Online fraude door jongeren in Zuidoost Drenthe: naar een integrale aanpak door politie, gemeenten en jongerenwerk

Online fraude door jongeren in Zuidoost Drenthe
Online fraud of juveniles in Southeast Drenthe
Student: Carmen van der Vinne
S3496082
c.van.der.vinne@student.rug.nl
Sociologie van Criminaliteit en Veiligheid
Rijksuniversiteit Groningen
Augustus 2022
Begeleider: prof. dr. René Veenstra
Referent: Marieke van Gerner-Haan

Voorwoord

Voor u ligt mijn afstudeerscriptie die is geschreven ter afronding van de opleiding sociologie van criminaliteit en veiligheid aan de Rijksuniversiteit Groningen. Deze scriptie omvat een kwalitatief onderzoek over een integrale aanpak van online fraude door jongeren in Zuidoost Drenthe. Daarnaast is er een systematische review geschreven over online fraude en phishing. Van februari 2022 tot augustus 2022 ben ik bezig geweest met het onderzoek en het schrijven van de scriptie.

Mijn scriptie is geschreven in opdracht van het basisteam Zuidoost Drenthe van de politie. Daar heb ik ook mijn afstudeerstage gelopen. Ik werd daar begeleid door Judith Brouwer en Etiënne Spalburg. De stageperiode bestond voornamelijk uit het leggen van contacten met de ketenpartners van de politie. Verder heb ik ook een goede eerste indruk gekregen van hoe het is om bij de politie te werken. Ik wil graag Judith Brouwer en Etiënne Spalburg bedanken voor het helpen met het vinden van een onderwerp voor mijn onderzoek en de hulp die ik van hen kreeg ten tijde van het onderzoek. Verder zou ik graag alle participanten van de interviews willen bedanken voor hun tijd en interesse in mijn onderzoek. Zonder hun medewerking had ik dit onderzoek nooit kunnen voltooien.

Naast mijn begeleiding vanuit de politie wil ik graag René Veenstra en Marieke van Gerner-Haan bedanken voor de hulp tijdens het schrijven van de scriptie. Mijn scriptiebegeleider, René Veenstra, heeft mij goed geholpen door zijn kritische vragen en feedback. Daardoor is mijn scriptie erg verbeterd. Marieke van Gerner-Haan wil ik graag bedanken voor de bruikbare feedback over het uitvoeren van kwalitatief onderzoek.

Ik wens u veel leesplezier toe.

Carmen van der Vinne
Emmen, augustus 2022

Abstract

De laatste jaren is een toevlucht genomen tot cybercriminaliteit, waaronder online fraude. In Zuidoost Drenthe zijn steeds meer jongeren in beeld die geldezel zijn. Geldezels zijn personen die tegen een kleine vergoeding hun bankpas ter beschikking stellen aan criminelen. De gemeenten Borger-Odoorn, Coevorden en Emmen vallen onder deze regio. Een veroordeling wegens online fraude heeft grote gevolgen voor jongeren bij het openen van een bankrekening, maar kan mogelijk ook leiden tot een criminele loopbaan. Het is een nieuwe vorm van criminaliteit waar nog geen concrete aanpak voor is geformuleerd. Daarom wordt in dit onderzoek richting een integrale aanpak gewerkt. Een integrale aanpak houdt in dat er verscheidene organisaties met eigen taken zullen bijdragen aan de bestrijding van een bepaalde criminaliteitsvorm.

De onderzoeksvraag in dit onderzoek luidt als volgt: “Hoe kan een integrale aanpak voor online fraude door jongeren worden opgezet door politie, gemeente en jongerenwerkers in de regio Zuidoost Drenthe?". De onderzoeksvraag is beantwoord aan de hand van een kwalitatief onderzoek, waarbij dertien mensen zijn geïnterviewd met behulp van een semigestructureerd interviewschema. Door middel van thematische analyse werden de interviews geanalyseerd. Daaruit is gebleken dat de basis voor een integrale samenwerking al grotendeels aanwezig is. Dat betekent dat de regie, doelstellingen, taakverdeling en het onderlinge contact over het algemeen goed worden opgepakt. Er zijn wel knelpunten te benoemen in de huidige samenwerkingen, namelijk middelen- en capaciteitsgebrek, gebrekkige informatie-uitwisseling en individuele knelpunten. Er zijn echter wel enkele aanbevelingen te doen voor de integrale aanpak voor online fraude. Allereerst wordt aanbevolen om meer afstemming te bereiken tussen de ketenpartners, omdat het op dit moment nog onduidelijk is op welke manier de partners online fraude proberen aan te pakken. Het is noodzakelijk om een duidelijk onderscheid te maken tussen preventieve en repressieve maatregelen. Ten tweede is het efficiënt om slechts één partner voorlichtingen over geldezels en cybercriminaliteit te laten geven, zodat de andere partners andere taken kunnen uitvoeren. Ten derde wordt het belang van jongerenwerk nog onderschat: jongerenwerkers zijn meer in contact met jongeren dan de jeugdagenten, waardoor jongerenwerkers een rol kunnen vervullen bij het signaleren van jongeren die zich bezighouden met online fraude. Vervolgonderzoek zou zich kunnen richten op een integrale aanpak waarbij verscheidene ketenpartners betrokken zijn of een groter gebied.

Inhoudsopgave

H1 Inleiding

Traditionele vormen van criminaliteit, zoals woninginbraken, nemen erg sterk af de laatste jaren (Felson, e.a., 2020), maar er is een toename van gedigitaliseerde criminaliteit en cybercriminaliteit. Gedigitaliseerde criminaliteit is de daadwerkelijke vervanger van traditionele criminaliteit: het is namelijk traditionele criminaliteit die deels online wordt gepleegd; het internet is dus enkel een middel (Servaas, e.a., 2021). Voorbeelden van gedigitaliseerde criminaliteit waar mensen zich schuldig aan maken zijn bijvoorbeeld online bedreigingen, fraude en phishing.

Bij cybercriminaliteit is van belang dat ICT zowel het middel als het doel is van de criminele handeling. Het gaat om strafbare feiten die gepleegd worden door gebruikmaking van elektronische communicatienetwerken en informatiesystemen of tegen dergelijke netwerken en systemen (Koops, 2014). Voorbeelden van cybercriminaliteit zijn Ddos aanvallen en hacken.

In dit onderzoek wordt gekeken naar gedigitaliseerde criminaliteit. Hierbij zal de nadruk worden gelegd op online fraude. Fraude is de opzettelijke misleiding om onrechtmatig voordeel te behalen (Openbaar Ministerie, z.d.). Vroeger was voornamelijk sprake van verticale fraude: burgers handelen bedrieglijk tegenover de overheid, zoals door belastingfraude, faillissementsfraude en witwassen. Tegenwoordig wordt veelvuldig gefraudeerd in horizontale verhouding: burgers bedriegen elkaar. Horizontale online fraude staat daarom in dit onderzoek centraal.

Er zijn enkele cijfers bekend die aanwijzingen geven dat er sprake is van een enorme toename van gedigitaliseerde criminaliteit in Nederland. De fraudehelpdesk zag in 2021 bijvoorbeeld een toename van het aantal meldingen van gedigitaliseerde criminaliteit van 10 procent ten opzichte van 2020. De schade die hierdoor is ontstaan, is bovendien fors toegenomen met 8 miljoen euro ten opzichte van het voorgaande jaar (NOS, 2022). De meeste meldingen betroffen WhatsAppfraude, waarbij de mobiele telefoon fungeert als middel om mensen op te lichten. Dat er de laatste jaren een toename is in delicten betreffende online fraude, zoals WhatsAppfraude, valt ook terug te zien in de rechtspraak. Een concreet voorbeeld van WhatsAppfraude is de vriend-in-noodfraude: familieleden of vrienden worden zogenaamd benaderd door een bekende met de mededeling dat ze een nieuw telefoonnummer gebruiken en zij geven vervolgens aan dat ze dringend geld nodig hebben. Vervolgens wordt (vaak) een geldbedrag overgemaakt via een betalingssysteem, zoals Tikkie, waardoor het geld op een rekening van een geldezel wordt gestort (Rechtbank Rotterdam, 2022). Geldezels zijn personen die tegen een kleine vergoeding hun bankpas ter beschikking stellen aan criminelen. Criminelen kunnen vervolgens ‘veilig’ hun gestolen geld opnemen via de bankrekening van de geldezel (Leukfeldt & Roks, 2020). Hierdoor ontlopen zij het risico om te worden opgepakt wegens online fraude en kunnen zij het gestolen geld gebruiken voor persoonlijke doeleinden. Geldezels zijn dus van groot belang in het proces van het witwassen van het gestolen geld. De laatste maanden zijn er steeds meer jonge geldezels in de regio Zuidoost Drenthe. Hieruit blijkt dat er in Zuidoost Drenthe ook sprake is van een toename in gedigitaliseerde criminaliteit.

Er zijn verschillende redenen voor de toevlucht naar gedigitaliseerde criminaliteit. Allereerst doet zich meer gelegenheid voor om online strafbare feiten te plegen. De gelegenheidstheorie veronderstelt immers dat gelegenheid de dief maakt (Cohen & Felson, 1979). Aangezien mensen meer thuis waren in verband met Covid-19 resulteerde dat in een daling van het aantal woninginbraken, maar heeft dat voor een toename in het aantal zaken betreffende online fraude gezorgd, zoals bijvoorbeeld marktplaatsfraude en WhatsAppfraude (Buil-Gil, e.a., 2020; Kruisbergen, e.a., 2021). Dit heeft natuurlijk te maken met het toegenomen gebruik van online-voorzieningen, zoals webshops en datingsites. Een tweede verklaring betreft het grensoverschrijdende karakter van gedigitaliseerde criminaliteit, zoals phishing (Bowkers, 2000). Er is een veel groter bereik aan mogelijke connecties die bijvoorbeeld nieuwe technieken kunnen aanleren aan de criminelen. Hierdoor ontstaan telkens nieuwe vormen van gedigitaliseerde criminaliteit waar de politie niet (goed) op kan reageren. Verder kan je als online fraudeur slachtoffers maken over de hele wereld. De derde verklaring heeft te maken met de kwetsbaarheid voor slachtofferschap. Het veelvuldig gebruikmaken van online platforms waar betaalverzoeken normaal zijn zorgt voor een hogere blootstelling aan de kans om slachtoffer van phishing te worden (Alseadoon, 2014; Sheng, e.a., 2010). Er worden steeds meer dagelijkse handelingen online verricht, zoals boodschappen doen, waardoor de kans groter wordt om slachtoffer te worden. Een vierde verklaring gaat over het daderschap. Vanwege de hoge mate van anonimiteit op het internet is de pakkans voor gedigitaliseerde criminaliteit veel lager dan bij traditionele vormen van criminaliteit, waardoor het aantrekkelijk wordt om online strafbare feiten te plegen (Bowkers, 2000). Jongeren zijn zich bewuster van hun handelingen op het internet aangezien zij hiermee opgegroeid zijn. Daardoor zien zij sneller in dat deze hoge mate van anonimiteit veel mogelijkheden biedt om online strafbare feiten te plegen. In combinatie met het ontdekken van de wereld zal dit mogelijk tot een toevlucht tot gedigitaliseerde criminaliteit leiden. Gelegenheid, het grensoverschrijdende karakter, de mate van activiteit en anonimiteit zijn enkele verklaringen voor de stijging in het aantal zaken van gedigitaliseerde criminaliteit, zoals phishing en andere vormen van online fraude.

Het is overigens niet verbazingwekkend dat veel jongeren actief zijn als crimineel in de onlinewereld. Deze groep is namelijk opgegroeid met het internet; in tegenstelling tot veel volwassenen die weinig kennis hebben over de werking van computers, hebben jongeren dit wel geleerd toen zij opgroeiden. Uit een onderzoek is bovendien gebleken dat ongeveer de helft van de ICT-studenten wel eens online een delict heeft gepleegd (Weulen Kranenbarg, e.a., 2022). Wederom geldt het gezegde “gelegenheid maakt de dief”: mensen met de benodigde kennis over ICT hebben eerder de mogelijkheid om online delicten te plegen dan mensen zonder enige kennis van ICT-middelen. Dit maakt de drempel voor ICT-studenten lager om online delicten te plegen en daarom zal het zich vaker voordoen. Meer in het algemeen geldt dit voor (vrijwel) alle jongeren: zij zijn opgegroeid met internet en hebben hierdoor (vaak) meer kennis van internet en computers dan hun (groot)ouders, waardoor zij zich eerder zullen begeven in de virtuele criminaliteit. Uit cijfers van de Monitor Zelfgerapporteerde Jeugdcriminaliteit blijkt dat tussen de 7 en 22 procent van de jongeren van tien tot tweeëntwintig jaar een vorm van cybercrime en/of gedigitaliseerde criminaliteit heeft gepleegd in 2014. De totale geregistreerde omvang van online fraude door jongeren is echter minder dan 1 procent (Beerthuizen, e.a., 2020). Er bestaat dus een discrepantie tussen de geregistreerde en zelf gerapporteerde cijfers van online fraude onder jongeren in

Nederland. Daarom is het van belang om vast te stellen in hoeverre dit in de regio Zuidoost Drenthe speelt en een integrale aanpak te formuleren om het probleem aan te pakken.

1.1 Online fraude: beleidsvragen

Uit cijfers van de politie blijkt dat de aard en omvang van (online) fraude niet gemakkelijk kan worden vastgesteld (Bloem, 2017). Alle vormen van fraude blijven zich telkens ontwikkelen, waardoor er geen volledig beeld kan worden geschetst van de totale omvang van (online) fraude. Bovendien wordt online fraude door de politie vaak geregistreerd als het delict 'oplichting', waardoor het lastig is om de omvang te bepalen, aangezien oplichting ook een traditionele vorm van criminaliteit is. Er is dus sprake van een gebrekkige vastlegging van de aangiftes. Verder hangt dit ook af van de complexiteit van sommige vormen van fraude en de slechte aanpak van fraude. Bovendien is de pakkans erg laag: bij sommige vormen van online fraude is deze minder dan 5 procent. Kortom, er zijn genoeg redenen om een integrale aanpak te formuleren om online fraude aan te pakken.

De huidige aanpak van online fraude (door jongeren) bestaat voornamelijk uit preventieve maatregelen of een veroordeling. Preventieve maatregelen voor jongeren zijn bijvoorbeeld voorlichtingen op scholen door agenten, HALT-medewerkers of maatschappelijk werkers over de gevolgen van online fraude. Een concreet voorbeeld is de mobiele-mediabus (politie.nl, z.d.). De mobiele-mediabus is een vrachtwagen die door Nederland rijdt waarin voorlichtingsmateriaal over strafbare feiten, zoals cyberpesten, sexting en geldezels, wordt tentoongesteld. Daarnaast zijn daar vaak jeugdagenten of jongerenwerkers aanwezig die een mondelinge uitleg geven.

Veroordelingen zijn repressief van aard. De jeugdige verdachte wordt opgepakt en eventueel veroordeeld door een rechter. Een mogelijk gevolg van een veroordeling wegens Whatsappfraude kan zijn dat de veroordeelde, zoals bijvoorbeeld een geldezel, voor een langere periode geen mogelijkheid heeft om een bankrekening te openen in Nederland (Gerechtshof Amsterdam, 2021). De veroordeling wegens online fraude leidt er namelijk toe dat banken een interne en externe melding maken van de verdachte activiteiten van de desbetreffende persoon. Hierdoor kunnen andere banken kennisnemen van de melding en bij de desbetreffende bank nadere informatie opvragen over de fraudeur. Dit heeft tot gevolg dat er gedurende langere periode niet op rechtmatige wijze geld kan worden verdiend door de schuldige van online fraude. Fraudeurs kunnen gedurende een periode van vijf jaar geen bankrekening openen als gevolg van deze meldingen. Dit zou daarom mogelijk leiden tot een toevlucht tot (andere) criminele activiteiten om toch aan geld te kunnen geraken. Bovendien zorgt online fraude op zichzelf al voor enorme gevolgen, zoals de eerdergenoemde financiële schade, maar het kan ook impact hebben op de emotionele gesteldheid van slachtoffers. Voornamelijk mensen met een laag inkomen ondervinden meer emotionele schade als gevolg van online fraude dan mensen met een hoger inkomen (Borwell, e.a., 2021). De financiële en emotionele schade van slachtoffers geven al aan dat de focus van de politie en haar samenwerkingspartners moet worden gelegd op het actief bestrijden van online fraude. Een aanpak waarbij de nadruk enkel op preventie ligt, is gezien de huidige statistische cijfers ongewenst.

Rond de aanpak van cybercriminaliteit heersen nog verschillende ideeën. Verschillende organisaties kunnen een rol spelen bij interventies (Rathenau Instituut, 2021). De overheid kan bijvoorbeeld nieuwe wet- en regelgeving maken zodat de online normen

worden vastgesteld. Hierdoor wordt duidelijk wat wel en niet mag op het internet. Bedrijven kunnen ook interveniëren door middel van blacklisting (zwarte lijst bij banken) of detectie van malafide betaalverzoeken (door eigenaren van tikkie, WhatsApp, mobiele providers of mail instanties). Maatschappelijke werkers kunnen hulpverlening bieden aan slachtoffers van online fraude of meer bewustzijn creëren door middel van lespakketten, voorlichtingen en reclames. De nadruk ligt in veel gevallen op preventie van online fraude, maar er kan ook worden gedacht aan verstorende interventies of de opsporing van cybercriminelen. Dit zijn voornamelijk taken die de politie uitvoert; waarbij andere partijen (lang) op de achtergrond blijven. Een integrale aanpak zou echter kunnen leiden tot een adequate aanpak voor jeugdige cybercriminelen. Een integrale aanpak houdt in dat er verscheidene organisaties met eigen taken zullen bijdragen aan de bestrijding van een bepaalde criminaliteitsvorm. Er bestaat een discrepantie tussen de geregistreerde en zelfgerapporteerde cijfers van cybercriminaliteit door jongeren, waardoor onderzoek wenselijk is. In dit onderzoek zal de focus komen te liggen op online fraude door jongeren in de regio Zuidoost Drenthe. In deze regio komen steeds meer jonge geldezels in beeld bij de politie, waardoor meer interesse ontstaat in deze regio om online fraude door jongeren te prioriteren en daarom meer te handhaven. In dit onderzoek zal worden gepoogd om een integrale aanpak te formuleren. Deze integrale aanpak zal worden geformuleerd voor beleidsmedewerkers openbare orde en veiligheid bij gemeenten, (jeugd)agenten en jongerenwerkers van de gemeente.

1.2 Relevantie

Een onderzoek naar de aanpak van online fraude door jongeren van de gemeente, politie en jongerenwerk is vanuit verschillende perspectieven relevant. Als eerste wordt de sociologische relevantie besproken. Daarna wordt duidelijk wat dit onderzoek zal toevoegen aan het bestaande wetenschappelijke onderzoek naar online fraude. Tot slot wordt gekeken naar de relevantie van dit onderzoek voor de politie.

1.2.1 Sociologische relevantie

In de Nederlandse maatschappij heerst een individualistische cultuur waarin mensen niet meer om elkaar denken, maar eerder gefocust zijn op hun eigen leven. Criminaliteit versterkt dit individualisme: mensen worden telkens meer uit elkaar gedreven doordat zij zich onveilig voelen in hun eigen omgeving. Ongeveer 33 procent van de Nederlanders voelde zich in het algemeen onveilig. Bijna 20 procent van de ondervraagden verwacht binnen twaalf maanden slachtoffer te worden van online oplichting (CBS, 2021). Er heerst dus een idee van onveiligheid onder burgers. Hierdoor ontstaat minder sociaal contact. Criminaliteit zorgt voor een verslechtering van de sociale cohesie in de maatschappij. Een van de centrale vraagstukken binnen de sociologie betreft sociale cohesie. Sociale cohesie gaat over de mate van verbondenheid en samenhang binnen een bepaalde groep mensen. Naarmate er meer sociale cohesie is binnen de samenleving zorgt dit ervoor dat mensen zich minder onveilig voelen en minder vaak slachtoffer worden van criminaliteit (Huygen & De Meere, 2008). Mensen kunnen zich op het internet ook onveilig voelen, één op de vijf Nederlanders vreest voor slachtofferschap van online fraude, en hierdoor kunnen mensen online ook steeds verder uit elkaar komen te staan. Om de sociale cohesie te bevorderen moet dan ook een integrale aanpak worden ontwikkeld om de onveiligheidsgevoelens van burgers op het internet weg te nemen.

Een andere reden waarom de integrale aanpak tussen gemeente en politie moet worden onderzocht zijn de ernstige gevolgen voor jongeren. Jongeren die online fraude

hebben gepleegd kunnen als gevolg hiervan gedurende vijf jaren geen bankrekening openen bij alle Nederlandse banken (Gerechtshof Amsterdam, 2021). Dit zorgt ervoor dat jongeren niet op rechtmatige wijze geld kunnen verdienen. Het is weliswaar zo dat veel jongeren nog (financieel) afhankelijk zijn van hun ouders, maar er wordt vaak al enige zelfstandigheid van de ouders verwacht naarmate de jongere ouder wordt. Dit kan door een veroordeling worden belemmerd, terwijl de jongere zelf ook naar onafhankelijkheid streeft. Dit kan naar alle waarschijnlijkheid betekenen dat ze zich nog verder gaan begeven in het criminele circuit. Dat is namelijk een van de manieren om alsnog aan geld te kunnen komen. Om de mogelijke groei van crimineel gedrag onder jongeren in te perken is het daarom van groot belang om een goede integrale aanpak op te stellen. Met een dergelijke aanpak kan online fraude door jongeren wellicht vaker worden voorkomen.

1.2.2 Wetenschappelijke relevantie

Er ligt nog een leemte in het onderzoek naar cybercrime gepleegd door Nederlandse jongeren. Dit kan hoofdzakelijk worden verklaard doordat cybercrime een relatief nieuwe criminaliteitsvorm is. Het huidige onderzoek richt zich voornamelijk op slachtoffers van gedigitaliseerde criminaliteit (Borwell, e.a., 2018a; Jansen & Leukfeldt, 2018). De meeste mensen schatten in dat zij zelf waarschijnlijk geen slachtoffer zullen worden van gedigitaliseerde criminaliteit en dat anderen uit hun omgeving daar meer kans op hebben (Cox, e.a., 2020). Slachtoffers van phishing blijken echter vaker en meer actief te zijn op het internet en online bankieren dan mensen die geen slachtoffer worden van phishing (Hutchings & Hayes, 2009). Verder zijn persoonlijkheidskenmerken, zoals neuroticisme, altruïsme en extraversie, ook bepalend voor de mate waarin mensen ingaan op een phishing aanval (Borwell, e.a., 2018b). 9 procent van de Nederlanders tussen de 15 en 25 jaar is in 2021 slachtoffer geworden van online fraude (CBS, 2022b). Andere onderzoeken zijn meer gericht op de werking van een cybercrimineel netwerk: welke mensen plegen cybercriminaliteit en hoe komt cybercriminaliteit tot stand (Dehghanniri & Borrion, 2021; Leukfeldt, e.a., 2017a; 2017b; Rooyakkers & Weulen Kranenbarg, 2020). Daarbij kan gedacht worden aan bepaalde risicofactoren die invloed hebben op het al dan niet ontstaan van cybercriminaliteit. Deze onderzoeken naar daderschap zijn echter niet specifiek gericht op jongeren.

Tegenwoordig zijn de meeste interventies gericht op preventie van slachtofferschap: op sociale media, maar ook op televisie wordt gewaarschuwd voor de tekenen van online fraude. In paragraaf 3.3 zal nader worden ingegaan op bestaande onderzoeken over interventies gericht op online fraude. Er wordt echter nauwelijks aandacht besteed aan het verbeteren van onderlinge samenwerkingsverbanden van de politie. De verrichte onderzoeken zijn vaak meer bestuurlijk van aard of hebben een ander thema dan het huidige onderzoek naar online fraude (Buirma, 2021; Boekhoorn & Speller, 2004; Terpstra & Kouwenhoven, 2004). Aangezien slechts een klein percentage van de slachtoffers van online fraude aangifte doet, kan een samenwerking met bijvoorbeeld gemeenten of jeugdwerkers leiden tot meer informatie en mogelijk ook tot nieuwe kennis om te interveniëren. Daarom wordt in dit onderzoek gekeken naar de mogelijkheden om een samenwerkingsverband tussen de politie, gemeenten en jongerenwerkers in Zuidoost-Drenthe op te zetten.

