheid bij traditionele criminele jeugdgroepen. Daarnaast zijn er 9 personen die door gemeenten zijn geïdentificeerd als betrokkenen bij traditionele criminele jeugdgroepen, en die niet direct verdacht worden van cybercrime, maar wel een relatie hebben met iemand die daarvan wordt verdacht. Dit beeld wordt bevestigd door de expertinterviews en de zaakreconstructies: in Noord-Nederland zijn talloze (hybride) cybercriminele jeugdgroepen actief (geweest). Deze zijn vooral bekend bij monodisciplinaire partners, vooral bij strafrechtelijke actoren (de politie en het OM) en (gedeeltelijk) bij enkele private partijen, waaronder banken en telecomproviders. Informatie over deze jeugdgroepen is gefragmenteerd aanwezig bij individuele partners en is niet breed toegankelijk voor lokale veiligheidscoalities.

7.2.2 *Wat zijn de kenmerken van nieuwe, nog onbekende cybercriminele jeugdgroepen?*

Volgens de expertinterviews, de zaakreconstructies en de politieregistraties kunnen jeugdgroepen die betrokken zijn bij cybercrime en die worden besproken in dit onderzoek op basis van de gepleegde delicten worden ingedeeld in twee groepen:

1. Hybride criminele jeugdgroepen: deze zijn actief in zowel traditionele criminaliteit (geweldsdelicten, vermogensdelicten, drugsdelicten, vernieling en misdrijven tegen de openbare orde) als cybercrime (bankhelpdeskfraude, verkoopfraude, phishing, vriend-in-nood-fraude en witwassen). Deze groepen lijken veelvuldig voor te komen en ontstaan met het doel om traditionele criminaliteit te plegen, maar breiden op een gegeven moment hun criminele activiteiten uit naar cybercrime.
2. Jeugdgroepen die exclusief betrokken zijn bij cybercrime (bankhelpdeskfraude, phishing, vriend-in-nood-fraude, online identiteitsfraude en verkoopfraude).

Hoewel deze activiteiten gepaard kunnen gaan met cybercrime in enge zin (zoals hacken) zijn er niet of nauwelijks jeugdgroepen bekend die zich hier specifiek op toeleggen.

De hybride en cybercriminele jeugdgroepen vertoonden wat betreft hun structuur en samenstelling aanzienlijke overeenkomsten. Daarom bespreken we ze samen bij de beantwoording van de deelvragen. Eventuele verschillen worden expliciet benoemd.

7.2.2.1 *Structuur en samenstelling*

Op basis van de expertinterviews, de zaakreconstructies en de politieregistraties hebben we slechts een beperkt beeld gekregen van de structuur en samenstelling van hybride en cybercriminele jeugdgroepen. Wat betreft de structuur kunnen dergelijke groepen worden ingedeeld in twee typen:

1. Dynamische groepen: deze ontstaan veelal ad hoc wanneer zich een gelegenheid voordoet om cybercrime te plegen. Ze hebben een hoge mate van fluïditeit en dynamiek, geen duidelijke hiërarchie en een korte levensduur.
2. Stabiele groepen: deze zijn doorgaans kleinschalig, met een vaste kerngroep van drie tot vijf leden, en vertonen een grotere mate van structuur en hiërarchie, al blijven de lagen buiten de kern dynamisch van samenstelling.

Beide typen groepen hebben doorgaans kernleden, professionele en/of gerekruteerde facilitators en geldezels of andere katvangers.

De cybercriminele jeugdgroepen die we beschrijven in deze studie, vertonen meerdere overeenkomsten met zowel de traditionele als de cybercriminele groepen die zijn beschreven in de literatuur. Daarbij kunnen deze samenwerkingsverbanden worden aangeduid als groepen in plaats van meer bureaucratische organisaties (Kleemans et al., 1998; Kleemans & Van de Bunt, 1999) vanwege hun relatief vaste kerngroep en enige mate van hiërarchie, structuur en dynamiek, vooral in de lagen buiten de kern. De groepen verschillen qua structuur en samenstelling weinig van (jeugd)groepen die betrokken zijn bij traditionele criminaliteit en die beschreven worden in de literatuur (zoals bij Adamse et al., 2024; Densley, 2012; Leukfeldt et al., 2016; Schwarzenbach & Jensen, 2024). Specifiek voor Nederlandse criminele jeugdgroepen komen de gevonden kenmerken overeen met die beschreven in de literatuur: het merendeel van de groepen heeft weinig structuur en geen hiërarchie, terwijl een klein deel hechter is en een duidelijkere structuur vertoont (Beke et al., 2000, 2013; Beke & Van Wijk, 2001).

Een mogelijke verklaring voor de sterke overeenkomsten tussen de cybercriminele jeugdgroepen in dit onderzoek en de traditionele criminele (jeugd)groepen in de literatuur is dat cybercriminele groepen vaak voort lijken te komen uit bestaande traditionele groepen. Daarmee ligt het voor de hand dat zij vergelijkbare kenmerken hebben qua structuur en samenstelling.

De groepen die we in deze studie beschrijven, vertonen daarnaast parallellen met de structuur en samenstelling van de groepen uit de literatuur die betrokken zijn bij financiële cybercrime (Bekkers et al., 2024; Bulanova-Hristova et al., 2016; Leukfeldt,

2014). Allereerst wordt ook in de literatuur onderscheid gemaakt tussen dynamische en stabielere cybercriminele groepen met vergelijkbare kenmerken. Opvallend is dat de stabielere cybercriminele jeugdgroepen deels overeenkomen met de structuur van ransomware-groepen (Matthijsse et al., 2023) en hacktivisme-groepen (Romagna & Leukfeldt, 2024a), vooral wat betreft hun duidelijke rolverdeling, hiërarchie, leidersfiguur en beperkte dynamiek.

Zowel bij de hybride als de cybercriminele jeugdgroepen is een zekere rolverdeling zichtbaar. Globaal zijn drie typen leden te onderscheiden: (1) kernleden; (2) facilitators; en (3) geldezels en katvangers. Daarmee vertonen deze groepen qua rolverdeling overeenkomsten met traditionele criminele (jeugd)groepen (Kleemans, 2007; Kleemans et al., 1998; Peeters & Dongen, 2022; RIEC, 2022; Van Gemert, 2005) én met eerder beschreven cybercriminele groepen (Leukfeldt et al., 2016; Leukfeldt, Lavorgna et al., 2017; Leukfeldt, 2014; Loggen & Leukfeldt, 2022).

Mogelijk kan dit worden verklaard doordat bij vrijwel alle cybercriminele activiteiten drie typen bijdragen nodig zijn: (1) een groot sociaal netwerk van potentiële mededaders om groepen te vormen en te coördineren; (2) het vermogen om goederen en diensten te leveren; en (3) uitvoerende actoren die het risico op identificatie van de kernleden minimaliseren. Kernleden beschikken doorgaans over een groot sociaal netwerk, vergelijkbaar met hun tegenhangers in traditionele criminele groepen. Facilitators leveren de noodzakelijke goederen en diensten, zoals phishing kits bij phishing of inbraakgereedschap bij woninginbraken (Bellotti et al., 2020; Duijn et al., 2014; Ficara et al., 2023). De derde groep bestaat bij cybercrime uit de geldezels of pasophalers. Bij drugshandel worden deze posities bekleed door bijvoorbeeld 'uithalers', die drugs uit zeecontainers moeten halen (Erasmus Universiteit Rotterdam, 2025).

Ons onderzoek voegt ook iets toe aan de bestaande literatuur over rolverdelingen binnen cybercriminele (jeugd)groepen. Waar in eerder onderzoek vooral phishing en banking malware centraal stonden (Bekkers et al., 2024; Bekkers & Leukfeldt, 2023; Leukfeldt et al., 2016; Leukfeldt, Lavorgna et al., 2017; Leukfeldt, 2014; Loggen & Leukfeldt, 2022), hebben wij in dit onderzoek ook andere vormen van financiële cybercrime geanalyseerd en beschreven: bankhelpdeskfraude, verkoopfraude en sextortion. In de literatuur wordt vaak gewezen op het belang van geldezels: personen die hun bankrekening en bankpas beschikbaar stellen, zodat wederrechtelijk verkregen voordeel kan worden doorgesluisd zonder dat kernleden in beeld komen bij de autoriteiten en banken (zie bijvoorbeeld Bekkers et al., 2024; Loggen & Leukfeldt, 2022). Alhoewel geldezels tegenwoordig nog steeds een rol spelen, zoals in de casussen over verkoopfraude en sextortion is beschreven, worden er inmiddels ook delicten gepleegd waarbij de klassieke geldezel niet langer noodzakelijk is. Dit geldt met name voor bankhelpdeskfraude. In plaats van het geld eerst over te maken naar een geldezelrekening en vervolgens contant op te nemen met de bankpas van de geldezel, wordt bij bankhelpdeskfraude doorgaans direct van de bankrekening van het slachtoffer geld opgenomen door zogenoemde pinners. Hoewel deze pinners dezelfde functie vervullen als geldezels (ervoor zorgen dat kernleden anoniem kunnen blijven) hoeven ze dus niet hun bankrekening ter beschikking te stellen.

Ondanks dit verschil blijven groepen dus gebruikmaken van individuen die dezelfde kernfunctie vervullen als geldezels: het afschermen van kernleden. Daarmee worden de meest risicovolle handelingen waarbij de pakkans het grootst is nog steeds uitgevoerd door andere actoren dan de kernleden. Hoewel de concrete taken per delict variëren,[26] blijft hun centrale functie hetzelfde. Zij vormen de cruciale schakel die ervoor zorgt dat kernleden anoniem blijven en buiten het zicht van de autoriteiten opereren. Alhoewel in de literatuur vooral veel aandacht wordt besteed aan geldezels (zoals bij Bekkers et al., 2024; Leukfeldt, 2014; Loggen & Leukfeldt, 2022; Soudijn & Zegers, 2012), is er relatief weinig bekend over de overkoepelende categorie van groepsleden die vergelijkbare faciliterende rollen vervullen, zoals pasophalers en pinners, en de mogelijke overeenkomsten en verschillen daartussen. Deze personen dragen actief bij aan het afschermen van kernleden en zijn daarom essentieel voor het functioneren en voortbestaan van dergelijke groepen.

Tot slot levert dit onderzoek nieuwe inzichten op in de structuur van cybercriminele jeugdgroepen, die in de literatuur nog nauwelijks zijn beschreven. Op basis van de politieregistraties en een socialenetwerkanalyse hebben we groepen schematisch kunnen weergeven. Daarbij valt op dat sommige groepen uit meerdere subgroepen (componenten) bestaan, die met elkaar verbonden zijn door één persoon. Dit zijn vermoedelijk *brokers* (Burt, 1992; Kleemans, 2007, 2013). Alhoewel in de literatuur over traditionele criminele groepen al het een en ander is beschreven over dit type rol, lijkt er nog weinig bekend te zijn over deze rol in de context van cybercrime.

7.2.2.2 *Ontstaan en groei*

Uit de expertinterviews, de zaakreconstructies en de politieregistraties is het beeld ontstaan dat de betrokken actoren beperkt zicht hebben op de ontstaans- en groeiprocessen van hybride en cybercriminele jeugdgroepen. Voor beide typen groepen hebben we meerdere overeenkomsten in de ontstaans- en groeiprocessen geïdentificeerd, al zijn er wel enkele verschillen:

1. Hybride groepen (of doorgroeigroepen) lijken te ontstaan vanuit traditionele criminaliteit en breiden hun activiteiten later uit naar cybercrime, vermoedelijk vanwege de hogere opbrengsten en lagere risico's.
2. Jeugdgroepen die exclusief betrokken zijn bij cybercrime starten direct met het plegen van cybercrime en gaan dit niet combineren met traditionele criminaliteit.

De toetreding tot beide typen jeugdgroepen kan op twee manieren verlopen:

1. Actieve rekrutering, waarbij groepsleden actief op zoek zijn naar nieuwe leden.
2. Geleidelijke betrokkenheid, waarbij een individu geleidelijk onderdeel wordt van een groep.

26 Bij phishing stelt een geldezel bijvoorbeeld een bankrekening ter beschikking (pasverstrekker), terwijl bij bankhelpdeskfraude de modus operandi kan zijn dat een bankpas van het slachtoffer wordt opgehaald (pasophaler).

In beide gevallen spelen zowel offline als online relaties een rol. Dat geldt ook voor fysieke en virtuele ontmoetingsplaatsen. Kernleden kunnen elkaar kennen van de straat, van school, uit de gevangenis of via vrienden. Daarnaast kunnen ze elkaar ontmoeten via online platformen, zoals Telegram en Snapchat. Facilitators, die onder andere phishingpanels en leads leveren, worden vooral via sociale media benaderd, terwijl geldezels via offline relaties en virtuele ontmoetingsplaatsen worden gerekruteerd, en kernleden veelal via offline relaties.

Ook in de literatuur is deze tweedeling beschreven (Bulanova-Hristova et al., 2016; Leukfeldt, Kleemans, et al., 2017a; Leukfeldt & Holt, 2022; Leukfeldt, 2014), al was het tot op heden minder duidelijk hoe deze groepen precies ontstaan. Uit dit onderzoek komt naar voren dat hybride groepen veelal een oorsprong hebben in traditionele criminaliteit, terwijl groepen die zich specifiek richten op cybercrime vanaf hun ontstaan gericht lijken op cybercrime. Deze inzichten bieden aanknopingspunten voor aanpakken en interventies: doordat hybride groepen veel kenmerken delen met traditionele criminele groepen, zouden bestaande aanpakken en interventies voor traditionele criminaliteit ook effectief kunnen zijn bij deze groep. Bovendien kunnen traditionele delicten ook een vroege indicatie vormen voor betrokkenheid bij cybercrime. Dit wordt ondersteund door onze analyse van de politieregistraties: van de 209 jongeren die bij gemeenten bekend waren als betrokkenen bij traditionele criminaliteit, konden er 13 (6,2%) in verband gebracht worden met (betrokkenheid bij het plegen van) cybercrime.

De toetreding tot jeugdgroepen kan op twee manieren verlopen: (1) via actieve rekrutering of (2) via geleidelijke betrokkenheid. Dit sluit aan bij wat er in voorgaand onderzoek is beschreven over toetreding tot traditionele criminele (jeugd)groepen (Adamse et al., 2024; Beke et al., 2000; CCV, 2022; Kleemans & Van Koppen, 2020; Programma Straatwaarde(n), 2020; RIEC, 2022). Offline banden tussen groepsleden (zoals vriendschappen, familierelaties of romantische relaties) blijven het meest frequent voorkomen, vooral bij kernleden, geldezels en gerekruteerde facilitators. Dit komt overeen met bevindingen over traditionele criminele (jeugd)groepen (Adamse et al., 2024; De Boer et al., 2022; Densley, 2012; Kleemans et al., 1998; Kleemans & De Poot, 2008) en sluit grotendeels aan bij eerdere studies naar groepen die betrokken waren bij financiele cybercrime (Leukfeldt et al., 2016; Leukfeldt, Lavorgna et al., 2017; Leukfeldt, 2014; Loggen & Leukfeldt, 2022).

Hoewel online ontmoetingsplekken werden gebruikt om mededaders te vinden, hebben we nauwelijks relaties geïdentificeerd die online zijn ontstaan en die sterker waren dan vluchtige samenwerkingsrelaties, terwijl eerdere onderzoeken deze sterke sociale banden (in beperkte mate) wél rapporteerden (zoals Leukfeldt et al., 2016). Mogelijk hangt dit samen met de observatie dat financiële cybercrime technisch gezien minder complex is geworden (Loggen & Leukfeldt, 2022). Hierdoor zijn online samenwerkingen mogelijk minder noodzakelijk en spelen bestaande offline vertrouwensrelaties juist een grotere rol. Daarbij zien we wel twee belangrijke verschillen. Ten eerste lijken fysieke ontmoetingsplekken in onze studie minder gebruikt te worden in vergelijking met

de literatuur, terwijl het gebruik van virtuele plekken juist een prominentere plek lijkt in te nemen.

Hoewel offline banden en fysieke ontmoetingsplekken nog steeds belangrijk lijken bij het ontstaan en de groei van cybercriminele jeugdgroepen (vooral bij het rekruteren van kernleden), komt uit onze resultaten ook naar voren dat steeds meer gebruik wordt gemaakt van virtuele ontmoetingsplekken, vooral bij het zoeken naar facilitators en geldezels. Hoewel eerdere studies al het gebruik van dergelijke virtuele ontmoetingsplaatsen beschreven, zowel bij traditionele criminaliteit als bij cybercrime (Bekkers et al., 2022; Bekkers & Leukfeldt, 2023; RIEC, 2022; Wolsink et al., 2023), laat ons onderzoek zien dat hun belang lijkt toe te nemen.

Experts geven aan dat het gebruik van virtuele ontmoetingsplaatsen de afgelopen jaren is toegenomen, vooral het gebruik van laagdrempelige en gebruiksvriendelijke platforms, waarbij Telegram het populairst is. Dit is met name het geval voor het vinden van professionele facilitators. Deze zijn relatief eenvoudig te vinden op deze platforms, wat de barrière voor deelname aan cybercriminele groepen verlaagt.

De toename in het gebruik van virtuele ontmoetingsplaatsen kan mogelijk worden verklaard door de voordelen die ze hebben ten opzichte van fysieke en eerdere virtuele ontmoetingsplaatsen (zoals *underground* fora en het dark web). Ze zijn eenvoudig toegankelijk, gebruiksvriendelijk en vereisen minimale inspanning om aan deel te nemen (Bekkers & Leukfeldt, 2023; Garkava et al., 2024; Leukfeldt et al., 2016; Romagna & Leukfeldt, 2024b). Daarnaast zijn ze schaalbaar, maken ze het mogelijk om over grote afstanden te communiceren (Garkava et al., 2024; Soudijn & Zegers, 2012) en bieden ze betere anonimiteit en veiligheid dan fysieke plekken, wat de drempel om sociale contacten aan te gaan en deel te nemen aan criminele activiteiten mogelijk verlaagt (Odinot et al., 2018).

In eerdere studies is naar voren gekomen dat zowel traditionele als cybercriminele groepen lokaal verankerd kunnen zijn, waarbij leden bij elkaar in de buurt wonen (Kleemans & De Poot, 2008; Kruisbergen et al., 2018b; Leukfeldt et al., 2019). Het gebruik van virtuele ontmoetingsplaatsen maakt samenwerking over grotere afstanden mogelijk, waardoor groepen minder lokaal verankerd kunnen zijn. Tegelijkertijd blijken sommige virtuele plaatsen alsnog lokaal georiënteerd te zijn. Zo kunnen Telegramgroepen expliciet verwijzen naar geografische kenmerken, zoals postcodes of plaatsnamen. Deze groepen lijken dus de voordelen van virtuele plaatsen te combineren met die van offline banden.

Ondanks de sterke nadruk op offline banden en Telegramgroepen met lokale componenten laat onze socialenetwerkanalyse zien dat ten minste een deel van de cybercriminele jeugdgroepen niet of in mindere mate lokaal verankerd is. Daarnaast heeft onze analyse de geografische spreiding van groepsleden in kaart gebracht. Hoewel eerdere studies (bijvoorbeeld Leukfeldt et al., 2019; Leukfeldt, 2014) ingingen op de lokale verankering van cybercriminele groepen, ontbraken hierbij kwantitatieve analyses. In dit onderzoek hebben we dit wel gedaan: aan de hand van de postcodes van de 109 geïdentificeerde verdachten in de politieregistraties, hebben we in kaart gebracht in welke regio's zij woonachtig waren en hoe ze per groep verspreid waren over Nederland.

Hieruit blijkt dat 57,7% van de geïdentificeerde groepen bestond uit leden die woonachtig waren in dezelfde of nabijgelegen gemeenten, allen in Noord-Nederland. Van deze 15 groepen woonden alle leden van 5 groepen (33,3%) in dezelfde Noord-Nederlandse gemeente; 4 van deze 5 groepen bestonden uit slechts 2 individuen. Daarnaast waren de leden van drie groepen (1, 2, 6) geografisch verspreid over heel Nederland, en hadden 7 andere groepen leden die allemaal buiten Noord-Nederland woonachtig waren.

7.2.3 *Wat zijn de kenmerken van individuele leden van nieuwe, nog onbekende cybercriminele jeugdgroepen?*

In dit onderzoek zijn vrijwel uitsluitend daders geïdentificeerd die betrokken zijn bij financiële cybercrime, zoals phishing, bankhelpdeskfraude, aan- en verkoopfraude, smishing en sextortion. De hier beschreven daderkenmerken hebben dan ook specifiek betrekking op deze groep. De leden van hybride en cybercriminele jeugdgroepen vertonen veel overeenkomsten qua demografische gegevens, criminele carrières en motivaties. Om die reden worden beide groepen gezamenlijk beschreven. Eventuele verschillen geven we duidelijk aan. Wel hebben we onderscheid gemaakt tussen kernleden en geldezels, omdat zij wél verschillende kenmerken (kunnen) vertonen.

7.2.3.1 *Demografische kenmerken*

Uit de expertinterviews, de zaakreconstructies en de politieregistraties komt naar voren dat de leden van hybride en cybercriminele jeugdgroepen doorgaans tussen de 12 en 28 jaar zijn. Binnen deze groepen vervullen jongeren verschillende rollen, waarbij leeftijd en geslacht vaak samenhangen met hun positie. Kernleden zijn meestal meerderjarig en tussen de 20 en 24 jaar, terwijl geldezels en katvangers doorgaans jonger zijn, tussen de 15 en 17 jaar. Toch komen ook volwassen geldezels voor. De meeste kernleden zijn man, al vervullen vrouwen specifieke rollen, zoals die van beller bij bankhelpdeskfraude. Geldezels kunnen zowel man als vrouw zijn.

De etnische achtergrond van kernleden is zeer divers en lijkt eveneens samen te hangen met de rol binnen de groep. Het opleidingsniveau van kernleden varieert ook sterk: van niet- of laagopgeleid tot (hoog)opgeleid. De meeste kernleden en geldezels hebben een relatief lagere sociaaleconomische status, lijken uit achterstandswijken te komen en een deel heeft een problematische gezinssituatie. In dat laatste aspect zien we overigens behoorlijke verschillen: sommige kernleden en geldezels groeien op in stabiele gezinnen, terwijl anderen een instabiele achtergrond lijken te hebben. Over het algemeen lijken de cognitieve vaardigheden beperkt. Vooral geldezels blijken vaak kwetsbaar en weten niet altijd waar ze precies aan meewerken, al bestaan er ook uitzonderingen.

Deze kenmerken overlappen deels met bevindingen uit de literatuur over traditionele jeugdige daders en personen die betrokken zijn bij financiële cybercrime. Daarbij gaat het bijvoorbeeld om een relatief lagere sociaaleconomische status en opleidingsniveau (Beke et al., 2000, 2013; Calderoni et al., 2022; Chen et al., 2021; De Boer et al., 2022;

Frualdo, 2019; Jegede et al., 2016; Kleemans & Van Koppen, 2020; Peeters & Dongen, 2022; Programma Straatwaarde(n), 2020; Weerman, 2014), en een instabielere gezinssituatie (Calderoni et al., 2022; Ibrahim, 2016; Ogunleye et al., 2020; Peeters & Dongen, 2022; Programma Straatwaarde(n), 2020; RIEC, 2022).

Tegelijkertijd zijn er ook duidelijke verschillen zichtbaar. Uit de expertinterviews, de zaakreconstructies en de politieregistraties komt naar voren dat het opleidingsniveau van verdachten sterk uiteenloopt. De relatief lagere sociaaleconomische status die in de literatuur wordt beschreven, doet echter vermoeden dat het merendeel ook een laag opleidingsniveau heeft. Toch treffen we óók daders met een hoog opleidingsniveau aan. Dit contrasteert met zowel de literatuur over financiële cybercrime als die over traditionele criminaliteit. Een vergelijkbare variatie zien we bij de etnische achtergrond: waar de literatuur over traditionele daders vooral wijst op een oververtegenwoordiging van etnische minderheden (Calderoni et al., 2022; De Boer et al., 2022; Kleemans & Van Koppen, 2020; Programma Straatwaarde(n), 2020), laten onze resultaten een veel diverser beeld zien.

De gedeeltelijke overlap in kenmerken tussen de cyberdaders in onze studie en de traditionele daders uit de literatuur kan verklaard worden doordat een deel van de cyberdaders in het verleden betrokken was bij traditionele criminaliteit. De geconstateerde verschillen wijzen er echter ook op dat zich mogelijk een nieuwe groep ontwikkelt, die direct instroomt bij financiële cybercrime, zonder een voorgeschiedenis in traditionele criminaliteit. Deze groep heeft wellicht niet dezelfde kenmerken als de traditionele daders, wat mede zou kunnen verklaren waarom zij niet eerst offline criminaliteit plegen.

Daarnaast biedt ons onderzoek een genuanceerd beeld van de daderkenmerken van jongeren die betrokken zijn bij financiële cybercrime. Hoewel een groot deel overeenkomt met het profiel van traditionele daders (zoals een relatief laag opleidingsniveau, een problematische thuissituatie en een lagere sociaaleconomische status) zien we ook duidelijk verschillen. Sommige jongeren hebben juist een relatief hoog opleidingsniveau, een stabiele thuissituatie en werk. Dit lijkt vooral te gelden voor de digitale starters die zich uitsluitend bezighouden met cybercrime.

In de literatuur is beschreven dat daders die betrokken zijn bij gedigitaliseerde criminaliteit over het algemeen andere kenmerken hebben dan jongeren die betrokken zijn bij cybercrime in enge zin (Loggen et al., 2024a, 2024b). Onze bevindingen bevestigen dat de jongeren die in dit onderzoek zijn beschreven en die betrokken zijn bij gedigitaliseerde criminaliteit deels dezelfde kenmerken hebben als in de literatuur worden beschreven. Tegelijkertijd zien we ook verschillen. Zo lijkt het opleidingsniveau bij gedigitaliseerde criminaliteit volgens de literatuur doorgaans relatief laag te zijn (Loggen et al., 2024a), terwijl dit bij cybercrime in enge zin juist hoger lijkt te liggen (Loggen et al., 2024b). In ons onderzoek zijn inderdaad verdachten met een laag opleidingsniveau geïdentificeerd, maar er zijn ook uitzonderingen op deze regel.

7.2.3.2 *Criminele carrière*

Op basis van de politieregistraties, de zaakreconstructies en de expertinterviews zijn drie typen criminele carrières te onderscheiden onder jongeren en jongvolwassenen die actief zijn binnen hybride en cybercriminele jeugdgroepen:

1. Overstappers: jongeren die hun criminele carrière beginnen met het plegen van traditionele criminaliteit (zoals drugsdelicten, woningovervallen en wapengeweld) en later overstappen naar cybercrime. Na deze overstap richten ze zich uitsluitend op cybercrime, vooral online fraude.
2. Hybride plegers: jongeren die gelijktijdig betrokken zijn bij zowel traditionele delicten als cybercrime.
3. Digitale starters: jongeren die hun criminele carrière direct beginnen met cybercrime en zich niet bezighouden met traditionele delicten. Zij hebben mogelijk niet de persoonlijkheidskenmerken om traditionele delicten te plegen of ze kiezen bewust voor cybercrime vanwege de hoge opbrengsten en lagere risico's.

Overstappers en hybride plegers lijken veelvuldig voor te komen. Overstappers, hybride daders en digitale starters kunnen gespecialiseerd zijn in één type cybercrime (zoals phishing) of juist generalistisch te werk gaan en betrokken zijn bij meerdere cyberdelicten (zoals phishing, bankhelpdeskfraude en verkoopfraude). Jongeren die hun criminele carrière beginnen met cybercrime en uitsluitend cybercrime plegen, beschikken volgens enkele respondenten voor een deel niet over de persoonlijkheidskenmerken die nodig zijn om traditionele delicten te plegen. Zij missen bijvoorbeeld 'het lef' om fysieke delicten te plegen en kiezen daarom voor online vormen van criminaliteit. Dit kan verklaren waarom zij direct zijn begonnen met cybercrime.
De bestaande literatuur besteedt slechts in zeer beperkte mate aandacht aan de criminele carrière van individuen die betrokken zijn bij financiële cybercrime. Er wordt bijvoorbeeld vermeld dat sommige daders in het verleden actief waren in de traditionele criminaliteit, dat zij cybercrime en traditionele misdrijven tegelijkertijd plegen of dat zij direct instromen in financiële cybercrime (zoals in Leukfeldt & Holt, 2022; Leukfeldt, 2014; Loggen et al., 2024a). De bevinding dat daders hybride kunnen zijn en beide typen delicten tegelijk plegen, is door een zeer beperkt aantal eerdere studies beschreven (Leukfeldt, Kleemans et al., 2017a; Loggen et al., 2024a; R. Roks et al., 2021). In dit onderzoek hebben we echter in meer detail beschreven dat deze groep daders al een lange geschiedenis van traditionele criminaliteit lijkt te hebben. Deze geschiedenis lijkt groter dan in eerder onderzoek is beschreven. Met deze studie voegen wij daarom een nieuwe bijdrage toe: de introductie van een classificatie van criminele carrières binnen de financiële cybercrime.

7.2.3.3 *Motivaties*

Uit de expertinterviews, de zaakreconstructies en de politieregistraties komt naar voren dat de belangrijkste motivaties om financiële cybercrime te plegen financieel gewin is. Die motivaties zijn: het verkrijgen van status en financieel gewin. Dit komt overeen met de bevindingen uit onderzoeken naar de motivaties van cyberdaders in West-Afri-

kaanse landen (Adejoh et al., 2019; Chen et al., 2021; Ogunleye et al., 2020). Bovendien sluit dit aan bij de motieven die worden toegeschreven aan jongeren die zijn betrokken bij traditionele criminele groepen (CCV, 2022; De Boer et al., 2022; Programma Straatwaarde(n), 2020; RIEC, 2022).
Financieel gewin en status zijn nauw met elkaar verweven: status wordt in belangrijke mate ontleend aan het bezit en het kunnen etaleren van luxegoederen, zoals merkkleding, dure telefoons en auto's, die zijn aangeschaft met de opbrengsten uit cybercrime.

7.2.4 *Wat is de aard van de delicten waarmee nieuwe, nog onbekende cybercriminele jeugdgroepen zich bezighouden?*

Op basis van de expertinterviews, de zaakreconstructies en de politieregistraties kunnen de delicten die door deze jeugdgroepen worden gepleegd variëren, afhankelijk van de type groep. Hybride groepen zijn betrokken bij zowel cybercrime als traditionele criminaliteit. Binnen de cybercriminele activiteiten zijn twee vormen te onderscheiden. Allereerst worden delicten gepleegd waarbij digitale middelen worden ingezet om traditionele criminaliteit te faciliteren, zoals het verkopen van drugs via Telegram. Ten tweede zijn deze groepen actief in online fraude, waaronder bankhelpdeskfraude, verkoopfraude, phishing en vriend-in-nood-fraude. Bij al deze vormen speelt social engineering een cruciale rol. Voorbeelden van traditionele delicten zijn gewelds-, vermogens- en drugsdelicten, vernieling en misdrijven tegen de openbare orde. Het merendeel van deze delicten lijkt financieel gemotiveerd te zijn.
Daarnaast bestaan er groepen die zich uitsluitend toeleggen op (financiële) cybercrime, zoals bankhelpdeskfraude, phishing, vriend-in-nood-fraude, online identiteitsfraude en verkoopfraude. Een mogelijke verklaring voor het vinden van enkel groepen betrokken bij financiële cybercrime, is dat de resultaten zijn gebaseerd op groepen die al geïdentificeerd zijn. Groepen die nog niet op de radar staan van de autoriteiten zijn daarom niet meegenomen in de analyse. De mogelijkheid bestaat dat deze niet-geïdentificeerde groepen betrokken zijn bij cybercrime in enge zin. Dat zou dan een mogelijke verklaring bieden voor het gebrek aan dit type groepen in ons onderzoek.

7.2.4.1 *Modus operandi*

Een van de meest voorkomende vormen van cybercrime die wordt gepleegd door de jeugdgroepen in ons onderzoek, is bankhelpdeskfraude. Bij deze vorm van online fraude doen daders zich telefonisch voor als bankmedewerkers en proberen zij slachtoffers (vaak ouderen) ervan te overtuigen dat er iets mis is met hun bankrekening. We hebben meerdere casussen geïdentificeerd waarbij de 'bankmedewerker' Fries sprak, terwijl het slachtoffer ook Fries was, of een Gronings dialect had en sprak met een Gronings slachtoffer. Bovendien is één zaak beschreven waarin de daders in contact met het slachtoffer gebruikmaakten van de naam van een echte bankmedewerker.
De exacte modus operandi varieert, maar bestaat uit vier veelgebruikte methoden:

1. Het thuis ophalen van bankproducten: hierbij wordt de bankpas van het slachtoffer opgehaald en vervolgens wordt contant geld van de rekening opgenomen door

'cashers'. Daarnaast proberen cyberdaders bij deze werkwijze ook zo veel mogelijk waardevolle spullen van het slachtoffer mee te nemen.
2. Slachtoffers cadeaukaarten laten kopen: aan slachtoffers wordt gevraagd om cadeaukaarten te kopen, die daarna door de daders worden opgehaald.
3. Overmaken naar een 'veilige' rekening: slachtoffers worden overgehaald om geld over te maken naar een bankrekening die volgens de daders 'veilig' is.
4. Meekijken en overmaken via software: daders gebruiken software zoals AnyDesk om op afstand mee te kijken op de computer/smartphone van het slachtoffer om zo geldbedragen over te maken naar bijvoorbeeld webwinkels.

Naast bankhelpdeskfraude zijn jeugdgroepen ook betrokken bij andere vormen van fraude.
Bij verkoopfraude werden online goederen aangeboden, waarbij slachtoffers betaalden voor producten die vervolgens niet geleverd werden. Phishing vond plaats via betaalverzoeken die leidden naar frauduleuze websites, waarmee toegang werd verkregen tot de bankrekeningen van slachtoffers.
Daarnaast hebben we één groep geïdentificeerd die zich bezighield met sextortion. In deze casus werd een slachtoffer benaderd via een website, waarbij de dader zich voordeed als jonge vrouw. Het contact werd voortgezet via WhatsApp, waarbij seksueel getinte berichten en foto's werden uitgewisseld. Na enige tijd werd het slachtoffer telefonisch benaderd door een persoon die zich voordeed als de vader van de vermeende jonge vrouw (in werkelijkheid waren de jonge vrouw en de vader dezelfde persoon). Deze 'vader' beweerde dat het om zijn 16-jarige dochter ging en zette het slachtoffer onder druk om een geldbedrag te betalen, anders zou hij naar de politie gaan.
Naast de hierboven beschreven financiële cybercrimes zijn cybercriminele jeugdgroepen ook betrokken bij het witwassen van het wederrechtelijk verkregen voordeel. Uit ons onderzoek komen meerdere manieren van witwassen naar voren:
1. Geldezels: hierbij worden veelal jongeren gerekruteerd die hun bankpas en bankrekening beschikbaar stellen voor het witwassen van wederrechtelijk verkregen voordeel.
2. Cadeaukaarten of goederen: illegaal verkregen geld wordt omgezet in onder andere cadeaukaarten, Paysafe-kaarten, beltegoed of luxegoederen, waaronder kleding, accessoires en elektronica.
3. Bankpassen van slachtoffers: met de bankpassen van slachtoffers wordt contant geld opgenomen.
4. Betaalverzoeken aan slachtoffers: naar slachtoffers werden betaalverzoeken gestuurd om hun geld over te maken naar een 'veilige' rekening. In werkelijkheid werden hiermee goederen betaald.
5. Cryptovaluta: daders kopen met het gestolen geld cryptovaluta's.
6. Ondernemingen: ondernemingen worden ingezet om het wederrechtelijk verkregen voordeel wit te wassen.

7.2.4.2 *De verwevenheid tussen cybercrime en traditionele criminaliteit*

Cybercrime en traditionele criminaliteit raken steeds vaker met elkaar verweven, zo blijkt uit de expertinterviews, de zaakreconstructies en de politieregistraties. Soms worden beide typen naast elkaar gepleegd, zonder directe relatie. In andere gevallen is er een sterkere, meer directe verbinding tussen traditionele criminaliteit en cybercrime, waarbij cybercrime veelal voorafgaat aan de traditionele delicten. Zonder cyber zouden de traditionele delicten niet of veel moeilijker te plegen zijn. Deze meer directe verwevenheid is zichtbaar op drie gebieden:

1. Investeren in traditionele criminaliteit: illegaal verkregen voordeel uit cybercrime wordt vaak geïnvesteerd in traditionele criminele activiteiten, waaronder drugs.
2. Geweldsincidenten: cybercrime kan gepaard gaan met geweld, zoals schietincidenten waar cybercrime aan ten grondslag ligt. Voorbeelden zijn: schietpartijen tussen voormalige mededaders die samen cybercrime hebben gepleegd en het laten afgaan van explosieven bij huizen van concurrenten op het gebied van cybercrime.
3. Witwassen en ondermijnende criminaliteit: de opbrengsten van cybercrime worden witgewassen via verschillende methoden, zoals de inzet van geldezels, cadeaukaarten, cryptovaluta en bedrijven. In dat laatste geval lijkt er sprake te zijn van een versmelting tussen de onder- en bovenwereld en is mogelijk sprake van ondermijnende criminaliteit.

7.2.5 ***Spoor 1 en 2: een vergelijking***

Traditionele criminele jeugdgroepen en cybercriminele jeugdgroepen vertonen meerdere overeenkomsten. Qua structuur en samenstelling lijken beide typen te bestaan uit een relatief stabiele kerngroep met daaromheen een meer dynamische schil. Ook is er sprake van een vergelijkbare rolverdeling: kernleden vervullen leidinggevende functies, terwijl leden in de buitenste lagen uitvoerende taken verrichten, waardoor kernleden grotendeels anoniem kunnen blijven.