Eerdere onderzoeken naar een integrale aanpak gaan voornamelijk over andere vormen van criminaliteit, zoals bijvoorbeeld het wapenbezit onder jongeren (CCV, 2020) en ondermijning (Van der Torre & Tops, 2022; Tops & Schilders, 2016). De top600-aanpak is

een goed voorbeeld van een integrale aanpak van verschillende criminaliteitsvormen (Van Grinsven & Verwest, 2017). Er wordt een specifieke aanpak bedacht per persoon die op de lijst van de top600 staat. Meer dan veertig organisaties spelen een rol bij het bestraffen en zorgen voor personen die op de lijst van de top600 staan. De regisseur zorgt ervoor dat alle problematiek in kaart wordt gebracht, zoals politiecijfers, eerdere delicten, het sociale netwerk, zorg en woonplaats van de mensen op de lijst. Alle partners van de top600 kunnen vervolgens hun eigen taken en bevoegdheden gebruiken om een zo optimaal mogelijke uitkomst voor de desbetreffende persoon op de lijst. De mensen op deze lijst zijn veelplegers in Amsterdam. In dit onderzoek wordt echter specifiek gefocust op enkele delictsvormen die onder de noemer van online fraude vallen. Het gaat om online aan- en verkoopfraude en alle varianten van phishing. Bovendien is deze integrale aanpak specifiek voor de regio Zuidoost Drenthe. Dit komt doordat de huidige werkwijzen van de samenwerkingsverbanden tussen de politie, gemeente Emmen, Borger-Odoorn en Coevorden en de jongerenwerkers in deze regio de leidraad zijn voor het onderzoek. Wellicht kunnen sommige delen van de aanpak universeel worden toegepast, maar zal er meer specifiek gekeken worden naar de huidige omstandigheden in Zuidoost Drenthe. Er moet overigens worden gesteld dat er landelijk gezien nog geen (concrete) integrale aanpak voor online fraude door jongeren is opgesteld, waardoor deze integrale aanpak wellicht als voorbeeld voor andere regio's kan dienen.

1.2.3 Relevantie politie

In de regio Zuidoost-Drenthe merkt de politie dat de samenwerking tussen politie en gemeente niet naar behoren werkt. Sinds begin 2015 is de verantwoordelijkheid voor de zorg van jongeren weggelegd voor de gemeente (NJI, z.d.). Concreet houdt dit in dat de gemeente beleid moet formuleren welke gericht is op vroegsignalering en het tijdig bieden van de juiste hulp op maat. Dan kan worden gedacht aan het vroegtijdig signaleren van criminele activiteiten van jongeren en hierop adequaat reageren door middel van bijvoorbeeld een gesprek met de ouders of het inschakelen van politie of jongerenwerkers. Uit de eerste evaluatie van de Jeugdwet komt naar voren dat gemeenten wel een samenwerkingsverband tussen verschillende partners stimuleren, maar dat er van een gezamenlijk werkproces geen sprake is (Friele, e.a., 2018). Kortom, dit stemt overeen met het idee dat heerst binnen de politie Zuidoost-Drenthe. Zij zouden graag een betere samenwerking willen realiseren in hun regio met de gemeente en jongerenwerkers. Jongerenwerkers zijn mensen met een zorgachtergrond die zich bezighouden met problematiek in hun regio omtrent jongeren, zoals bijvoorbeeld psychische problemen, maar ook jongeren die actief zijn in het criminele circuit. Aangezien online fraude op dit moment een groot landelijk probleem is, wordt dit onderzoek nader toegespitst op dit onderwerp. Afgelopen jaar werden er bijvoorbeeld twee verdachten aangehouden in Noord-Nederland wegens een grote cybercrime-zaak over bankhelpdeskfraude en witwassen (OM, 2021). Een van deze verdachten was slechts achttien jaar oud en hieruit blijkt dat cybercrime onder jongeren in de eenheid Noord-Nederland zeker een aandachtspunt zou moeten zijn voor de politie. Dit onderzoek moet dan ook bijdragen aan een verbeterde aanpak van online fraude door politie en de gemeenten in Zuidoost Drenthe, maar wellicht ook in andere regio's.

1.3 Probleemstelling

In dit onderzoek wordt gezocht naar de verbeterpunten in de huidige aanpak van online fraude door de politie in Zuidoost Drenthe. Op dit moment wordt voornamelijk gekeken naar preventieve maatregelen om te voorkomen dat jongeren online strafbare feiten gaan plegen.

Een collectieve, integrale aanpak van de gemeente, politie en jongerenwerkers ontbreekt echter nog. Bij veel andere vormen van jeugdcriminaliteit wordt echter wel samengewerkt tussen deze partners. Bij overlast door jongeren wordt bijvoorbeeld gebruik gemaakt van een zogenaamde ‘groepsscan’ waarbij een problematische groep jongeren in kaart wordt gebracht door de politie (CCV, z.d. b). Vervolgens gaat de gemeente gezamenlijk met agenten en jongerenwerkers een plan van aanpak maken naar aanleiding van deze groepsscan. Voor online fraude door jongeren wordt echter nog niet met een integrale aanpak samengewerkt, terwijl online fraude op dit moment wel degelijk een ernstig probleem is binnen de Nederlandse samenleving. Bij de politie in Zuidoost Drenthe wordt dit ook opgemerkt en daarom willen zij graag een eerste stap maken richting een integrale aanpak. De onderzoeksvraag die dient te worden beantwoord luidt als volgt: “Hoe kan een integrale aanpak voor online fraude door jongeren worden opgezet door politie, gemeente en jongerenwerkers in de regio Zuidoost Drenthe?". Daarvoor is het van belang dat duidelijk wordt hoe de integrale aanpak op dit moment wordt ingevuld, welke wensen de partners hebben en hoe de integrale aanpak zou moeten functioneren volgens algemene theorieën.

De deelvragen die binnen dit onderzoek zullen worden beantwoord luiden als volgt:

1. Welke kennis hebben de gemeente, politie en jongerenwerkers (voortaan: ketenpartners) over de omvang van online fraude in de regio Zuidoost Drenthe?
2. Hoe ziet de huidige samenwerking tussen de ketenpartners eruit?
3. Wat zijn knelpunten binnen de huidige samenwerkingsverbanden?
4. Wat gaat juist goed binnen huidige samenwerkingsverbanden?
5. Hoe willen de ketenpartners invulling geven aan een integrale aanpak van online fraude door jongeren?

1.4 Samenvatting

Uit verschillende cijfers komt naar voren dat er in Nederland steeds meer sprake is van cyber- en gedigitaliseerde criminaliteit. Er zijn verschillende verklaringen voor deze toename in cyber- en gedigitaliseerde criminaliteit, waaronder de hoge mate van anonimiteit en de extra gelegenheid om online delicten te plegen. Het is dan ook van groot belang om cybercriminaliteit aan te pakken. Een van deze vormen van gedigitaliseerde criminaliteit die in veelvoud voorkomt is online fraude. Op dit moment worden al verscheidene interventies ingezet om bijvoorbeeld online fraude tegen te gaan, waarbij de nadruk voornamelijk ligt op preventie. Op verschillende gebieden omtrent jeugdcriminaliteit wordt veelvuldig samengewerkt tussen de politie, beleidsmedewerkers van de gemeente en jongerenwerkers. Een integrale aanpak van online fraude door jongeren ontbreekt echter nog, terwijl jonge geldezels steeds vaker in het nieuws komen. Dit vermoeden heerst ook onder de agenten in de regio Zuidoost Drenthe. Daarom moet worden gekeken naar een integrale aanpak om dit te bestrijden.

1.5 Leeswijzer

In het eerste hoofdstuk is een introductie gegeven op het onderwerp van het onderzoek. Verder zijn de maatschappelijke, sociologische en wetenschappelijke relevantie beschreven. Aangezien dit onderzoek in opdracht van de politie is uitgevoerd, is de relevantie voor de politie ook beschreven. Het tweede hoofdstuk is een systematische review van alle relevante verschenen artikelen over online fraude en phishing. Het derde hoofdstuk bestaat uit een theoretisch kader waarin de vorming van een phishing netwerk, de motieven van jongeren om

online fraude te plegen, mogelijke interventies en algemene theorieën over samenwerkingsverbanden worden uitgelegd. De onderzoeksmethode wordt nader uitgelegd in het vierde hoofdstuk. In het vijfde hoofdstuk worden de resultaten van het onderzoek beschreven. In het laatste hoofdstuk worden een conclusie, aanbevelingen en enkele discussiepunten gegeven.

H2 Systematische review

Het doel van deze systematische review is om een onbevooroordeelde synthese van alle relevante onderzoeken in deze scriptie weer te geven. Deze systematische review is gericht op online fraude. Fraude is de opzettelijke misleiding om onrechtmatig voordeel te behalen. Online fraude is fraude die wordt gepleegd met behulp van het internet. In dit onderzoek zal voornamelijk de nadruk worden gelegd op verschillende vormen van phishing, zoals Whatsappfraude. Andere vormen van online fraude zijn bijvoorbeeld aan- en verkoopfraude op websites, zoals Marktplaats, maar deze vormen worden niet meegenomen in de review.

2.1 Methode

Voor deze review werden enkele zoektermen ingevoerd in de zoekmachine SocIndex. De eerste zoekterm luidde als volgt [online or internet or virtual or digital or web] AND [fraud] AND [perpetrator or abuser or offender]. Toen kwamen er in totaal 65 hits, waarvan er 33 op het eerste gezicht bruikbaar waren voor mijn onderzoek. De criteria van inclusie waren:

- De artikelen zijn na 2005 gepubliceerd. Artikelen die voor die tijd zijn geschreven zijn niet van belang, omdat online fraude pas opkwam;
- Het moest gaan om online fraude en niet om andere vormen van (cyber)criminaliteit;
- Het moest gaan om daderschap, dus artikelen over slachtoffers werden niet meegenomen;
- Daarnaast waren de onderzoeken over bedrijven die te maken kregen met online fraude buiten beschouwing gelaten.

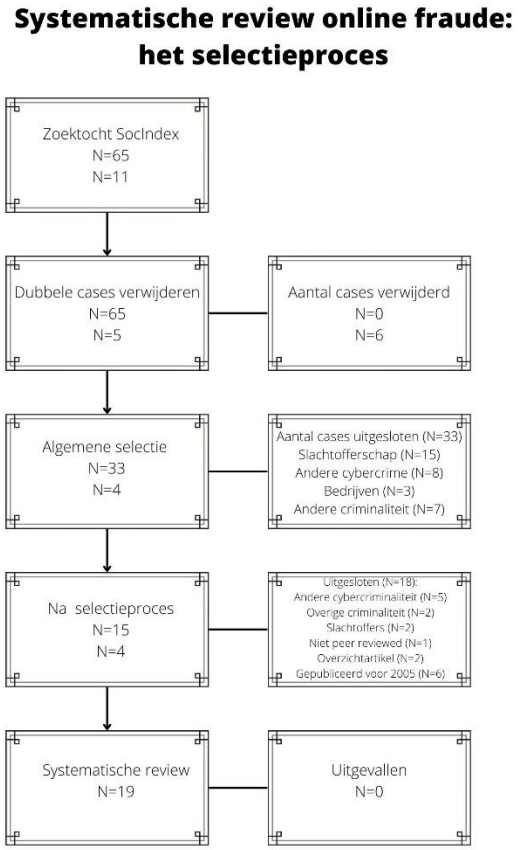
Bepaalde artikelen waren weggelaten, omdat deze onderwerpen niet relevant waren voor mijn onderzoek, zoals slachtofferschap (N=14) of andere vormen van gedigitaliseerde criminaliteit zoals bijvoorbeeld datingfraude (N=8), gedigitaliseerde criminaliteit waarbij bedrijven slachtoffer zijn (N=3) en niet peer reviewed artikelen (N=2). Verder waren er nog zeven artikelen die overige criminaliteitsvormen bespraken die dus niets met gedigitaliseerde criminaliteit te maken hadden. Daardoor kwam ik op 33 artikelen uit die moesten worden beoordeeld op bruikbaarheid.

Onderwerpen zoals de modus operandi, cybercrime netwerken, motieven, maar ook de verschillen tussen online en offline criminaliteit vielen onder de criteria. Na het lezen van de samenvattingen van de artikelen kwam ik tot vijftien artikelen over online fraude. De tweede zoekterm die was ingevoerd was [phishing] AND [perpetrator or abuser or offender]. Er waren in totaal elf resultaten, maar enkele resultaten kwamen ook al voor in de vorige zoekactie. Hierdoor waren er nog vier andere resultaten toegevoegd aan de lijst. Dat maakte een totaal van negentien artikelen die werden meegenomen in de systematische review. Deze worden hierna besproken.

2.2 Dataverzameling

Uiteindelijk waren er negentien artikelen gelezen. In *figuur 1* is het selectieproces stapsgewijs weergegeven. Daarna kon het analyseren van de artikelen beginnen. In eerste instantie had ik algemene gegevens, zoals het soort onderzoek, de participanten van de onderzoeken en de locatie, weergegeven in een tabel. Vervolgens had ik een tabel gemaakt met daarin de volgende informatie: auteurs, titel van het artikel, de publicatiedatum van het artikel, de betekenis van online fraude, een korte samenvatting en de belangrijke informatie voor het

huidige onderzoek. Uiteindelijk had ik de samenvatting gebruikt voor de derde paragraaf en de overige informatie staat vermeld in *tabel 2.*



Figuur 1: Selectieproces artikelen systematische review.

2.3 Resultaten

In deze systematische review werden verschillende belangrijke aspecten van de onderzoeken meegenomen, waaronder het soort onderzoek, de participanten, het land van onderzoek, de hoofdonderwerpen van het onderzoek, de betekenis van online fraude in de onderzoeken, een korte samenvatting per onderzoek en de belangrijkste zaken voor het huidige onderzoek.

2.3.1 Algemene informatie

In totaal waren er negentien artikelen meegenomen in deze review. De algemene informatie van de onderzoeken zijn schematisch weergegeven in *tabel 1*. In de onderzoeken werden verschillende soorten onderzoeksmethodes gebruikt. Er werd onderscheid gemaakt tussen kwantitatief, kwalitatief, mixed methods, verkennend onderzoek en politiegegevens. De verkennende onderzoeken bestonden voornamelijk uit beschrijvende informatie over online fraude. Wanneer verhoren en soortgelijke bronnen afkomstig van de politie werden gebruikt voor het onderzoek was sprake van gebruik van politiegegevens. In twee onderzoeken was bijvoorbeeld gebruik gemaakt van een kwalitatieve methode waarbij observaties zijn waargenomen op online fora (MacDonalds & Frank, 2017; Holt, e.a., 2015). Er was ook sprake van triangulatie in een van de onderzoeken, omdat zowel gebruik was gemaakt van interviews als van observaties (Roks, e.a., 2021). In dergelijke gevallen wordt wel gesproken van *mixed methods*. De meeste participanten van de onderzoeken waren daders. In de overige onderzoeken waren de volgende mensen onderzocht: slachtoffers, jongeren tussen tien en

achttien jaar, internetgebruikers, witwassers en beleidsmakers. Een van de onderzoeken was verkennend van aard, waarbij geen participanten waren betrokken (Shun Yung & Huang, 2011). De onderzoeken die waren meegenomen in de systematische review hadden onderzoekspopulaties uit Nederland, Australië, Nigeria, wereldwijd, Engeland, Verenigde Staten en Macedonië.

Tabel 1: Algemene informatie over de onderzoeken (N=19).

Soort onderzoek	Participanten	Locatie
Kwantitatief (4)	Daders (9)	Nederland (7)
Kwalitatief (5)	Slachtoffers (3)	Wereldwijd (4)
Mixed methods (3)	Jongeren tussen 10 en 18 jaar (1)	Australië (3)
Verkennend onderzoek (3)	Internetgebruikers (1)	Verenigde Staten (2)
Politiegegevens (4)	Witwassers (1)	Nigeria (1)
	Beleidsmakers (1)	Engeland (1)
	IT-experts (1)	Macedonië (1)
	Overheid (1)	
	Geen (1)	

2.3.2 Thematische onderwerpen

In de negentien bestudeerde artikelen kwamen zeven hoofdonderwerpen naar voren, namelijk online tegenover offline criminaliteit, cijfers van online fraude, cybercrime netwerken, interventies, motieven, de modus operandi en de beleidsimplicaties. Hierna worden alle artikelen per thema besproken. In *tabel 2* wordt de overige relevante informatie weergegeven.

Online vs. offline criminaliteit

In een van de onderzoeken (Kruisbergen, e.a., 2019) werd gekeken naar de verschillen in witwassen tussen traditionele en cyber- en gedigitaliseerde criminaliteit. Het witwassen van het geld van criminele activiteiten geschiedde traditioneel door middel van het kopen van luxegoederen, huizen en bedrijven of investeringen voor het plegen van nieuwe/andere delicten. Sinds de opkomst van cyber- en gedigitaliseerde criminaliteit wordt het geld op een nieuwe manier witgewassen, namelijk door de inkoop van bitcoins.

Een ander onderzoek waarin de verschillen tussen online en offline criminaliteit aan de orde komt gaat over het gebruik van online fora en de arrestaties van de criminelen (Holt, e.a., 2015). De criminelen op online fora proberen altijd het risico op oplichting zo minimaal mogelijk te houden. Dit doen zij door hun gedrag aan te passen, waardoor de opbrengsten van de aankopen (of verkoop) maximaal zijn. Dit gebeurt ook bij offline criminaliteit. De manier waarop de risico's worden geminimaliseerd en de winst wordt gemaximaliseerd verschilt echter van offline criminaliteit. De hoge mate van anonimiteit op online fora zorgt voor extra veel risico voor de koper, omdat zij niet weten met wie zij zakendoen. Daarom wordt vaak gebruik gemaakt van online beoordelingssystemen. De betrouwbaarheid van deze systemen is echter ook niet te garanderen. De beoordelingssystemen zorgen ervoor dat de verkopers worden beoordeeld door de kopers. Hierdoor verschuift het risico van de koper naar de verkoper van de (illegale) goederen. Daarom wordt in sommige gevallen gebruik gemaakt van tussenpersonen die de koop en verkoop van (illegale) goederen faciliteren. Desondanks blijft het lastig voor de politie om arrestaties te verrichten, omdat er geen fysieke ontmoetingen zijn en de criminelen anoniem zijn.

Het internet en sociale media worden veelal gebruikt om criminele daden te faciliteren (Roks, e.a., 2021). In sommige gevallen verbetert het crime script door het gebruik van het internet. Traditionele misdaden worden gemakkelijker gefaciliteerd door sociale media, bijvoorbeeld bij het aanbieden van gestolen goederen. Maar veel criminelen gaan ook cyber- en gedigitaliseerde criminaliteit plegen naast de gebruikelijke illegale activiteiten. In dit onderzoek naar online fraude in de regio Zuidoost Drenthe ligt de focus echter op daderschap van jongeren. Daar speelt een ander onderzoek juist op in (Kerstens & Jansen, 2016). Slachtofferschap en daderschap van online fraude blijken namelijk invloed te hebben op elkaar. Jongeren hebben als slachtoffer van online fraude meer kans om zelf dader te worden. Daar speelt het motief 'wraak' een grote rol bij.

Cijfers en ontwikkeling van online fraude

Drie van de achttien onderzoeken zijn cijfermatig van aard. Een concreet voorbeeld wordt gegeven over Macedonië. In Macedonië zijn schrikbarende cijfers van zowel het aantal slachtoffers als daders van online fraude (Rashkovski, e.a., 2016). Het is een dunbevolkt land waar veel daders en slachtoffers van online fraude zijn. In veel landen is er echter een bepaalde discrepantie tussen het aantal geregistreerde en daadwerkelijke gevallen van economische online fraude. Er wordt wel gesproken van een *error marge* in de data (Levi, 2017a). Als gevolg hiervan is het lastig voor de politie en andere veiligheidsinstanties om adequate maatregelen te nemen om economische online fraude te bestrijden. Een opvallende bevinding is echter wel dat de gemiddelde financiële schade van online fraude kleiner wordt, maar er meer slachtoffers van online fraude komen (Macdonald & Frank, 2017). Er worden dus lagere bedragen gebruikt om mensen op te lichten, maar hierdoor ontvangen de daders wel meer geld. Naar schatting zijn er 81.000 mensen actief op fora als online fraudeur. Hieruit kan echter niet worden geconcludeerd dat er sprake is van een toename van online fraude gedurende de laatste jaren. Dit komt doordat cijfers over daderschap ontbreken of zeer onzeker zijn.

Phishing ontwikkelt zich sterk de laatste jaren (Teherani & Pontell, 2021). De meest gebruikelijke vorm van phishing bestaat uit het lukraak verzenden van grote hoeveelheden e-mails naar potentiële slachtoffers. Ondanks deze bevinding is geconstateerd dat *spear phishing* steeds populairder wordt onder de cybercriminelen. Dit zijn gepersonaliseerde berichten van cybercriminelen om de slachtoffers te doen overtuigen van de echtheid van het bericht, zoals bijvoorbeeld het gebruik van foto's, bekende bedrijfsnamen of persoonlijke informatie van het slachtoffer. Er zijn verschillende vormen van phishing: Business E-Mail Compromise (BEC), Smishing, Vishing, Spear phishing en Whaling (zie: *tabel 2*). Een mogelijke beschermingsmaatregel tegen phishing is de Multi Factor Authenticatie-code. De code is gelinkt aan het account van de desbetreffende internetgebruiker en moet worden ingevoerd om in te kunnen loggen. Deze code verandert echter iedere minuut, waardoor het lastiger wordt voor daders om mensen online op te lichten.

Cybercrime netwerken

In vijf artikelen werd de totstandkoming van het netwerk en de werkwijzen van online fraudeurs besproken (Hutchings & Hayes, 2009; Leukfeldt, e.a., 2017b, 2017c, 2017d; Leukfeldt, 2014). Er kan een onderscheid worden gemaakt tussen een crimineel netwerk en samenplegen (Hutchings & Hayes, 2009). Soms kan slechts worden gesproken van een groep criminelen die sporadisch samenwerkt. Daarbij kan gedacht worden aan het samenplegen van

een bepaalde aanval op computers, het uitwisselen van kennis en kunde over hacken en frauderen en het delen van gegevens van slachtoffers. In veel gevallen worden via het internet diensten aangeboden door mensen met technologische kennis. Dan hoeft er niet per se sprake te zijn van een cybercrimineel netwerk. Voor jongeren geldt dat zij niet per se onderdeel zijn van een netwerk, maar vaker worden ze gezien als toevallige samenplegers of zelfs vrienden of kennissen van personen die wel in het cybercrime netwerk zitten. Daarom is het belangrijk om na te gaan hoe een cybercrime netwerk kan worden gevormd en welke rol jongeren mogelijk spelen in een cybercrime netwerk.

Sommige netwerken worden gevormd in de offlinewereld, terwijl andere netwerken worden gevormd via online fora (Leukfeldt, 2014). Bij de vorming van een netwerk kan onderscheid worden gemaakt tussen vier vormen (Leukfeldt, e.a., 2017b). De eerste vorm is een netwerk dat volledig wordt gevormd via fysieke sociale contacten. Wanneer de kernleden elkaar via fysieke wegen hebben gevonden, maar de specialistische kennis via het internet wordt verkregen dan is sprake van de tweede vorm. De derde variant bestaat uit kernleden die elkaar hebben leren kennen via online fora en overige leden worden via sociale contacten gerekruteerd in de fysieke sfeer. De laatste variant bestaat volledig uit leden die elkaar via online fora hebben ontmoet. Het overgrote deel van de cybercrime netwerken wordt nog steeds voornamelijk gevormd vanuit sociale contacten in de offlinewereld. Opvallend is dat de meeste cybercrime netwerken hoofdzakelijk bestaan uit mensen zonder de vereiste technologische kennis. De wijze waarop een cybercrime netwerk wordt gevormd is van belang voor het toepassen van verschillende interventies.