Ook in de ontstaans- en groeiprocessen zijn parallellen zichtbaar. In beide gevallen spelen offline banden en fysieke ontmoetingsplaatsen een belangrijke rol, net als actieve rekrutering en geleidelijke betrokkenheid. Een belangrijk onderscheid is echter het gebruik van online platforms. Traditionele criminele jeugdgroepen steunen sterk op offline banden, terwijl cybercriminele jeugdgroepen in toenemende mate gebruik lijken te maken van platforms als Telegram en Snapchat, vooral om facilitators te benaderen. Een mogelijke verklaring hiervoor is het belang van fysieke aanwezigheid bij traditionele criminaliteit versus cybercrime. Traditionele delicten vereisen doorgaans fysieke aanwezigheid en materieel, bijvoorbeeld bij een woninginbraak. Vanwege deze noodzaak blijven traditionele criminele jeugdgroepen mogelijk sterk leunen op offline banden. Voor financiële cybercrime, zoals bankhelpdeskfraude, geldt dat die op afstand kan worden gepleegd, zelfs door leden die in verschillende regio's wonen. In dit onderzoek zijn daar meerdere voorbeelden van beschreven. Voor deze delicten is fysiek contact tussen leden minder belangrijk, wat het gebruik van online kanalen voor

rekrutering kan verklaren. Bovendien is voor cybercrime doorgaans digitaal materieel nodig, dat eenvoudig te verkrijgen is via internet.
Hoewel de structuur en de samenstelling gedeeltelijk overeenkomen, lijken cybercriminele jeugdgroepen vanwege het gebruik van online platforms beter in staat om zich snel aan te passen wanneer een lid wegvalt. Nieuwe leden kunnen immers relatief eenvoudig online worden geworven. Voor traditionele groepen is dit mogelijk complexer.
Wanneer we inzoomen op de kenmerken van de individuele leden, doen zich ook overeenkomsten en verschillen voor. Zo komt de leeftijd van de leden overeen, wat te verwachten was, omdat het in beide gevallen om *jeugdgroepen* gaat. Een andere overeenkomst is dat de meerderheid uit jongens en mannen bestaat, al komen vrouwen in mindere mate ook voor. Ook de grote variatie in etnische achtergrond, opleidingsniveau, thuissituatie en sociaaleconomische status is vergelijkbaar. Dit valt deels te verklaren doordat een groot deel van de financiële cyberdaders eerder traditionele delicten heeft gepleegd en daarmee hetzelfde profiel deelt.
Het grootste verschil zien we bij de daders die hun criminele carrière direct in de financiële cybercrime beginnen: de digitale starters. Zij hebben mogelijk niet de persoonlijkheidskenmerken om traditionele delicten te plegen of kiezen bewust voor cybercrime vanwege de hoge opbrengsten en lagere risico's. Uit onze resultaten blijkt bovendien dat deze groep niet op een later moment de overstap maakt naar traditionele criminaliteit, terwijl traditionele daders wél de overstap maken naar financiële cybercrime.
Tot slot zijn er overeenkomsten in motivatie. Zowel traditionele als cybercriminele jeugdgroepen lijken vooral gericht op het snel verkrijgen van financieel gewin. Dit is opnieuw te verklaren door de overlap tussen beide groepen: veel financiële cyberdaders zijn afkomstig uit de traditionele criminaliteit. Dit suggereert dat het vooral gaat om opportunistische daders, die steeds de meest toegankelijke en lucratieve weg zoeken om snel geld te verdienen – vroeger via traditionele criminaliteit, nu vooral via financiële cybercrime.

7.3 Spoor 3: de (integrale) aanpak

Het derde spoor richt zich op de (integrale) aanpak van cybercriminele jeugdgroepen. Daarbij bespreken we eerst in hoeverre de betrokken actoren zicht hebben op de groepen die in de eerdere sporen zijn geïdentificeerd. Vervolgens gaan we in op manieren om de (integrale) aanpak van cybercriminele jeugdgroepen te bevorderen.

7.3.1 *In hoeverre hebben actoren die betrokken zijn bij de (integrale) aanpak van criminele jeugdgroepen in Noord-Nederland zicht op de onder onderzoeksvraag 1 en 2 geïdentificeerde cybercriminele groepen?*

De door ons aangeschreven lokale veiligheidscoalities, onder regie van gemeenten, hebben geen zicht op cybercriminele jeugdgroepen. Uit de expertinterviews blijkt dat ditzelfde geldt voor meerdere monodisciplinaire actoren, in ieder geval voor: scholen, jongerenwerkers en leerplichtambtenaren. Zij hebben wel in beperkte mate zicht op

traditionele criminele jeugdgroepen. Het gebrek aan zicht op cybercriminele jeugdgroepen lijkt te worden veroorzaakt door twee factoren; enerzijds leunen deze actoren te sterk op straatinformatie en anderzijds beschikken ze over onvoldoende kennis om cyberdaders te kunnen identificeren.
Strafrechtelijke partners, vooral de politie en het OM, hebben meer zicht, mede dankzij de informatie uit aangiftes en data-analyses, terwijl ze minder afhankelijk zijn van straatinformatie. Actoren zoals banken en telecomproviders verrijken het beeld van de politie en het OM. Toch blijft het zicht op jeugdgroepen beperkt: vooral geldezels en andere katvangers worden geïdentificeerd, terwijl kernleden veelal uit beeld blijven. Uit de vijf zaakreconstructies en de expertinterviews met politie- en OM-medewerkers blijkt dat er wel degelijk data beschikbaar zijn om deze groepen grotendeels in kaart te brengen, maar dat dit type onderzoek veel capaciteit vergt en dat die momenteel schaars is.

7.3.2 *In hoeverre en op welke wijze kan de (integrale) aanpak van cybercriminele jeugdgroepen worden bevorderd?*

Als laatste hebben we onderzocht in hoeverre en op welke wijze de huidige (integrale) aanpak van jeugdgroepen betrokken bij cybercrime kan worden verbeterd. Daarbij hebben we specifiek gekeken naar wat de aanpak precies inhoudt, de mate van delict specificiteit van de aanpak, verbeterpunten, best practices, en in hoeverre interventies gericht op jeugdige cyberdaders kunnen bijdragen aan het verstoren van groepen.

7.3.2.1 *Wat houdt de (integrale) aanpak van cybercriminele jeugdgroepen in? Welke actor (mono) of actoren (integraal) zijn erbij betrokken?*

De aanpak van cybercriminele jeugdgroepen kan op basis van de expertinterviews en de zaakreconstructies in drie categorieën worden ingedeeld: (1) een volwaardige integrale aanpak; (2) een multidisciplinaire aanpak bij het in kaart brengen van een groep, waarbij de interventies monodisciplinair worden uitgevoerd; en (3) een monodisciplinaire aanpak.
Een volwaardige integrale aanpak omvat de samenwerking tussen meerdere lokale actoren, bij het in kaart brengen van een cybercriminele groep én bij het implementeren van interventies. Deze aanpak blijkt een zeldzaamheid: slechts één casus voldeed hieraan (C1), terwijl tijdens meerdere expertinterviews de waarde van een dergelijke interdisciplinaire aanpak werd benadrukt. Het samenwerkingsverband in casus C1 werd gevormd door het RIEC Noord-Nederland, gemeenten, de politie, het OM, de Belastingdienst en de Arbeidsinspectie. Deze aanpak biedt meerdere voordelen, waaronder een rijker informatiebeeld en complementaire interventiemogelijkheden.
Ons onderzoek laat zien dat integrale kansen vaak onbenut blijven, terwijl een integrale aanpak in potentie een rijker informatiebeeld en een breder palet aan interventiemogelijkheden oplevert. Het meer benutten van bestaande integrale samenwerkingsstructuren voor de aanpak van cybercrime lijkt dan ook wenselijk.

In de praktijk leunt de aanpak van cybercrime nog vooral op de inspanningen van partners in de strafrechtketen. Hierbij is de scope van het opsporingsonderzoek vaak beperkt: het aantal subjecten en de delicten waarvoor bewijs wordt verzameld zijn doorgaans afgebakend. Hierdoor wordt meestal slechts naar één of een selectie van subjecten en delicten gekeken, waardoor andere betrokkenen en strafbare feiten buiten beeld blijven. Integrale samenwerking biedt de mogelijkheid om de scope van het onderzoek (de informatievergaringsfase) en de interventies te verbreden.
De multidisciplinaire samenwerking met monodisciplinaire uitvoering is een samenwerkingsvorm waarbij meerdere partijen gezamenlijk informatie uitwisselen bij het in kaart brengen van een groep. Daarbij ligt de uitvoering van interventies uiteindelijk bij één actor, vooral de strafrechtelijke actoren. Samenwerkingen tussen de politie, het OM en gemeenten, en tussen de politie, het OM en banken en telecomproviders vallen hieronder. Daarbij wordt vooral informatie gedeeld met de politie en het OM voor de strafrechtelijke opsporing. Er zijn ook enkele voorbeelden bekend waarbij de politie informatie heeft gedeeld met gemeenten, zoals de kenmerken en ronsellocaties van geldezels in een Noord-Nederlandse stad.
De monodisciplinaire aanpak is een aanpak van cybercriminele jeugdgroepen door één actor of sector (waaronder de politie, het OM, gemeenten, banken, telecomproviders en jongerenwerkers) zonder structurele samenwerking met andere partijen. Deze gefragmenteerde aanpak, die in de praktijk het meest voorkomt, richt zich op maatregelen die variëren van strafrechtelijke vervolging tot het blokkeren van bankrekeningen en voorlichting. Deze interventies richten zich niet specifiek op groepen, maar zijn generiek. Geconstateerd is dat de mono-aanpak voor verbetering vatbaar is: het effect van interventies is veelal onduidelijk en er is behoefte aan een sterkere samenwerking.

7.3.2.2 *In hoeverre is de (integrale) aanpak delictspecifiek en in welke mate volstaat deze voor de aanpak van cybercriminele jeugdgroepen?*

Uit de expertinterviews en de zaakreconstructies blijkt dat in de praktijk verschillende aanpakken en interventies worden toegepast om jeugdgroepen te verstoren. Deze kunnen integraal van aard zijn en zich specifiek richten op traditionele criminaliteit, evenals monodisciplinair die zijn gericht op cybercrime (zoals HackShield, MKB Cyber Campus en het blokkeren van bankrekeningen of telefoonnummers). Het kan ook gaan om interventies die toegepast kunnen worden op beide typen delicten (zoals strafrechtelijke vervolging).
Bestaande samenwerkingsverbanden kunnen bijdragen aan de aanpak van jeugdgroepen. De meest voorkomende is de integrale jeugdgroepenaanpak via het 7-stappenmodel. Dergelijke samenwerkingsstructuren zijn niet specifiek voor één soort criminaliteit en zijn tot dusver vooral toegepast op traditionele criminaliteit en zelden of niet op cybercrime. Over het algemeen dragen deze aanpakken en interventies bij aan het verminderen van de problematiek en het uiteenvallen van traditionele jeugdgroepen.

De uitzondering hierop vormt de RIEC-casus. Hoewel deze casus suggereert dat ook het traditionele interventierepetoire[27] van partners kan bijdragen aan de aanpak van een cybercriminele jeugdgroep, is daarvoor nog onvoldoende bewijs voorhanden. Een ander samenwerkingsverband dat mogelijkheden biedt, is de Electronic Crime Task Force, die zich wél expliciet richt op cybercrime. Zij zijn vooral een platform voor informatiedeling en niet voor het implementeren van een aanpak of toepassen van interventies. In zijn algemeenheid geldt dat binnen de samenwerkingsverbanden (nog) niet gewerkt wordt met cybercrime-specifieke interventies. Dit lijkt deels te komen doordat het nog onontgonnen terrein is, maar ook doordat dergelijke interventies waarschijnlijk onvoldoende bekend zijn.

7.3.2.3 *Wat zijn verbeterpunten in de huidige aanpak van cybercriminele jeugdgroepen?*

Op basis van de politieregistraties, de zaakreconstructies en de expertinterviews hebben we meerdere verbeterpunten gevonden voor de huidige aanpak van cybercriminele jeugdgroepen. De kern daarbij is dat meerdere samenwerkingsmogelijkheden onbenut blijven, vooral de meer structurele samenwerkingsverbanden, zoals het RIEC en de jeugdgroepenaanpak. Een mogelijk startpunt van dergelijke integrale aanpakken zou politie-informatie kunnen zijn. De integratie van cybercrime-aanpakken in bestaande samenwerkingsstructuren vergt dat we eerst beter zicht hebben en dus in staat zijn om te signaleren. Daarnaast vraagt dit om de toepassing en evaluatie van interventies die in de literatuur beschreven zijn, evenals van interventies die al in de praktijk bestaan, zoals het RIEC-interventierepertoire. Waar nodig vraagt dit ook om de ontwikkeling van nieuwe interventies, zodat ketenpartners handvatten hebben om op te treden tegen deze vorm van (groeps)criminaliteit, die voor hen veelal nog onbekend is.
Om het zicht op cybercriminele jeugdgroepen te verbeteren, moeten praktijkprofessionals bekwaam zijn in het vroegtijdig signaleren en proactief optreden. Ook moeten zij deze signalen efficiënt kunnen delen met lokale actoren. Om de betrokkenheid van jongeren bij cybercrime in een vroeg stadium te kunnen signaleren en om proactief op te kunnen treden, hebben praktijkprofessionals kennis en inzicht nodig op het gebied van cybercrime. Volgens de respondenten lijkt het daar veelal aan te ontbreken. Bovendien verloopt het delen van dergelijke signalen stroef, waardoor ze niet de juiste partners bereiken en het informatiebeeld over cybercriminele jeugdgroepen beperkt blijft. Daarom is er behoefte aan:

- het vergroten van de kennis van praktijkprofessionals (zoals politieagenten en jongerenwerkers). Zij moeten cybercrime offline en online kunnen signaleren: voor vroegsignalering en om proactief op te kunnen treden;
- het verbeteren van de samenwerking tussen de politie, gemeenten en private partijen, waaronder basis- en middelbare scholen, jongerenwerkers, banken en telecom-

27 Denk aan: dwangsommen, het terugvorderen van onterecht verkregen steun en boetes wegens bepaalde arbeidsovertredingen.

providers. Zo kunnen zij sneller signalen uitwisselen en zorgen voor een betere informatiedeling;
- het aanstellen van laagdrempelige, centrale aanspreekpunten binnen de gemeente en de politie.

Daarnaast is het noodzakelijk om nieuwe interventies te ontwikkelen en deze (net als de bestaande interventies) te evalueren, zodat ketenpartners handvatten hebben om op te treden tegen deze vorm van (groeps)cybercriminaliteit die voor hen veelal nog onbekend is. Daarbij is behoefte aan:
- de ontwikkeling van interventies die specifiek gericht zijn op verschillende groepen binnen cybercriminele groepen, zoals kernleden en geldezels;
- het evalueren van deze interventies.

7.3.2.4 *Wat zijn best practices uit de (integrale) aanpak van cybercriminele jeugdgroepen?*

Uit de RIEC-casus komt naar voren dat de samenwerking met verschillende partners aanzienlijke voordelen biedt. Door het combineren van unieke informatiebronnen ontstaat een rijker informatiebeeld. Het onderbrengen van dergelijke casussen bij het RIEC biedt mogelijkheden voor de uitwisseling van persoonsgegevens. Bovendien beschikt iedere partner over eigen bevoegdheden en instrumenten. Die combinatie leidt in potentie tot een gecoördineerde en rijkere aanpak dan een monodisciplinaire interventie. Daarmee kan een cybercriminele groep mogelijk effectief worden verstoord, al is het effect van de interventies in deze casus niet geëvalueerd.
Belangrijk hierbij is wel dat een dergelijke integrale samenwerking moet zijn ingebed binnen bestaande samenwerkingsstructuren. De reden hiervoor is dat er dan regels vastliggen over de uitwisseling van gegevens en de (complementaire) inzet van interventies van de verschillende partners. Zonder een dergelijke geformaliseerde samenwerkingsstructuur kan een integrale samenwerking juist leiden tot (juridische) obstakels.
Hoewel we in dit onderzoek geen casus hebben geïdentificeerd waarin de jeuggroepenaanpak (7-stappenmodel) daadwerkelijk is toegepast op een cybercriminele groep, wordt het model door respondenten wel gezien als een waardevolle blauwdruk. De flexibiliteit en brede toepasbaarheid maken het model geschikt voor een integrale aanpak, mits die goed wordt aangepast aan de digitale context.

7.3.2.5 *In hoeverre kunnen interventies die zich richten op jeugdige cyberdaders bijdragen aan de aanpak van cybercriminele jeugdgroepen?*

In de literatuur zijn meerdere aanpakken en interventies beschreven die zijn gericht op traditionele en/of cybercriminele jongeren en jeugdgroepen, zoals het 7-stappenmodel (als onderdeel van de jeugdgroepenaanpak), de RIEC-aanpak, de integrale aanpak online fraude en de interventies die zijn gericht op daderschap van cybercrime onder jongeren, zoals beschreven door Oosterwijk en Fischer (2017). In de praktijk wordt echter niet of nauwelijks gebruikgemaakt van deze interventies binnen de aanpak van

cybercriminele jeugdgroepen. Wat het effect van zulke specifieke cyberinterventies is, valt dus op basis van ons onderzoek niet vast te stellen. Duidelijk is wel dat deze interventies in de breedte van de lokale veiligheidspraktijk onbekend zijn, terwijl tegelijkertijd het signaal is dat lokale actoren om handvatten voor de aanpak van cybercriminele jongeren verlegen zitten. Het onder de aandacht brengen van deze interventies biedt daarom mogelijkheden om lokale actoren beter te ondersteunen in de aanpak van cybercriminele jeugdgroepen.

8 Aanbevelingen, beperkingen en toekomstig onderzoek

Dit onderzoek is gestart naar aanleiding van signalen van veiligheidspartners in Noord-Nederland dat zij moeite hebben met (1) het in kaart brengen en (2) aanpakken van jongeren en jeugdgroepen betrokken bij cybercriminele activiteiten, en (3) behoefte hebben aan meer kennis over dit onderwerp: zowel over het fenomeen zelf, als over de manieren om dergelijke groepen te identificeren en effectief aan te pakken. Ons onderzoek bevestigt de vermoedens van de gemeenten: gemeenten hebben nauwelijks zicht op cybercriminele jeugdgroepen, terwijl we in dit onderzoek talloze groepen hebben geïdentificeerd. Hierdoor kunnen zij geen regie voeren op de aanpak daarvan. De centrale aanbeveling luidt daarom om dit zicht op cybercriminele jeugdgroepen te vergroten.

8.1 Beter herkennen van cybercrime-gerelateerde signalen

Het vergroten van het zicht op cybercriminele jeugdgroepen vereist dat praktijkprofessionals bekwaam zijn in vroegtijdig signaleren[28] en proactief optreden, waarbij wordt ingezet op preventie en niet wordt gewacht tot jongeren in aanraking komen met justitie.
Vooral voor de politie, de gemeenten en hun lokale veiligheidspartners (zoals jongerenwerk en scholen) ligt hier een belangrijke taak. Om de betrokkenheid van jongeren bij cybercrime in een vroeg stadium te kunnen signaleren en om proactief op te kunnen treden, hebben praktijkprofessionals (meer) kennis en inzicht nodig op het gebied van cybercrime. Dit onderzoek laat zien dat beide nog onvoldoende aanwezig zijn. Daarom doen wij de volgende aanbevelingen:

- Organiseer trainingen waarin professionals in de hele (lokale) veiligheids- en rechthandhavingsketen leren om betrokkenheid van jongeren bij cybercrime te herkennen. De trainingen moeten inzicht bieden in de verschijningsvormen en risico's van cybercrime, maar vooral ook handvatten geven om betrokkenheid bij cybercrime (vroegtijdig) te herkennen.
- Gebruik vroegsignaleringsindicatoren, zoals betrokkenheid bij offline criminaliteit, het bezit van meerdere simkaarten/telefoons en het bezit van goederen die, gezien iemands financiële positie, niet op een legale manier verkregen kunnen zijn. Deze indicatoren kunnen, aangevuld met inzichten uit ander onderzoek, als basis

28 Het tijdig identificeren van jongeren die een verhoogd risico lopen op betrokkenheid bij cybercrime.

dienen voor signalering van criminele betrokkenheid in het algemeen, en cybercrime in het bijzonder.
- Signaleer breder en leun specifiek voor cybercrime niet alleen op signalen 'van de straat'. Ook online surveillance en toezicht zijn noodzakelijk, net als het delen van signalen die daaruit voortkomen. Dat is deels een taak van de politie, maar ook jongerenwerkers en andere professionals kunnen hieraan bijdragen.

In eerste instantie treden ketenpartners zo veel mogelijk zelf handelend op. Denk aan een jongerenwerker die in gesprek gaat met een jongere die online interesse toont in bankhelpdeskfraude. Waar dat nodig en mogelijk is, worden signalen gedeeld met andere partijen, zoals gemeenten en/of de politie, binnen de juridische kaders van bestaande samenwerkingsstructuren, zoals de jeugdgroepenaanpak.