Een ander onderscheid dat wordt gemaakt tussen cybercrime netwerken gaat over hightech en lowtech netwerken (Leukfeldt, e.a., 2017c; 2017d). Bij lowtech aanvallen worden e-mails verstuurd waarin (1) vervolgens wordt gebeld met het slachtoffer om gegevens te verkrijgen of (2) via de e-mail verdere stappen worden ondernomen om de bankgegevens te krijgen. Er wordt slechts in de beginnende fase gebruik gemaakt van het internet om vervolgens in de fysieke sferen verder te opereren door bijvoorbeeld het inschakelen van personen die bankpasjes komen ophalen en geld pinnen, de zogenaamde geldezels. In hightech netwerken wordt gebruik gemaakt van malware waarbij identificatiecodes worden opgespoord. Hoe meer technologie moet worden gebruikt, des te minder het contact tussen dader en slachtoffer. Vaak zijn hightech netwerken internationaler van aard. In Nederland wordt bijvoorbeeld nog vaak via een lowtech netwerk online gefraudeerd en zijn de netwerken niet erg internationaal georiënteerd. Voor hightech netwerken die via fora werken geldt dat het misschien handig is om de opsporingsonderzoeken te richten op jongeren die een ICT-studie volgen, meer specifiek de jongeren die een fascinatie hebben voor programmeren en coderen. Zij zijn namelijk vaak betrokken in dit soort netwerken, omdat zij de benodigde kennis hebben om bijvoorbeeld spyware te installeren. Daar zou rekening mee moeten worden gehouden met het inzetten van interventies.

Interventies

In een Australisch onderzoek (Cross & Richards, 2017) werd het idee van slachtoffers onderzocht dat de politie altijd alle zaken oplost. Deze ideeën krijgen burgers door het kijken naar crimeseries op tv, zoals CSI. Dergelijke series blijken inderdaad invloed te hebben op de verwachtingen van burgers richting de politie. Een mogelijke interventie zou dus kunnen zijn dat televisieprogramma's en documentaires worden gemaakt om burgers te informeren over

online fraude en het voorkomen daarvan (Cross & Richards, 2017). Een andere mogelijke interventie is meer preventief van aard. Uit een ander onderzoek (Drew & Farrell, 2018) blijkt dat potentiële slachtoffers van online fraude met een hoge kans op slachtofferschap geen maatregelen nemen ondanks dat ze wel deze kennis hebben over maatregelen die hen kunnen beschermen. Er kan dan onderscheid worden gemaakt tussen harde en zachte maatregelen. Harde preventieve maatregelen zijn fysieke barrières, zoals antivirussoftware, firewalls en wachtwoordbescherming. Zachte maatregelen zijn bijvoorbeeld het delen van een minimale hoeveelheid informatie op sociale media, extra beveiliging op online fora en chatrooms installeren, enkel bekende mensen op sociale media accepteren als vriend/volger en het negeren van e-mails van onbekenden. Het blijkt ook dat de agenten meer zouden moeten onderwijzen over preventie en dat de bescherming die dit aan slachtoffers zou kunnen geven. In hoofdstuk drie worden nog andere interventies besproken die mogelijk kunnen worden ingezet om online fraude tegen te gaan. Daarnaast werd in een ouder onderzoek al gesteld dat er ook een rol bij banken ligt om online fraude te voorkomen (Shun Yung & Huang, 2011). Er werd gesteld dat de bescherming van klanten zou verbeteren door het invoeren van een tweestapsverificatie. Inmiddels wordt dit al enkele jaren gebruikt.

Motieven

In een onderzoek naar de motieven van mensen (Ibrahim, 2016) wordt onderscheid gemaakt tussen drie vormen van gedigitaliseerde criminaliteit (TCF): sociaaleconomisch gemotiveerd (financieel motief), psychosociaal (psychologisch motief) en geopolitiek (politiek motief). In Nigeria blijkt alle gedigitaliseerde criminaliteit economisch gemotiveerd te zijn. In Nigeria zijn de meeste jonge cybercriminelen actief op het gebied van online fraude. De slechte sociaaleconomische achtergrond van Nigeria verklaart het hoge cijfer van gedigitaliseerde criminaliteit. In hoofdstuk drie worden de motieven voor online fraude nog nader toegelicht. De motieven van een dader kunnen mogelijk ook een rol spelen bij de keuze voor een bepaalde interventie.

Modus operandi

De werkwijze van online oplichters wordt ook wel modus operandi genoemd (Maimon, e.a., 2019). Een belangrijk onderdeel hiervan is het aantonen van de urgentie om geld over te maken. Oplichters proberen via onlineverkoopsites geld te ontfutselen om de koop te versnellen. De eerste, initiële mails met verbale bewoordingen van urgentie, zoals ‘ASAP’ en ‘soon’, leiden niet vaak tot succes (slechts in 20 procent van de gevallen). In corresponderende mails werken verbale bewoordingen van urgentie beter. Bovendien worden er meer mails verstuurd wanneer gebruik wordt gemaakt van verbale aansporingen. Kortom, dergelijke verbale bewoordingen die urgentie aangeven zorgen ervoor dat slachtoffers wel of juist niet worden overgehaald om te betalen voor goederen die te koop worden aangeboden op het internet. Dit is een belangrijk aspect om slachtoffers te overtuigen van de echtheid van de e-mail.

Beleidsimplicaties

Een effectief beleid jegens online fraude bestaat uit de volgende vier vereisten (Levi, e.a., 2017b):

1. De staat moet een beleid maken waarin duidelijk wordt welke organisaties een rol spelen, verantwoordelijkheid hebben voor en middelen hebben om online fraude te bestrijden;
2. Nationale en internationale ketenpartners moeten zowel voor als na het plegen van het strafbare feit samenwerken;
3. Een nieuwe methodiek ontwikkelen door betrokken organisaties om daders en netwerken op te kunnen sporen, omdat er op dit moment nog geen opsporingsmethode is ontwikkeld die effectief is voor alle betrokken organisaties;
4. Er kan niet altijd reactief worden gehandeld door alle betrokken organisaties, dus de focus moet op preventie worden gelegd. Hier ligt ook een rol bij voorzorg door de politie.

Bij het opstellen van beleid moet rekening worden gehouden met de snelle technologische ontwikkelingen die onder meer phishing kunnen doen veranderen. Maar er zijn ook andere zaken die kunnen worden meegenomen, zoals het verhogen van de pakkans, het verhogen van de kosten van cybercrime en meer verantwoordelijkheid leggen bij internetproviders en andere ICT-organisaties.

Tabel 2: Analyse van de artikelen van de systematische review met daarin vermeld: de auteurs, de titel van het onderzoek, de betekenis van online fraude en belangrijke informatie voor het huidige onderzoek (N=19).

Auteur	**Titel (publicatiejaar)**	**Betekenis online fraude**	**Belangrijke conclusies voor het huidige onderzoek**
Shun Yung & Huang	The Evolutional View of the Types of Identity Thefts and Online Frauds in the Era of the Internet (2011)	Online fraude wordt gedefinieerd als het online stelen van iemands identiteit. Identiteitsfraude houdt het volgende in: het stelen van bepaalde persoonskenmerken van het slachtoffer, zoals creditcard gegevens, waarvoor het slachtoffer geen toestemming heeft gegeven. Voorbeelden van horizontale online fraude zijn phishing, spyware, transactiefraude en advance fee	Banken maken het voor criminelen gemakkelijk om geld te kunnen stelen van hun klanten, omdat er maar één verificatie stap nodig is om geld te kunnen overmaken. Terwijl het stelen van een bankpas twee verificatie stappen heeft: bezit van de pas en kennis van de pincode. NB: Dit artikel is ouder, want tegenwoordig heb je ook online extra verificatie nodig, zoals een toegangscode. Kortom, er ligt ook een rol bij banken bij de bescherming van hun klanten. Een mogelijk voorbeeld is een bepaalde identiteitscode voor gebruik van het internet in te voeren.

		fraude. Advance fee fraude is een vorm van fraude waarbij van tevoren een klein geldbedrag wordt overgemaakt aan een persoon die beweert dat ze een grote som geld kunnen ontvangen. Ook wel voorschotfraude genoemd.	
Leukfeldt	Cybercrime and social ties (2014)	-	Er worden verschillende interventies genoemd die zijn meegenomen in paragraaf 3.3. Banken moeten ook een belangrijke rol spelen bij de bestrijding van phishing.
Holt, Smirnova, Ting Chua & Copes	Examining the risk reduction strategies of actors in online criminal markets (2015)	-	Criminelen die actief zijn op online fora maken gebruik van beoordelingssystemen en tussenpersonen om minder risico op arrestatie te hebben dan criminelen in de offlinewereld.
Ibrahim	Social and contextual taxomony of cybercrime: socialeconomic theory of Nigerian cybercriminals (2016)	Cyberfraude wordt geschaard onder sociaaleconomische cyberdelicten.	In Nigeria zijn de meeste jonge cybercriminelen actief op het gebied van online fraude. De sociaaleconomische achtergrond van Nigeria verklaart het hoge cijfer van cybercrime
Kerstens & Janssen	The victim perpetrator overlap in financial cybercrime: evidence and reflection on the overlap of youths online victimization and perpetration (2016)	Online fraude wordt hier gezien als online veilingfraude, virtuele diefstal en identiteitsfraude.	Jongeren hebben enige overlap met slachtofferschap en daderschap van online fraude. Slachtoffers van financiële cybercrime zullen zelf vaker dader zijn met als motief wraak.

Rashkovski, Naumovski & Naumovski	Cybercrime Tendencies and Legislation in the Republic of Macedonia (2016)	Hier wordt cybercrime onderverdeeld in een tak van criminaliteit die wordt gepleegd met behulp van het internet, namelijk internetcriminaliteit.	Veel daders van gedigitaliseerde criminaliteit, zoals online fraude, komen uit Macedonië.
Cross & Richards	The ACA effect: examining how current affairs programs shape victim understandings and responses to online fraud (2017)	Online fraude is een incident waarbij slachtoffers worden bedrogen om er enig voordeel (financieel of anders) uit te halen.	Een mogelijke interventie zou kunnen zijn dat televisieprogramma's en documentaires worden gemaakt om burgers te informeren over online fraude en het voorkomen daarvan.
Leukfeldt, Kleemans & Stol	Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks (2017)	-	Kernleden zijn de leden in het netwerk die de phishing aanvallen opzetten, coördineren en andere leden leiden. De aanjagers zijn de mensen die vakspecialistische kennis hebben om de aanval te kunnen laten slagen. Zij kunnen in twee groepen worden onderverdeeld. De professionele aanjagers lenen hun diensten aan iedereen uit. De gerekruteerde aanjagers zijn specifiek door dit netwerk ingehuurd voor een specifieke taak. Opvallend is dat de netwerken hoofdzakelijk bestaan uit mensen zonder technische kennis. Er is slechts een ICT'er benodigd om mensen online op te lichten.
Leukfeldt, Kleemans & Stol	Origin, growth and criminal capabilities of cybercriminal	Phishing aanvallen kunnen worden onderverdeeld in	Fora zijn cruciaal voor de ontwikkeling van cybercrime netwerken, zoals

	networks. An international empirical analysis (2017)	twee vormen: low tech en high tech gedigitaliseerde criminaliteit. Dit hangt af van de mate van ICT gebruik en de contacten met slachtoffers.	ontmoetingsplek. Kopen van techniek en platform om gestolen spullen te verkopen. Voor hightech netwerken die via fora werken geldt dat het misschien handig is om de opsporing te richten op jongeren die ICT studeren waarbij grote fascinatie is voor programmeren en coderen. Zij zijn namelijk vaak betrokken in dit soort netwerken.
Leukfeldt, Kleemans & Stol	A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists (2017)	Phishing wordt gezien als aanvallen op het onlinebankleven van de slachtoffers. Daarbij worden de persoonlijke gegevens afhandig gemaakt van de slachtoffers middels het internet, zoals via een mail of sms waarbij ze zich voordoen als een autoriteit.	Het artikel geeft veel voorbeelden bij de rollen die in een phishingnetwerk worden vervuld en legt de taken van de criminelen uit.
Levi	Assessing the trends, scale and nature of economic cybercrimes: overview and issues (2017)	Phishing is de poging om persoonlijke informatie te verkrijgen om dit te kunnen gebruiken om mensen geld afhandig te maken via het internet.	Er bestaat een gat tussen de daadwerkelijke aantallen van financiële cyberfraude en de cijfers hiervan.
Levi, Doig, Gundur, Wall & Williams	Cyberfraud and the implications for effective risk-based responses: themes from UK-research (2017)	Cyberfraude is fraude waarbij bepaalde band met het internet is.	Bij het opstellen van beleid moet rekening worden gehouden met de snelle technologische ontwikkelingen die phishing snel kunnen doen veranderen.

			Maar er zijn ook andere zaken die kunnen worden meegenomen, zoals pakkans verhogen, kosten van cybercrime hoger maken, meer verantwoordelijkheid bij internetproviders en andere ICT-organisaties
Macdonald & Frank	Shuffle up and deal: use of a capture–recapture method to estimate the size of stolen data markets (2017)	-	Een van de verklaringen voor de slechte vastlegging van cijfers van online fraude is dat er geen eenduidige betekenis wordt gegeven aan online fraude. Bovendien wordt er geen onderscheid gemaakt tussen offline en online fraude. Tot slot worden weinig aangiftes gedaan van online fraude.
Drew & Farrell	Online victimization risk and self-protective strategies: developing policy-led cyber fraud prevention programs (2018)	Cyberfraude wordt onderverdeeld in twee categorieën. Als het onder cybercriminaliteit valt dan gaat het om illegale toegang, illegale onderschepping, data onderscheppen, systemen onderscheppen, misbruik van middelen of hacken. Bij gedigitaliseerde criminaliteit kan gedacht worden aan oplichting (romantische relaties, erfenissen, investeringsoplichting en financiële transacties) en identiteitsfraude	Onderscheid tussen harde en zachte maatregelen. Harde preventieve maatregelen zijn fysieke barrières, zoals antivirussoftware, firewalls en wachtwoordbescherming. Zachte maatregelen zijn minimale hoeveelheid informatie op sociale media, extra beveiliging op online fora en chatrooms, alleen bekende mensen op sociale media accepteren en negeren van mails van onbekenden. Het blijkt ook dat de politie mensen meer moet onderwijzen over preventie en dat dit werkt.

Hutchings	Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission (2019)	Computerfraude is het op oneerlijke wijze verkrijgen van enig voordeel door middel van het gebruik van computers, waardoor financieel verlies wordt geleden door het slachtoffer.	Op jonge leeftijd werken de jongeren niet per se op basis van een georganiseerd netwerk samen, maar wordt vaker gesproken van sociale contacten of online vrienden waar ze samen delicten mee plegen.
Kruisbergen, Leukfeldt, Kleemans & Roks	Money talks money laundering choices of organized crime offenders in a digital age (2019)	Onderscheid tussen witwassers van traditionele, gedigitaliseerde en cybercriminaliteit.	Geldezels zijn makkelijk te vervangen wanneer ze een lage positie innemen in het criminele netwerk. Cybercrime lijkt bovendien nog steeds sterk in het lokale netwerk af te spelen
Maimon, Santos & Park	Online deception and situations conducive to the progression of non-payment fraud (2019)	Online fraude wordt gedefinieerd als online dating scams, online bedreigingen, online verkoopoplichting, zoals het niet leveren van goederen of niet betalen van goederen.	Uit de modus operandi van online fraudeurs blijkt dat een oplichtingsbericht tenminste moet bestaan uit woorden waarin de urgentie van het overmaken van geld centraal staat.
Ghazi-Tehrani & Pontell	Phishing evolves: Analyzing the Enduring Cybercrime (2021)	Phishing is een frauduleuze poging om persoonlijke informatie van het slachtoffer te verkrijgen door zich voor te doen als een betrouwbare instantie middels een technologisch apparaat.	Er zijn verschillende vormen van phishing: Business E-Mail Compromise (BEC), Smishing, Vishing, Spear phishing en Whaling. BEC houdt in dat een mail wordt verzonden namens een werkgever aan een werknemer met een lagere functie met het verzoek om geld over te maken. Smishing is phishing via SMS. Vishing is de telefonische variant van phishing. Spear phishing is

			een gerichte phishing aanval waarbij persoonlijke informatie wordt gebruikt om het slachtoffer te overtuigen van de echtheid van het bericht. Whaling is een variant van spear phishing waarbij werkgevers worden opgelicht door zogenaamde werknemers.
Roks, Leukfeldt en Densley	The Hybridization of Street Offending in the Netherlands (2021)	-	Geldezels worden zowel via sociale media als offline gerekruteerd. De offline wereld blijft vooralsnog een belangrijke rol spelen in het vormen van een crimineel netwerk.

H3 Theoretisch kader

In dit hoofdstuk wordt eerst een indruk gegeven van de mogelijke motieven van jongeren om online fraude te plegen. Vervolgens wordt gekeken naar de samenstelling van een phishing netwerk. Daarna worden bestaande interventies om online fraude aan te pakken onder de loep genomen. Tot slot wordt gekeken naar de samenwerking tussen de politie en verschillende samenwerkingspartners, zoals de gemeente en jongerenwerkers.

3.1 Motieven online fraude

Om de juiste interventie te kiezen moet eerst worden gekeken naar motieven om een bepaald delict te plegen. Er zijn verschillende motieven om online fraude te plegen. Er zijn echter sommige mensen, geldezels, die soms niet weten dat zij illegaal bezig zijn. Het gaat dan om mensen die geloven dat ze een functie hebben bij een bepaald bedrijf waar zij geldbedragen voor moeten overmaken naar buitenlandse rekeningen. Dit soort geldezels is dus niet op de hoogte van de criminele activiteiten en kan soms zelf als slachtoffer worden gezien (Hulsse, 2017). Hieruit blijkt eigenlijk dat geen sprake is van een crimineel motief. De geldezel is dan erg naïef en onwetend over de gevolgen van zijn/haar handelingen, maar er is in dit geval ook geen sprake van een echt motief.

Een eerste motief is financieel van aard. Jongeren streven naar onafhankelijkheid van hun ouders en dat houdt ook financiële onafhankelijkheid in (Moffitt, 1993). Wanneer jongeren zelf voldoende geld verdienen om aan hun (materiële) behoeften te kunnen voldoen dan wordt gesproken van onafhankelijkheid van de ouders. Hierdoor wordt een levensstijl gecreëerd door de jongeren waarin zij met niemand rekening hoeven te houden (Leukfeldt & Kleemans, 2019). Met cyberdelicten, zoals internetoplichting en phishing, kan op gemakkelijke wijze veel geld worden verdiend. Daarbij kan gedacht worden aan de vriend-in-noodfraude die tegenwoordig erg populair is onder cybercriminelen. Hierdoor zullen deze jongeren ook meer status verkrijgen binnen hun vriendengroep (Moffitt, 1993; Dijkstra & Veenstra, 2019). De status van deze jeugdige cybercriminelen verbetert doordat zij meer statusgoederen, zoals dure kleding en technologie, kunnen kopen. Status en erbij horen zijn doelen van jeugdigen, waardoor antisociaal gedrag aantrekkelijk wordt en jongeren vaker zich in het (online) criminele circuit zullen begeven. Al met al kan worden gesteld dat gedigitaliseerde criminaliteit, zoals internetoplichting en phishing, bijdraagt aan het verkleinen van de *maturity gap*. Dat houdt in dat het gat tussen de adolescentie en volwassenheid kleiner wordt doordat jongeren eerder onafhankelijk en autonoom worden door middel van (cyber)criminaliteit dan jongeren die dat niet doen. Hierdoor zullen mogelijk steeds meer jongeren volgen die het (cyber)criminele circuit ingaan.

Een ander motief is dat sommige jongeren zien dat hun vrienden gedigitaliseerde criminaliteit plegen. Jongeren streven ernaar om erbij te horen en zullen daarom hun vrienden die online fraude plegen nadoen (Bowkers, 1999; Dijkstra & Veenstra, 2019). Zij zien namelijk dat hun vrienden meer geld hebben dan zij. Hierdoor willen zij ook meer geld te besteden hebben en zullen zij eerder geneigd zijn om ook mensen online op te lichten door middel van whatsapp-berichten, nepadvertenties op marktplaats of andere vormen van online fraude. Wederom komt het fenomeen erbij horen of geliefd zijn om de hoek kijken. Dit willen zij bereiken door mee te doen met het online oplichten van mensen. Daardoor zal het aantal jeugdige verdachten van online fraude kunnen toenemen.

Andere mogelijke motieven zijn het vervullen van behoeften van spanning, adrenalinekick, plezier of macht (Van der Wagen, e.a., 2020). Het gaat dan om het zoeken naar sensatie. Jongeren proberen de wereld nog te ontdekken en daarbij hoort ook het zoeken naar uitersten. In dit geval kan het resulteren in het maken van misbruik van anderen hun onoplettendheid bij bijvoorbeeld online aankopen of het stelen van iemands identiteit om een betaalverzoek te sturen waar slachtoffers gehoor aan geven. De sensatiebehoeften worden dus vervuld door mensen online op te lichten. Maar in veel gevallen zullen verscheidene motieven gelijktijdig optreden.

3.2 Crime script

Een crime script is een model waarin alle stappen, rollen en handelingen van een bepaalde criminaliteitsvorm worden weergegeven (Ekblom & Gill, 2016; Dehghanniri & Borrion, 2021). Hierbij ligt de nadruk op de benodigdheden en handelingen voor het voltooien van een bepaalde delictsvorm. Crime scripts zijn uitermate geschikt om de belangrijkste rollen binnen het criminele netwerk te achterhalen en op basis daarvan interventies uit te voeren om een crimineel netwerk te ontwrichten (Clarke & Tilley, 2010). Voor 24 soorten gedigitaliseerde criminaliteit zijn er al crime scripts gemaakt (Dehghanniri & Borrion, 2021). In dit onderzoek wordt de nadruk gelegd op online fraude en meer specifiek op phishing. Dit is een vorm van internetfraude waarbij persoonlijke informatie wordt ingewonnen door criminelen door middel van bijvoorbeeld e-mails, WhatsAppberichten of sms-berichten (Lastdrager, 2014). De persoonsgegevens worden dan onderschept doordat criminelen een link sturen waarin de persoonlijke (betaal)gegevens moeten worden ingevuld, waardoor pincodes en andere wachtwoorden gemakkelijk afhandig kunnen worden gemaakt. Er is gekozen voor phishing aangezien één op de drie Nederlanders in 2018 te maken heeft gehad met een phishing bericht (CBS, 2019). Hieruit blijkt de grootschaligheid van deze vorm van online fraude.

Een crime script voor online fraude/phishing kan in drie fases worden verdeeld: voorbereiding, uitvoering en nazorg (Clarke & Cornish, 1985). In *figuur 2* is dit schematisch weergegeven. Tijdens de eerste fase (voorbereiding) wordt een crimineel netwerk gevormd. Dit kan op verschillende manieren gebeuren, zowel via online als offline benaderingen. Er kunnen grofweg vier verschillende rollen worden onderscheiden die in een cybercrimineel netwerk zitten. De leden van de kerngroep nemen de leiding over alle personen in het netwerk (Loggen & Leukfeldt, 2022). Zij hebben het initiatief genomen om phishing aanvallen te plegen. Soms zijn dit ook mensen die de vereiste technologische kennis hebben om zelfstandig de phishing aanval uit te voeren, maar in veel gevallen zijn daar facilitators voor nodig. Er kunnen twee soorten facilitators worden onderscheiden: professionele en gerekruteerde facilitators. Professionele facilitators worden door verschillende cybercriminele netwerken ingeschakeld voor uiteenlopende zaken, waaronder het maken van malware, opzetten van een phishing website, verstrekken van identiteitsgegevens en het rekruteren van geldezels (Leukfeldt, e.a., 2017d). Daarnaast kan het ook gaan om mensen die de mails vertalen naar de juiste spreektaal van het land waarin de slachtoffers woonachtig zijn. De gerekruteerde facilitators zijn in vaste dienst van het criminele netwerk. Het kan dan bijvoorbeeld gaan om bankmedewerkers die gegevens delen over hun klanten, recruiters van geldezels, *cashers* van het witgewassen geld of telefonistes om bankgegevens te verkrijgen (Leukfeldt, e.a., 2017d). De laatste groep zijn geldezels. Zij zijn cruciale schakels binnen het proces van phishing: zonder deze mensen kunnen de criminelen het verworven geld niet zonder sporen in eigen handen krijgen. Het benaderen van deze drie soorten leden kan via

virtuele (Soudijn & Zegers, 2012) of fysieke wegen (Leukfeldt, 2014) plaatsvinden, zoals via online fora, sociale media, op straat of via-via.