8.2 Structurele en periodieke monitoring

Om structureel meer zicht te krijgen op cybercriminele jeugdgroepen, kan in de politiesystemen periodiek de query worden uitgevoerd die voor dit onderzoek is ontwikkeld. Deze query brengt groepen in kaart op basis van politieregistraties, waarbij:
- de registratie betrekking heeft op een cybercrime (zowel cybercrime in enge zin alsook een zekere mate van gedigitaliseerde criminaliteit);
- minimaal twee verdachten betrokken zijn;
- de verdachten tussen de 12 en 24 jaar oud zijn;
- ten minste één verdachte in Groningen, Friesland of Drenthe woont.

Momenteel vinden er al periodieke (jeugd)overleggen plaats tussen de gemeenten en de politie. Het advies is om periodiek de resultaten van een dergelijke query in te brengen, bijvoorbeeld in het 7-stappenmodel van de jeugdgroepenaanpak.
De uitvoering van de query ligt bij de politie. In samenspraak met het OM kan worden besloten om hele groepen en/of sleutelfiguren daarbinnen strafrechtelijk aan te pakken, afhankelijk van wat het meest effectief en haalbaar is. Tegelijkertijd is een louter strafrechtelijke aanpak ontoereikend. Deze doet onvoldoende recht aan de omvang van de cybercrime-problematiek in de maatschappij. Politie-informatie over cybercriminele jeugdgroepen die niet leidt tot een opsporingsonderzoek kan daarom worden ingebracht in bestaande samenwerkingsstructuren, zoals de jeugdgroepenaanpak en het RIEC, en dient als startpunt voor een integrale aanpak. Binnen deze structuren kan het informatiebeeld over die groepen worden verrijkt en kunnen interventies worden gekozen uit een breder repertoire dan uitsluitend strafrechtelijke maatregelen.

8.3 Samenwerkingsstructuren beter benutten

Hoewel er al meerdere structurele samenwerkingsverbanden bestaan (zoals de jeugdgroepenaanpak en het RIEC), worden deze in de praktijk nog nauwelijks benut voor de aanpak van cybercrime, terwijl ze daar wel geschikt voor lijken.

Om bestaande samenwerkingsstructuren beter te benutten, is meer inzicht nodig in de criteria waaraan casussen moeten voldoen om daar ingebracht te kunnen worden. De politie heeft hierin een sleutelrol vanwege haar informatiepositie. Onder de geldende juridische voorwaarden kunnen de politie en gemeentelijke partners (zoals het jongerenwerk) gemeenten voeden met relevante informatie en kunnen ze signalen delen over hybride of cybercriminele jeugdgroepen. Dat is nodig, omdat gemeenten een regiefunctie hebben binnen bestaande samenwerkingen. Zij kunnen dan bepalen waar een casus het beste ingebracht kan worden, samen met de betrokken partners en met inachtneming van de inzetcriteria per samenwerkingsverband.
Hoe en waar een groep het beste kan worden ingebracht, is afhankelijk van de informatiebron waarop de identificatie berust. Het delen van persoonsgegevens in een samenwerkingsstructuur vraagt om een weloverwogen voortraject:

- Identificatie op basis van politie-informatie. Is een groep geïdentificeerd via politiegegevens, dan ligt het voor de hand dat de politie en het OM eerst gezamenlijk beoordelen of een strafrechtelijke aanpak haalbaar en opportuun is. Is dit niet het geval, dan kan worden gekeken naar integrale kansen. Voorwaarde is wel dat vooraf helder is welke criteria er gelden om een casus in te kunnen brengen in de jeugdgroepenaanpak, in het RIEC of in een ander samenwerkingsverband.
- Identificatie op basis van lokale partnerinformatie. Komt een groep in beeld via lokale partners, zoals scholen, jongerenwerk of wijkteams, dan verloopt het proces vaak anders. Deze partijen wegen doorgaans eerst zelf af of zij handelingsmogelijkheden hebben binnen hun eigen mandaat en instrumentarium. Pas wanneer zij onvoldoende mogelijkheden zien of wanneer de problematiek groter is dan hun bereik, kan opschaling naar een samenwerkingsstructuur volgen. Dit vraagt om duidelijke afspraken en korte lijnen tussen lokale partners, de politie en gemeenten, zodat een eventuele opschaling efficiënt en zorgvuldig kan plaatsvinden.

Tot slot blijkt uit de resultaten van ons onderzoek dat cybercriminele jeugdgroepen (deels) kunnen ontstaan en groeien via online ontmoetingsplaatsen. Hierdoor hoeven mededaders elkaar niet meer fysiek te ontmoeten, wat de lokale verankering van deze groepen mogelijk vermindert. Leden wonen niet meer in dezelfde gemeente, stad of zelfs buurt, maar kunnen nu verspreid zijn over verschillende delen van Nederland. Het aanpakken van leden binnen slechts één gemeente, met de veronderstelling dat dit alle leden van de groep omvat, is in dergelijke gevallen niet voldoende. Dit benadrukt de noodzaak voor een bredere, interregionale samenwerking tussen verschillende organisaties die verantwoordelijk zijn voor het verstoren van deze groepen.

8.4 Aanbevelingen voor de jeugdgroepenaanpak

In de jeugdgroepenaanpak blijken jongeren voor te komen die bij de politie bekend zijn vanwege traditioneel afwijkend gedrag, maar die soms óók betrokken blijken bij cybercrime. Deze aanwijzingen worden nu vaak gemist. Zo zijn in de analyse van politieregistraties in Noord-Nederland 109 verdachten en 26 groepen geïdentificeerd die

betrokken zijn bij cybercrime. Van deze 109 verdachten waren er 4 ook in beeld bij gemeenten vanwege betrokkenheid bij traditionele criminele jeugdgroepen. Daarnaast hebben gemeenten 9 personen geïdentificeerd als betrokkene bij traditionele criminele jeugdgroepen, die niet direct verdacht worden van cybercrime, maar wel een relatie hebben met iemand die daarvan wordt verdacht.
Een eerste aanbeveling is om de resultaten van de query (zie paragraaf 8.2) in te brengen in een geschikte bestaande samenwerkingsstructuur. Specifiek voor jeugdgroepen kan dit gedaan worden via de groepsscanonderdeel van het 7-stappenmodel. Dit vraagt om een (landelijke) aanpassing van de groepsscan en de query. Hierbij kan per groepslid een volledig overzicht met antecedenten én verdenkingen worden gegenereerd, met specifieke aandacht voor cybercrime.
Een uitdaging hierbij is dat dit zicht zich vaak beperkt tot geldezels en andere leden die zich lager in de groep bevinden. Toch is het waardevol voor gemeenten om te weten welke jongeren binnen hun regio als geldezel of katvanger fungeren, omdat dit mogelijkheden biedt om hen gericht aan te pakken of te helpen. Voor een effectieve bestrijding van cybercriminele jeugdgroepen is het echter essentieel dat ook de kernleden van deze groepen worden geïdentificeerd en aangepakt.

8.5 Aanpakken en effectiviteit

De aanpak van cybercrime vindt momenteel veelal monodisciplinair plaats. Multidisciplinaire samenwerkingen voor informatievoorziening met een monodisciplinaire uitvoering zijn mogelijk, en bestaande samenwerkingsstructuren worden niet of nauwelijks benut, terwijl ze zich daar (ogenschijnlijk) wel voor lenen. Een brede aanpak met het traditionele interventierepertoire kan toepasbaar en succesvol zijn en lijkt soms zelfs effectiever dan een delictspecifieke benadering. Tegelijkertijd bestaat er onder professionals behoefte aan handvatten die specifiek zijn toegesneden op cybercrime. Dergelijke instrumenten zijn echter nog beperkt beschikbaar en voor zover ze al bestaan, zijn ze vaak onbekend.
Hoewel er dus aanwijzingen bestaan dat het traditionele interventierepertoire ook toegepast kan worden op cybergroepen (zoals bij de RIEC-casus), is er te weinig bekend over de effectiviteit van deze interventies en aanpakken. Meer onderzoek is nodig om vast te stellen welke aanpakken werken bij cybercriminele jeugdgroepen en om waar nodig interventies te ontwikkelen of te optimaliseren.
Met die kanttekening is dit ons advies:

- Zorg voor meer bekendheid: bevorder de bekendheid van beproefde interventies binnen de rechtshandhavingspraktijk. Voorbeelden zijn de Geldezelaanpak en Hack_Right (voor een uitgebreider overzicht, zie CCV, 2023b).
- Zorg voor een gerichte inzet: zet monodisciplinair en in gelegenheidssamenwerkingen zo veel mogelijk in op interventies die kansrijk zijn gebleken.
- Zorg voor nieuwe ontwikkeling**:** tegelijkertijd is er ruimte en een noodzaak om interventies te blijven ontwikkelen, bij uitstek tegen de opportunistische jonge

doelgroep die online fraude pleegt. Daar zijn tot op heden weinig op maat gesneden interventies tegen voorhanden.

Bij deze drie aanbevelingen is het essentieel om de processen en uitkomsten systematisch te evalueren.

8.6 Beperkingen en toekomstig onderzoek

Dit onderzoek heeft waardevolle en unieke inzichten opgeleverd in het ontstaan, de groei, de structuur, de samenstelling en de gepleegde delicten van cybercriminele jeugdgroepen die actief zijn in Noord-Nederland. Daarnaast hebben we een duidelijker beeld gekregen van de kenmerken van cyberdaders en de wijze waarop cybercriminele jeugdgroepen worden geïdentificeerd en aangepakt. Daarmee biedt dit onderzoek nieuwe inzichten en concrete aanknopingspunten voor een effectievere bestrijding van cybercriminaliteit onder jongeren in Nederland. Tegelijkertijd kent het onderzoek enkele beperkingen. Deze zijn deels al besproken in hoofdstuk 2.
Ten eerste kan er sprake zijn van *selection bias*. De geïnterviewde experts zijn geselecteerd via ons consortium en hadden allen affiniteit met het thema 'cyber'. Hierdoor bestaat het risico dat hun perspectief afwijkt van dat van andere professionals binnen de veiligheidsketen. Bovendien kunnen individuen die bereid zijn tot een interview mogelijk andere informatie verstrekken dan degenen die geen interview willen geven. Politiemedewerkers die betrokken zijn bij internationale *high profile* opsporingsonderzoeken kunnen bijvoorbeeld een interview mijden om zo geen gevoelige en vertrouwelijke informatie prijs te geven. Ook worden expertinterviews beperkt door wat respondenten willen en kunnen delen. Hoewel zij beschikken over waardevolle kennis, inzichten en ervaringen, kunnen deze zich tijdens de interviews hebben gemengd met invullingen, interpretaties of aannames. Hierdoor hoeft hetgeen zij beschreven niet altijd volledig overeen te komen met de feitelijke situatie. Het beeld dat wij in de resultaten hebben geschetst is daarmee niet noodzakelijk volledig of sluitend, maar weerspiegelt de kennis die respondenten konden aangedragen.
Ten tweede speelt bij dit onderzoek het probleem van het *dark number*: het deel van de criminaliteit dat buiten beeld blijft. De geïnterviewde experts, de zaakreconstructies en de politieregistraties bieden uitsluitend informatie over groepen die al geïdentificeerd zijn. Groepen die nog niet op de radar staan van de autoriteiten zijn daarom niet meegenomen in de analyse. Deze niet-geïdentificeerde groepen zijn mogelijk betrokken bij cybercrime in enge zin. Dat zou een verklaring kunnen bieden voor het gebrek aan dit type groepen in ons onderzoek. Vanwege het veelvuldige gebruik van ICT voor de uitvoering van delicten door deze groepen (Matthijsse et al., 2023; Romagna & Leukfeldt, 2024b) is het goed mogelijk dat online relaties voor deze groepen juist wél een belangrijke rol spelen (Romagna & Leukfeldt, 2024b; Soudijn & Zegers, 2012).
Deze groepen kunnen ook andere kenmerken vertonen. Toekomstig onderzoek zou daarom ook cyberdaders zelf kunnen interviewen die nog onbekend zijn bij de autoriteiten, omdat zij waardevolle inzichten kunnen bieden over groepen die nog niet door

de autoriteiten zijn geïdentificeerd. Deze zouden kunnen worden benaderd via sociale mediaplatforms, zoals Snapchat of TikTok. In het verleden hebben enkele onderzoekers (Romagna & Leukfeldt, 2024b) en journalisten (Jansen et al., 2022) via deze kanalen met succes daders benaderd en geïnterviewd.

Ten derde richtte dit onderzoek zich uitsluitend op cybercriminele jeugdgroepen die actief zijn in Noord-Nederland, wat de generaliseerbaarheid van onze bevindingen beperkt. Ons doel was echter niet om een representatief beeld te geven, maar om via een brede momentopname een methodiek voor de identificatie van groepen te ontwikkelen die ook buiten Noord-Nederland toegepast kan worden. Toekomstig onderzoek kan zich richten op andere regio's in Nederland, en op het buitenland, om te toetsen in hoeverre de ontwikkelde methodiek ook daar effectief is bij het identificeren van cybercriminele jeugdgroepen. Daarnaast kan worden onderzocht in welke mate de beschreven kenmerken van groepen en hun leden zijn terug te vinden bij groepen die actief zijn in andere delen van Nederland, of zelfs in andere landen.

Tot slot verdient de definitie van groepen gehanteerd in dit onderzoek nadere aandacht. In de analyse van de politieregistraties hebben we er bewust voor gekozen om ook samenwerkingsverbanden die bestaan uit slechts twee verdachten mee te nemen. Daarnaast gold als selectiecriterium dat verdachten al als een groep werden beschouwd wanneer zij verdacht werden van het plegen van één gezamenlijk delict. Het gezamenlijk vóórkomen van twee personen in dezelfde registratie kan echter ook op toeval berusten. Hoewel zij in dat geval samen bij een delict betrokken zijn, betekent dit niet automatisch dat zij een structureel samenwerkingsverband vormen of tot dezelfde groep behoren.

Op basis van de vastgestelde criteria hebben we 26 netwerken geïdentificeerd. Wanneer echter striktere selectiecriteria worden toegepast – waarbij pas van een groep wordt gesproken als deze bestaat uit minimaal 3 verdachten die samen ten minste twee delicten hebben gepleegd – neemt het aantal geïdentificeerde groepen af met 17, tot een totaal van 9. Van deze 17 afvallende groepen bestaan er 11 uit slechts twee leden, en worden 6 groepen slechts in één politieregistratie gezamenlijk vermeld.

De inhoudelijke analyse van de 6 nader onderzochte groepen toont echter aan dat het aantal door de politie officieel aangedragen verdachten een onderschatting vormt van het werkelijke aantal betrokken personen. Dit komt omdat verdachten vaak onderdeel zijn van een grotere groep dan is vastgelegd in de bedrijfsprocessensystemen van de politie. Dit ondersteunt de keuze om ook de groepen bestaande uit 2 leden, zoals afgeleid uit de officiële gedeelde informatie, in de analyse op te nemen. Een vergelijkbare redenering geldt voor het aantal geregistreerde delicten: sommige individuen worden wel in de registraties genoemd, maar ontbreken in de officieel aangedragen data. Bovendien hadden de officiële gegevens geen betrekking op opsporingsonderzoeken, betroffen de politieregistraties slechts een beperkte periode van één jaar, en is het goed mogelijk dat mededaders wel meerdere delicten samen hebben gepleegd, maar dat deze niet in registraties zijn vastgelegd.

Deze beperkingen kunnen in vervolgonderzoek worden ondervangen door een langere onderzoeksperiode voor de politieregistraties te hanteren, opsporingsonderzoeken

erbij te betrekken, en politieregistraties kwalitatief te analyseren om zo alle betrokken verdachten in kaart te brengen. Dit heeft daarnaast het voordeel dat ook de onderlinge relaties tussen verdachten preciezer in kaart kunnen worden gebracht.
Verder is er behoefte aan onderzoek naar de geografische verspreiding van cybercriminele jeugdgroepen. Uit eerder onderzoek is naar voren gekomen dat deze groepen veelal lokaal verankerd zijn omdat mededaders elkaar ontmoeten via offline banden. Maar de werkelijke geografische spreiding blijft onduidelijk. Hoewel het merendeel van de cybercriminele jeugdgroepen in ons onderzoek ook lokaal verankerd is, komt uit de resultaten naar voren dat dergelijke groepen mogelijk minder lokaal zijn ingebed dan eerder werd gedacht, gezien het belang van online ontmoetingsplaatsen en meerdere voorbeelden van groepen waarbij leden in verschillende delen van Nederland wonen. Toekomstig onderzoek zou kunnen verkennen in hoeverre deze geografische spreiding daadwerkelijk plaatsvindt en welke implicaties dit heeft voor de aanpak en samenwerking tussen regio's.
Tot slot is meer onderzoek nodig naar de factoren die mogelijk samenhangen met de betrokkenheid van jongeren bij cybercrime. Een beter begrip van de onderliggende mechanismen en risicofactoren kan lokale partners helpen bij het ontwikkelen van gerichte interventies en kan bijdragen aan het verminderen van het risico dat jongeren betrokken raken bij cybercrime, zoals beschreven in paragraaf 8.4.

Referenties

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*, 14773708241250278. https://doi.org/10.1177/14773708241250278

Adejoh, S. O., Tunde, A. A., Waziri, A. & Nnenna, M. E. (2019). *'Yahoo Boys' Phenomenon in Lagos Metropolis: A Qualitative Investigation*. https://doi.org/10.5281/ZENODO.3366298

Adou, E. F. S. & Kolé, M. S. (2020). 'Je suis au bara' or the deviant use of the Internet among Abidjan's scammers. In J. Atchoua, J. Bogui & S. Diallo (Red.), *Digital technologies and African societies* (1ste dr., p. 107-126). Wiley. https://onlinelibrary.wiley.com/doi/10.1002/9781119777304.ch6

Akkermans, M., Derksen, E., Kennis, M., Kloosterman, R. & Moons, E. (2024). *Veiligheidsmonitor 2023*, p. 118. WODC.

Akkermans, M., Kloosterman, R., Moons, E., Reep, C. & Tummers-van der Aa, M. (2022). *Veiligheidsmonitor 2021*. Centraal Bureau voor de Statistiek.

Albini, J. L. (1971). *The American Mafia: Genesis of a legend*. Appleton- Century-Crofts.

APWG. (2025). *Phishing activity trends report: 4th quarter 2024*. Anti Phishing Working Group. https://docs.apwg.org/reports/apwg_trends_report_q4_2024.pdf

Auguie, B. (2010). *gridExtra: Miscellaneous Functions for 'Grid' Graphics* [Software]. https://doi.org/10.32614/CRAN.package.gridExtra

Beijersbergen, K. A., Tollenaar, N., Kros, M., Piersma, T. W. & Weijters, G. (2023). *De effectiviteit van de Top600-aanpak: Een vergelijkend recidiveonderzoek onder veelplegers* (No. Cahier 2023-18; p. 180). WODC.

Beke, B. M. W. A., Ferwerda, H., Van der Torre, E. & Bervoets, E. (2013). *Jeugdgroepen en Geweld. Van signalering naar aanpak*, p. 170. Boom Lemma uitgevers.

Beke, B. M. W. A. & Van Wijk, A. Ph. (2001). Problematische jeugdgroepen: Typen, kenmerken en achtergronden. *Delikt en Delinkwent*.

Beke, B. M. W. A., Van Wijk, A. Ph. & Ferwerda, H. (2000). *Jeugdcriminaliteit in groepsverband ontrafeld. Tussen rondhangen en bendevorming*, p. 152. WODC.