De tweede fase kan beginnen wanneer het 'team' is samengesteld. Tijdens deze fase worden de gegevens van de slachtoffers afhandig gemaakt door middel van bijvoorbeeld e-mails, WhatsAppberichten of sms-berichten. Er wordt ook wel gesproken van de uitvoering van de online fraude/phishing. In deze fase wordt contact opgenomen met de potentiële slachtoffers door middel van e-mails, WhatsAppberichten of sms-berichten. Er zijn twee opties voor het verkrijgen van de persoonlijke informatie (Loggen & Leukfeldt, 2022; Leukfeldt, 2014; Soudijn & Zegers, 2012). De eerste optie is door een link te versturen waardoor mensen naar een phishing website worden gestuurd waarbij de slachtoffers zelf de persoonlijke gegevens invoeren en deze daardoor kenbaar worden bij de criminelen. De andere optie is het gebruikmaken van een link waardoor bepaalde malware wordt geïnstalleerd op de computer waardoor alle handelingen die op die computer worden verricht worden geregistreerd. Hierdoor worden persoonlijke gegevens kenbaar wanneer deze worden gemonitord door de malware. Wanneer de potentiële slachtoffers op één van deze twee weblinks klikt en hun gegevens invullen, zullen de betaalgegevens (spoedig) kenbaar zijn voor de criminelen. De volgende stap in het proces bestaat uit het in handen krijgen van de betaalpas van het slachtoffer. Dit kan door middel van het opsturen van de pas of door de betaalpas aan de deur op te halen waarbij de criminelen zich voordoen als werknemer van een bank. Als deze stappen zijn verricht dan is de uitvoerende fase voltooid.

De laatste fase bestaat uit het opnemen van het geld. In deze laatste fase is de rol van de geldezel een belangrijke spil. Zonder de geldezel zullen de criminelen namelijk niet hun delict kunnen voltooien. Geldezels zorgen ervoor dat de criminelen niet in verband kunnen worden gebracht met het betreffende delict, doordat geldezels als tussenpersoon functioneren tussen het slachtoffer en de dader. Het opnemen van het geld kan op verschillende manieren gebeuren: het kopen van (luxe)goederen met de betaalpas van het slachtoffer, online aankopen doen met de betaalpas, het aanschaffen van bitcoins of het opnemen van contant geld (Peretti, 2008; Custers, e.a., 2019). Tegenwoordig wordt overigens steeds vaker in crypto valuta witgewassen. Uiteindelijk worden de geldezels betaald voor hun diensten en kunnen de criminelen de aangeschafte goederen en/of cadeaukaarten verkopen.

Jongeren zullen hoofdzakelijk functioneren als geldezel binnen een cybercrime netwerk. De laatste jaren heeft er namelijk een stijging plaatsgevonden in het aantal geldezels tussen de twaalf en eenentwintig jaar (Bekkers, e.a., 2020). Dit heeft veel te maken met het motief van een geldezel: gemakkelijk geld verdienen. Verder blijkt dat mensen met een ICT-studie vaker actief zijn op het gebied van cybercrime, waardoor sommige jongeren ook actief kunnen zijn op basis van hun specialistische kennis (Weulen Kranenbarg, e.a., 2022). Er moet dus rekening worden gehouden met de posities van jongeren binnen het criminele netwerk om op basis daarvan een werkende interventie te kunnen opstellen.

Figuur 2: Crime script van een phishing netwerk.

3.3 Interventies

Crime scripts worden gebruikt om te bepalen of en voor wie een interventie moet worden ingezet. Wanneer een bepaalde schakelrol wordt uitgeschakeld dan kan het hele criminele proces mogelijk worden ontwricht. In de voorbereidende fase van phishing wordt het bestaande netwerk uitgebreid met specialistische kennis en geldezels. Deze worden op verschillende manieren benaderd. De benaderingswijzen kunnen mogelijk worden beïnvloed door opsporingsdiensten door middel van een interventie.

Een eerste mogelijke interventie is gericht op de voorbereidende fase, dus tijdens de vorming van een cybercrimineel netwerk. De online fora waar cybercriminelen elkaar ontmoeten moeten worden ontwricht (Soudijn & Zegers, 2012). Het uit de lucht halen van een forum gericht op het faciliteren van cyber- of gedigitaliseerde criminaliteit kan voor ontwrichting zorgen binnen een crimineel netwerk, want de benodigde vaardigheden en/of contacten voor het opzetten van een (nieuwe) phishing aanval worden hierdoor (tijdelijk) lastiger gemaakt. Er moet echter wel rekening mee worden gehouden dat er al snel een nieuw forum kan worden opgezet aangezien tegenwoordig erg gemakkelijk en snel websites kunnen worden gemaakt. Een andere interventie die ook gericht is op de online ontmoetingsplaats voor cybercriminelen is gericht op het ontwrichten van onderling vertrouwen (Akerhof, 1970; Soudijn & Zegers, 2012). Wanneer criminelen elkaar onderling niet goed kunnen vertrouwen dan zullen zij niet met elkaar willen samenwerken. Er moet dus voor worden gezorgd dat de

fora meer informatie hebben over hun leden dan de leden zelf. Er moet dus informatie asymmetrie ontstaan om het vertrouwen met betrekking tot de mogelijke samenwerkingspartners van het forum te schaden. Dat vertrouwen kan worden geschaad door mensen in te huren die onrust zaaien over de gang van zaken op het forum. Hierdoor zullen steeds minder mensen gebruik maken van het forum en zal er minder sprake zijn van online fraude. Een laatste interventie is gericht op de fysieke benaderingswijze van hulppersonen voor het cybercrimenetwerk. Jongeren zullen op ontmoetingsplaatsen voor jongeren worden benaderd, denk daarbij aan scholen of sportplaatsen, waardoor het van belang is om toezichthouders te laten ingrijpen. Toezichthouders, zoals leerkrachten en trainers, kunnen contact opnemen met de politie om de verdachte personen te laten arresteren zodat er minder jonge geldezels/IT-specialisten worden geronseld om online fraude te plegen.

Andere interventies zijn gericht op de slachtoffers van phishing, of eerder het voorkomen van slachtoffers. Deze interventies zien dus op de uitvoerende fase binnen het crime script. De digitale geletterdheid van burgers moet omhoog om zo te voorkomen dat ze slachtoffer worden van online fraude. Mensen die meer digitaal geletterd zijn ontvangen vaker phishing-e-mails, maar reageren hier minder vaak op (Graham & Triplett, 2017). Een interventie gericht op het herkennen van phishing-e-mails zal dus de kans op slachtofferschap van phishing verkleinen. Een mogelijke preventieve maatregel voor jonge daders is het informeren van leerkrachten in het basis- en op het middelbare onderwijs over de gevolgen van gedigitaliseerde criminaliteit en hierbij dit te onderwijzen aan jongeren, daarbij moet gedacht worden aan het lesgeven over gedragscodes omtrent online respect betreffende eigendom van computers (tegengaan van hacken) en respect voor de wet om bijvoorbeeld online fraude tegen te gaan (Bowkers, 1999). Aangezien gedigitaliseerde criminaliteit sinds 2020 meer in het nieuws is gekomen wordt het hoog tijd dat scholen hun leerlingen gaan informeren over ethische principes met betrekking tot het internet. Hierdoor krijgen leerlingen niet louter les over de werking van computers, maar voortaan ook over het correct gebruik maken van computers. Een actueel voorbeeld van een dergelijke preventieve interventie is *Framed*, waarin jongeren op school een game spelen die bewustwording over de gevolgen cyber- en gedigitaliseerde criminaliteit moet vergroten (ccv, z.d. a). Jongeren die sowieso al traditionele criminaliteit plegen zullen echter waarschijnlijk niet vatbaar zijn voor dergelijke trainingen. Deze interventievorm zal niet voor iedere leerling even succesvol zijn. Aangezien sommige leerlingen al een levensstijl hebben waarin makkelijk geld kan worden verdiend door middel van traditionele criminaliteit en cyber- en gedigitaliseerde criminaliteit slechts een kleine stap in een andere richting is voor hen. Daarom moeten verschillende interventies gelijktijdig worden gebruikt om online fraude door jongeren te voorkomen.

De politie kan ook nog anders te werk gaan wanneer zij bezig zijn met het opsporen van cybercriminelen. Uit een onderzoek blijkt dat de verdachten van phishing ook actief zijn in de offlinewereld als crimineel (Leukfeldt, 2014). Het onderzochte phishing netwerk uit Amsterdam is tot stand gekomen door sociale contacten in de fysieke wereld. De kernleden kenden elkaar van andere misdaden die zij eerder hadden gepleegd. Dat maakt het interessant voor onderzoek naar online fraude. Wanneer de politieonderzoek doet naar andere vormen van (financiële) criminaliteit moeten zij ook letten op signalen van betrokkenheid bij online fraude door deze criminelen. Dat kan bijvoorbeeld naar voren komen uit getapte telefoongesprekken over geldezels of gestolen bankgegevens, maar kan ook blijken door de vondst van vele bankpassen tijdens een huiszoeking. Een andere organisatie die mogelijk

maatregelen kan nemen zijn banken. Sommige facilitators zijn namelijk bankpersoneel. Zij verstrekken persoonlijke gegevens van klanten of passen gegevens aan. Wanneer banken het beleid aanpassen voor het opzoeken en wijzigen van gegevens kan dat mogelijk ertoe leiden dat minder bankpersoneel de mogelijkheid heeft om gerekruteerd te kunnen worden in een phishingnetwerk. Een mogelijke interventie kan bestaan uit een strengere autorisatie voordat dergelijke persoonsgegevens kunnen worden opgezocht en/of gewijzigd (Leukfeldt, 2014).

Interventies kunnen zowel repressief als preventief zijn. Tegenwoordig wordt voornamelijk gewaarschuwd voor online fraude, zoals de vriend-in-noodfraude, via sociale media, reclames en reclameborden op straat. De focus ligt vooralsnog op preventie en minder bij opsporing. Gedigitaliseerde criminaliteit blijft zich echter telkens maar ontwikkelen en hierdoor ontstaan veel nieuwe vormen van online fraude (Rooyakkers & Weulen Kranenbarg, 2020). Het is daarom niet altijd mogelijk om tijdig preventieve maatregelen te nemen om (potentiële) slachtoffers te beschermen. Er zal vanuit verscheidene perspectieven moeten worden gekeken om gedigitaliseerde criminaliteit aan te pakken. Er wordt nog weinig aandacht besteed aan de samenwerking tussen politie en gemeente op het gebied van openbare orde en veiligheid. Terwijl deze twee organisaties wel degelijk op elkaar aangewezen zijn om samen te werken tegen (cyber)criminaliteit, waaronder dus ook online fraude valt. De gemeente moet namelijk een rol vervullen op het gebied van openbare orde en veiligheid, waarbij de politie ondergeschikt is aan de burgemeester. De partijen kunnen elkaars kennis en mogelijkheden aanvullen middels een integrale aanpak. Er zijn dus verschillende soorten interventies mogelijk om jeugdige fraudeurs aan te pakken, maar een integrale aanpak lijkt ook interessant te zijn om online fraude door jongeren aan te pakken.

3.4 Samenwerkingspartners

Sinds de overheveling van de jeugdhulp naar de gemeente moeten gemeenten, jongerenwerkers en politie nauw samenwerken. Bij deze samenwerking ligt de regierol bij de gemeente. Er wordt wel gesproken van een integrale samenwerking. Daar tegenover staat de traditionele aanpak waarin politie en justitie zich hoofdzakelijk bezighouden met criminaliteitsbestrijding (Buirma, 2021). De samenwerkingspartners dragen namelijk gezamenlijk bij aan een effectieve aanpak op basis van goede uitwisseling van informatie tussen de partijen en een adequate inzet van bevoegdheden voor elk van de partners (Hirsch Ballin, 2019). Alle partners van het samenwerkingsverband hebben verschillende expertises en bevoegdheden, waardoor het van groot belang is dat de onderlinge doelen van de organisaties op elkaar worden afgestemd en dat er op deze manier een gezamenlijk doel voor de samenwerkingspartners wordt geformuleerd. Daarom moeten er afspraken worden gemaakt welke organisatie ingrijpt voor bepaalde activiteiten die jongeren plegen en welke bevoegdheden in die specifieke gevallen op dat moment kunnen worden gebruikt. Het is daarom belangrijk om de bevoegdheden van de drie samenwerkingspartners kort door te nemen.

De gemeente heeft sinds de invoering van de Jeugdwet de regierol over jeugd. Met regierol wordt het sturen van het samenwerkingsverband bedoeld (Pröpper e.a., 2004). Met de invoering van deze wet wilde de (centrale) overheid ervoor zorgen dat er meer persoonsgerichte hulp kan worden geboden aan jongeren. Dit komt doordat de centrale overheid verwacht dat een lokale overheid meer contacten heeft in de regio om jongeren met problemen te helpen. Daar vallen bijvoorbeeld contacten met agenten en jongerenwerkers onder. Er wordt dus van gemeenten verwacht dat zij de verbindende schakel zijn tussen de

jongeren en hun samenwerkingspartners. Hieruit blijkt dat de overheid een grotere rol krijgt in veiligheidsvraagstukken. Er wordt echter nog steeds een actieve houding van de politie verwacht op lokaal niveau, zoals in woonwijken, rond scholen en het uitgaansgebied (Terpstra & Kouwenhoven, 2004). Over het algemeen treedt de politie steeds meer op de achtergrond terug en zal zich daarbij meer gaan richten op zijn eigen hoofdtaken, zoals het opsporen van strafbare feiten en het geven van hulpverlening. De politie heeft daarmee dus een ondersteunende rol binnen de jeugdproblematiek. Jongerenwerkers zijn daarentegen mensen met een zorgachtergrond die zich bezighouden met problematiek in hun regio omtrent jongeren, zoals bijvoorbeeld psychische problemen, maar ook jongeren die actief zijn in het criminele circuit.

3.4.1 Samenwerkingsmodellen

Er zijn verschillende modellen ontwikkeld die de samenwerking tussen ketenpartners kunnen weergeven. Ketenpartners zijn organisaties van buitenaf die betrokken zijn bij de totstandkoming van een dienst of product. In dit geval zijn de gemeente en jongerenwerkers de ketenpartners van de politie. Er kunnen vijf samenwerkingsmodellen worden onderscheiden: het communicatiemodel, het coöperatiemodel, het coördinatiemodel, het federatiemodel en het fusiemodel (Johnston & Shearing, 2003). In het communicatiemodel is eigenlijk alleen sprake van onderlinge communicatie en uitwisseling van informatie tussen de ketenpartners. Wanneer organisaties elk hun eigen grenzen en identiteit behouden, maar wel gezamenlijk werken dan wordt wel gesproken van een coöperatiemodel. Binnen het coördinerende model werken de organisaties op systematische wijze samen aan een bepaald probleem waarbij ze gezamenlijk middelen gebruiken, maar ook de nodige grenzen hanteren. Wanneer organisaties hun eigen verantwoordelijkheden behouden, maar wel een gezamenlijke focus hanteren wordt het federatiemodel gehanteerd. Als de organisaties nauwelijks meer van elkaar te onderscheiden zijn en intensief samenwerken is sprake van het fusiemodel. Binnen de samenwerking tussen politie, beleidsmedewerkers van de gemeente, buitensporig opsporingsambtenaren (voortaan: Boa’s) en jongerenwerkers kan op basis van een van deze modellen worden samengewerkt om gedigitaliseerde criminaliteit door jongeren tegen te gaan. Een van deze vijf verschillende samenwerkingsmodellen zal als leidraad dienen voor de formulering van de integrale aanpak.

3.4.2 Vereisten voor een goede samenwerking

Een goede samenwerking tussen de gemeente en politie berust op verschillende aspecten: afhankelijkheid, voldoende middelen en capaciteit, gezamenlijke percepties, onderling vertrouwen en leiderschap (Buirma, 2021). Het aspect van afhankelijkheid moet worden bewerkstelligd om een goede informatie-uitwisseling op gang te brengen en zorgt er daarnaast voor dat de samenwerkingspartners eerder geneigd zijn om iets voor elkaar te doen. De politie zal bijvoorbeeld informatie moeten delen over problematiek, voordat de gemeente hierop kan acteren. De gemeente zal namelijk pas handelen als een probleem groot wordt, dus als er sprake is van prioriteit. Het tweede aspect gaat over de beschikbaarheid van voldoende middelen en capaciteit: om een goede samenwerking tot stand te brengen moeten alle samenwerkingspartners evenveel bijdragen aan het project. De partners moeten allemaal een gelijkwaardig onderdeel zijn van het samenwerkingsverband. Daarom moet er voldoende personeel, tijd en middelen beschikbaar zijn om het doel van het samenwerkingsverband te behalen. Het derde aspect gaat over gezamenlijke percepties. Hiermee wordt bedoeld dat alle partners vergelijkbare ideeën hebben over de oorzaak van het probleem, de doelstelling van

de samenwerking en de mogelijke oplossing voor het probleem. Consensus is dus van groot belang binnen een samenwerkingsverband. Daarnaast is onderling vertrouwen tussen de partners van groot belang. Wanneer het vertrouwen ontbreekt zullen de partners minder informatie uitwisselen en zal wantrouwen ontstaan over de mate van zorgvuldigheid waarmee met deze informatie wordt omgegaan. Onderling vertrouwen bestaat onder andere uit het vertrouwen op elkaars krachten, deskundigheid, bedoelingen, inzet, betrokkenheid en motivatie van de deelnemers (Terpstra & Kouwenhoven, 2004). Het laatste aspect betreft leiderschap: er moet enige mate van coördinatie teweeg worden gebracht, zodat alle partners de regels kennen omtrent de samenwerking, de onderlinge rolverdelingen moeten helder zijn en iemand moet verantwoordelijkheid nemen voor de handelingen van het samenwerkingsverband. Als deze vijf aspecten goed worden ingevuld dan kan een goede samenwerking ontstaan tussen de ketenpartners.

3.4.3 Mogelijke knelpunten

Het functioneren van een samenwerkingsverband berust op het conformeren aan de gemaakte afspraken binnen het verband, maar berust ook op de overige vereisten voor een samenwerkingsverband die al eerder zijn besproken. Niet ieder samenwerkingsverband werkt naar behoren. Er zijn daarom ook veelvoorkomende knelpunten in de samenwerking tussen verschillende partners.

Een eerste knelpunt is de beschikbaarheid van voldoende middelen en capaciteit. Binnen de Nederlandse politiekorpsen heerst al jaren een tekort aan personeel (politie.nl, 2022; Terpstra, e.a., 2016). Er wordt echter verwacht dat dit tekort aan personeel rond 2025 is opgelost, maar dit heeft geen invloed op de huidige samenwerkingsverbanden. Doordat de politie te weinig personeel beschikbaar heeft kan het voorkomen dat de samenwerkingsverbanden voor de politie minder prioriteit hebben gekregen. De politie moet in eerste instantie de dagelijkse taken uitvoeren, zoals noodhulpdiensten. Hierdoor zal minder tijd beschikbaar zijn voor de samenwerkingspartners en wordt onvoldoende tijd vrijgemaakt voor het bestrijden van online fraude door middel van een integrale aanpak. Bovendien zijn de beschikbare middelen voor de bestrijding van online fraude gering. Tot nu toe richt de overheid zich voornamelijk op preventieve maatregelen om online fraude tegen te gaan door middel van waarschuwingen over online fraude of het herkennen van online fraude berichten. Aangezien het een criminaliteitsvorm is die veel onderhevig is aan vernieuwing moeten er nieuwe (repressieve) interventies worden ontwikkeld om het tegen te gaan. Daarvoor zijn echter wel veel (financiële) middelen nodig bij de verschillende partners om dit te realiseren. Daarnaast is er meer tijd nodig om te kunnen werken aan het gezamenlijke doel: bestrijding van online fraude door jongeren. Het ontbreekt echter vaak aan voldoende financiële middelen en tijd om gedigitaliseerde criminaliteit, zoals online fraude, aan te pakken. Er bestaan echter meer taken van de politie, gemeentemedewerkers en jongerenwerkers die ook aandacht vereisen, waardoor geen prioriteit wordt gesteld voor de bestrijding van online fraude.

Een ander knelpunt betreft de informatie-uitwisseling tussen de partners (Terpstra & Kouwenhoven, 2004). Alle partners hebben belangrijke informatie over de jongeren die online fraude plegen. Het is van belang om alle beschikbare informatie met elkaar te delen zodat er een compleet beeld ontstaat over de verdachte jongeren. De politie heeft strafrechtelijke informatie, jongerenwerkers hebben sociale informatie over bijvoorbeeld familie en vrienden van de verdachte en gemeenten hebben persoonlijke informatie, zoals

adresgegevens. Wanneer de politie geen informatie heeft vastgelegd over de jeugdige verdachte zal er überhaupt geen mogelijkheid zijn om de verdachte jongeren aan te pakken. Daarom is het van belang dat de politie haar gegevens deelt met de andere partners. Bovendien moet de verschafte informatie zo volledig mogelijk zijn om online fraude aan te kunnen pakken. Tot dusver is de informatie niet volledig vastgesteld: 10 procent van de slachtoffers van cybercriminaliteit in 2021 is slachtoffer van online fraude. Ongeveer 25 procent van de slachtoffers van phishing staan geregistreerd onder de noemer 'overig' (Akkermans, e.a., 2022). Hieruit blijkt dat de registratie niet volledig is waardoor het aanpakken van deze groep verdachten van overige vormen van phishing erg lastig zal verlopen. De politie geeft echter aan dat de andere samenwerkingspartners onvoldoende informatie delen, waardoor zij niet altijd alle beschikbare informatie kunnen gebruiken bij de opsporing van verdachten.

Een laatste knelpunt gaat over de afspraken tussen partners. In veel gevallen worden afspraken binnen een samenwerkingsverband vastgelegd door middel van een contract of convenant. Hierin worden onder andere de doelstelling van de samenwerking en de bevoegdheden, de verantwoordelijkheden en plichten van de samenwerkingspartners vastgelegd (Terpstra & Kouwenhoven, 2004). Na verloop van tijd zal het convenant op de achtergrond geraken en wordt meer teruggegrepen op informele afspraken tussen de partners. Informele afspraken berusten op onderling vertrouwen. Dit heeft enerzijds positieve effecten, zoals een betere onderlinge afstemming van taken en het delen van informatie tussen partijen. Anderzijds leidt dit echter ook tot onduidelijkheden over de taken, bevoegdheden en verantwoordelijkheden van de partners waardoor de samenwerking niet goed meer verloopt. Een ander mogelijk probleem ontstaat wanneer werknemers die actief waren in het samenwerkingsverband vertrekken bij de instantie, waardoor het onderlinge vertrouwen met een nieuwe werknemer moet worden opgebouwd. Informele afspraken zorgen er dan voor dat onduidelijkheid zal ontstaan. Daarom kan beter worden vastgehouden aan formele afspraken.