Bekkers, L. M. J., Leukfeldt, E. R. & Kleemans, E. (2024). Recruiting co-offenders for financial cybercrime: An analysis of police investigations into cybercriminal networks. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-024-09556-y

Bekkers, L. M. J. & Leukfeldt, E. R. (2023). Recruiting money mules on Instagram: A qualitative examination of the online involvement mechanisms of cybercrime. *Deviant Behavior*, *44*(4), 603-619. https://doi.org/10.1080/01639625.2022.2073298

Bekkers, L. M. J., Moneva, A. & Leukfeldt, E. R. (2022). Understanding cybercrime involvement: A quasi-experiment on engagement with money mule recruitment ads on Instagram. *Journal of Experimental Criminology*. https://doi.org/10.1007/s11292-022-09537-7

Bekkers, L. M. J., 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

Bellotti, E., Spencer, J., Lord, N. & Benson, K. (2020). Counterfeit alcohol distribution: A criminological script network analysis. *European Journal of Criminology*, *17*(4), 373-398. https://doi.org/10.1177/1477370818794870

Borwell, J., Jansen, J. & Stol, W. (2022). The Psychological and Financial Impact of Cybercrime Victimization: A Novel Application of the Shattered Assumptions Theory. *Social Science Computer Review*, *40*(4), 933-954. https://doi.org/10.1177/0894439320983828

Bossler, A. M. (2021a). Neutralizing cyber attacks: Techniques of neutralization and willingness to commit cyber attacks. *American Journal of Criminal Justice*, *46*(6), 911-934. https://doi.org/10.1007/s12103-021-09654-5

Bossler, A. M. (2021b). Perceived formal and informal sanctions in deterring cybercrime in a college sample. *Journal of Contemporary Criminal Justice*, *37*(3), 452-470. https://doi.org/10.1177/10439862211001630

Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Brenner, S. W. (2002). Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships. *North Carolina Journal of Law & Technology*, *4*(1), 1-50.

Bulanova-Hristova, G., Kasper, K., Odinot, G., Verhoeven, M., Pool, R., De Poot, C., Werner, Y. & Korsell, L. (2016). *Cyber-OC – Scope and manifestations in selected EU member states*, p. 298.

Bureau Beke. (z.d.). *Handreiking duiding problematisch jeugdgroepgedrag*. https://bureaubeke.nl/bureau/kerntaken/van-shortlistmethodiek-of-groepsaanpak-naar-7-stappenmodel/

Burt, R. S. (1992). *Structural holes*. Harvard University Press.

Calderoni, F., Campedelli, G. M., Comunale, T., Marchesi, M. E. & Savona, E. U. (2020). *Recruitment into organised criminal groups: A systematic review*. Australian Institute of Criminology.

Calderoni, F., Comunale, T., Campedelli, G. M., Marchesi, M., Manzi, D. & Frualdo, N. (2022). Organized crime groups: A systematic review of individual-level risk factors related to recruitment. *Campbell Systematic Reviews*, *18*(1), e1218. https://doi.org/10.1002/cl2.1218

Cayubit, R. F. O., Rebolledo, K. M., Kintanar, R. G. A., Pastores, A. G., Santiago, A. J. A. & Valles, P. B. V. (2017). A Cyber Phenomenon: A Q-Analysis on the Motivation of Computer Hackers. *Psychological Studies*, *62*(4), 386-394. https://doi.org/10.1007/s12646-017-0423-9

CCV. (z.d.-a). *Inspirerende start programma Preventie met Gezag*. Geraadpleegd 10 september 2023, van https://hetccv.nl/inspirerende-start-programma-preventie-met-gezag/

CCV. (z.d.-b). *'Preventie met gezag'-gemeenten enthousiast over jeugd- en cyberprojecten*. https://hetccv.nl/preventie-met-gezag-gemeenten-enthousiast-over-jeugd-en-cyberprojecten/

CCV. (2018). *Aanpak criminele jeugdgroepen*, p. 2. Centrum voor Criminaliteitspreventie en Veiligheid.

CCV. (2022). *Aanpak risicojeugd en jeugdgroepen: Houd jongeren uit de georganiseerde criminaliteit*, p. 9. Centrum voor criminaliteitspreventie en veiligheid.

CCV. (2023a). *Het 7-stappenmodel: Werkproces aanpak problematische jeugdgroepen en groepsgedrag*. Centrum voor Criminaliteitspreventie en Veiligheid.

CCV. (2023b). *Interventies op het gebied van jeugd en cybercrime*. Centrum voor Criminaliteitspreventie en Veiligheid. https://hetccv.nl/app/uploads/2023/12/Interventies-op-het-gebied-van-Jeugd-en-Cybercrime-DEF-20231212.pdf

CCV. (2024, 23 september). *Oproep: Verbeter samen met het CCV het 7-stappenmodel*. https://wegwijzerjeugdenveiligheid.nl/actueel/verbeter-met-het-ccv-het-stappenmodel/

Chen, S., Yuan, Y., Luo, X., Jian, J. & Wang, Y. (2021). Discovering group-based transnational cyber fraud actives: A polymethodological view. *Computers & Security*, *104*, 102217. https://doi.org/10.1016/j.cose.2021.102217

Chon, K. H. (2016). *Cybercrime precursors: Towards a model of offender resources* [PhD Thesis, Australian National University]. http://hdl.handle.net/1885/107344

Choo, K.-K. R. & Smith, R. G. (2008). Criminal Exploitation of Online Systems by Organised Crime Groups. *Asian Journal of Criminology*, *3*(1), 37-59. https://doi.org/10.1007/s11417-007-9035-y

Chua, Y. T. & Holt, T. J. (2016). A Cross-National Examination of the Techniques of Neutralization to Account for Hacking Behaviors. *Victims & Offenders*, *11*(4), 534-555. https://doi.org/10.1080/15564886.2015.1121944

Csárdi, G., Nepusz, T., Müller, K., Horvát, S., Traag, V., Zanini, F. & Noom, D. (2024). *igraph for R: R interface of the igraph library for graph theory and n etwork analysis* (Versie v2.0.2) [Software]. Zenodo. https://zenodo.org/doi/10.5281/zenodo.7682609

Davidson, J., Aiken, M., Phillips, K. & Farr, R. (2022). *European youth cybercrime, online harm and online risk taking: 2022 Research report*. Institute for Connected Communities, University of East London.

De Boer, H., Ferwerda, H. & Kuppens, J. (2022). *Do or Don't: Kennissynthese ingroeimechanismen en rekruteringsprocessen van jongeren in de georganiseerde criminaliteit*. WODC.

De Jonge, E. (2016). *cbsodataR: Statistics Netherlands (CBS) Open Data API Client* [Software]. https://doi.org/10.32614/CRAN.package.cbsodataR

De Seranno, S. & Colman, C. (2023). Entry Mechanisms into the Belgian Synthetic Drugs Market. *Journal of Drug Issues*, 00220426231205523. https://doi.org/10.1177/00220426231205523

Densley, J. A. (2012). Street Gang Recruitment: Signaling, Screening, and Selection. *Social Problems*, *59*(3), 301-321. https://doi.org/10.1525/sp.2012.59.3.301

Dragos. (2023). *Ics/ot cybersecurity: Year in review 2022*, p. 70. Dragos.

Duijn, P. A. C., Kashirin, V. & Sloot, P. M. A. (2014). The Relative Ineffectiveness of Criminal Network Disruption. *Scientific Reports*, *4*(1), 4238. https://doi.org/10.1038/srep04238

ECLI:NL:RBNNE:2022:5360, No. ECLI:NL:RBNNE:2022:5360 (Rechtbank Noord-Nederland 1 december 2022).

ECLI:NL:RBNNE:2024:51, No. ECLI:NL:RBNNE:2024:51 (Rechtbank Noord-Nederland 12 januari 2024).

ECLI:NL:RBNNE:2024:52, No. ECLI:NL:RBNNE:2024:52 (Rechtbank Noord-Nederland 12 januari 2024).

ENISA. (2024). *Enisa threat landscape 2024: July 2023 to June 2024*. ENISA.

Erasmus Universiteit Rotterdam. (2025, maart 17). *Cocaïne in de Rotterdamse haven: Een kat-en-muisspel*. https://www.eur.nl/nieuws/cocaine-de-rotterdamse-haven- een-kat-en-muisspel

Esbensen, F.-A. & Weerman, F. M. (2005). Youth Gangs and Troublesome Youth Groups in the United States and the Netherlands: A Cross-National Comparison. *European Journal of Criminology*, *2*(1), 5-37. https://doi.org/10.1177/1477370805048626

European Union Agency for Law Enforcement Cooperation. (2021). *IOCTA 2021: Internet organised crime threat assessment 2021*. Publications Office of the European Union; DOI.org (CSL JSON). https://data.europa.eu/doi/10.2813/113799

Europol. (2020, 13 maart). *The SIM highjackers: How criminals are stealing millions by highjacking phone numbers*. https://www.europol.europa.eu/media-press/newsroom/news/sim-highjackers-how-criminals-are-stealing-millions-highjacking-phone-numbers

Europol. (2024). *IOCTA, internet organised crime threat assessment 2024*. Publications Office. https://data.europa.eu/doi/10.2813/442713

FBI. (2025, januari 30). *Cybercrime websites selling hacking tools to transnational organized crime groups seized*. https://www.justice.gov/usao-sdtx/pr/cybercrime-websites-selling-hacking-tools-transnational-organized-crime-groups-seized

Felson, M. (2003). The Process of Co-offending. In M. J. Smith & D. B. Cornish (Red.), *Theory for practice in situational crime prevention. Crime prevention studies* (Vol. 16, p. 149-167). Criminal Justice Press.

Felson, M. (2006). *The Ecosystem for Organized Crime*, p. 20. HEUNI paper nr 26.

Fereday, J. & Muir-Cochrane, E. (2006). Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development. *International Journal of Qualitative Methods*, *5*(1), 80-92. https://doi.org/10.1177/160940690600500107

Ferwerda, H. (2000). Jeugdcriminaliteit onder de loep. De groep als negatieve voedingsbodem. *J* – tijdschrift over jongeren*, *1*, 34-44.

Ferwerda, H., Beke, B. M. W. A. & Bervoets, E. (2017). De onzichtbare invloed van bovenlokale criminele netwerken op de wijk. *Tijdschrift voor de Politie*.

Ferwerda, H., Brouwer, N., Hölzken, I. & Kroese, L. (2021). *Misdaadcarrières voorkomen en doorbreken: Van analyse van het netwerk naar aanpak*. Bureau Beke.

Ferwerda, H. & Kloosterman, A. (2004). *Jeugdgroepen in beeld: Stappenplan en randvoorwaarden voor de shortlistmethodiek*. Advies- en Onderzoeksgroep Beke; Politie Gelderland-Midden.

Ferwerda, H. & Van Ham, T. (2010). *Problematische Jeugdgroepen in Nederland: Omvang, aard en politieproces beschreven*. Bureau Beke.

Ferwerda, H. & Van Ham, T. (2011). *Problematische Jeugdgroepen in Nederland; Omvang en aard in het najaar van 2010*. Bureau Beke. http://www.beke.nl/doc/2010/Prob_jeugdgoep_najaar_2010.pdf

Ferwerda, H. & Van Ham, T. (2014). *Problematische jeugdgroepen in Nederland: Omvang en aard in het najaar van 2014*. Bureau Beke.

Ferwerda, H. & Van Ham, T. (2017). Lessen uit de aanpak van jeugdgroepen. *Justitiële verkenningen*, *43*(1), 112-126. https://doi.org/10.5553/JV/016758502017043001008

Ficara, A., Curreri, F., Fiumara, G. & De Meo, P. (2023). Human and Social Capital Strategies for Mafia Network Disruption. *IEEE Transactions on Information Forensics and Security*, *18*, 1926-1936. https://doi.org/10.1109/TIFS.2023.3256706

Fox, B. & Holt, T. J. (2021). Use of a multitheoretic model to understand and classify juvenile computer hacking behavior. *Criminal Justice and Behavior*, *48*(7), 943-963. https://doi.org/10.1177/0093854820969754

Frualdo, N. (2019). A *systematic review of factors leading to recruitment into organized crime*. Northwestern University.

Fusch, P. & Ness, L. (2015). Are We There Yet? Data Saturation in Qualitative Research. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2015.2281

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

Gemeente Amsterdam. (z.d.). *Aanpak problematische jeugdgroepen*. Geraadpleegd 23 mei 2022, van https://www.amsterdam.nl/wonen-leefomgeving/veiligheid/aanpak-problematische-jeugdgroepen/

Gemeente Rotterdam. (2023). *Uitvoeringsprogramma Preventie met Gezag*.

Gemeente Schiedam. (z.d.). *Preventie met Gezag*. Geraadpleegd 10 september 2023, van https://www.schiedam.nl/a-tot-z/preventie-met-gezag#:~:text=Het%20programma%20Preventie%20met%20Gezag,Verschillende%20organisaties%20werken%20hieraan%20mee.

Holman, T. (2016). Gonna Get Myself Connected. The Role of Facilitation in Foreign Fighter Mobilizations. *Perspectives on Terrorism*, *10*(2), 2-23.

Holt, T. J., Navarro, J. N. & Clevenger, S. (2020). Exploring the moderating role of gender in juvenile hacking behaviors. *Crime & Delinquency*, *66*(11), 1533-1555. https://doi.org/10.1177/0011128719875697

Holt, T. J. & Steinmetz, K. F. (2021). Examining the role of power-control theory and self-control to account for computer hacking. *Crime & Delinquency*, *67*(10), 1491-1512. https://doi.org/10.1177/0011128720981892

Hutchings, A. (2014). Crime from the keyboard: Organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change*, *62*(1), 1-20. https://doi.org/10.1007/s10611-014-9520-z

Ibrahim, S. (2016). Causes of socioeconomic cybercrime in Nigeria. *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, 1-9. https://doi.org/10.1109/ICCCF.2016.7740439

Interpol. (2024, 12 maart). *INTERPOL campaign warns against cyber and financial crimes*. https://www.interpol.int/News-and-Events/News/2024/INTERPOL-campaign-warns-against-cyber-and-financial-crimes

Jansen, N., Van Hulzen, D. & Schellevis, J. (2022, 14 december). *Dit zijn de jongeren achter online oplichting: 'Het is een soort hype'*. https://nos.nl/artikel/2456409-dit-zijn-de-jongeren-achter-online-oplichting-het-is-een-soort-hype

Jegede, A. E., Elegbeleye, A. O., Olowookere, E. I. & Olorunyomi, B. R. (2016). Gendered alternative to cyber fraud participation: An assessment of technological driven crime in Lagos state, Nigeria. *Gender & Behaviour*, *14*(3), 7672-7692.

Jeugdboa.nl. (z.d.). *Methode PLUS MIN MEE®*. Geraadpleegd 10 september 2023, van https://jeugdboa.nl/methode-plus-min-mee/

Jewkes, Y. & Yar, M. (2012). Policing Cybercrime in the twenty-first century. In T. Newburn (Red.), *Handbook of Policing* (2nd ed). Taylor and Francis.

Kao, D.-Y., Huang, F. F.-Y. & Wang, S.-J. (2009). Persistence and desistance: Examining the impact of re-integrative sha ming to ethics in taiwan juvenile hackers. *Computer Law and Security Review*, *25*(5), 464-476. https://doi.org/10.1016/j.clsr.2009.05.009

Kemp, L., Zolghadriha, S. & Gill, P. (2020). Pathways into organized crime: Comparing founders and joiners. *Trends in Organized Crime*, *23*(3), 203-226. https://doi.org/10.1007/s12117-019-09371-w

Kleemans, E. R. (2007). Organized Crime, Transit Crime, and Racketeering. *Crime and Justice*, *35*(1), 163-215. https://doi.org/10.1086/501509

Kleemans, E. R. (2013). *Theoretical Perspectives on Organized Crime*. Oxford University Press; https://academic.oup.com/edited-volume/38662/chapter/335786027

Kleemans, E. R. (2016). Organized Crime Research: Challenging assumptions and informing policy. In E. Cockbain & J. Knutsson (Red.), *Applied police research: Challenges and opportunities* (pp. 57-67). Routledge.

Kleemans, E. R. & De Poot, C. J. (2008). Criminal Careers in Organized Crime and Social Opportunity Structure. *European Journal of Criminology*, *5*(1), 69-98. https://doi.org/10.1177/1477370807084225

Kleemans, E. R. & Van de Bunt, H. G. (1999). The social embeddedness of organized crime. *Transnational Organized Crime*, *5*(1), 19-36.

Kleemans, E. R., Van den Berg, E. A. I. M. & Van de Bunt, H. G. (1998). *Georganiseerde criminaliteit in Nederland: Rapportage op basis van de WODC-monitor*, p. 179. WODC.

Kleemans, E. R. & Van Koppen, V. (2020). Organized Crime and Criminal Careers. *Crime and Justice*, *49*, 385-423. https://doi.org/10.1086/707318

Klein, M. W. & Maxson, C. L. (2006). *Street gang patterns and policies*. Oxford University Press; K10plus ISBN.

Kruisbergen, E. & De Jonge, M. (2023). Voorkomen is beter dan genezen…, toch?: Over goed bedoelde maar potentieel schadelijke vormen van preventie van ondermijning. *Tijdschrift voor Veiligheid*, *22*(3), 3-24. https://doi.org/10.5553/TvV/.000057

Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R. & Roks, R. A. (2018). *Georganiseerde criminaliteit en ICT*, p. 165. WODC.

Kruisbergen, E. W., Leukfeldt, R., Kleemans, E. R. & Roks, R. A. (2018b). Criminele geldstromen en ICT: Over innovatieve werkwijzen, oude zekerheden en nieuwe flessenhalzen. *Justitiële verkenningen*, *44*(5), 23-39. https://doi.org/10.5553/JV/016758502018044005003

Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R. & Roks, R. A. (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

Landelijk projectteam proeftuinen. (2016). *Werkproces integrale aanpak problematische jeugdgroepen en groepsgedrag*.

Lavorgna, A. (2013). *Transit crimes in the internet age: How new online criminal opportunities affect the organization of offline transit crimes* [University of Trento]. https://core.ac.uk/download/pdf/35317313.pdf

Lee, J. R. & Holt, T. J. (2020). Assessing the Factors Associated With the Detection of Juvenile Hacking Behaviors. *Frontiers in Psychology*, *11*, 840. https://doi.org/10.3389/fpsyg.2020.00840

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. https://doi.org/10.1016/j.chb.2021.106979

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., Kleemans, E. R. & Stol, W. P. (2016). Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks. *British Journal of Criminology*, 1-19. https://doi.org/10.1093/bjc/azw009

Leukfeldt, E. R., Kleemans, E. R. & Stol, W. P. (2017a). A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change*, *67*(1), 21-37. https://doi.org/10.1007/s10611-016-9662-2

Leukfeldt, E. R., Kleemans, E. R. & Stol, W. P. (2017b). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change*, *67*(1), 39-53. https://doi.org/10.1007/s10611-016-9663-1

Leukfeldt, E. R., Lavorgna, A. & Kleemans, E. R. (2017). Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research*, *23*(3), 287-300. https://doi.org/10.1007/s10610-016-9332-z

Leukfeldt, E. R., Loggen, J. & Veenstra, S. (z.d.). *Criminele jeugdnetwerken in een digitaliserende samenleving: Handreikingen voor de integrale aanpak van (cyber)criminele jeugdnetwerken op lokaal niveau.* 2021.

Leukfeldt, E. R., Spithoven, R. & Misana-ter Huurne, E. (2020). De lokale aanpak van cybercrime. Risicocommunicatie als antwoord op een grenzeloos vraagstuk. In C. De Poot, E. Lievens, W. Stol & L. De Kimpe (Red.), *Politie en cybercrime*. Gompel & Svacina.