3.5 Samenvatting

Al met al kan worden gesteld dat jongeren verschillende motieven hebben om te beginnen als online fraudeur. Vaak zullen verschillende motieven gelijktijdig een rol spelen bij de keuze om al dan niet te frauderen. De meeste jongeren die actief zijn in de online fraude zullen actief zijn als geldezel of IT-specialist binnen een phishing-netwerk. Dit valt te verklaren door de financiële motieven van geldezels en de vakkennis van IT-specialisten omtrent het internet en computers om mensen op te kunnen lichten. De rol die jongeren binnen het criminele netwerk vervullen speelt vervolgens een rol bij de keuze voor het inzetten van bepaalde interventies. Interventies kunnen preventief of repressief van aard zijn. Enkele voorbeelden van interventies zijn gericht op het verhogen van de digitale geletterdheid, online ontmoetingsplaatsen van de criminelen uit de lucht halen en lespakketten, zoals het spel *Framed*. Daarnaast is het mogelijk om op een meer integrale wijze het probleem aan te pakken. Er zijn vijf verschillende samenwerkingsmodellen die kunnen fungeren als basis voor de samenwerking in Zuidoost Drenthe. Een goede samenwerking tussen de gemeente en politie berust op verschillende aspecten: afhankelijkheid, voldoende middelen en capaciteit, gezamenlijke percepties, onderling vertrouwen en leiderschap. Er zijn echter ook knelpunten in de samenwerking waar eventueel rekening mee moet worden gehouden. Daarbij kan gedacht worden aan personeelstekorten, financiële obstakels, gebrekkige informatie-uitwisseling en slechte afspraken. De huidige samenwerkingsverbanden van de gemeenten en

politie worden als basis gebruikt voor de nieuwe integrale aanpak van online fraude door jongeren. Hier zal ook rekening worden gehouden met de algemene vereisten voor een goede samenwerking en de mogelijke knelpunten hiervan.

H4 Methodologie

In dit hoofdstuk wordt de methode van het onderzoek beschreven. In de eerste paragraaf zal worden beschreven waarom gekozen is voor kwalitatief onderzoek. De beschrijving van de participanten en de wijze van dataverzameling worden omschreven in paragraaf 4.2. Vervolgens wordt het interviewschema nader toegelicht in paragraaf 4.3. In de vierde paragraaf wordt de analysemethode beschreven. In paragraaf 4.5 worden de concepten van *trustworthiness* beschreven. Als laatst wordt ingegaan op ethische kwesties binnen dit onderzoek.

4.1 Onderzoeksmethode

Dit onderzoek naar een integrale aanpak voor online fraude in Zuidoost Drenthe was kwalitatief van aard. Er was gekozen om gebruik te maken van een kwalitatief onderzoek, omdat de ervaringen van de samenwerkingspartners kenbaar moesten worden gemaakt. Er lag de nadruk op het begrijpen en interpreteren van bepaalde handelwijzen van de betrokken organisaties en redeneringen voor deze handelwijzen (Roose & Meuleman, 2017). Deze ervaringen konden vervolgens leiden tot enkele verbeterpunten in de huidige samenwerking tussen de politie en gemeenten. De huidige stand van zaken gaat echter meer in het algemeen over jeugdcriminaliteit en niet zozeer over online fraude. In dat opzicht zouden huidige samenwerkingen over jeugdproblematiek als voorbeeld kunnen dienen om een integrale aanpak voor online fraude door jongeren te kunnen realiseren. De ketenpartners konden hierbij ook hun wensen laten weten met betrekking tot de inhoud van de aanpak. Dit was gedaan door middel van het afnemen van verscheidene interviews met personen die betrokken zijn bij het opstellen en uitvoeren van beleid. Daarbij waren de volgende personen betrokken: beleidsmedewerkers bij de afdeling van openbare orde en veiligheid van de gemeente, jongerenwerkers en politieagenten. Daarna werden de verschillende handelwijzen van de politie, gemeenten en jongerenwerkers met elkaar vergeleken door middel van inductieve codes. Op basis van specifieke waarnemingen was een algemene regel geformuleerd (Hennink, e.a., 2010). Dit werd gedaan door codes te formuleren van de afgenomen interviews met behulp van het programma atlas.ti.

Het onderzoek was gedaan door middel van het afnemen van interviews. Daarvoor was gekozen zodat er zo min mogelijk beïnvloeding was van andere personen op de wensen met betrekking tot de samenwerking van bijvoorbeeld andere agenten, jongerenwerkers of beleidsambtenaren van de gemeente. Daardoor kreeg je de meest waarheidsgetrouwe weergave van de ervaringen van de betrokken personen binnen het samenwerkingsverband. Bij een van de interviews waren twee beleidsmedewerkers aanwezig, waardoor eerder gesproken kan worden van een focusgroep. In dit geval was er wel voor gekozen om gezamenlijk een interview af te nemen, omdat een van de medewerkers slechts één week in dienst was op het moment van de afname van het interview. Hierdoor kon deze medewerker niet zelfstandig antwoord geven op alle vragen. Om toch de beleidsmedewerkers in de regio te hebben gesproken was daarom gekozen voor een interview met twee personen. De interviews waren opgenomen en daarnaast werd voorafgaand aan het interview aan alle deelnemers gevraagd of zij het toestemmingsformulier voor de deelname wilden ondertekenen. Alle interviews werden woordelijk getranscribeerd. Bovendien waren de interviews geanonimiseerd. De opnames waren opgeslagen op een veilige y-schijf van de universiteit. Nadat het onderzoek was afgerond werden alle opnames verwijderd.

4.2 Participanten en dataverzameling

De te onderzoeken populatie in dit onderzoek bestond uit beleidsmedewerkers bij de gemeente, politieagenten op het gebied van jeugdcriminaliteit en jongerenwerkers in Zuidoost Drenthe. De data waren verzameld middels verscheidene interviews. In *tabel 3* zijn alle relevante gegevens over de participanten weergegeven. Alle wijkagenten jeugd uit de regio Zuidoost Drenthe waren geïnterviewd. Daarnaast was de operationeel expert Jeugd ook geïnterviewd. Alle agenten die konden worden geïnterviewd waren dus geïnterviewd. Hierdoor was deze groep volledig gedekt. Bij de politiebureaus in Exloo en Klazienaveen zijn echter geen wijkagenten jeugd in dienst, waardoor hier minder goede uitspraken over konden worden gedaan. Via de operationeel expert werden de contactgegevens van de beleidsmedewerkers van de afdeling openbare orde en veiligheid van alle gemeenten uitgewisseld. In de regio Zuidoost Drenthe zijn in totaal drie gemeenten: Borger-Odoorn, Emmen en Coevorden. Emmen heeft een grote afdeling openbare orde en veiligheid, waarbij één beleidsmedewerker specifiek zich inzet voor jeugdcriminaliteit. Daarom was zij geïnterviewd. In Coevorden was naast de beleidsmedewerker openbare orde en veiligheid ook een beleidsmedewerker met het thema jeugd geïnterviewd. In Borger-Odoorn waren twee beleidsmedewerkers gelijktijdig geïnterviewd. Via de beleidsmedewerkers waren vervolgens gegevens van jeugdinstellingen ingewonnen. Er kan wel worden gesproken van de sneeuwbalmethode. Voor de jongerenwerkers geldt dat een keuze was gemaakt om vanuit elke gemeente één instelling te interviewen met jongerenwerkers. Het gaat om de volgende drie instellingen: Sedna (Emmen), Andes (Borger-Odoorn) en Maatschappelijk Welzijn (Coevorden). Het eerste interview was met een medewerker van Maatschappelijk Welzijn. Deze medewerker is coördinator, waardoor hij ook betrokken is bij de overleggen met de andere ketenpartners. Bij Sedna in Emmen waren twee medewerkers vanuit de praktijk geïnterviewd, een van Klazienaveen en een van Emmen. De laatste jongerenwerker is werkzaam in de praktijk in de gemeente Borger-Odoorn.

Tabel 3: Participanten van de interviews.

Participant	**Partner**	**Functie**	**Werkplek**
Participant 1	Politie	Operationeel expert Jeugd	Coevorden
Participant 2	Politie	Wijkagent- jeugd	Coevorden
Participant 3	Gemeente	Beleidsmedewerker Openbare Orde en Veiligheid – jeugd	Emmen
Participant 4	Politie	Wijkagent – jeugd	Emmen
Participant 5	Politie	Wijkagent – jeugd	Emmen
Participanten 6 en 7	Gemeente	Beleidsmedewerkers Openbare Orde en Veiligheid	Borger-Odoorn
Participant 8	Gemeente	Beleidsmedewerker Jeugd	Coevorden
Participant 9	Gemeente	Beleidsmedewerker Openbare Orde en Veiligheid	Coevorden
Participant 10	Maatschappelijk welzijn	Jongerenwerker	Coevorden
Participant 11	Sedna	Jongerenwerker	Klazienaveen
Participant 12	Sedna	Jongerenwerker	Emmen
Participant 13	Andes	Jongerenwerker	Borger-Odoorn

4.3 Operationalisatie interviewschema

In dit onderzoek werd gebruik gemaakt van een semigestructureerd interviewschema (zie: *bijlage I*). Daarin werden verschillende onderwerpen centraal gesteld, waarna vervolgens kon worden doorgevraagd op bepaalde onderwerpen die ter sprake kwamen. Hierdoor had het interview eerder de vorm van een gesprek. Het interview begon met een korte introductie waarin ik mijzelf voorstelde en kort het doel van het onderzoek besprak. Daarna werden enkele ethische principes doorgenomen, zoals goedkeuring van de opname en anonimiteit. Op het interviewschema stond ook een kopje met achtergrondinformatie, maar daar was bij geen van de twaalf interviews naar gevraagd. Vervolgens kon het interview echt beginnen. Allereerst werden enkele introducerende vragen gesteld om te weten te komen welke werkzaamheden de participant precies verricht en hoe de participant verbonden was met jeugd- en/of gedigitaliseerde criminaliteit. Daarna werden vragen gesteld om een antwoord te kunnen formuleren op de deelvragen. De eerste vraag ging over de kennis van het daderschap van jongeren van online fraude in de regio Zuidoost Drenthe. Vervolgens werd gevraagd welke interventies op dit moment worden ingezet om online fraude te voorkomen en/of bestrijden. De theorie van paragraaf 3.3 speelde hier een centrale rol in. Verder gingen enkele vragen over de samenwerking tussen de gemeente, politie en jongerenwerkers op dit moment. Deze vragen werden gesteld om vast te stellen hoe intensief de samenwerking op dit moment is en of er ook een mogelijkheid bestaat om de integrale aanpak uit te kunnen voeren als die eenmaal is geformuleerd. Er werd gevraagd naar de knelpunten binnen de samenwerking, maar ook naar de dingen die op dit moment goed gaan. De laatste deelvraag ging over de werkwijze om een integrale aanpak op te zetten: “Hoe ziet een ideale aanpak van online fraude door jongeren er volgens u uit?”. Er was nog een afsluitende vraag gesteld over de toekomstperspectieven. Daarmee werd geprobeerd om te achterhalen of online fraude mogelijk een prioritering zou kunnen krijgen in de (nabije) toekomst. Aan de hand van deze vragen was de integrale aanpak geformuleerd.

4.4 Analysemethoden

Tijdens het onderzoek was gebruik gemaakt van thematische analyse (Braun & Clarke, 2012). Thematische analyse houdt in dat bepaalde patronen die telkens naar voren kwamen in de interviews zijn gebruikt om de onderzoeksvraag te beantwoorden. Bij thematische analyses worden zes stappen doorlopen. De eerste stap bestaat uit het bekend raken met de data. Aangezien alle interviews door mij waren afgenomen en getranscribeerd was ik al bekend met de data voorafgaand aan de analyse. Tijdens de analyse waren de interviews enkele keren doorgelezen om vervolgens pas de initiële codes te maken. De tweede stap bestond uit het coderen van de transcripten. Daarvoor moesten alle transcripten eerst worden geïmporteerd in het programma Atlas.ti. Vervolgens werden aan bepaalde gedeeltes codes toegevoegd. In de derde stap was vervolgens het overkoepelende thema van deze onderling samenhangende codes vastgesteld. Oftewel er werden bepaalde groepen samengesteld die eenzelfde hoofdonderwerp hadden. Vervolgens waren in de vierde stap alle codes en thema's nog een keer doorgenomen om de uiteindelijke codes vast te stellen. Het codeboek met alle thema's, codes en voorbeelden werd geformuleerd in de vijfde stap. In *bijlage II* staat dit codeboek. De laatste stap bestond uit het rapporteren van de gevonden resultaten. De deelvragen en de onderzoeksvraag werden aan de hand van de gevonden codes en thema's beantwoord.

4.5 Betrouwbaarheid in kwalitatief onderzoek

Binnen kwalitatief onderzoek wordt de term '*trustworthiness*' gebruikt om de bepalen hoe betrouwbaar het onderzoek is (Shenton, 2004). Het gaat om de volgende vier principes: geloofwaardigheid, overdraagbaarheid, betrouwbaarheid en objectiviteit. Geloofwaardigheid gaat over de overeenstemming van de bevindingen met de werkelijkheid. Om de geloofwaardigheid te bevorderen had ik gebruik gemaakt van een semigestructureerd interviewschema, waarbij de mogelijkheid was tot doorvragen. Interviews zijn een alom bekend middel om kwalitatief onderzoek te verrichten. Er zijn echter geen verschillende kwalitatieve onderzoeksmethoden naast elkaar gebruikt. Ik ben een keer bij een gemeentelijk beleidsoverleg geweest ter observatie waarin ik heb gekeken hoe veiligheidsbeleid wordt opgesteld door de gemeente. Dit is echter eenmalig geweest, waardoor nog niet van triangulatie kan worden gesproken. Thematische analyse is een gerenommeerde onderzoeksstrategie die veelvuldig in de praktijk wordt gebruikt. Nadat de interviews waren getranscribeerd hadden alle participanten nog de mogelijkheid om hier op- of aanmerkingen op te geven. Daarna was pas overgegaan tot het coderen van de interviews. De participanten waren niet onafhankelijk geselecteerd, omdat er een voorwaarde is dat ze werkzaam zijn in de regio Zuidoost Drenthe. Bovendien zijn de participanten geselecteerd door middel van de sneeuwbalmethode: de operationeel specialist van de politie had me verwezen naar de beleidsmedewerkers van de gemeenten en de beleidsmedewerkers hadden mij verwezen naar jongerenwerkers. De jongerenwerkers waren bovendien niet allemaal betrokken bij de overleggen met de ketenpartners, waardoor het ook niet een goede afspiegeling is van de te onderzoeken populatie. Aan alle participanten was de mogelijkheid gegeven om eerlijk te kunnen antwoorden door middel van het aangeven dat de participant niet verplicht is tot antwoorden en door de nadruk te leggen op de vrijwillige deelname aan het onderzoek. Hieruit volgt dat sprake is van een redelijk geloofwaardig onderzoek.

Overdraagbaarheid is de mate van generaliseerbaarheid van de uitkomsten van een kwalitatief onderzoek. Er waren in totaal vijf verschillende organisaties betrokken in dit onderzoek, namelijk de politie, gemeenten, Sedna, Andes en Maatschappelijk Welzijn. Deze bevinden zich allemaal in Zuidoost Drenthe, waardoor uitspraken kunnen worden gedaan over deze gehele regio. Het gaat om de volgende plekken Borger-Odoorn, Coevorden, Emmen en Klazienaveen. Sommige deelnemers van het onderzoek hadden geen rol bij de overleggen, zoals de wijkagenten jeugd en drie jongerenwerkers. Zij zijn echter wel verantwoordelijk voor de uitvoering van het beleid, maar hadden nauwelijks informatie over de totstandkoming van beleid en de knelpunten die zich hierbij voordoen. In tegenstelling tot de andere deelnemers hadden zij wel meer informatie over de huidige stand van zaken qua omvang van online fraude in de regio. Een andere beperking betrof deelnemer 6, want deze deelnemer werkte nog maar kort bij deze gemeente, waardoor zij weinig wist over de gang van zaken in deze regio. Dit was opgelost, doordat een andere ervaren medewerker bij het interview aanwezig was (participant 7). Er waren in totaal dertien mensen betrokken bij dit onderzoek. De gehele laag van de politie omtrent het thema jeugd was volledig afgedekt. Voor alle gemeenten was ten minste één persoon op de openbare orde en veiligheid afdeling geïnterviewd. In Coevorden was zelfs nog een medewerker van de afdeling jeugd geïnterviewd om een beeld te krijgen welke rol zij hebben bij een overleg. Van elke gemeente was ten minste één jongerenwerker geïnterviewd. Hieruit kan worden geconcludeerd dat de steekproef de regio Zuidoost Drenthe voldoende afdekt om hier geldige uitspraken over te kunnen doen. Wanneer buiten deze regio gebruik zou worden gemaakt van de integrale

aanpak moet men voorzichtig zijn in verband met de verschillende context ten opzichte van Zuidoost Drenthe. De interviews varieerden van 25 tot 66 minuten. De data waren verzameld in de periode van 29 maart 2022 en 24 mei 2022. Hieruit volgt dat de resultaten generaliseerbaar zijn voor de regio Zuidoost Drenthe.

Het derde concept betreft zekerheid. Zekerheid ontstaat door overeenstemming tussen de onderzoeksopzet en de uitvoering van het onderzoek. In het huidige onderzoek kwamen deze zeer sterk overeen. De eerste interviews waren namelijk al afgenomen voordat ik de onderzoeksopzet had ingeleverd. Daardoor waren veel afspraken al gepland voor de interviews. Uiteindelijk was er nog één extra interview afgenomen met een medewerker van de afdeling Jeugd van de gemeente Coevorden. Hiermee werd bepaald of er mogelijk ook een rol was weggelegd voor deze afdeling bij de integrale aanpak. Van tevoren was dit niet ingecalculeerd, waardoor de uitvoering iets uitgebreider werd dan was gepland. Tijdens de periode van dataverzameling waren in totaal twaalf interviews afgenomen. De eerste twee interviews waren het minst goed uitgevoerd. Dit komt doordat het al even geleden was dat ik een interview had afgenomen. Hierdoor was ik nog niet goed genoeg in het stellen van vervolgvragen op de gegeven antwoorden. Na het tweede interview verliepen de interviews al veel beter, omdat ik beter in de theorie zat en meer inzicht had in de werking van integrale samenwerkingen door de verkregen informatie van participant 1 en 2. Tegen het einde van de periode van dataverzameling aan verliepen de interviews ook minder soepel dan voorheen. De participanten hadden namelijk vrijwel geen ervaring met overleggen met de ketenpartners. Hierdoor konden enkele vragen niet (volledig) worden beantwoord. Vanuit het jongerenwerk was namelijk slechts één van de participanten betrokken bij overleggen, namelijk participant 10. De laatste drie interviews waren daarom iets lastiger om af te nemen. Het is overigens niet per definitie slecht dat de laatste interviews minder goed verliepen, omdat dit ook kon duiden op verzadiging. Dat houdt in dat de belangrijkste informatie al was verkregen door de eerdere interviews.

De interviews waren vervolgens woordelijk uitgewerkt aan de hand van de opnames en werden nog naar de participanten gestuurd ter controle. Alle participanten vonden dat de interviews goed waren uitgewerkt volgens hun eigen ervaringen in het werkveld. Nadat ik een reactie had gekregen van de participanten kon ik starten met het coderen. Het proces van coderen was al uitgelegd in paragraaf 4.4 ‘Analysemethoden'. Het coderen verliep over het algemeen goed. Er was enkel verwarring ontstaan tussen de codes ‘financieel’ en 'geldverdienen'. Deze omvatten het financiële knelpunt respectievelijk het financiële motief. Sommige codes waren uiteindelijk nog samengevoegd, zoals ‘HALT-taak’ valt nu onder ‘taak van overige partners’, ‘interventie huis-aan-huisbladen’ valt onder ‘overige preventieve maatregelen’, ‘vals geld uitgeven’ valt onder ‘gedigitaliseerde criminaliteit Coevorden’ en ‘verzender tikkies’ valt nu onder ‘gedigitaliseerde criminaliteit Coevorden’. De code ‘leeftijd cybercriminelen’ was verwijderd, omdat deze slechts één keer naar voren kwam in de twaalf interviews. Dus er is sprake van een bepaalde mate van zekerheid, omdat de opzet en uitvoering van het onderzoek sterk overeenkwamen.

De laatste stap om betrouwbaarheid vast te stellen gaat om objectiviteit. Dit gaat over de wijze waarop de resultaten waren verzameld. Er moest namelijk sprake zijn van enige mate van objectiviteit ten tijde van de verslaglegging en het beschrijven van de resultaten. Daarin was triangulatie ook weer van belang. Van triangulatie is in dit onderzoek geen sprake. Er is enkel gebruik gemaakt van kwalitatief onderzoek middels interviews. De data

van de politie is openbaar te vinden op www.data.politie.nl , maar hier wordt geen onderscheid gemaakt in online fraude en ‘fraude’, waardoor de data uit alle gemeenten niet zonder meer kunnen worden overgenomen vanuit de cijfers over ‘horizontale fraude' per gemeente. Dit komt doordat veel cyberdelicten nog niet een eigen wettelijke strafbaarstelling hebben, waardoor deze onder de gewone strafbaarstelling van fraude worden afgehandeld. Hierdoor kon er geen kwantitatieve component worden toegevoegd aan het onderzoek. Er was ook geen tweede kwalitatieve onderzoeksmethode uitgevoerd. De participanten waren onbekenden voor mij, waardoor ik op een objectieve manier die interviews kon afnemen. Hierdoor was het ook waarschijnlijker dat de participanten geen gewenste antwoorden gaven. De interviews waren woordelijk uitgewerkt, waardoor het objectief werd meegenomen tijdens het coderen. Wederom was er tijdens het coderen geen sprake van vooringenomenheid, want de codes vloeiden logischerwijze voort uit de interviews. Al met al kan worden gesproken van een objectieve verslaglegging van de resultaten. Aangezien alle concepten van betrouwbaarheid in enige mate zijn afgedekt kan worden gesproken van een redelijk betrouwbaar onderzoek.

4.6 Ethische principes

Het verkrijgen van ‘geïnformeerde toestemming’ was niet voldoende om te kunnen spreken van een ethisch verantwoord onderzoek. In het geïnformeerde toestemmingsformulier waren de volgende principes besproken: vrijwillige deelname, geen verplichting tot antwoord, anonimiteit, veilig omgaan met verkregen data en het gebruik van de data is enkel ten behoeve van de master thesis. Daarnaast was de duur van het interview ook aangegeven. Veel van deze principes waren daarnaast ook nog mondeling doorgenomen op de opname, zodat kon worden geverifieerd of de participant zijn rechten had begrepen. Het is erg belangrijk om je als onderzoeker aan deze ethische principes te houden wanneer gebruik wordt gemaakt van kwalitatief onderzoek. Ten eerste doordat gevoelige informatie wordt ingewonnen. Daarnaast moeten de onderzoekers vertrouwelijk omgaan met de verkregen informatie. Het gaat er voornamelijk om dat de data enkel gebruikt werd voor mijn master thesis en na afloop van het onderzoek weer werden verwijderd.

Aan het begin van de interviews was eerst een korte introductie gegeven op mijn onderzoek. Daarna werden de ethische principes nogmaals doorgenomen. Er was onder meer aangegeven dat te allen tijde kan worden afgezien van het interview indien dat mogelijk schade zou kunnen opleveren voor de participant. Bovendien was aangegeven dat slechts een klein aantal mensen kennis konden nemen van de interviews, namelijk de scriptiebegeleider, de referent en ikzelf. De andere betrokkenen hadden wel de mogelijkheid om kennis te nemen van de thesis zelf, maar niet van de opnames en uitgewerkte interviews. Er was ook duidelijk aangegeven waarom de interviews werden opgenomen en dat de identiteit van de participant werd beschermd. De participanten waren tijdens het interview zo veel mogelijk aan het woord, waarbij ik de mogelijkheid had om door te vragen, uitleg te geven of aan te geven dat ik luisterde door middel van een knikje of "ja” te zeggen. Mijn eigen overtuigingen waren niet naar voren gekomen, waardoor de participant zelf zijn/haar eigen ideeën kon delen zonder beïnvloeding van een ander. In een enkel geval had ik de participanten enigszins gestuurd naar een antwoord. Dat gebeurde dan door voorbeelden te geven van mogelijke zaken die van belang zijn voor een integrale aanpak of te vragen naar de rol van de gemeente op het gebied van cybercriminaliteit. Ik had echter nooit mijn eigen ideeën of mening te

kennen gegeven als dat werd gevraagd, maar had ik enkel voorbeelden of uitleg gegeven. Hierdoor waren alle ethische principes goed gewaarborgd.

H5 Resultaten

In dit hoofdstuk wordt de onderzoeksvraag beantwoord: “Hoe kan een integrale aanpak voor online fraude door jongeren worden opgezet door politie, gemeente en jongerenwerkers in de regio Zuidoost Drenthe?". In de eerste paragraaf wordt gekeken naar de kennis van de ketenpartners over het daderschap van jongeren in de regio Zuidoost Drenthe met betrekking tot online fraude. De huidige samenwerking tussen de gemeenten, politie en jongerenwerkers wordt vervolgens in paragraaf 5.2 besproken. Daarbij worden de knelpunten, maar ook de sterke kanten van de samenwerking tussen de ketenpartners besproken. In de derde paragraaf wordt gekeken naar de invulling die de verschillende ketenpartners willen geven aan de integrale aanpak van online fraude door jongeren. Tot slot worden enkele aanbevelingen gedaan voor de integrale aanpak.

5.1 Kennis van ketenpartners over online fraude in Zuidoost Drenthe

Aan alle participanten is gevraagd of ze te maken hebben met cyber- of gedigitaliseerde criminaliteit ten tijde van hun werkzaamheden. Daarnaast is gevraagd naar daderschap van online fraude door jongeren in hun regio. Hierna zal per gemeente worden besproken welke informatie bij hen bekend is over online fraude door jongeren.

In de gemeente Borger-Odoorn heerst nog de vraag of zij wel een rol hebben bij problematiek rondom cybercriminaliteit. Zij stellen namelijk dat er voornamelijk een rol is weggelegd voor het Openbaar Ministerie. Zelf doen zij op dit moment nog niks aan online fraude:

> “Op dit moment niet. We hebben het er recent, in maart, in het bestuurlijk overleg over gehad. Dat zijn de burgemeesters, de basisteamchef en de officier van justitie. Wij hebben toen vanuit Borger-Odoorn de vraag gesteld dat we dit [online fraude] op de agenda zien staan, maar hoe zitten we hier nu in? Dus het is eigenlijk nog vers, net begonnen.”- P.07

Er is dus nog volop overleg over de rol van de burgemeester bij cybercriminaliteit. Bovendien is het mogelijk dat er helemaal geen rol is weggelegd voor de burgemeester, omdat het niet speelt in zijn gebied. De gemeente Borger-Odoorn is een groot uitgestrekt gebied met inwoners met verschillende (sociaaleconomische) achtergronden. Er kan een gebied worden aangewezen met een goede sociaaleconomische achtergrond en een gebied met een minder goede sociaaleconomische achtergrond. Dat wordt zowel door de beleidsmedewerkers van de gemeente als door de jongerenwerker aangegeven. Door deze inkomenskloof in de gemeente is er een grote kans aanwezig dat jongeren wel actief zijn op het gebied van online fraude. Dat valt dan te verklaren doordat ze weinig financiële middelen hebben om te kunnen voorzien in hun (materiële) behoeften:

> “We weten het niet, maar de kans dat het bij ons in de gemeente of deze regio plaatsvindt is wel iets hoger. Het is een makkelijke manier van geld verdienen. Een groot deel van deze gemeente en regio heeft het sociaaleconomisch niet heel breed. Er speelt hier ook veel verslavingsproblematiek. Dit kunnen allemaal aanjagers zijn om net even dat stapje verder te gaan. Ik weet dus niet of het gebeurt, maar de kans hierop acht ik wel aannemelijk.” - P.07

Er zijn echter geen duidelijke indicaties bij de gemeente Borger-Odoorn dat jongeren zich bezighouden met online fraude. Zij krijgen echter wel te horen dat jongeren in de regio vaak

slachtoffer zijn van phishing en andere vormen van online fraude. Bij Andes is echter wel kennis van het feit dat jongeren mogelijk actief zijn als online fraudeur:

> “We hebben wel signalen gehad van de politie, maar zij mogen ook niet alles met ons delen. Er is nu geen jongere die ik kan bedenken die daarmee in aanraking is gekomen.” - P.13

In de gemeente Coevorden spelen dezelfde ideeën. Vanuit de gemeente wordt de vraag opgeworpen of er wel een rol is voor de burgemeester op het gebied van online fraude en andere vormen van cybercriminaliteit. De burgemeester heeft het gezag over de politie wanneer het gaat om openbare orde en veiligheid, dus bij zaken zoals overlast en ondermijning. Strafbare feiten die achter gesloten deuren afspelen die geen directe gevolgen hebben voor de openbare orde vallen daar tot nu toe (nog) niet onder. Cybercriminaliteit wordt gepleegd in de privésfeer achter de voordeur. Bovendien gaat het om criminaliteit dat zich afspeelt op het internet. De discussie is nog of er dan wel of niet sprake is van een probleem van openbare orde:

> “Weinig. Ik moet eerlijk zeggen dat wij als gemeente daar nog heel weinig op inzetten. De vraag speelt ook of wij dat moeten. Hebben wij als gemeente namelijk wel een verantwoordelijkheid voor cybercriminaliteit? Moeten wij daar een aanpak op hebben? Hoe moeten wij zo'n aanpak dan uitvoeren? Doen we dat zelf of in samenwerking met de politie? […] De online fraude blijft op dit moment meer liggen bij de politie dan bij de gemeente. Wij weten ervan. In de maandrapportages krijgen wij bijvoorbeeld ook wel de cijfers van online fraude en cybercriminaliteit, maar wij doen daar als gemeente nog niet iets actiefs mee. […] Dat is op dit moment de discussie die er speelt. Als gemeente wordt elke keer een stuk van die cybercriminaliteit opgepakt. We vragen ons dan af of het onder openbare orde en veiligheid onder de portefeuille van de burgemeester of ICT valt.” – P.09

In Coevorden zijn naast de algemeen adviseur openbare orde en veiligheid ook nog vier anderen geïnterviewd. Bij deze participanten speelt natuurlijk niet de vraag of er wel een rol weggelegd is voor de burgemeester. Zij krijgen echter wel het een en ander mee over cybercriminaliteit in de gemeente Coevorden. Participant 8 geeft aan dat ze vanaf de zijlijn wel eens meekrijgt dat jongeren online actief zijn, maar noemt daarbij als voorbeeld een gameverslaving. Daarnaast speelt er op dit moment een zaak waarbij een jongere online criminaliteit pleegt. De precieze vorm van cybercriminaliteit wordt niet benoemd, maar het gaat niet om online fraude. Er werd in dat geval wel de actieve samenwerking met de politie opgezocht (P.09). Vanuit het jongerenwerk (P.10) en de politie (P.01; P.02) komt naar voren dat er geldezels actief zijn in de gemeente:

> “[…] Wat ik wel weet is dat wij steeds meer te maken krijgen met *moneymuling*. […] Dat zien we, dat horen we, dat haal je ook wel in het systeem naar voren. Jongeren lenen voor 20 of 50 euro hun pinpas uit en hun pincode. “Dan stort ik daar geld op en dat wordt dat gewoon doorgestort naar de andere" zeggen de ronselaars. Gewoon witwassen.” - P.01

> “[…] Er zijn hier ook geldezels. Jongelui die geld wordt aangeboden om hun rekening eventjes open te stellen voor andere doeleinden. Zodat ze daar geld mee kunnen verdienen. Dus dat komt hier ook voor.” - P.02

> "In de afgelopen twee jaar is er maar één keer een jongere geweest die als geldezel geld heeft verdiend. " - P.10

In de gemeente Emmen wordt niet de vraag opgeroepen of cybercriminaliteit een taak is van openbare orde en veiligheid. Binnen deze gemeente is (nog) niks bekend over jongeren die mensen oplichten via het internet. Ze krijgen wel cijfers binnen over cybercriminaliteit en online fraude, maar dat gaat over slachtoffers (P.03). Het jongerenwerk bij Andes heeft geen kennis over online fraude door jongeren in Emmen (P.12) en Klazienaveen (P.11). Bovendien geven ze aan dat ze het lastig vinden om jongeren te controleren op het gebruik van hun telefoons (P.12). Bij de jeugdagenten is echter wel een indicatie dat jongeren actief zijn als geldezel:

> "Dan lopen we er wel eens tegenaan dat bijvoorbeeld een jongere allemaal bankpasjes heeft. Dat heb ik wel eens meegemaakt. Dan gaan er natuurlijk alarmbellen rinkelen. Je gaat vervolgens na wat er hier aan de hand is. Wordt hij gebruikt? Of is hij [de jongere] er zelf mee bezig? Dus op die manier loop ik er wel eens tegen aan. Ik leg dat dan vast en dat meld ik bij de afdeling. Je communiceert dat bijvoorbeeld met de recherche of dat soort afdelingen." - P.04

> "Je ziet steeds meer geldezels, *money mules*. Dat gebeurt echt heel veel. Jongeren zijn zich niet bewust van wat er gebeurt en er gaat gebeuren als zij hun pasje wel uitlenen. Ze zien alleen in dat ze heel snel veel geld kunnen verdienen. Zo worden ze eigenlijk een beetje de loopjongen van de grotere criminelen. [...] Het kan best wel eens zijn dat er eentje [geldezel] naar binnen wordt gehaald, dat die dan wordt opgepakt. Dat wil je niet, maar die is vaak slachtoffer van iemand die boven hem of haar staat." - P.05

Samenvattend kan worden gesteld dat er bij de gemeenten de discussie heerst of zij wel een rol hebben op het gebied van cybercriminaliteit. Zij vragen zich daarom dus ook af of zij wel betrokken moeten worden bij een integrale aanpak voor online fraude. Daarbij geven ze wel aan dat ze op het preventieve vlak wel bepaalde dingen zouden kunnen doen, zoals informeren op sociale media of in huis-aan-huisbladen (P.06; P.07). Een andere opvallende bevinding is dat er bij de politie in Zuidoost Drenthe een beter beeld is van jonge daders van online fraude dan bij de andere ketenpartners. De medewerkers van de gemeente (P.03; P.06; P.07; P.08; P.09) en de jongerenwerkers (P.10; P.11; P.12; P.13) hebben geen (volledig) beeld van jongeren die opduiken als geldezel in Zuidoost Drenthe. Er is wel een beeld van het aantal slachtoffers van online fraude. Bovendien lijkt het jongerenwerk iets beter op de hoogte te zijn van het aantal gevallen van online fraude door jongeren dan het gemeentepersoneel. De verschillende jongerenwerkers geven namelijk aan dat ze wel eens signalen hebben gekregen van geldezels bij hen in de wijken. Kortom, de cijfers van daders van online fraude, zoals het aantal geldezels, moeten door de politie worden bekendgemaakt bij de andere ketenpartners. Wellicht zorgt dit er ook voor dat de gemeente de problematiek van gedigitaliseerde criminaliteit wel gaat oppakken.

5.2 Samenwerking tussen de ketenpartners

Sinds 2020 wordt actief samengewerkt tussen de politie, gemeenten en jongerenwerkers in Zuidoost Drenthe. Het begon in Emmen en later volgden ook de twee andere gemeenten. Daarvoor bestond er ook al een samenwerking tussen de ketenpartners, maar deze was niet integraal en ook niet structureel. Naast deze drie ketenpartners zijn er ook nog andere instanties betrokken bij de verschillende overleggen, zoals bijvoorbeeld

woningbouwcorporaties, bureau HALT en het Openbaar Ministerie. Op dit moment gaan de overleggen over bijvoorbeeld Jonge Aanwas (P.03) en ad hoc problematiek (P.06; P.07). Sommige overleggen hebben dus één thema en andere overleggen gaan echt over de waan van de dag, dus over problemen die op dit moment spelen. Het valt participant 3 overigens ook op dat er vaker op korte termijn wordt samengewerkt met ketenpartners dan op lange termijn. Deze participant zou echter graag willen zien dat er vaker op de lange termijn wordt samengewerkt met de ketenpartners, zoals bijvoorbeeld wel op het gebied van ondermijning gebeurt.

> "Ja, dat is eigenlijk altijd de valkuil binnen de veiligheid dat je ad hoc bezig bent. Het probleem is nu en moet je nu oplossen. Dat snap ik. Alleen dan blijf je rennen, omdat je nooit komt tot een structurele aanpak om het probleem te voorkomen. Je rent er alleen maar achterna. Dat is een valkuil." - P.03

Daar is prioritering voor nodig. Binnen het jaarwerkplan van de politie staat cybercriminaliteit hoog aangeschreven. Dat houdt in dat de politie in 2022 meer aandacht wil besteden aan cybercriminaliteit. Bij de gemeente heerst ook de discussie of zij een rol hebben bij cybercriminaliteit, zoals eerder al naar voren kwam. Daar wordt wel mee aangetoond dat de partners inzien dat cybercriminaliteit een probleem is dat steeds groter wordt. Bij alle participanten is bekend dat er veel slachtoffers zijn van online fraude, maar tot dusver is er nog geen (integrale) aanpak geformuleerd. Om de aanpak te formuleren voor een specifiek thema is het verstandig om de huidige samenwerking tussen de ketenpartners te beschrijven.

5.2.1 Samenwerking op het gebied van jeugdcriminaliteit

Er zijn drie verschillende samenwerkingsverbanden in de regio Zuidoost Drenthe. De eerste samenwerking is tussen de gemeente Borger-Odoorn, de politie en Andes. In dit gebied wordt niet structureel samengewerkt tussen de ketenpartners. Er wordt in dit geval meer ad hoc samengewerkt aan problemen die spelen in de gemeente. Vanuit het jongerenwerk wordt wel steeds meer samengewerkt met de politie (P.13). Er lijkt geen sprake te zijn van structureel contact tussen de medewerkers van openbare orde en veiligheid en de andere ketenpartners. Participant 6 en 7 geven het volgende aan over de samenwerking met jongerenwerk:

> "Ik werk heel weinig met jongerenwerk. Die kom ik eigenlijk alleen tegen met een maatschappelijk incident, dus als er iets gebeurd is. Ik attendeer hen vooral op dingen die hier spelen, op het moment dat een bepaalde criminaliteitsvorm opkomt dan attendeer ik hen hierop. Ik vraag of ze hierover contact met jongeren opnemen en hier ook aandacht aan willen besteden. De thema's van nu zitten voornamelijk in de radicalisering 'Jonge aanwas'. Dan attendeer ik jongerenwerk erop dat er een training 'jonge aanwas' komt." - P.07

De tweede samenwerking is tussen de gemeente Coevorden, de politie en Maatschappelijk Welzijn Coevorden. Hier is wel sprake van een structurele samenwerking tussen de drie instanties. Er zijn verschillende structurele overleggen waar deze partijen bij betrokken zijn. In de gemeente Coevorden worden de taken geformuleerd als actiepunten (P.09). De actiepunten zijn de gemaakte afspraken tijdens een overleg. Na een bepaalde periode wordt vervolgens geëvalueerd of de actiepunten zijn uitgevoerd en hoe ze zijn uitgevoerd. Daardoor wordt het overleg meer structureel van aard. In de gemeenten Coevorden en Emmen vinden de overleggen op regelmatige basis plaats, namelijk eens in de vier á zes weken. In de gemeente Emmen is ook een structurele samenwerking tussen de gemeente, politie en Sedna.

Er zijn overleggen met een bepaald thema, zoals Volwassenheid (P.03), maar soms is er ook incidenteel overleg nodig over ad hoc problematiek. De taken worden tijdens een overleg als volgt verdeeld:

> "Elke partner pakt zijn eigen expertise daarin en zijn eigen tools. En als je van elkaar weet wat de mogelijkheden en onmogelijkheden zijn dan kun je het uiteindelijk het beste bereiken." - P.03

Uiteindelijk hebben alle partners eigen bevoegdheden die ze kunnen inzetten. In eerste instantie willen de betrokken ketenpartners ervoor zorgen dat jongeren niet in de problemen komen door het krijgen van een strafblad. Ze zullen daarom eerst vanuit een zorg- en dienstverlenend verband zorgdragen voor de jongere die het criminele pad op gaat (P.08). Dit kan bijvoorbeeld worden gedaan door de jongerenwerkers, maar wordt ook gedaan door de afdeling Jeugd (P.08) bij de gemeenten. De afdeling Jeugd bestaat onder meer uit jeugdconsulenten, maar ook uit de buurtsportcoaches die op een laagdrempelige manier inwoners van een gemeente aanmoedigen om meer te bewegen. Er zal worden geprobeerd om de jongere weer het goede pad op te krijgen zonder een mogelijke vervolging door gesprekken te voeren of samen te gaan sporten. Wanneer deze eerste aanpak om de jeugdcriminaliteit te doen stoppen niet werkt, zal worden gegrepen naar een andere aanpak, namelijk strafrechtelijk optreden (P.08). De politie zal meer vanuit het strafrechtelijke gebied optreden door bijvoorbeeld jongeren op te sporen, te verhoren en eventueel arresteren (P.04). Vervolgens zal dan de taak verschuiven naar het Openbaar Ministerie om de jongere te vervolgen. Het uiteindelijke doel is voor alle ketenpartners in beginsel hetzelfde:

> "[…] Je doel is uiteindelijk natuurlijk om het te doen laten stoppen. Dat zou je doel zijn. Tenminste dat is in mijn gedachte het doel. Maar dan moet je in het plan van aanpak kijken en dan moet je met elkaar kijken wat het doel zou moeten zijn. Nou je wil er met elkaar voor zorgen dat er consequenties aan hangen en je wil ervoor zorgen dat de minderjarige niet nog dieper in de problemen komt. Ik denk dat dat uiteindelijk je doel is." -P.01

Daarin probeert elke ketenpartner ook zijn/haar eigen doelstellingen te behalen door het uitvoeren van de eigen taken. Dat gaat over het algemeen heel goed wanneer traditionele criminaliteit moet worden bestreden. De ketenpartners zijn dan op de hoogte van elkaars mogelijkheden. Op het gebied van online fraude weten de partners echter niet goed van elkaar wie bepaalde taken uitvoeren. Er worden bepaalde verwachtingen uitgesproken, maar de concrete afstemming van de partners op elkaar ontbreekt. Participant 13 weet bijvoorbeeld helemaal niet of de plaatselijke gemeente iets doet aan de bestrijding van online fraude. Er is ook al bewustzijn over de mogelijke problemen betreffende de onderlinge afstemming tussen de ketenpartners:

> "[…] Maar het is wel goed om elkaar op de hoogte te houden, zodat je ook altijd weet wat zich in bepaalde dorpen en wijken afspeelt. Anders ga je allemaal op eigen gelegenheid dingen doen die je misschien overlappen of allebei de andere kant op werken. Daar valt wel winst te behalen." - P.10

Het is daarom van belang dat in de integrale aanpak duidelijk wordt welke bevoegdheden alle partners hebben op het gebied van online fraude en welke handelingen zij van elkaar kunnen verwachten. Anders is het zeer aannemelijk dat partners allemaal gaan inzetten op

preventieve maatregelen. Op dit moment worden namelijk voorlichtingen genoemd als middel om online fraude door jongeren te verminderen. De voorlichtingen moeten in ieder geval bestaan uit het vermelden van de consequenties van een veroordeling wegens online fraude, omdat het vaak zo is dat jongeren niet door hebben dat er consequenties zijn als je je bankpas uitleent aan een onbekend persoon die je daarvoor geld aanbiedt. Een van de participanten gaf aan dat voorlichtingen die worden gegeven door agenten effectiever zijn, omdat agenten een bepaalde mate van gezag uitstralen waardoor kinderen en jongeren eerder iets van ze zullen aannemen (P.01). Een andere participant gaf daarentegen aan dat de politie een slecht imago heeft onder de jeugd en dat een voorlichting door jongerenwerkers daardoor effectiever zou zijn (P.13). Hier lijkt dus een discrepantie te bestaan. Daardoor is het niet duidelijk welke ketenpartner het beste de voorlichtingen kan geven. Het is echter wel duidelijk dat het niet efficiënt is om elke ketenpartner een voorlichting te laten geven op middelbare scholen of andere plekken waar jongeren veel komen. Daarom moet duidelijk worden afgesproken wie voorlichtingen gaat geven en wanneer dat plaats zal moeten vinden. Daarnaast moeten andere middelen ook worden doorgenomen die mogelijk goed kunnen werken om geldezels te voorkomen, zoals bijvoorbeeld het inzetten van de mobiele-mediabus (P.02) of de game *framed* (P.04; P.05), informeren via huis-aan-huisbladen (P.06; P.07) en informeren via sociale media (P.13). Verder moet duidelijk worden welke bevoegdheden de politie heeft om online fraude aan te pakken. Er bestaan namelijk nu enkel veronderstellingen over de bevoegdheden van de politie. Participant 8 benoemt heel abstract de rol is van de politie, namelijk signaleren, melden en handhaven. Daardoor weten de andere partners niet van elkaar wat ze kunnen verwachten.

5.2.2 Knelpunten

Op dit moment kunnen er verscheidene punten worden aangewezen die de huidige samenwerking lastig maken. De afstemming over de uit te voeren taken tussen de ketenpartners is daar één van. Het gaat verder nog om de volgende knelpunten: financiën, tijd, personeelstekort, verloop van personeel, ziekteverzuim, het ontbreken van cijfers en individuele knelpunten. Hierna zullen alle knelpunten kort worden doorgenomen.

De vijf instanties die betrokken zijn bij dit onderzoek worden allemaal gefinancierd vanuit het Rijk. De gemeente en politie zijn overheidsinstanties en de instanties van het jongerenwerk worden gefinancierd door middel van subsidies die afkomstig zijn van de gemeente. Hierdoor hebben bezuinigingen vanuit de overheid invloed op de mogelijkheden van alle betrokkenen bij de integrale aanpak. Participant 2 heeft bijvoorbeeld aangegeven dat er minder voorlichtingen worden gegeven op scholen als gevolg van bezuinigingen vanuit de overheid. Vanuit de gemeente Emmen is bovendien aangegeven dat er te weinig jongerenwerkers zijn voor deze gemeente, doordat er te weinig financiële middelen zijn kunnen er geen extra jongerenwerkers worden gesubsidieerd door de gemeente. In het grote gebied zijn op dit moment slechts drie jongerenwerkers werkzaam. Het zou gewenst zijn om meer mensen in dienst te nemen, aldus participant 3. Maar op het moment dat er echt iets speelt worden er altijd extra financiële middelen ter beschikking gesteld. Het moet dan wel om urgente problematiek gaan (P.03). Toch zou er meer financiële steun nodig zijn vanuit de overheid om alle zaken goed op orde te stellen bij de samenwerking tussen de ketenpartners.

Een verbonden probleem daaraan is het personeelstekort. Vrijwel alle participanten benoemden het personeelstekort bij de politie als knelpunt:

> "Ja dat is heel erg lastig. Ik denk dat wij, maar ook de politie daar continu wel tegenaan lopen dat we die capaciteit niet kunnen aanvullen. Je krijgt er niet zomaar meer mensen bij. Je kan niet als medewerker zeggen dat we er iemand bij willen. Dat kan je wel aangeven, maar dat wordt heel vaak niet gedaan. Dus dan komt er ook niemand. Daarnaast is er ook een gigantische krapte op de arbeidsmarkt, dus het is ook niet altijd even makkelijk om iemand te vinden die volledig is opgeleid en helemaal op vlieghoogte is. Daar kunnen we niet zo veel aan doen." - P.09

Wanneer er te weinig opleidingscapaciteit is dan blijven de tekorten bij de politie voortbestaan. Op dit moment zijn wijkagenten niet veel meer te vinden in hun wijk, maar draaien ze voornamelijk noodhulpdiensten. Hierdoor kunnen zij minder goed problematiek signaleren dat zich afspeelt in de wijk, waardoor ze in de toekomst mogelijk achter de feiten aan zullen lopen (P.10). Bovendien is er minder tijd om een integrale samenwerking aan te gaan wanneer de agenten de basistaken enkel kunnen uitvoeren. Er wordt echter ook aangegeven dat het personeelstekort bij vrijwel iedere instantie speelt, dus ook bij de gemeenten en het jongerenwerk. Hierdoor wordt een integrale samenwerking nog lastiger. Daarnaast speelt verloop ook een grote rol bij de gemeente en het jongerenwerk. Veel personeelsleden werken pas sinds kort bij hun werkgever en er vertrekken ook veel mensen (P.12). Dit heeft als gevolg dat er nog weinig onderling contact is over mogelijke signalen van jeugdcriminaliteit en nog geen sprake is van onderling vertrouwen om informatie te kunnen delen. Het verloop van personeel kan daarom een integrale samenwerking in de weg zitten. Ziekte onder het personeel kan ook roet in de samenwerking gooien, doordat bepaalde taken gedurende langere periode niet meer worden uitgevoerd. Deze drie knelpunten zien allemaal op capaciteit. Er is echter geen directe oplossing voor deze problematiek, omdat dit vanuit het Rijk zou moeten komen.