Leukfeldt, E. Rutger. (2014). Cybercrime and social ties: Phishing in Amsterdam. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-014-9229-5

Leukfeldt, E. Rutger & Holt, T. J. (2020). Examining the Social Organization Practices of Cybercriminals in the Netherlands Online and Offline. *International Journal of Offender Therapy and Comparative Criminology*, *64*(5), 522-538. https://doi.org/10.1177/0306624X19895886

Leukfeldt, E. Rutger & Kleemans, E. R. (2021). Breaking the Walls of Silence: Analyzing Criminal Investigations to Improve Our Understanding of Cybercrime. In A. Lavorgna & T. J. Holt (Red.), *Researching Cybercrimes* (pp. 127-144). Springer International Publishing. https://link.springer.com/10.1007/978-3-030-74837-1_7

Leukfeldt, E. Rutger, Notté, R. & Malsch, M. (2018). *Slachtofferschap van online criminaliteit: Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit*, p. 186. NSCR.

Leukfeldt, E. Rutger & Roks, R. A. (2021). Cybercrimes on the Streets of the Netherlands? An Exploration of the Intersection of Cybercrimes and Street Crimes. *Deviant Behavior*, *42*(11), 1458-1469. https://doi.org/10.1080/01639625.2020.1755587

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, *4*(3), 324. https://doi.org/10.4103/2249-4863.161306

Loggen, J. & Leukfeldt, E. 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. https://doi.org/10.1007/s12117-022-09448-z

Loggen, J., Moneva, A. & Leukfeldt, E. R. (2024a). A systematic narrative review of pathways into, desistance from, and risk factors of financial-economic cyber-enabled crime. *Computer Law & Security Review*, *52*, 105858. https://doi.org/10.1016/j.clsr.2023.105858

Loggen, J., Moneva, A. & Leukfeldt, E. R. (2024b). Pathways into, desistance from, and risk factors related to cyber-dependent crime: A systematic narrative review. *Victims & Offenders*, 1-32. https://doi.org/10.1080/15564886.2024.2370295

Lusthaus, J., Kleemans, E., Leukfeldt, E. R., Levi, M. & Holt, T. J. (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

Magouirk, J., Atran, S. & Sageman, M. (2008). Connecting Terrorist Networks. *Studies in Conflict & Terrorism*, *31*(1), 1-16. https://doi.org/10.1080/10576100701759988

Maimon, D. & Louderback, E. R. (2019). Cyber-Dependent Crimes: An Interdisciplinary Review. *Annual Review of Criminology*, *2*(1), 191-216. https://doi.org/10.1146/annurev-criminol-032317-092057

Matthijsse, S. R., Van 't Hoff-de Goede, M. S. & Leukfeldt, E. R. (2023). Your files have been encrypted: A crime script analysis of ransomware attacks. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-023-09496-z

McGuire, M. & Dowling, S. (2013). *Cyber crime: A review of the evidence Research Report 75; Summary of key findings and implications* [75]. Home Office UK. https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

Meijer, P. C., Verloop, N. & Beijaard, D. (2002). Multi-method triangulation in a qualitative study on teachers' practic al knowledge: An attempt to increase internal validity. *Quality and Quantity*, *36*, 145-167. Zotero. https://doi.org/10.1023/A:1014984232147

Mellor, B., MacRae, L., Pauls, M. & Hornick, J. P. (2005). *Youth gangs in canada: A preliminary review of programs and services*, p. 103. Canadian Research Institute for Law and the Family (CRILF).

Ministerie van Justitie en Veiligheid, Politie, Openbaar Ministerie & Vereniging Nederlandse Gemeenten. (2022, maart 10). *Convenant jeugdgroepaanpak*.

Mishra, S. & Soni, D. (2020). Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis. *Future Generation Computer Systems*, *108*, 803-815. https://doi.org/10.1016/j.future.2020.03.021

Moffitt, T. E. (Red.). (2007). A Review of Research on the Taxonomy of Life-Course Persistent Versus Adolescence-Limited Antisocial Behavior. In *The Cambridge Handbook of Violent Behavior and Aggression* (1ste dr., p. 49-74). Cambridge University Press. https://doi.org/10.1017/cbo9780511816840.004

Morris, R. G. & Blackburn, A. G. (2009). Cracking the code: An empirical exploration of social learning theory and computer crime. *Journal of Crime and Justice*, *32*(1), 1-34. https://doi.org/10.1080/0735648X.2009.9721260

Müller, K. (2017). *here: A Simpler Way to Find Your Files*, p. 1.0.1 [Software]. https://CRAN.R-project.org/package=here

Ministerie van Justitie en Veiligheid. (z.d.). *Aanpak problematische Jeugdgroepen*. Ministerie van Justitie en Veiligheid.

Ministerie van Justitie en Veiligheid. (2024). *Actieplan 2024*, p. 11. Ministerie van Justitie en Veiligheid. https://open.overheid.nl/documenten/dpc-ce0298ac2bf3346d-36d681989513f4792fc089bc/pdf

Nguyen, T. & Luong, H. T. (2021). The structure of cybercrime networks: Transnational computer fraud in Vietnam. *Journal of Crime and Justice*, *44*(4), p. 419-440. https://doi.org/10.1080/0735648X.2020.1818605

NJI. (2023, 30 januari). *Overlast door jongeren*. https://www.nji.nl/cijfers/overlast

Nurse, J. R. C. & Bada, M. (2019). The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations. In A. Attrill-Smith, C. Fullwood, M. Keep & D. J. Kuss (Red.), *The Oxford Handbook of Cyberpsychology* (pp. 690-715). Oxford University Press. https://academic.oup.com/edited-volume/41352/chapter/352517258

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

Odinot, G., Verhoeven, M. A., Pool, R. L. D. & De Poot, C. J. (2017). *Organised Cybercrime in the Netherlands*. WODC. http://hdl.handle.net/20.500.12832/179

Ogunleye, Y. O., Ojedokun, U. A. & Aderinto, A. A. (2020). Pathways and motivations for cyber fraud involvement among female unde rgraduates of selected universities in south-west Nigeria. *International Journal of Cyber Criminology*, *13*(2), 309-325. https://doi.org/10.5281/ZENODO.3702333

Oosterwijk, K. & Fischer, T. (2017). *Interventies jeugdige daders cybercrime*, p. 81. WODC.

Openbaar Ministerie. (2024). *Cybercrimebeeld Nederland 2024*. https://fts.politie.nl/cybercrimebeeld/

Openbaar Ministerie. (2025). *Vijftien verdachten verhoord: 39 aangiftes van oplichting behandeld door politie en OM*. https://www.om.nl/actueel/nieuws/2025/03/25/vijftien-verdachten-verhoord-39-aangiftes-van-oplichting-behandeld-door-politie-en-om

Ouellet, M., Bouchard, M. & Charette, Y. (2019). One gang dies, another gains? The network dynamics of criminal group persistence*. *Criminology*, *57*(1), 5-33. https://doi.org/10.1111/1745-9125.12194

Paoli, L. (2014). The Italian Mafia. In L. Paoli (Red.), *The Oxford Handbook of Organized Crime*. Oxford University Press. http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199730445.001 .0001/oxfordhb-9780199730445-e-025

Pebesma, E. & Bivand, R. (2023). *Spatial Data Science: With Applications in R* (1ste dr.). Chapman and Hall/CRC. https://www.taylorfrancis.com/books/9780429459016

Pedersen, T. L. (2017a). *ggraph: An Implementation of Grammar of Graphics for Graphs and Networks* [Software]. https://doi.org/10.32614/CRAN.package.ggraph

Pedersen, T. L. (2017b). *tidygraph: A Tidy API for Graph Manipulation* [Software]. https://doi.org/10.32614/CRAN.package.tidygraph

Pedersen, T. L. (2019). *patchwork: The Composer of Plots* [Software]. https://doi.org/10.32614/CRAN.package.patchwork

Peersman, C., Williams, E., Edwards, M. & Rashid, A. (2022). *Understanding motivations and characteristics of financially-motivated cybercriminals*, p. 23. Bristol Cyber Security Group, University of Bristol. https://arxiv.org/abs/2203.08642

Peeters, T. & Dongen, T. (2022). *Schijnwerpers op de straat*. Verwey-Jonker Instituut; Zotero.

Polman, I. (2016). *7-stappenmodel, de praktijk*, p. 87.

Programma Straatwaarde(n). (2020). *Definiëring jonge aanwas, doorgroeier, negatief rolmodel*. RIEC Midden-Nederland.

Pyrooz, D. C. & Densley, J. A. (2016). Selection into Street Gangs: Signaling Theory, Gang Membership, and Criminal Offending. *Journal of Research in Crime and Delinquency*, *53*(4), p. 447-481. https://doi.org/10.1177/0022427815619462

R Core Team. (2024). *R: A Language and Environment for Statistical Computing* [Software]. https://www.r-project.org/

RIEC. (2019). *Werkproces integrale casusaanpak door het Regionaal Informatie en Expertise Centrum (RIEC): Model van de manier van werken bij de integrale casusaanpak*, p. 33.

RIEC. (2022). *Fenomeenanalyse Jeugdige Ondermijners Limburg*. Regionaal Informatie en Expertise Centrum Limburg.

Rijksoverheid. (z.d.). *Aanpak voorkomen ondermijnende jeugdcriminaliteit*. Geraadpleegd 6 december 2025, van https://www.rijksoverheid.nl/onderwerpen/ondermijning/ondermijnende-jeugdcriminaliteit

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

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. https://doi.org/10.5553/JV/016758502020046002004

Roks, R. A. & Van den Broek, J. (2018). #HOUHETSTRAAT: Straatcultuur op social media? *Tijdschrift over Cultuur & Criminaliteit*, *7*(3), 31-50. https://doi.org/10.5553/TCC/221195072017007003003

Romagna, M. & Leukfeldt, E. R. (2024a). Hacktivism: From Loners to Formal Organizations? Assessing the Social Organization of Hacktivist Networks. *Deviant Behavior*, 1-21. https://doi.org/10.1080/01639625.2024.2431066

Romagna, M. & Leukfeldt, E. R. (2024b). Social Opportunity Structures in Hacktivism: Exploring Online and Offline Social Ties and the Role of Offender Convergence Settings in Hacktivist Networks. *Victims & Offenders*, 1-23. https://doi.org/10.1080/15564886.2024.2372054

Rozema, L. T. (2018). *Eindevaluatie aanpak problematische jeugdgroepen*, p. 17. Gemeente Groningen.

RStudio Team. (2024). *RStudio: Integrated Development Environment for R* [Software]. http:// www. rstud io. com/

Ruiter, S., Van Leuken, M., Van Ruitenburg, T., Schiks, J. & Leukfeldt, R. (2023). *In- en doorstroom van online criminaliteit in de strafrechtketen*, p. 186. NSCR.

Schellevis, J. & Van Hulzen, D. (2022, 14 december). *Jongeren vaker betrokken bij fraude en cybercrime, politie maakt zich zorgen*. https://nos.nl/artikel/2456322-jongeren-vaker-betrokken-bij-fraude-en- cybercrime-politie-maakt-zich-zorgen

Schiks, J., Bekkers, L. M. J. & Leukfeldt, R. (2021). *Naar een interventie tegen geldezels: Een experiment op Instagram*, p. 16. De Haagse Hogeschool.

Schwarzenbach, A. & Jensen, M. (2024). Extremists of a feather flock together? Community structures, transitivity, and patterns of homophily in the US Islamist co-offending network. *PLOS ONE*, *19*(6), e0298273. https://doi.org/10.1371/journal.pone.0298273

Sciarrone, R. (2014). 'Ndrangheta: A Reticular Organization. In N. Serenata (Red.), *The 'Ndrangheta and Sacra Corona Unita* (Vol. 12, p. 81-99). Springer International Publishing. https://link.springer.com/10.1007/978-3-319-04930-4_6

Seigfried-Spellar, K. C., O'Quinn, C. L. & Treadway, K. N. (2015). Assessing the relationship between autistic traits and cyberdeviancy in a sample of college students. *Behaviour & Information Technology*, *34*(5), 533-542. https://doi.org/10.1080/0144929X.2014.978377

Seigfried-Spellar, K. C. & Treadway, K. N. (2014). Differentiating Hackers, Identity Thieves, Cyberbullies, and Virus Writers by College Major and Individual Differences. *Deviant Behavior*, *35*(10), 782-803. https://doi.org/10.1080/01639625.2014.884333

Seigfried-Spellar, K. C., Villacís-Vukadinović, N. & Lynam, D. R. (2017). Computer criminal behavior is related to psychopathy and other antisocial behavior. *Journal of Criminal Justice*, *51*, 67-73. https://doi.org/10.1016/j.jcrimjus.2017.06.003

Selzer, N. & Oelrich, S. (2021). Saint or satan? Moral development and dark triad influences on cybercriminal intent. In M. Weulen Kranenbarg & E. R. Leukfeldt (Red.), *Cybercrime in context: Vol. I* (pp. 175-194). Springer International Publishing. https://link.springer.com/10.1007/978-3-030-60527-8_11

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-z

Spapens, T. & Moors, H. (2020). Intergenerational transmission and organised crime. A study of seven families in the south of the Netherlands. *Trends in Organized Crime*, *23*(3), 227-241. https://doi.org/10.1007/s12117-019-09363-w

Storrod, M. L. & Densley, J. A. (2017). '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

Tollenaar, N., Beijers, J. & Van der Laan, A. M. (2024). *Monitor zelfgerapporteerde jeugddelinquentie 2023*, p. 129. WODC.

Udris, R. (2016). *Cyberdeviance among Adolescents*. https://doi.org/10.18910/56042

Van der Wagen, W., Fischer, T., Matthijsse, S. & Van 't Zand, E. (2021). Unique offender, unique response? Assessing the suitability and effectiveness of interventions for cyber offenders. In M. Weulen Kranenbarg & E. R. Leukfeldt (Red.), *Cybercrime in*

context: Vol. I (pp. 371-390). Springer International Publishing. https://link.springer.com/10.1007/978-3-030-60527-8_20

Van der Wagen, W., Weulen Kranenbarg, M. & Oerlemans, J.-J. (2020). Inleiding. In W. Van der Wagen, M. Weulen Kranenbarg & J.-J. Oerlemans (Red.), *Basisboek cybercriminaliteit: Een criminologisch overzicht voor studie en praktijk*. Boom Criminologie; Open WorldCat.

Van Dijk, M., Kleemans, E. & Eichelsheim, V. (2019). Children of Organized Crime Offenders: Like Father, Like Child? An Explorative and Qualitative Study Into Mechanisms of Intergenerational (Dis)Continuity in Organized Crime Families. *European Journal on Criminal Policy and Research*, *25*(4), p. 345-363. https://doi.org/10.1007/s10610-018-9381-6

Van Gemert, F. (2005). Youth Groups and Gangs in Amsterdam: An Inventory based on the Eurogang Expert Survey. In S. H. Decker & F. M. Weerman (Red.), *European street gangs and troublesome youth groups: Findings from the Eurogang Research Program* (pp. 147-169). Altamira Press.

Van Gemert, F. & Weerman, F. M. (2013). Youth groups and street gangs in the Netherlands from 1985 to 2013. In Efus (Red.), *EU Street Violence; Youth Groups and Violence in Public Spaces*. European Forum for Urban Security (Efus); Zotero.

Van Loon, T. & Jansen, A. (2017). *Gezamenlijke aanpak Jeugdgroepen Oost-Nederland*, p. 43. Radboud Universiteit; Zotero.

Van Uden, A. (2019). *Jeugdgroepen en goed politiewerk Een empirisch onderzoek naar de aanpak in Nederland*. Radboud Universiteit.

Van Wegberg, R. S. (2020). *Outsourcing Cybercrime* [Dissertation]. TU Delft.

Veenstra, S. (2023). Het ontrafelen en integraal aanpakken van een cybercrimineel jeugdnetwerk: Geleerde lessen uit RIEC-casuïstiek in Noord-Nederland. *Tijdschrift voor Veiligheid*, *22*(2), 59-71. https://doi.org/10.5553/TvV/.000055

Veenstra, S., Leukfeldt, E. R. & Boes, S. (2013). Fighting crime in a digitized society: The criminal justice system and public-private partnerships in the netherlands. In W. Ph. Stol & J. Jansen (Red.), *Cybercrime and the police*. Eleven International Publishing.

Wall, D. S. (2015). Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2677113

Wasserman, S. & Faust, K. (1994). *Social network analysis: Methods and applications*. Cambridge University Press.

Weerman, F. M. (2014, 10 september). *Jongeren en 'gangs': Lidmaatschap heeft negatieve gevolgen, maar is meestal kortdurend*. https://www.nemokennislink.nl/publicaties/jongeren-en-gangs/

Weerman, F. M. (2017). *Jeugdbendes en problematische jeugdgroepen in Nederland en Europa*. NSCR.

Whitley, B. E., Kite, M. E. & Adams, H. L. (2013). *Principles of research in behavioral science* (3rd ed). Psychology Press; Library of Congress ISBN.

Wickham, H., Averick, M., Bryan, J., Chang, W., McGowan, L., François, R., Grolemund, G., Hayes, A., Henry, L., Hester, J., Kuhn, M., Pedersen, T., Miller, E., Bache, S., Müller, K., Ooms, J., Robinson, D., Seidel, D., Spinu, V., Yutani, H. (2019). *Welcome to the Tidyverse* [Software]. https://joss.theoj.org/papers/10.21105/joss.01686

Wickham, H. & Bryan, J. (2015). *readxl: Read Excel Files* [Software]. https://doi.org/10.32614/CRAN.package.readxl

Wickham, H., Chang, W., Henry, L., Pedersen, T. L., Takahashi, K., Wilke, C., Woo, K., Yutani, H., Dunnington, D. & Van Den Brand, T. (2007). *ggplot2: Create Elegant Data Visualisations Using the Grammar of Graphics* [Software]. https://doi.org/10.32614/CRAN.package.ggplot2

Wickham, H., Pedersen, T. L. & Seidel, D. (2011). *scales: Scale Functions for Visualization* [Software]. https://doi.org/10.32614/CRAN.package.scales

WODC. (2021). *Monitor jeugdcriminaliteit 2020*. WODC.

Wolsink, J., Van Esseveldt, J., Derksen, E., Brouwer, N. & Ferwerda, H. (2023). *Het (boven)lokale netwerk in Paddepoel ontleed: De invloed van criminele netwerken op jongeren in een Groningse wijk*, p. 117. Bureau Beke.

Yar, M. (2005). Computer Hacking: Just Another Case of Juvenile Delinquency? *The Howard Journal of Criminal Justice*, *44*(4), 387-399. https://doi.org/10.1111/j.1468-2311.2005.00383.x

Bijlagen

Bijlage A **De e-mail naar experts**

Onderwerp: Interview onderzoek *'Criminele jeugdnetwerken in een digitaliserende samenleving'*

Beste [naam expert],

Wij zijn dr. Rutger Leukfeldt, Joeri Loggen en Sander Veenstra, als onderzoekers verbonden aan De Haagse Hogeschool (HHS), het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving (NSCR), en het Regionaal Informatie- en Expertise Centrum (RIEC) Noord-Nederland.

Wij sturen u deze e-mail, omdat wij van onze consortiumpartners vernomen hebben dat u mogelijk geïnteresseerd bent om door ons te worden geïnterviewd in het kader van ons onderzoek. Dit onderzoek is getiteld 'Criminele jeugdnetwerken in een digitaliserende samenleving: Handreikingen voor de integrale aanpak van (cyber)criminele jeugdnetwerken op lokaal niveau' en heeft tot doel het ontwikkelen van handvatten waarmee lokale veiligheidspartners gezamenlijk zicht kunnen krijgen op cybercriminele jeugdnetwerken en de mogelijkheden voor de integrale aanpak daarvan.

Het interview duurt ongeveer 60 tot 90 minuten. Tijdens dit interview zullen we vragen stellen over criminele jeugdnetwerken die bij een of meer veiligheidspartners op lokaal niveau bekend zijn. Daarnaast gaat een deel van de vragen over de mate waarin 'nieuwe' cybercriminele netwerken bekend zijn (bij lokale veiligheidscoalities). Tot slot zijn we geïnteresseerd in de aanpak van cybercriminele jeugdnetwerken in Noord-Nederland.