Het volgende knelpunt is nauw verbonden met het voorgaande knelpunt, namelijk tijd. Het tijdstekort houdt eigenlijk in dat er veel problemen zijn waar een integrale aanpak wenselijk voor zou zijn, maar er geen tijd is voor het maken en uitvoeren van een dergelijke aanpak:

> "[…] Dat zijn misschien wel de makkelijke punten om erbij te pakken: altijd zeggen dat er te weinig tijd of personeel is. Het is momenteel wel gewoon aan de orde. Dat er gewoon ook heel veel andere dingen moeten gebeuren. Doordat er momenteel wel krapte is bij ons." - P.04

Daar komt het punt van ad hoc werken weer terug. Deze problematiek wordt over het algemeen goed aangepakt, omdat hier prioriteit voor is. De problematiek die zich op de lange termijn afspeelt raakt hierdoor op de achtergrond. Bij het opstellen van een groepsscan komt het bijvoorbeeld geregeld voor dat een jeugdgroep niet langer voor overlast zorgt wanneer de scan is afgerond (P.01). Dat komt doordat er niet veel tijd is om een groepsscan op te stellen vanwege de prioriteit om de noodhulpdiensten in te vullen (P.04). De wijkagenten hebben tegenwoordig slechts 30 procent van hun werkweek de tijd om in de wijk te zijn, waardoor er minder signalen worden opgevangen. Dit speelt echter ook bij de gemeente, omdat er veel thema's zijn die op de korte termijn moeten worden opgepakt (P.03). Kortom, het tijdgebrek is nauw verbonden met de problematiek rondom het personeel. Wanneer er te weinig personeel is, zullen veel taken moeten worden uitgevoerd door minder mensen. Hierdoor zullen de problemen van het moment eerder worden opgepakt dan problemen die zich op de lange termijn ontwikkelen.

De laatste knelpunten zijn individuele knelpunten van de betrokken organisaties. Het gaat dan om de gemeenten en de politie. Vanuit het jongerenwerk waren namelijk geen knelpunten naar voren gekomen. Door de gemeente Emmen was het volgende aangegeven:

> "Dat jongeren zich daarmee bezighouden is voor mij juist een kenmerk van die cybercrime, hoe snel dat gaat. Die technologische ontwikkelingen gaan ongeveer net zo snel als wij het leren. Dat is ook hoe ik het dan zie. Dus dat gaat net zo snel. De gemeente gaat nog altijd zo traag als dat het altijd heeft gedaan. […] Dat is dus wat het zo ingewikkeld maakt. Je moet eigenlijk snel schakelen, terwijl het systeem niet daartoe in staat is." - P.03

Gedigitaliseerde criminaliteit, zoals online fraude, is voor de gemeente lastig om aan te pakken. Er is geen expertise op dit gebied binnen de gemeenten in Zuidoost Drenthe te vinden (P.08). Hierdoor kunnen de medewerkers van Openbare Orde en Veiligheid lastig bijblijven met de ontwikkelingen op het gebied van online fraude en andere vormen van gedigitaliseerde criminaliteit. De traagheid van de gemeente zorgt ervoor dat er lastig grip kan worden gekregen op online fraude. Een ander knelpunt in het formuleren van een integrale aanpak bestaat uit de verschillen tussen de drie gemeenten in Zuidoost Drenthe. In de gemeente Borger-Odoorn is het integraal samenwerken nog niet goed ontwikkeld, terwijl het in Coevorden en Emmen al redelijk goed ontwikkeld is. Bij alle drie de gemeenten ligt de basis er al wel, maar in Borger-Odoorn wordt in de praktijk weinig samengewerkt. Hierdoor is nog geen sterk onderling vertrouwen ontwikkeld met alle ketenpartners. Dat zorgt ervoor dat de uitvoering van de integrale aanpak lastiger zal verlopen.

De overige individuele problematiek ligt bij de politie. Het eerste knelpunt is voor de hand liggend: de onregelmatigheid van het politiewerk. Participant 4 heeft bijvoorbeeld aangegeven dat het niet altijd betrouwbaar is wanneer agenten wel of niet aanwezig zijn bij overleggen en andere afspraken. Het werk van een politieagent is wisselend, omdat het geen 9 tot 5 baan is, maar een baan met ochtend-, late- en nachtdiensten. Daarnaast werken ze natuurlijk ook 's weekends, waardoor het soms lastig is om met alle ketenpartners bijeen te komen. Een ander knelpunt dat zich de laatste jaren afspeelt als gevolg van het tijd- en personeelsgebrek is dat er afstand is ontstaan tussen de politie en burgers:

> "Dat kan wel, maar dat is meer dat bijvoorbeeld een wijkagent of als wij zelf minder in de wijk kunnen zijn. De communicatie is prima, maar die signaleert minder snel iets. Doordat hij minder snel de informatie krijgt. Dat het bijvoorbeeld onrustig in de wijk is. Mensen zeggen heel vaak dat ze gebeld hebben, maar dat ze ons niet aan de telefoon krijgen. Zulke dingen gebeuren. Of dat er iemand uitvalt door ziekte en dat een andere wijkagent dat dan moet oppakken. De dingen worden dan niet zo snel opgepakt als dat ze gewend zijn. Dus krijg je, als je niet snel je verhaal kwijt kan, dat mensen niet meer bellen. Er ontstaat dan een afstand." - P.05

Al met al zijn er verschillende knelpunten die een samenwerking tussen de politie, gemeente en jongerenwerkers moeilijker maken. Aan sommige knelpunten valt niet veel te doen, zoals financiën en personeel gebonden problemen. Er valt echter wel winst te behalen bij de afstemming tussen de ketenpartners door bijvoorbeeld elkaars bevoegdheden en mogelijkheden te leren kennen. Daardoor kan dubbel werk, in de vorm van preventieve maatregelen, worden voorkomen. Een ander punt was eerder al benoemd in paragraaf 5.1: de politie heeft als enige partner de cijfers van online fraude goed in beeld. Dit zou beter

kenbaar moeten worden gemaakt aan de andere ketenpartners, zodat zij kunnen bepalen of er prioriteit is bij de aanpak hiervan.

5.2.3 Sterke punten samenwerking

De huidige samenwerking bestaat niet enkel uit knelpunten, want er gaan ook veel zaken wel goed, zoals het onderlinge contact, de taakverdeling, de regierol van de gemeente en de duidelijke doelstellingen. Bovendien wordt aangegeven dat het jongerenwerk een waardevolle toevoeging is aan de samenwerking. Zij signaleren veel problematiek die speelt bij hen in de wijk:

> "[…] Wij zullen nooit zeggen wat er precies gezegd wordt in de gesprekken met jongeren. Maar wij zien wel heel veel, omdat we altijd in de wijk zijn. Wat je daar ziet kan heel waardevol zijn. Alleen nu komt het op een grote hoop, omdat het niet gedeeld mag worden." - P.10

De jongerenwerkers mogen in het algemeen zeggen wat er in de wijk speelt, maar mogen daarbij geen personen aanwijzen. Zij mogen wel aangeven waar bepaalde jongeren vaak te vinden zijn en wat ze vermoedelijk doen (P.13). Eigenlijk zouden jongerenwerkers een belangrijkere rol moeten hebben bij het signaleren van jeugdcriminaliteit, want zij zijn tegenwoordig meer de oren en ogen in de wijk dan de wijkagenten.

Vrijwel alle participanten geven aan dat de medewerkers van de gemeente Emmen en Coevorden de rol als regievoerder goed oppakken. Participant 12 noemt hen zelfs de kartrekkers van de overleggen, maar geeft daarbij ook aan dat er een belangrijke rol voor de politie is als kartrekker. De jeugdagent uit Coevorden heeft echter aangegeven dat de gemeente nog wel vaker de regierol op zich mogen nemen. Voor Borger-Odoorn geldt echter een ander verhaal, want daar zijn immers amper samenwerkingen. Bij Andes is het zelfs niet bekend wie de regie zou moeten hebben tijdens een overleg (P.13). Hier valt nog veel te halen qua verbeteringen in de samenwerking tussen de ketenpartners.

De doelen van de samenwerkingen zijn duidelijk voor de samenwerkingspartners. Eigenlijk gaf iedereen aan dat zij handelen in het belang van het kind: ze willen dat de jongeren niet verder verwikkeld raken in het criminele circuit. Daarbij voeren alle partners hun eigen taken uit en handelen ze ook overeenkomstig hun eigen doelen. Jongerenwerk heeft bijvoorbeeld als doel om positieve contacten te onderhouden met jongeren (P.10). Nadat de doelstelling van de samenwerking is vastgesteld, kan worden overgegaan tot de verdeling van de taken. Dat is ook een sterk punt in de huidige samenwerking bij alle drie de gemeenten. Vooral in Coevorden lijkt het goed in orde te zijn. Daar worden de taken duidelijk genoteerd, tussentijds is er contact over de uitvoering en de taakuitoefening wordt na een bepaalde periode geëvalueerd. Wanneer bepaalde taken niet kunnen worden uitgevoerd wegens ziekte of een andere reden dan wordt dit doorgegeven (P.09). Het actieplan van Coevorden werkt goed, maar in de andere gemeenten worden de taken ook verdeeld naar eigen expertise van de partners en wordt na verloop van tijd geëvalueerd. Het onderlinge contact tussen de ketenpartners is erg goed: "De 'korte lijntjes' zijn goed" (P.08). De meeste partners zijn goed bereikbaar via de telefoon om kort bepaalde zaken door te kunnen nemen.

Kortom, de basisprincipes zijn inmiddels goed geïmplementeerd tussen de ketenpartners in Zuidoost Drenthe. Er valt echter nog wel winst te behalen in de gemeente

Borger-Odoorn. Dat komt doordat hier vaker op korte termijn de samenwerking wordt opgezocht. Hier zou al winst kunnen worden behaald door een samenwerking met de ketenpartners aan te gaan op de lange termijn. Maar op dit moment wordt de regie wel goed gevoerd door deze medewerkers bij de gemeente Borger-Odoorn.

5.3 Wensen voor de integrale aanpak

Aan alle participanten is gevraagd welke invulling zij zouden willen geven aan de integrale aanpak voor online fraude. Vanuit het jongerenwerk komen verschillende wensen naar voren: het betrekken van verscheidene netwerkpartners (waaronder ook HALT), strikte verdeling tussen preventieve en repressieve taken, structureel contact/overleg en een speciale expertise afdeling bij alle ketenpartners. Daarnaast wordt als voorbeeld gegeven om een preventieve maatregel te maken waarin slachtoffers van phishing en andere vormen van online fraude aan het woord komen om hun verhaal te doen over de impact die de oplichting op hen heeft gemaakt. Dat zou eventueel in een filmpje op Instagram kunnen worden geplaatst (P.13).

Er komen soortgelijke wensen naar voren vanuit de politie. Er zal eerst cijfermatig moeten worden aangetoond waar de criminaliteit plaatsvindt en door wie. Dat zal uit een politieonderzoek moeten blijken. Daarna kan prioriteit worden gesteld vanuit de politie en de andere ketenpartners om online fraude aan te pakken. Alle ketenpartners moeten een duidelijke taak krijgen bij de bestrijding van online fraude, zoals de gemeente, het jongerenwerk, maar ook ouders, scholen en banken. Verder wordt aangegeven dat er expertise moet zijn op ICT-gebied om deze criminaliteitsvorm goed aan te kunnen pakken (P.02; P.04; P.05).

Bij de meeste gemeenten heerst nog de discussie over hun rol bij de bestrijding van online fraude en andere vormen van cybercriminaliteit. Op dit moment kan er al wel preventief worden gehandeld door bijvoorbeeld te informeren in huis-aan-huisbladen over online fraude (P.09). Het zal daarom van belang worden om afstemming tussen alle ketenpartners te krijgen over hun taken, verantwoordelijkheden en bevoegdheden op het gebied van online fraude. Dit zal als eerst duidelijk moeten worden voor alle partners. Het is daarnaast van groot belang om een duidelijk meldpunt voor online fraude te maken, zodat slachtoffers weten waar ze terecht kunnen. Het signaleren van verdachte jongeren moet bovendien niet alleen worden gedaan door (jeugd)agenten, maar ook door jongerenwerkers (P.07). Jongerenwerkers zijn immers ook de oren en ogen in de wijk. Verder is het van belang om een expertise te ontwikkelen op dit gebied bij gemeenten. Dan kan gedacht worden aan een eigen IT-afdeling per gemeente of een beleidsadviseur openbare orde en veiligheid met het thema cybercriminaliteit. Tot slot wordt nog aangegeven dat de samenwerking moet worden opgezocht met buurgemeenten:

> “[…] Veel van onze jeugdigen gaan bijvoorbeeld naar school in Emmen. Dus je hebt de regio ook nodig om zicht te houden op dit probleem. Ik zeg wel 'probleem’ maar misschien is het nog helemaal geen probleem. Dus ik denk wel dat we op het moment dat we dit prioriteit gaan geven dat we elkaar in die verbinding weten te vinden over dit onderwerp. […] Ja dat denk ik wel, want heel veel van onze jeugdigen gaan in Stadskanaal, Assen en Emmen naar school. Dat is waar onze jongeren heen gaan. […] Je kan als gemeente zelf een hele leuke campagne opzetten, maar veel van die communicatiestrategieën worden landelijk of regionaal ontwikkeld. Dat komt natuurlijk veel beter aan als je dat gezamenlijk met je buurgemeenten tegelijk inzet.

> Dat de school in Stadskanaal in week 3 een programma draait over fraude en dat Esdal College [Emmen] datzelfde programma draait in diezelfde week. Zodat ze er ook een gesprek over hebben op het moment dat ze hier in Borger voor de supermarkt staan." - P.06

Er zijn drie wensen die door verscheidene participanten naar voren zijn gebracht. Allereerst gaat het om de wens om een ICT-afdeling of een cybercrimeteam op te zetten bij de ketenpartners, zodat er meer kennis beschikbaar wordt om adequaat te kunnen handelen. De tweede wens gaat het over signaleren. De politie en het jongerenwerk moeten meer samenwerken om gezamenlijk een uitstekende informatiepositie te kunnen krijgen over de problematiek in de wijken. De derde wens gaat over afstemming tussen de ketenpartners. Er moet duidelijkheid worden geschapen over de bevoegdheden van alle betrokken partijen bij de integrale aanpak. Hierdoor kunnen de taken beter worden verdeeld over de ketenpartners.

5.4 Integrale aanpak

Sinds 2020 wordt nauwer samengewerkt tussen de gemeenten, politie en jongerenwerkers in de regio Zuidoost-Drenthe. In de gemeenten Emmen en Coevorden wordt op reguliere basis integraal samengewerkt tussen de ketenpartners. Dat betekent dat er vaker op lange termijn wordt gewerkt om bepaalde problematiek op te lossen in de gemeente. In de gemeente Borger-Odoorn wordt op incidentele basis samengewerkt tussen de gemeente, politie en jongerenwerkers. Hier valt winst te behalen. Over het algemeen worden de basisprincipes van een integrale samenwerking goed opgepakt, aldus de participanten. De gemeente pakt goed haar regierol op bij de samenwerking en leidt vaak de overleggen. De partners komen de gemaakte afspraken goed na. In de gevallen waarin dat niet gebeurt, wordt dat goed gecommuniceerd naar elkaar. Tussen de centrale overleggen door wordt dus onderling contact gehouden tussen verschillende betrokkenen. Hierdoor komt men niet tegenover onvoorziene omstandigheden te staan wanneer een evaluatiemoment plaatsvindt. Over en weer wordt informatie uitgewisseld, maar vanwege wet- en regelgeving kan dat niet volledig worden gedaan. Er mag slechts tot op zekere hoogte informatie worden uitgewisseld in verband met de privacy van de burgers. Tussen de gemeente en de politie is daarom een convenant opgesteld. Hierin staan duidelijke afspraken over het uitwisselen van informatie. De jongerenwerkers zijn hier geen onderdeel van, dus in dergelijke gevallen waarin contact wordt gezocht met jongerenwerk moet de Algemene Verordening Gegevensbescherming (AVG) in acht worden genomen.

In de gemeente Emmen wordt een BOB-structuur gehanteerd om te bepalen of het probleem een integrale aanpak behoeft:

> "Dan zou ik een BOB-structuur toepassen: beeld, oordeelsvorming, besluitvorming. Dus we gaan eerst samen een beeld vormen van wat het probleem is, hoe groot het probleem is, wie vindt het een probleem, wat maakt dit een probleem. Dan moet je vervolgens oordelen: hoe beoordelen we dit, hoe kan dit zo ontstaan en wat hebben we dan te doen. Om vervolgens naar een besluit te gaan: dit is de aanpak die we erop loslaten. Dit zouden we kunnen doen om het probleem op te lossen. Met elkaar. Dan eigenlijk iedereen binnen het eigen vakgebied." - P.03

Vanuit de beeldvorming moet dus worden bekeken hoe groot de aard en omvang van online fraude door jongeren in de regio Zuidoost Drenthe is. Hiervoor was al vastgesteld dat de politie een beter beeld heeft van de jonge daders dan de andere ketenpartners. Het is daarom

van belang dat de politie signalen van geldezels of andere jeugdige online fraudeurs krijgt. Aangezien de politie kampt met een groot personeelstekort kunnen agenten minder aanwezig zijn in de wijk. De mogelijke oplossing hiervoor is dat het jongerenwerk meer zal fungeren als waarnemer in de wijk. Zij kunnen mogelijk meer signaleren doordat zij dagelijks in de wijk te vinden zijn en contact hebben met de jongeren. Indien het mogelijk is zou bijvoorbeeld een convenant kunnen worden opgesteld waarin wordt vastgesteld welke informatie over jongeren mag worden gedeeld met de politie. Hierdoor zal een betere informatiepositie ontstaan en kunnen jongeren mogelijk vroegtijdig nog buiten het criminele circuit worden gehouden. De grootte van het probleem is op dit moment echter niet vastgesteld. Dat komt door de administratieve gang van zaken bij de politie. Desondanks komt vanuit de agenten in Zuidoost Drenthe naar voren dat jongeren in deze regio redelijk vaak worden opgepakt als geldezel.

Vanuit deze signalen van de politie is het mogelijk om een oordeel te kunnen vellen over online fraude door jongeren in deze regio. Hiertoe zijn de motieven van jongeren onderzocht. Veelal komt het financiële motief naar voren, maar er komt ook vaak naar voren dat jongeren zich niet bewust zijn van hun handelingen. Daar zou vanuit de preventieve kant op kunnen worden ingegaan tijdens een voorlichting of bijvoorbeeld een filmpje op Instagram. Vanuit de repressieve kant moet actiever worden opgetreden door de politie, zodat de pakkans verhoogd wordt. De lage pakkans is namelijk een ander motief dat naar voren komt uit de interviews. De motieven van jongeren om online fraude te plegen kunnen dus een rol spelen bij de keuze om interventies in te zetten.

Voordat interventies kunnen worden ingezet moeten de taken worden verdeeld. Het is namelijk inefficiënt wanneer verscheidene ketenpartners gaan inzetten op het preventieve vlak. Daarom moet sprake zijn van afstemming voordat het actieplan kan worden opgesteld. De politie en Boa’s hebben een rol bij het repressieve vlak. De politie en jongerenwerk moeten intensief samenwerken om signalen op te halen. Boa’s zouden mogelijk ook een rol kunnen hebben, mits de gemeenten het erover eens worden dat zij een taak hebben op het gebied van online fraude. De andere partners kunnen inzetten op het preventieve vlak. Dit alles wijst erop dat het coördinerende model wordt gehanteerd bij deze integrale aanpak. Er is niet louter sprake van informatie-uitwisseling, maar er wordt op een intensieve en systematische manier samengewerkt tussen de ketenpartners. Daarbij worden wel de eigen verantwoordelijkheden en bevoegdheden behouden, waardoor sprake is van coördinatie.

Kortom, er ligt al een redelijk goede basis voor een integrale aanpak. De regie wordt goed opgepakt door de gemeente. Verder zijn de doelen van de samenwerking duidelijk bij alle ketenpartners en wordt veel contact gehouden tussen de partners onderling. Dat contact gaat voornamelijk over bepaalde probleemjongeren in de wijken of over de uitgevoerde taken. Op het gebied van online fraude is er nog geen integrale aanpak ontwikkeld. Op dit moment wordt door alle drie de ketenpartners voornamelijk de focus gelegd op preventie. Voorbeelden van preventieve maatregelen zijn voorlichtingen over geldezels, de inzet van de mobiele-mediabus en gesprekken voeren met jongeren. Het is opvallend dat de ketenpartners niet weten wat de andere ketenpartners doen tegen online fraude. Er moet daarom meer afstemming tussen de ketenpartners plaatsvinden om online fraude zo efficiënt en goed mogelijk aan te kunnen pakken. Bovendien zou het beter zijn als één of twee ketenpartners zich richten op preventie. Het zou verstandig zijn als de politie zich meer kan richten op het repressieve vlak, omdat zij kampen met een personeelstekort. Een ICT-afdeling of

cybercrimeteam zou gewenst zijn om het repressieve vlak beter op te kunnen pakken. Het preventieve zou de politie dan achterwege kunnen laten. Een betere afstemming tussen de ketenpartners zal leiden tot een goede integrale samenwerking, waarbij zowel op preventief als repressief vlak geacteerd kan worden door de ketenpartners.

H6 Conclusie en discussie

6.1 Beantwoording van de onderzoeksvraag

In dit onderzoek is beschreven hoe een integrale aanpak voor online fraude door jongeren kan worden ingevuld door de politie, gemeenten en jongerenwerkers in de regio Zuidoost Drenthe. De daarbij behorende onderzoeksvraag luidt als volgt: “Hoe kan een integrale aanpak voor online fraude door jongeren worden opgezet door politie, gemeente en jongerenwerkers in de regio Zuidoost Drenthe?". Dit is gedaan middels het afnemen van interviews. Aan de hand van literatuur zijn vijf deelvragen opgesteld.

De eerste deelvraag is geformuleerd om te bepalen of er op dit moment al prioriteit moet worden gegeven aan online fraude in de regio Zuidoost Drenthe. Er is naar voren gekomen dat veel betrokkenen geen weet hebben van de omvang van daderschap van jongeren met betrekking tot online fraude. Zij waren echter wel op de hoogte van slachtoffers in de regio, dus er is zeker sprake van een probleem in de regio Zuidoost Drenthe. Binnen de politie was meer bekend over het aantal jonge geldezels en online fraudeurs in Zuidoost Drenthe. Zij hebben al een beter beeld van de aard en omvang hiervan, maar hebben dit (nog) niet gedeeld met de ketenpartners. Dit zouden zij goed in kaart moeten brengen en vervolgens moeten delen om ervoor te zorgen dat de andere partners ook op de hoogte zijn van de omvang van de problematiek. Aan de hand daarvan moet worden bepaald of prioriteit gewenst is om deze problematiek aan te kunnen pakken. Uit een eerder onderzoek blijkt dat er een gat is tussen de daadwerkelijke aantallen en de geregistreerde cijfers van daders van online fraude (Levi, 2017a). Er bestaat een error marge, waarmee rekening moet worden gehouden bij de prioritering.

Nadat prioriteit is vastgesteld kan een integrale aanpak worden opgesteld. Vanuit de literatuur wordt een algemeen kader geschetst voor een integrale samenwerking tussen verschillende ketenpartners. Samenwerkingen kunnen plaatsvinden op basis van vijf verschillende modellen (Johnston & Shearing, 2003). Voor deze integrale aanpak wordt de derde variant aangeraden: het coördinerende model. Dit houdt in dat alle ketenpartners binnen hun eigen bevoegdheden en taken handelen, maar dat wel sprake zal zijn van een intensieve en integrale samenwerking. Er moet niet alleen informatie met elkaar worden gedeeld, maar er zal ook actief moeten worden bijeengekomen om de stand van zaken te bespreken. Dit moet structureel gebeuren, zodat de snelle ontwikkelingen op het gebied van online fraude worden bijgehouden.