Anonimiteit en veilige opslag van de gegevens worden gegarandeerd. Zo worden de transcripten van de interviews gepseudonimiseerd en zullen deze op geen enkele manier naar u te herleiden zijn. Verder zullen uw gegevens worden opgeslagen op beveiligde, versleutelde servers. In de bijlage van deze e-mail vindt u het informed consent formulier, waarin deze zaken in meer detail worden uitgelegd.

Het onderzoek kan zowel op locatie als online worden afgenomen (bijvoorbeeld via Teams).

Zou u uw interesse in deelname aan het interview willen bevestigen, dan kunnen we een afspraak inplannen?

Alvast hartelijk dank!

Met vriendelijke groet,
Joeri Loggen, Rutger Leukfeldt en Sander Veenstra

Bijlage B Informed consent formulier experts

Informed consent

Naam en doel van het onderzoek
Dit interview is onderdeel van het onderzoek 'Criminele jeugdnetwerken in een digitaliserende samenleving: Handreikingen voor de integrale aanpak van (cyber)criminele jeugdnetwerken op lokaal niveau'. Het doel van dit onderzoek is het ontwikkelen van handvatten waarmee lokale veiligheidspartners gezamenlijk zicht kunnen krijgen op cybercriminele jeugdnetwerken en de mogelijkheden voor de integrale aanpak daarvan.

Gang van zaken tijdens het interview
Het interview duurt ongeveer 60 tot 90 minuten. Tijdens dit interview zullen we vragen stellen over criminele jeugdnetwerken die bij een of meer veiligheidspartners op lokaal niveau bekend zijn.
Daarnaast gaat een deel van de vragen over de mate waarin 'nieuwe' cybercriminele netwerken bekend zijn (bij lokale veiligheidscoalities). Tot slot zijn we geïnteresseerd in de aanpak van cybercriminele jeugdnetwerken in Noord-Nederland.
Het interview zal worden opgenomen door middel van een versleutelde audio-recorder. Het interview is geheel vrijwillig. Tijdens het interview hoeft u onze vragen niet te beantwoorden. U mag ook te allen tijde het interview beëindigen, zonder opgave van een reden. Na afloop van het onderzoek mag u uw medewerking intrekken. Uw data zullen dan worden vernietigd en niet worden meegenomen in deze studie.

Potentiële risico's
Wij kunnen ons voorstellen dat de interviews negatieve herinneringen naar boven kunnen halen, bijvoorbeeld over de negatieve impact die een crimineel netwerk heeft (gehad) op uzelf of slachtoffers. U heeft te allen tijde het recht het interview te stoppen, te pauzeren of geen antwoord te geven op de vragen.

Vertrouwelijkheid van uw persoonsgegevens en onderzoeksgegevens
Wij hebben maatregelen genomen om uw persoonsgegevens en onderzoeksgegevens te beschermen. Het interview wordt opgenomen op een versleutelde audio-recorder. Het transcript wordt gepseudonimiseerd in overeenstemming met de richtlijnen van

het NSCR en de HHS. Zodra het interview is getranscribeerd, zal de audio-opname vernietigd worden. De transcripten worden opgeslagen op Research Drive, een versleutelde server gehost in Nederland. De transcripten zijn alleen toegankelijk voor de onderzoekers.
Voor dit onderzoek zijn wij alleen geïnteresseerd in uw antwoorden op onze vragen. Uw persoonsgegevens zijn voor dit onderzoek niet relevant. Deze zullen dus ook niet worden opgeslagen. Wel zal u een respondentnummer krijgen, zodat we het transcript van dit interview kunnen verwijderen, mocht u zich willen terugtrekken.
Vanuit De Haagse Hogeschool wordt veel waarde gehecht aan 'Open Access'. Met uw expliciete toestemming zal na afronding van dit onderzoek het gepseudonimiseerde transcript, dat op geen enkele manier naar u te herleiden is, worden gearchiveerd via DANS Easy. Dit is een Nederlandse database (in Nederland gehost) waar data op kunnen worden gearchiveerd. Deze database wordt beheerd door de Koninklijke Nederlandse Akademie van Wetenschappen (KNAW) en de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO). Uw gepseudonimiseerde transcript zal hier alleen op worden geüpload wanneer u hier expliciet toestemming voor geeft. Na het uploaden zal uw transcript niet openbaar zijn en alleen worden gedeeld indien er vanuit een andere onderzoeksinstelling hiertoe een verzoek wordt ingediend. Alleen wanneer wij dit verzoek en het bijbehorende onderzoek als van goede kwaliteit beoordelen, wordt het transcript gedeeld.

Vragen
Wanneer u na afloop van dit interview wilt stoppen met het onderzoek, of als u vragen, klachten of andere opmerkingen heeft, kunt u contact opnemen met de hoofdonderzoeker dr. Rutger Leukfeldt (0646610144; E.R.Leukfeldt@hhs.nl).

Toestemmingsverklaring
Met de ondertekening van dit document geeft u aan dat u minstens 18 jaar oud bent; dat u goed bent geïnformeerd over het onderzoek, de manier waarop de onderzoeksgegevens worden verzameld, gebruikt en behandeld en welke eventuele risico's u zou kunnen lopen door te participeren in dit onderzoek.

1. Ik ben voldoende geïnformeerd over dit onderzoeksproject. Het doel van mijn deelname in dit onderzoek is voor mij helder uitgelegd en ik weet wat dit voor mij betekent;
2. Ik ga akkoord met dit interview. Mijn deelname is vrijwillig. Er is geen expliciete of impliciete dwang voor mij om aan dit onderzoek deel te nemen;
3. Ik heb dit formulier gelezen en begrepen. Al mijn vragen zijn naar tevredenheid beantwoord;
4. Ik heb een kopie ontvangen van dit toestemmingsformulier dat ook ondertekend is door de onderzoekers;
5. Mijn deelname houdt in dat ik word geïnterviewd door onderzoekers van De Haagse Hogeschool. Het interview zal maximaal 90 minuten duren. Ik geef toe-

stemming dat er tijdens het interview geluidsopnames worden gemaakt, evenals schriftelijke notities;
6. Ik ben mij bewust van de rechten die ik heb als deelnemer;
7. Ik weet dat dit onderzoeksproject is beoordeeld en goedgekeurd door de Ethische Adviescommissie van De Haagse Hogeschool. Voor vragen, bezwaren of klachten kan ik contact opnemen met de hoofdonderzoeker dr. Rutger Leukfeldt. In geval dit niet mogelijk of wenselijk is, kan ik contact opnemen met De Haagse Hogeschool via research@hhs.nl;
8. Ik ga ermee akkoord dat mijn gepseudonimiseerde gegevens, die op geen enkele manier naar mij te herleiden zijn, worden gearchiveerd in de DANS Easy database, en daarmee beschikbaar worden voor andere onderzoekers en kennisinstellingen.
   ☐ JA
   ☐ NEE

Naam deelnemer: _____

Handtekening Bijlage deelnemer: Handtekening onderzoeker:

_____ _____

Datum: _____ Datum: _____

Bijlage C **Interviewprotocol experts**

Inleiding
Hartelijk dank voor het deelnemen aan ons onderzoek. Dit interview is onderdeel van een onderzoek naar cybercriminele jeugdnetwerken in Noord-Nederland, gefinancierd door Politie en Wetenschap. De aanleiding voor dit onderzoek is dat veiligheidspartners in Noord-Nederland aangeven het zicht te verliezen op criminele jeugdnetwerken. Dit is deels het gevolg van de verschuiving van traditionele criminaliteit naar cybercriminaliteit.

In het onderzoek richtten we ons op drie verschillende sporen:
1. *Traditionele criminele jeugdnetwerken die al bekend zijn bij lokale veiligheidscoalities*
2. *Nieuwe criminele jeugdnetwerken die zich hoofdzakelijk op het plegen van cybercrime toeleggen (en daardoor niet of minder zichtbaar zijn)*
3. *De integrale aanpak van deze (cyber)criminele jeugdnetwerken*

We richten ons op criminele jeugdnetwerken die zich bezighouden met een of meerdere type gedigitaliseerde criminaliteit en/of cybercrime in enge zin. We richten ons dus niet op maar één specifieke vorm van cybercrime, maar op alle vormen van cybercrime. We definiëren jeugd als jongeren en jongvolwassenen van 12 tot 24 jaar oud. Tot slot richten we ons specifiek op (cyber)criminele jeugdnetwerken die actief zijn in Noord-Nederland, dus Drenthe, Groningen en Friesland.
Wij zouden u graag over deze drie sporen een aantal vragen willen stellen. Een deel van deze vragen zullen betrekking hebben op individuele leden van de jeugdnetwerken. Wij zijn voor dit interview niet geïnteresseerd in namen of andere informatie die herleidbaar zou kunnen zijn naar deze personen. We zijn alleen geïnteresseerd in achtergrondinformatie. Het interview zal ongeveer 90 minuten in beslag nemen. Alles wat u met ons deelt, is vertrouwelijk en zal alleen voor ons, de onderzoekers, toegankelijk zijn. De informatie wordt gepseudonimiseerd en opgeslagen op versleutelde locaties. Wij zorgen ervoor dat uw antwoorden niet naar u te herleiden zijn.

1. Algemeen
Voordat we beginnen met het bespreken van de drie sporen, zouden we eerst wat meer over uw achtergrond en functie willen weten.

– Geslacht [noteren man/vrouw]
– Bij welke organisatie bent u werkzaam [naam organisatie, afdeling]

– Wat is uw functie?
– Op welke wijze bent u betrokken bij (de aanpak van) cybercrime / (cyber)criminele jeugdnetwerken?
– Hoe lang houdt u zich al bezig met cybercrime?

2. Spoor 1

Binnen spoor 1 staan criminele jeugdnetwerken centraal die bij een of meer veiligheidspartners op lokaal niveau bekend zijn. Het gaat hierbij dus om netwerken waarvan de lokale veiligheidscoalities op de hoogte zijn, waarbij de leden tussen de 12 en 24 jaar oud zijn, en die actief zijn in de provincies Drenthe, Groningen en/of Friesland. We zullen u een aantal specifieke vragen stellen om meer inzicht te krijgen in hun eventuele cybercriminele activiteiten en – als daarvan sprake is - de structuur, groei, en leden van deze netwerken.

[Per subonderdeel langslopen]

[Voor ieder netwerk dat beschreven wordt opnieuw langslopen. Zorg ervoor dat netwerken duidelijk uit elkaar worden gehaald]

Bij meerdere netwerken: een netwerk bespreken dat exemplarisch is voor de meeste netwerken waar de respondent zicht op heeft. Bij alle onderwerpen die aan bod komen steeds expliciet vragen naar eventuele verschillen met de andere netwerken.

– Heeft u ervaring met traditionele criminele jeugdnetwerken die nu actief zijn (ja = volgende vraag/nee = door naar spoor 2)?
– Om hoeveel netwerken gaat het?

Per netwerk alle vragen langslopen

– Van welke traditionele verschijningsvormen van overlast en crime zijn deze groepen bekend?
– Bevatten deze netwerken cyber-elementen ? (ja = volgende vraag/nee = door naar spoor 2)
– Hoe heeft u zicht gekregen op dit netwerk?
– Wat zijn de kenmerken van deze (cyber)criminele jeugdnetwerken?
– Structuur:
  - In hoeverre is zicht op deze kenmerken?
  - Aantal leden
  - Rollen/structuur binnen het netwerken
  - Mate van hiërarchie
  - Stabiliteit/flexibiliteit van groep kernleden
  - Mate van dynamiek van het netwerk
  - Aanwezigheid van geweld binnen het netwerk
  - Onderlinge conflicten tussen verschillende netwerken
  - Gebruik van facilitators (hoe worden deze gerekruteerd?)

– Ontstaan en groei:
  - In hoeverre is zicht op deze kenmerken?
  - Hoe raken individuen betrokken bij de netwerken (via offline/online contacten?)
  - Ontmoetingsplaatsen
  - Banden tussen leden (offline, online, via welke online kanalen?)

De volgende vragen gaan over de individuele leden van de netwerken. Nogmaals, we zijn niet geïnteresseerd in identificeerbare gegevens, zoals namen. We zijn alleen geïnteresseerd in achtergrondinformatie. Als u zich niet comfortabel voelt met het delen van deze informatie, zou u dan meer in het algemeen de kenmerken van dit netwerken kunnen bespreken?
– Wat zijn de kenmerken van de individuele leden van deze (cyber)criminele jeugdnetwerken?
– Demografische kenmerken:
  - Leeftijd
  - Geslacht
  - Etnische achtergrond
  - Opleiding
  - Werk
  - Sociaaleconomische status
  - Thuissituatie (alleenstaand/samenwonend, thuiswonend bij ouders, probleemgezin)
  - Hobby's/vrije tijdsbesteding
  - Intelligentie
– Criminele carrière
  - Zijn de leden first offenders? (Zo niet, met welke delicten hebben ze zich dan voorafgaand aan het plegen van cybercrime beziggehouden?)
  - Wat zijn de motivaties van de jongeren om cybercrime te plegen?
  - Hoe raken deze individuen betrokken bij cybercrime? (pathway)
– Wat is de aard van de delicten waarmee deze (cyber)criminele jeugdnetwerken zich bezighouden?
  - Welke traditionele delicten plegen ze? Wat is de MO?
    - In welke mate speelt geweld een rol bij het plegen van deze delicten?
    - Wat is de rol van geweld bij het afschermen van deze delicten?
  - Welke cybercriminele delicten plegen ze? Wat is de MO?
    - In welke mate speelt geweld een rol bij het plegen van deze delicten?
    - Wat is de rol van geweld bij het afschermen van deze delicten?
  - Wat is de mate van verwevenheid tussen traditionele delicten en cyberdelicten?
  - Hoe actief is het netwerk? (hoe vaak plegen ze delicten?)

3. Spoor 2

Binnen spoor 2 staan 'nieuwe' cybercriminele jeugdnetwerken centraal. Het gaat hierbij dus om netwerken die zich hoofdzakelijk toeleggen op cybercriminaliteit. Een vereiste is dat de leden tussen de 12 en 24 jaar oud zijn, zich met 1 of meerdere vormen van cybercrime in enge zin of gedigitaliseerde criminaliteit bezighouden en actief zijn in de provincies Drenthe, Groningen en/of Friesland. We zullen u een aantal specifieke vragen stellen om inzicht te krijgen in de mate waarin zulke 'nieuwe' cybercriminele netwerken bekend zijn (bij lokale veiligheidscoalities), maar ook om meer zicht te krijgen op de structuur, groei, en leden van deze netwerken.

[Per subonderdeel langslopen]

[Voor ieder netwerk dat beschreven wordt opnieuw langslopen. Zorg ervoor dat netwerken duidelijk uit elkaar worden gehaald]

Bij meerdere netwerken: een netwerk bespreken dat exemplarisch is voor de meeste netwerken waar de respondent zicht op heeft. Bij alle onderwerpen die aan bod komen steeds expliciet vragen naar eventuele verschillen met de andere netwerken.

- In hoeverre kent u criminele jeugdnetwerken die zich hoofdzakelijk op cybercrime toeleggen? (ja = volgende vraag/nee = door naar spoor 3)?
- Om hoeveel netwerken gaat het?
- Hoe is zicht ontstaan op dit netwerk?
  - Wordt dit gedeeld met de gemeente?
- In hoeverre zijn gemeenten en hun zorg en veiligheidspartners – die van oudsher belast zijn met de aanpak van de criminele jeugdnetwerken – bekend met deze netwerken?
  - Waarom wel/niet
  - In geval niet
    - Hoe komt het dat u wel van het bestaan van dit netwerk weet?
  - Wat is de mate waarin geregistreerde online criminaliteitscijfers of andere bronnen worden geraadpleegd?
  - In hoeverre biedt de cybercriminele aard van hun activiteiten daarvoor een verklaring?
  - Heeft u suggesties om ervoor te zorgen dat dit netwerk wel in beeld komt bij de lokale veiligheidscoalitie?

Per netwerk alle vragen langslopen

- Wat zijn de kenmerken van deze (cyber)criminele jeugdnetwerken?
- Structuur:
  - In hoeverre is zicht op deze kenmerken?
  - Aantal leden
  - Rollen/structuur binnen het netwerken
  - Mate van hiërarchie
  - Stabiliteit/flexibiliteit van groep kernleden

  - Mate van dynamiek van het netwerk
  - Aanwezigheid van geweld binnen het netwerk
  - Onderlinge conflicten tussen verschillende netwerken
  - Gebruik van facilitators (hoe worden deze gerekruteerd?)
- Ontstaan en groei:
  - In hoeverre is zicht op deze kenmerken?
  - Hoe raken individuen betrokken bij de netwerken (via offline/online contacten?)
  - Ontmoetingsplaatsen
  - Banden tussen leden (offline, online, via welke online kanalen?)
- De volgende vragen gaan over de individuele leden van de netwerken. Nogmaals, we zijn niet geïnteresseerd in identificeerbare gegevens, zoals namen. We zijn alleen geïnteresseerd in achtergrondinformatie. Als u zich niet comfortabel voelt met het delen van deze informatie, zou u dan meer in het algemeen de kenmerken van dit netwerken kunnen bespreken?
- Wat zijn de kenmerken van de individuele leden van deze (cyber)criminele jeugdnetwerken?
- Demografische kenmerken:
  - Leeftijd
  - Geslacht
  - Etnische achtergrond
  - Opleiding
  - Werk
  - Sociaaleconomische status
  - Thuissituatie (alleenstaand/samenwonend, thuiswonend bij ouders, probleemgezin)
  - Hobby's/vrije tijdsbesteding
  - Intelligentie
- Criminele carrière
  - Zijn de leden first offenders? (Zo niet, met welke delicten hebben ze zich dan voorafgaand aan het plegen van cybercrime beziggehouden?)
  - Wat zijn de motivaties van de jongeren om cybercrime te plegen?
  - Hoe raken deze individuen betrokken bij cybercrime? (pathway)
- Wat is de aard van de delicten waarmee deze (cyber)criminele jeugdnetwerken zich bezighouden?
  - Welke traditionele delicten plegen ze? Wat is de MO?
    - In welke mate speelt geweld een rol bij het plegen van deze delicten?
    - Wat is de rol van geweld bij het afschermen van deze delicten?
  - Welke cybercriminele delicten plegen ze? Wat is de MO?
    - In welke mate speelt geweld een rol bij het plegen van deze delicten?
    - Wat is de rol van geweld bij het afschermen van deze delicten?
  - In hoeverre komen deze cybercriminele netwerken – voor zover bekend – voort uit een 'traditioneel' crimineel jeugdnetwerk?

- Wat is de mate van verwevenheid tussen traditionele delicten en cyberdelicten?
- Hoe actief is het netwerk? (hoe vaak plegen ze delicten?)

4. Spoor 3: Integrale aanpak
Tot slot zijn we geïnteresseerd in de aanpak van cybercriminele jeugdnetwerken in Noord-Nederland. Daarbij zijn we geïnteresseerd in zowel de aanpak in het algemeen, als de aanpak van de verschillende casussen die u hiervoor heeft besproken. Wij zouden van u graag meer horen over een dergelijke aanpak.

[onderstaande vragen per netwerk uitvragen]
[vervolgens onderstaande vragen doornemen m.b.t. de aanpak van cybercriminele jeugdnetwerken in het algemeen]

– Hoe ziet bij uw organisatie de bestaande aanpak van het hiervoor besproken cybercriminele jeugdnetwerk/cybercriminele jeugdnetwerken in het algemeen eruit?
– Hoe ontstaat zicht op een crimineel netwerk en hoe is dat georganiseerd?
– Wat is de wijze waarop de groepsaanpak is georganiseerd?
– In hoeverre is er sprake van een integrale aanpak van dit cybercriminele jeugdnetwerk?
  - Welke actor(en) is/zijn hierbij betrokken?
  - Hoe ziet die aanpak eruit? (gebruik 7-stappenmodel?)
  - Is deze aanpak delictspecifiek (i.e. specifiek gericht op cyberdelicten)?
  - Hoe effectief is deze aanpak in de aanpak van cybercriminele jeugdnetwerken? (is deze aanpak geëvalueerd? Zo nee, wat is uw inschatting over de effectiviteit?)
– Wat zijn naar uw mening de sterke punten van deze aanpak?
– Wat zijn naar uw mening verbeterpunten van deze aanpak?
– Zijn er bij uw organisatie ook interventies die nog in ontwikkeling zijn? Hoe zien deze eruit?
– In hoeverre denk u dat interventies die zich richten op individuele jeugdige cyberdaders kunnen bijdragen aan de aanpak van cybercriminele jeugdnetwerken?
– Worden er vanuit uw organisatie maatregelen genomen gericht op individuen om hen te weerhouden te beginnen met cybercrime?
– Worden er vanuit uw organisatie maatregelen genomen gericht op individuele leden om hen te laten stoppen met cybercrime?

Dit is het einde van het interview. heeft u nog opmerkingen of dingen die u wilt toevoegen?
We zullen het interview niet woord voor woord uitwerken, maar op grote lijnen samenvatten, om zo onze onderzoeksvragen te beantwoorden? Wilt u het transcript inzien? Wilt u het concept onderzoeksrapport inzien?

Bijlage D Codeboek expertinterviews

1. Spoor 1

- Van welke traditionele verschijningsvormen van overlast en crime zijn deze groepen bekend?
- Bevatten deze netwerken cyber-elementen ? (ja = volgende vraag/nee = door naar spoor 2)
- Hoe heeft u zicht gekregen op dit netwerk?
- Wat zijn de kenmerken van deze (cyber)criminele jeugdnetwerken?
- Structuur:
  - In hoeverre is zicht op deze kenmerken?
  - Aantal leden
  - Rollen/structuur binnen het netwerken
  - Mate van hiërarchie
  - Stabiliteit/flexibiliteit van groep kernleden
  - Mate van dynamiek van het netwerk
  - Aanwezigheid van geweld binnen het netwerk
  - Onderlinge conflicten tussen verschillende netwerken
  - Gebruik van facilitators (hoe worden deze gerekruteerd?)
  - Ontstaan en groei:
  - In hoeverre is zicht op deze kenmerken?
  - Hoe raken individuen betrokken bij de netwerken (via offline/online contacten?)
  - Ontmoetingsplaatsen
  - Banden tussen leden (offline, online, via welke online kanalen?)
- Wat zijn de kenmerken van de individuele leden van deze (cyber)criminele jeugdnetwerken?
  - Demografische kenmerken:
  - Leeftijd
  - Geslacht
  - Etnische achtergrond
  - Opleiding
  - Werk
  - Sociaaleconomische status
  - Thuissituatie (alleenstaand/samenwonend, thuiswonend bij ouders, probleemgezin)
  - Hobby's/vrije tijdsbesteding

  - Intelligentie
  - Criminele carrière
  - Zijn de leden first offenders? (Zo niet, met welke delicten hebben ze zich dan voorafgaand aan het plegen van cybercrime beziggehouden?)
  - Wat zijn de motivaties van de jongeren om cybercrime te plegen?
  - Hoe raken deze individuen betrokken bij cybercrime? (pathway)
- Wat is de aard van de delicten waarmee deze (cyber)criminele jeugdnetwerken zich bezighouden?
  - Welke traditionele delicten plegen ze? Wat is de MO?
  - In welke mate speelt geweld een rol bij het plegen van deze delicten?
  - Wat is de rol van geweld bij het afschermen van deze delicten?
  - Welke cybercriminele delicten plegen ze? Wat is de MO?
  - In welke mate speelt geweld een rol bij het plegen van deze delicten?
  - Wat is de rol van geweld bij het afschermen van deze delicten?
  - Wat is de mate van verwevenheid tussen traditionele delicten en cyberdelicten?
  - Hoe actief is het netwerk? (hoe vaak plegen ze delicten?)

2. Spoor 2

- In hoeverre kent u criminele jeugdnetwerken die zich hoofdzakelijk op cybercrime toeleggen? (ja = volgende vraag/nee = door naar spoor 3)?
- Om hoeveel netwerken gaat het?
- Hoe is zicht ontstaan op dit netwerk?
  - Wordt dit gedeeld met de gemeente?
- In hoeverre zijn gemeenten en hun zorg en veiligheidspartners – die van oudsher belast zijn met de aanpak van de criminele jeugdnetwerken – bekend met deze netwerken?
  - Waarom wel/niet
  - In geval niet
  - Hoe komt het dat u wel van het bestaan van dit netwerk weet?
  - Wat is de mate waarin geregistreerde online criminaliteitscijfers of andere bronnen worden geraadpleegd?
  - In hoeverre biedt de cybercriminele aard van hun activiteiten daarvoor een verklaring?
  - Heeft u suggesties om ervoor te zorgen dat dit netwerk wel in beeld komt bij de lokale veiligheidscoalitie?

Per netwerk alle vragen langslopen

- Wat zijn de kenmerken van deze (cyber)criminele jeugdnetwerken?
- Structuur:
  - In hoeverre is zicht op deze kenmerken?
  - Aantal leden
  - Rollen/structuur binnen het netwerken
  - Mate van hiërarchie

  - Stabiliteit/flexibiliteit van groep kernleden
  - Mate van dynamiek van het netwerk
  - Aanwezigheid van geweld binnen het netwerk
  - Onderlinge conflicten tussen verschillende netwerken
  - Gebruik van facilitators (hoe worden deze gerekruteerd?)
- Ontstaan en groei:
  - In hoeverre is zicht op deze kenmerken?
  - Hoe raken individuen betrokken bij de netwerken (via offline/online contacten?)
  - Ontmoetingsplaatsen
  - Banden tussen leden (offline, online, via welke online kanalen?)
- Wat zijn de kenmerken van de individuele leden van deze (cyber)criminele jeugdnetwerken?
- Demografische kenmerken:
  - Leeftijd
  - Geslacht
  - Etnische achtergrond
  - Opleiding
  - Werk
  - Sociaaleconomische status
  - Thuissituatie (alleenstaand/samenwonend, thuiswonend bij ouders, probleemgezin)
  - Hobby's/vrije tijdsbesteding
  - Intelligentie
  - Criminele carrière
  - Zijn de leden first offenders? (Zo niet, met welke delicten hebben ze zich dan voorafgaand aan het plegen van cybercrime beziggehouden?)
  - Wat zijn de motivaties van de jongeren om cybercrime te plegen?
  - Hoe raken deze individuen betrokken bij cybercrime? (pathway)
- Wat is de aard van de delicten waarmee deze (cyber)criminele jeugdnetwerken zich bezighouden?
  - Welke traditionele delicten plegen ze? Wat is de MO?
  - In welke mate speelt geweld een rol bij het plegen van deze delicten?
  - Wat is de rol van geweld bij het afschermen van deze delicten?
  - Welke cybercriminele delicten plegen ze? Wat is de MO?
  - In welke mate speelt geweld een rol bij het plegen van deze delicten?
  - Wat is de rol van geweld bij het afschermen van deze delicten?
  - In hoeverre komen deze cybercriminele netwerken – voor zover bekend – voort uit een 'traditioneel' crimineel jeugdnetwerk?
  - Wat is de mate van verwevenheid tussen traditionele delicten en cyberdelicten?
  - Hoe actief is het netwerk? (hoe vaak plegen ze delicten?)

3. Spoor 3: Integrale aanpak

- Hoe ziet bij uw organisatie de bestaande aanpak van het hiervoor besproken cybercriminele jeugdnetwerk/cybercriminele jeugdnetwerken in het algemeen eruit?
- Hoe ontstaat zicht op een crimineel netwerk en hoe is dat georganiseerd?
- Wat is de wijze waarop de groepsaanpak is georganiseerd?
- In hoeverre is er sprake van een integrale aanpak van dit cybercriminele jeugdnetwerk?
  - Welke actor(en) is/zijn hierbij betrokken?
  - Hoe ziet die aanpak eruit? (gebruik 7-stappenmodel?)
  - Is deze aanpak delictspecifiek (i.e. specifiek gericht op cyberdelicten)?
  - Hoe effectief is deze aanpak in de aanpak van cybercriminele jeugdnetwerken? (is deze aanpak geëvalueerd? Zo nee, wat is uw inschatting over de effectiviteit?)
- Wat zijn naar uw mening de sterke punten van deze aanpak?
- Wat zijn naar uw mening verbeterpunten van deze aanpak?
- Zijn er bij uw organisatie ook interventies die nog in ontwikkeling zijn? Hoe zien deze eruit?
- In hoeverre denkt u dat interventies die zich richten op individuele jeugdige cyberdaders kunnen bijdragen aan de aanpak van cybercriminele jeugdnetwerken?
- Worden er vanuit uw organisatie maatregelen genomen gericht op individuen om hen ervan te weerhouden te beginnen met cybercrime?
- Worden er vanuit uw organisatie maatregelen genomen gericht op individuele leden om hen te laten stoppen met cybercrime?

Bijlage E Codeboek zaakreconstructies

Analyse framework

1. Zaakgegevens
1. Geef een korte beschrijving van de casus
2. Beschrijf de betrokken instantie(s) bij het onderzoek naar het netwerk
3. Beschrijf de startdatum van het onderzoek
4. Beschrijf de datum van afsluiting van het onderzoek
5. Beschrijf de gegevens van de geïnterviewde respondenten

2. Overzicht (opsporings)onderzoek
1. Geef een beschrijving van de aanleiding van het onderzoek naar het netwerk
2. Beschrijf hoe de zaak aan het licht is gekomen (de aanleiding tot het onderzoek, bijvoorbeeld een aangifte)
3. Beschrijf hoe zicht is ontstaan op dit netwerk (de methode die is gebruikt om het netwerk te ontrafelen, bijvoorbeeld een netwerkanalyse op basis van politiegegevens)
4. Beschrijf in hoeverre de zorg- en veiligheidspartners bekend waren met dit netwerk
5. Geef een beschrijving van de afbakening van het onderzoek
6. Beschrijf het doel van het onderzoek

3. Het samenwerkingsverband

Structuur en samenstelling
1. Beschrijf of het netwerk al bekend was met het plegen van traditionele criminaliteit en is doorgegroeid naar cybercrime, of dat het om een 'nieuw' netwerk gaat
2. Beschrijf in hoeverre er bij het onderzoek naar het netwerk zicht was op de kenmerken gerelateerd aan de structuur en samenstelling (punt 3-9)
3. Beschrijf het totaal aantal verdachten en/of leden van het netwerk
4. Geef een beschrijving van de rolverdeling en de verschillende rollen binnen het netwerk
5. Geef een beschrijving van de mate van hiërarchie binnen het netwerk
   - Beschrijf in hoeverre er sprake was van een leidersfiguur
   - (indien van toepassing) Geef een beschrijving van de vaste kern van het netwerk (aantal leden, rol, mate van stabiliteit/dynamiek)

6. Beschrijf de mate van dynamiek binnen het netwerk
   – In hoeverre varieert het aantal leden binnen het netwerk
7. (indien van toepassing) Geef een beschrijving van het gebruik van geweld binnen het netwerk
8. (indien van toepassing) Geef een beschrijving van onderlinge conflicten tussen verschillende netwerken
9. Beschrijf het gebruik van facilitators door het netwerk
   – Hoe worden de facilitators gerekruteerd?
   – Welke goederen en/of diensten leveren de facilitators?
   – Welke rol spelen de facilitators binnen het netwerk?

Ontstaan en groei

1. Beschrijf in hoeverre er bij het onderzoek naar het netwerk zicht was op de kenmerken gerelateerd aan het ontstaan en de groei (punt 2-5)
2. Geef een beschrijving van hoe en wanneer het samenwerkingsverband is ontstaan
3. Beschrijf hoe individuen betrokken raken bij het netwerk (sneeuwbaleffect en/of rekrutering; offline/online sociale contacten)
4. Beschrijf de ontmoetingsplaatsen van de leden van het netwerk
   – Beschrijf in hoeverre er gebruik wordt gemaakt van online offender convergence settings
5. Geef een beschrijving van de banden tussen leden (zoals familie, vrienden, buren, wijk, school) en de mate waarin offline/online social ties daarin een rol spelen
   – Beschrijf de rol die vertrouwen hierin speelt
6. Beschrijf in hoeverre sprake is van lokale verankering van het netwerk

4. Kenmerken van leden

Beschrijven per lid

1. Beschrijf de demografische kenmerken
   – Leeftijd
   – Geslacht
   – Etnische achtergrond
   – Opleiding
   – Werk
   – Sociaaleconomische status
   – Thuissituatie
2. Beschrijf de criminele carrière
   – Zijn de leden first offenders? Zo niet, geef een beschrijving van hun criminele achtergrond
   – Beschrijf de motivatie(s) om cybercriminele delicten te plegen
   – Beschrijf hoe individuen in het algemeen betrokken raken bij cybercrime

5. Activiteiten en werkwijze

Delicten

1. Geef een beschrijving van de delicten waar het netwerk zich mee bezighoudt
   - Beschrijf de traditionele delicten en de gebruikte modus operandi
   - Beschrijf de cybercriminele delicten en de modus operandi
   - Beschrijf wat de relatie is tussen geweld en het plegen/afschermen van deze delicten
     - Waarom is deze relatie er?
2. Geef een beschrijving van de mate van verwevenheid tussen de traditionele delicten en cyberdelicten
3. Beschrijf in hoeverre er sprake is van een netwerk dat uitsluitend online criminaliteit pleegt, of een traditioneel netwerk dat het wederrechtelijk verkregen voordeel verkregen via cybercrime investeert in andere vormen van criminaliteit
4. Beschrijf hoe actief het netwerk was
5. Beschrijf hoe lang het netwerk actief was
6. Omvang, verdeling en besteding van het wederrechtelijk verkregen voordeel (wvv)
7. Geef een beschrijving van de schatting van het wvv
8. Beschrijf de wijze waarop binnen het samenwerkingsverband het wvv wordt verdeeld
9. Beschrijf waar (locatie, bijvoorbeeld land of stad) en waaraan het wvv wordt besteed

7. Aanpak

1. Beschrijf in hoeverre er sprake is van een integrale aanpak van dit netwerk
2. Beschrijf de actoren die betrokken zijn bij de aanpak
   - Beschrijf in hoeverre deze actoren met elkaar samenwerken bij de aanpak (dit kunnen ook bedrijven zijn waar de politie gegevens heeft gevorderd)
   - Indien er niet sprake was van samenwerking, beschrijf in hoeverre de versnipperde aanpak tot problemen heeft geleid
3. Beschrijf hoe deze aanpak is georganiseerd
4. Beschrijf hoe de aanpak eruitziet (welke interventies zijn toegepast op de casus?)
5. Beschrijf de mate waarin de aanpak delictspecifiek of groepsspecifiek is
6. Beschrijf hoe effectief deze aanpak is in de aanpak van het cybercriminele netwerk
7. Geef een beschrijving van de sterke punten van deze aanpak
8. Geef een beschrijving van de zwakke punten van deze aanpak
9. Beschrijf in hoeverre het doel van het onderzoek is bereikt
   - Indien er geen duidelijk doel is opgesteld, in hoeverre was de aanpak effectief in het stoppen van het criminele netwerk?
10. Beschrijf de belangrijkste leerervaringen van dit onderzoek en de aanpak
11. Beschrijf in hoeverre interventies die zich richten op jeugdige cyberdaders bijdragen aan de aanpak van cybercriminele jeugdnetwerken

Bijlage F Voorbeeld verstrekte politieregistraties

Tabel 1. Voorbeeld van de verkregen gepseudonimiseerde politiedata

Registratienummer	Delict	Verdachte_ID	Geboortedatum	Postcode
PL0100_REG_001	Bankhelpdeskfraude	1	2002-08-13	8015
PL0100_REG_001	Bankhelpdeskfraude	2	2004-11-29	8015
PL0100_REG_001	Bankhelpdeskfraude	3	2002-01-01	8015
PL0100_REG_002	Sextortion	2	2004-11-29	8015
PL0100_REG_002	Sextortion	4	2007-05-06	6262

Uitgaven in de reeks Politiekunde

1. Criminaliteit in de virtuele ruimte
P. van Amersfoort, L. Smit & M. Rietveld, DSP-groep, Amsterdam/TNO-FEL, Den Haag, 2002

2. Cameratoezicht. Goed bekeken?
I. van Leiden & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem, 2002

3. De 10 stappen van Publiek-Private Samenwerking (PPS)
J.C. Wever, A.A. van Pel & L. Smit, DSP-groep, Amsterdam/TNO-FEL, Den Haag, 2002

4. De opbrengst van projecten. Een verkennend onderzoek naar de bijdrage van projecten aan diefstalbestrijding
C.J.E. In 't Velt, e.a., NPA-Onderzoeksgroep, LSOP, Apeldoorn, 2003

5. Cameratoezicht. De menselijke factor
A. Weitenberg, E. Jansen, I. van Leiden, J. Kerstholt & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem/TNO, Soesterberg, 2003

6. Jeugdgroepen in beeld. Stappenplan en randvoorwaarden voor de shortlistmethodiek
H.B. Ferwerda & A. Kloosterman, Advies- en Onderzoeksgroep Beke & Politieregio Gelderland-Midden, Arnhem, 2004 (vierde druk 2006)

7. Hooligans in beeld.Van informatie naar aanpak
H.B. Ferwerda & O. Adang, Advies- en Onderzoeksgroep Beke, Arnhem/ Onderzoeksgroep Politieacademie Apeldoorn, 2005

8. Richtlijnen auditieve confrontatie
J.H. Kerstholt, A.G. van Amelsvoort, E.J.M. Jansen & A.P.A. Broeders, TNO Defensie en Veiligheid, Soesterberg/Politieacademie, Apeldoorn/NFI, Den Haag, 2005

9. Niet verschenen

10. De opsporingsfunctie binnen de gebiedsgebonden politiezorg
O. Zoomer, IPIT, Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2006

11. Inzoomen en uitzoomen op Zaandam
I. van Leiden & H.B. Ferwerda, Advies- en onderzoeksgroep Beke, Arnhem 2006

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

101.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

130. Online blauw. Een onderzoek naar de rol van basisteams in de aanpak van digitale criminaliteit en ervaringen van slachtoffers met de politie
R. van Steden, S. ter Woerds, A. Merk, K. Schuppers, M. Willekers, D. Valk-van Waarde, R. Jansen, S. Ruiter. Politie en Wetenschap, Amsterdam, juni 2025

131. Bruggenbouwers. Deel uitmaken en sturen van lokale samenwerkingsverbanden voor veiligheid en leefbaarheid
A. Walberg, N. van der Klok, R. Spithoven. M.m.v. S. Ebrahem MSc, B. Schuitema, E. Foppen, K. Wittebrood, J. Klopman BA. Politie en Wetenschap, Amsterdam; Saxion, juni 2025

132. Leren demonstreren. Een onderzoek naar nieuwe manieren van demonstreren en wat die betekenen voor de inzet en aanpak van de politie
H. Ferwerda, E. Berger, E. Derksen, J. van Esseveldt, J. Wolsink, J. Timmer. Bureau Beke Arnhem, Vrije Universiteit Amsterdam, maart 2026

133. De rol van social media in de betrokkenheid van jongeren bij zware en georganiseerde drugs- en geweldscriminaliteit
J. Bergers, S. van Deuren, R. Roks, S. Habets, R. Leukfeldt, V. Eichelsheim, Vrije Universiteit Amsterdam, Erasmus University Rotterdam, Netherlands Institute fort he Study of Crime and Law Enforcement, april 2026