Een goed functionerende integrale aanpak bestaat uit vijf elementen (Buirma, 2021): onderlinge afhankelijkheid van de ketenpartners, financiële middelen en capaciteit, gezamenlijke percepties over de juiste aanpak, onderling vertrouwen en leiderschap. De meeste basisprincipes worden grotendeels al vervuld bij bestaande integrale samenwerkingen: de gezamenlijke percepties stemmen overeen, onderling vertrouwen en leiderschap. De politie signaleert problematiek en deelt deze informatie met de ketenpartners. Vanuit hier kan een integrale samenwerking worden opgesteld, mits de problematiek prioriteit krijgt vanuit alle ketenpartners. Vervolgens wordt een doelstelling geformuleerd die alle betrokkenen nastreven bij de uitvoering van de opgelegde taken. Over het algemeen is tussentijds veel onderling contact om informatie te kunnen delen. In sommige gevallen is dat echter niet het geval, omdat informatie niet te allen tijde mag en kan worden gedeeld conform

de AVG of onderliggende convenanten. In dergelijke gevallen wordt vaak wel telefonisch contact opgenomen met (bekende) partners. Dergelijke gesprekken berusten op onderling vertrouwen, maar indien er nieuwe collega's zijn ontbreekt dit onderling vertrouwen en wordt niet alle informatie gedeeld. Een knelpunt betreft het verloop van collega's, dus in sommige gevallen ontbreekt onderling vertrouwen. Het is overigens ook opvallend dat alle betrokkenen aangeven dat er goed onderling contact is, maar ze eigenlijk niet weten hoe de ketenpartners online fraude aanpakken. Bij de afstemming tussen de ketenpartners valt dus nog winst te behalen door duidelijke afspraken te maken over de taken en bevoegdheden van de partners. De regie ligt bij de gemeente en daar wordt deze rol goed opgepakt, mits een integrale samenwerking op lange termijn nodig is. Het eerste en tweede element van een goede integrale samenwerking worden minder goed uitgevoerd in Zuidoost Drenthe. Er werd al verwacht dat middelen en capaciteit een knelpunt zouden zijn (Terpstra & Kouwenhoven, 2004). Dit blijkt ook zo te zijn in de praktijk. Bij overheidsinstanties wordt te weinig geld beschikbaar gemaakt om complexe problematiek, zoals online fraude, aan te kunnen pakken. Bovendien heerst een personeelstekort bij alle drie de ketenpartners. Men is zich vooral erg bewust van het personeelstekort bij de politie. Bij de andere ketenpartners lijkt het tekort nog te overzien te zijn. Hieruit blijkt dat er een gebrek is aan (financiële) middelen en capaciteit om dit probleem op te lossen. Dit heeft ook invloed op het element van afhankelijkheid. Doordat er te weinig personeel is, kan niet iedere samenwerking goed worden uitgevoerd. Als gevolg daarvan worden bijvoorbeeld cijfers over online fraude niet worden gedeeld of andere taken niet goed uitgevoerd. Dat leidt ertoe dat andere ketenpartners niet goed weten hoe online fraude op dit moment wordt bestreden. Andere knelpunten gaan over de afstemming met collega's over de bevoegdheden op het gebied van online fraude en knelpunten bij de organisaties zelf, zoals traagheid bij de gemeenten op het gebied van ICT-ontwikkelingen en de onregelmatigheid van het werk van de politie. Uit eerdere onderzoeken kwamen de volgende knelpunten naar voren: middelen en capaciteit (Terpstra, e.a., 2016), slechte informatie-uitwisseling (Terpstra & Kouwenhoven, 2004) en niet nakomen van gemaakte afspraken (Terpstra & Kouwenhoven, 2004). Er zijn nu specifieke knelpunten geformuleerd die onder deze algemene knelpunten kunnen worden geschaard. Financiële tekorten, personeelstekort, tijd, verloop van personeel en ziekteverzuim vallen onder het knelpunt 'middelen en capaciteit'. Onder het knelpunt 'slechte informatie-uitwisseling' zouden de volgende knelpunten in Zuidoost Drenthe kunnen worden geschaard: 'afstemming met ketenpartners' en 'het ontbreken van cijfers/data over online fraude'. De overige knelpunten ('afstand tussen politie en burgers', 'onregelmatigheid werk van de politie', 'traagheid bij de gemeente' en 'verschillen tussen gemeenten') zijn verbonden aan deze organisaties en kunnen niet onder een algemeen knelpunt worden geschaard. Daarom moet in het vervolg ook rekening worden gehouden met knelpunten die uniek zijn voor bepaalde ketenpartners.

Er zijn drie wensen verscheidene keren naar voren gekomen: het vormen van een ICT-afdeling of cybercrimeteam, signaleren door jongerenwerk en goede afstemming creëren. Met deze wensen is rekening gehouden bij het formuleren van de integrale aanpak. Allereerst moet de rol van de gemeente op het gebied van online fraude goed worden gedefinieerd. Hier zijn ze op dit moment al mee bezig. Vervolgens moet prioriteit worden gesteld. Dat kan worden gedaan door signalen vanuit het jongerenwerk en de politie over jongeren die online fraude plegen. Vervolgens moeten de andere ketenpartners worden ingelicht over de aard en omvang van het daderschap van de jonge geldezels en online fraudeurs in de regio Zuidoost Drenthe. Er zal dan een overleg moeten plaatsvinden waarin

alle ketenpartners aangeven welke taken en bevoegdheden zij hebben op het gebied van online fraude. Op deze manier kunnen zij afstemmen wie welke taken zal oppakken. Het repressieve zal moeten worden opgepakt door de politie door bijvoorbeeld een speciaal cybercrimeteam op te zetten in het basisteam Zuidoost Drenthe. Zij kunnen de complexe zaken dan oppakken nadat de agenten eerste signalen hebben gekregen van online fraude. De andere ketenpartners moeten bepalen welke preventieve maatregelen zij zullen nemen om online fraude te voorkomen. Het is in ieder geval aan te raden dat één ketenpartner zich zal bezighouden met het verzorgen van voorlichtingen, zodat er geen dubbel werk wordt gedaan. Het is overigens ook van belang dat ze onderling in contact blijven over de taakuitoefening. Dat zou bijvoorbeeld kunnen door wekelijks te telefoneren met elkaar over de stand van zaken. Maar er zou ook een structureel overleg kunnen worden ingepland waarin de uitvoering van de integrale aanpak wordt geëvalueerd. Gezien het personeelstekort bij de politie wordt het eerste voorstel aangeraden. Daarnaast zouden ze bijvoorbeeld een keer per drie of vier maanden bijeen kunnen komen om de effecten van de integrale aanpak na te gaan. Tot slot is het van belang dat de ketenpartners op de hoogte blijven van technologische ontwikkelingen, zodat ze niet achter de feiten aanlopen met de snelle ontwikkelingen die de online fraudeurs toepassen (Levi e.a., 2017b). De implementatie van deze aanbevelingen kan ertoe leiden dat online fraude die door jongeren wordt gepleegd in Zuidoost Drenthe wordt ingeperkt.

6.2 Beperkingen van het onderzoek

Dit onderzoek kent verschillende beperkingen die mogelijk de resultaten van het onderzoek hebben beïnvloed. Allereerst is het mogelijk dat de betrokken ketenpartners het probleem onderschatten. Op dit moment zijn er veel slachtoffers van phishing en andere vormen van online fraude, maar worden slechts weinig daders gearresteerd en veroordeeld. Er zullen echter meer daders zijn dan men nu in beeld heeft, waardoor sprake is van onderschatting van het aantal (jeugdige) daders van online fraude. Dit hebben de participanten zelf ook enkele keren aangegeven. Verder speelt altijd de vraag of de gevonden resultaten van een kwalitatief onderzoek zich daadwerkelijk voordoen in de praktijk. In principe kunnen kwalitatieve onderzoeken niet worden gegeneraliseerd naar een grotere populatie, waardoor de resultaten niet kunnen worden losgekoppeld van de context. Voor dit onderzoek zijn slechts 13 participanten geïnterviewd die allemaal te maken hebben met integrale samenwerkingen in Zuidoost Drenthe. Een van hen was werkzaam op de afdeling ‘jeugd’ in Coevorden, maar in de andere twee gemeenten zijn geen medewerkers van de afdeling ‘jeugd’ geïnterviewd die wel betrokken zijn bij integrale samenwerkingen betreffende jeugdproblematiek, zoals deze integrale aanpak. Naast deze drie ketenpartners zijn er vaak nog veel meer instanties betrokken bij integrale samenwerkingen, zoals bijvoorbeeld bureau HALT, het Openbaar Ministerie, Veiligthuis en jeugdinstellingen. Deze ketenpartners zijn niet geïnterviewd, waardoor niet alle betrokken partijen die mogelijk te maken zouden kunnen krijgen met deze aanbevelingen voor een integrale aanpak invloed hebben gehad op de totstandkoming hiervan.

De derde beperking gaat over de grote verschillen tussen de gemeenten onderling. In Coevorden en Emmen wordt veelvuldig samengewerkt door middel van integrale aanpakken, maar in Borger-Odoorn wordt dat in mindere mate gedaan. Zij werken voornamelijk samen op de korte termijn om een ad hoc probleem op te lossen. De basisprincipes van een integrale samenwerking zijn dus in verschillende mate geïmplementeerd door de drie gemeenten.

Bovendien zijn er andere samenstellingen van het aantal jeugdige inwoners en sociaaleconomische achtergronden in de drie gemeenten. Dit heeft invloed op het aantal jongeren die zich bezighouden met online fraude, waaruit ook blijkt dat de gemeenten onderling van elkaar verschillen. Met deze verschillen tussen de gemeenten zal rekening moeten worden gehouden bij de uitvoering van de integrale aanpak.

De vierde beperking betreft het selectie-effect van de participanten. De participanten zijn geselecteerd door middel van de sneeuwbalmethode. Participant 1 heeft een functie waardoor zij veel in contact is met ketenpartners van de politie. Vanuit deze contacten heb ik de participanten benaderd. Hierdoor is bijvoorbeeld geen contact gelegd met de coördinatoren van Andes en Sedna, terwijl zij juist betrokken zijn bij de overleggen met de ketenpartners. Er was echter wel een poging gedaan om contact met hen te krijgen, maar dat was niet gelukt. Er zijn jongerenwerkers vanuit de praktijk geïnterviewd die zoveel mogelijk hebben geprobeerd om antwoorden te formuleren op de vragen over de huidige overleggen. Een andere beperking betreft het zesde interview waarin twee participanten gelijktijdig zijn geïnterviewd. Participant 7 heeft mogelijk invloed gehad op de antwoorden van participant 6, andersom kan dat ook hebben plaatsgevonden. Er is toch voor gekozen om ze gelijktijdig te interviewen, omdat participant 6 in eerste instantie zou worden geïnterviewd en zij op dat moment slechts één week werkzaam was bij de gemeente Borger-Odoorn. Door participant 7 te betrekken bij het interview konden de ervaringen vanuit deze gemeente wel worden meegenomen.

De laatste beperking gaat over de betrouwbaarheid van het onderzoek. Een kwalitatief onderzoek is pas betrouwbaar als aan bepaalde vereisten is voldaan, waaronder het vereiste van geloofwaardigheid. Een van de vereisten van geloofwaardigheid is dat er verscheidene onderzoekers betrokken zijn geweest tijdens het verwerken van de data (Shenton, 2004). Het afnemen van interviews en het coderen van de interviews is door één onderzoeker gedaan (de schrijver van deze scriptie). Hierdoor is het mogelijk dat eigen ervaringen en meningen van de onderzoeker invloed hebben gehad op de resultaten. Dit komt doordat het interviewschema, de interviews en het coderen door een persoon is gedaan welke van tevoren literatuur had geraadpleegd over integrale samenwerkingen. Dit heeft mogelijk geleid tot beïnvloeding van het proces van dataverzameling en -verwerking. Ten tijde van het afnemen van de interviews en coderen heeft de onderzoeker altijd geprobeerd zo objectief mogelijk te handelen. Dat is bijvoorbeeld gedaan door te vragen naar de bedoeling van participanten met bepaalde uitspraken en het meermaals coderen van de transcripten. Verder is aan de vereisten van geloofwaardigheid en de overige drie concepten om een betrouwbaar onderzoek uit te voeren voldaan. Hierdoor is het aannemelijk dat een andere onderzoeker die exact dezelfde methode gebruikt voor het onderzoek in Zuidoost Drenthe tot vergelijkbare resultaten komt. De bespreking van deze beperkingen van het onderzoek moet bijdragen aan de overtuigingskracht van dit onderzoek.

6.3 Aanbevelingen

Aangezien online fraude een probleem is dat zich nog doorontwikkeld is het gewenst om vervolgonderzoek te doen naar een integrale aanpak om dit te bestrijden. Uit dit onderzoek is gebleken dat de basisprincipes van een integrale samenwerking redelijk goed worden toegepast. De basis voor een integrale samenwerking ligt er dus al. Voordat een integrale aanpak benodigd is moet eerst prioriteit zijn om het probleem aan te pakken. Daarom is er vervolgonderzoek gewenst naar de aard en omvang van online fraude door jongeren in

Zuidoost Drenthe. Dit zal dan moeten worden opgepakt door het basisteam van Zuidoost Drenthe, maar het jongerenwerk kan ook een rol spelen bij het signaleren van online fraude door jongeren. Zij zijn meer in de wijk, waardoor zij ook problematiek kunnen signaleren. Vanuit de bevindingen die hieruit voortvloeien, kan worden bepaald of deze integrale aanpak kan worden geïmplementeerd.

Ten tweede zou in de toekomst ook onderzoek kunnen worden gedaan naar een groter gebied. De daders van online fraude hoeven namelijk niet per se in hetzelfde gebied te wonen als het gebied waarin de slachtoffers woonachtig zijn. De onderzoeken zouden bijvoorbeeld door een district of in een eenheid kunnen worden uitgevoerd. Het district Drenthe omvat een groter gebied waarin de kans aannemelijker is dat er jonge daders zijn die zich bezighouden met online fraude. Het is dan echter wel lastiger om één aanpak te formuleren die geldt voor de politie, gemeenten en jongerenwerk. Dit komt doordat de werkwijzen van de gemeenten en jongerenwerk sterk van elkaar verschillen per regio. Dat blijkt ook al uit het huidige onderzoek. Een ander vervolgonderzoek zou zich mogelijk kunnen richten op een ander basisteam in Drenthe. Het zou dan kunnen gaan om het basisteam Noord-Drenthe of Zuidwest Drenthe. Dan zou exact hetzelfde onderzoek kunnen worden uitgevoerd in deze regio en kan een vergelijking worden gemaakt met het huidige onderzoek in Zuidoost Drenthe.

Een derde onderzoek dat in de toekomst kan worden uitgevoerd is een uitgebreidere variant van het huidige onderzoek. Bij dat onderzoek kunnen dan meer ketenpartners worden betrokken. Uit het huidige onderzoek is al gebleken dat bureau HALT bijvoorbeeld ook voorlichtingen geeft over geldezels. Daarom zou het ook verstandig zijn om bureau HALT bij een integrale aanpak te betrekken. Evenals andere instanties die mogelijk een rol kunnen spelen bij de integrale aanpak om online fraude te bestrijden, zoals banken en het Openbaar Ministerie.

Op dit moment is er nog geen integrale aanpak voor online fraude door jongeren geïmplementeerd, maar gezien de hoge slachtofferaantallen zou dat wel moeten gebeuren. Bovendien heeft een veroordeling wegens online fraude grote gevolgen, zoals het niet kunnen openen van een bankrekening bij (Nederlandse) banken gedurende een periode van vijf jaar. Het is daarom van belang om jongeren te informeren en beschermen tegen deze vorm van criminaliteit. De politie, maar ook andere ketenpartners, hebben daar een belangrijke rol bij. Het uiteindelijke doel is namelijk om te voorkomen dat jongeren verder verstrikt raken in het (cyber)criminele circuit. Daarin heeft de politie een belangrijke rol:

> “De jeugd is de toekomst. Dus we moeten heel zorgvuldig omgaan met onze jeugd en als je de jeugd een goede toekomst kunt bieden dan zul je de jeugd ook moeten vrijwaren van allerlei negatieve dingen. En daar moeten wij [politie] toch een beetje voor zorgen.” - P.02

Literatuurlijst

Akerhof, G.A. (1970). The market for “lemons”: quality uncertainty and the market mechanism. *Quaterly Journal of Economics 84* (3), 488–500.

Akkermans, M., Kloorsteman, R., Moons, E., Reep, C. & Tummers-van der Aa, M. (2022, maart). Veiligheidsmonitor 2021. 5. Online criminaliteit. [CBS publicatie]. Geraadpleegd van https://www.cbs.nl/nl-nl/longread/rapportages/2022/veiligheidsmonitor-2021/5-online-criminaliteit

Alseadoon, I. M. A. (2014). *The impact of users' characteristics on their ability to detect phishing emails.* Brisbane: Queensland University of Technology.

Beerthuizen, M. G. C. J., Sipma, T. & van der Laan, A. M. (2020). Aard en omvang van dader- en slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland. *WODC Cahier 2020-15*. Geraadpleegd van: https://repository.wodc.nl/bitstream/handle/20.500.12832/253/Cahier_2020_15_2921ab_Volledige_tekst_tcm28-462221.pdf?sequence=2&isAllowed=y

Bekkers, L., Schiks, J. & Leukfeldt, R. (2020, oktober). Naar een interventie tegen geldezels: een pilot in de gemeente Haarlem. De Haagse Hogeschool. Geraadpleegd van: https://hetccv.nl/fileadmin/Afbeeldingen/Onderwerpen/Cybercrime/Naar_een_interventie_tegen_geldezels_Een_pilot_in_de_gemeente_Haarlem.pdf

Bloem, B. (2017). Horizontale fraude in kaart. *Het Tijdschrift voor de Politie, 7* (3). Geraadpleegd van: https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/pdf/88976.pdf

Borwell, J., Jansen, J. & Stol, W. (2018a). Human factors leading to online fraud victimisation: Literature review and exploring the role of personality traits. In J. McAlaney, L.A. Frumkin and V. Benson (eds), *Psychological and behavioral examinations in cyber security* (pp. 26-45). IGI Global.

Borwell, J., Jansen, J. & Stol, W. (2018b). Persoonlijkheidskenmerken van e-fraudeslachtoffers. *Tijdschrift voor Veiligheid, 17*, 54-65. DOI:10.5553/TvV/187279482018017102005

Bowker, A. L. M. A. & Fielding, E. W. (1999, december). Juveniles and Computers: Should We Be Concerned? Federal Probation, 63(2), 40-43,

Bowker, A. L. M. A. & Ott, J. E. (2000, december). The Advent of the Computer Delinquent. *FBI Law Enforcement Bulletin, 69* (12), 7–11.

Braun, V. & Clarke, V. (2006). Thematic analysis. *American Psycological Association Handbook of Research Methods in Psychology 2*, 57-71. DOI:10.1037/13620-004

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S. & Díaz-Castaño, N., (2020). ‘Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK’, *European Societies 23* (1), p. 47-59. https://doi.org/10.1080/14616696.2020.1804973

Buirma, T., (2021, augustus). 1 + 1 = 3. Een onderzoek naar de invloed van samenwerking tussen de gemeente en politie op de effectiviteit van de aanpak van ondermijnende criminaliteit in Zoetermeer. [Scriptie, Erasmus Universiteit Rotterdam]. Geraadpleegd van https://thesis.eur.nl/pub/58580/

Centraal Bureau voor de Statistiek [CBS] (2019, oktober). Bezorgdheid over internetveiligheid maakt mensen alert. Geraadpleegd op 8 maart 2022 van https://www.cbs.nl/nl-nl/nieuws/2019/44/bezorgdheid-over-internetveiligheid-maakt-mensen-alert

Centraal Bureau voor de Statistiek [CBS] (2022a, maart). *Veiligheidsmonitor 2021. 3. Veiligheidsbeleving*. Geraadpleegd van https://www.cbs.nl/nl-nl/longread/rapportages/2022/veiligheidsmonitor-2021/3-veiligheidsbeleving

Centraal Bureau voor de Statistiek [CBS] (2022b, maart). Sociale veiligheid; persoonskenmerken [StatLine]. Geraadpleegd op 14 april 2022 van https://www.cbs.nl/nl-nl/cijfers/detail/85147NED

Centrum voor Criminaliteitspreventie en Veiligheid (2020, november) Actieplan Wapens en Jongeren. Geraadpleegd op 14 april 2022 van https://hetccv.nl/fileadmin/Bestanden/Nieuws/2016-1/Actieplan_Wapens_en_Jongeren_vs_DigiJust_2__002_.pdf

Centrum voor Criminaliteitspreventie en Veiligheid (z.d. a). Cybergame framed. Geraadpleegd op 22 maart 2022 van https://hetccv.nl/onderwerpen/cybercrime/praktijkvoorbeelden/cybergame-framed/

Centrum voor Criminaliteitspreventie en Veiligheid (z.d. b). Groepsscan voor de aanpak van problematische jeugdgroepen en groepsgedrag. Geraadpleegd op 11 april 2022 van https://hetccv.nl/onderwerpen/high-impact-crimes/hic-preventiewijzer/geweld/groepsscan-voor-de-aanpak-van-problematische-jeugdgroepen-en-groepsgedrag/

Clarke, R.V. & Cornish, D. B. (1985) Modeling offenders' decisions: A framework for research and policy. *Crime Justice 6*, 147–185. https://doi.org/10.1086/449106

Clarke, R. V. & Tilley, N. (2010, maart). *Situational Prevention of Organised Crimes*, 172-190. Willan Publishing. Milton.

Cohen, L.E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review 44*, 588-608.

Cox, E. B., Zhu, Q. & Balcetis, E. (2020, mei). Stuck on a phishing lure: differential use of base rates in self and social judgments of susceptibility to cyber risk. *Comprehensive Results in Social Psychology*, *4*(1), 25–52. https://doi-org.proxy-ub.rug.nl/10.1080/23743603.2020.1756240

Cross, C. & Richards, K. (2015). The "ACA Effect": Examining How Current Affairs Programs Shape Victim Understandings and Responses to Online Fraud. *Current Issues in Criminal Justice*, *27*(2), 163–178. https://doi-org.proxy-ub.rug.nl/10.1080/10345329.2015.12036039

Custers, B. H. M., Pool, R. L. D. & Cornelisse, R. (2019, november). Banking malware and the laundering of its profits. *European Journal of Criminology*, *16* (6), 728-745. https://doi-org.proxy-ub.rug.nl/10.1177/1477370818788007

Dehghanniri, H. & Borrion, H. (2021, juli). Crime scripting: A systematic review. *European Journal of Criminology*, *18*(4), 504–525. https://doi-org.proxy-ub.rug.nl/10.1177/1477370819850943

Dijkstra, J. K. & Veenstra, R. (2019). Jongeren, leeftijdsgenoten en criminaliteit. *Tijdschrift voor Criminologie, 61,* 280-292.

Drew, J. M. & Farrell, L. (2018). Online victimization risk and self-protective strategies: developing police-led cyber fraud prevention programs. *Police Practice & Research*, *19*(6), 537–549. https://doi-org.proxy-ub.rug.nl/10.1080/15614263.2018.1507890

Ekblom, P. & Gill, M. (2016) Rewriting the script: Cross-disciplinary exploration and conceptual consolidation of the procedural analysis of crime. *European Journal on Criminal Policy and Research, 21*(2), 319–339.

Felson, F., Jiang, S. & Xu, Y. (2020, maart). Routine activity effects of the Covid-19 pandemic on burglary in Detroit, March, 2020. *Crime Science 10*. https://doi.org/ 10.1186/s40163-020-00120-x

Friele, R. D., Bruning, M. R., Bastiaansen, I. L. W., De Boer, R., Bucx, A. J. E. H., De Groot, J. F., Pehlivan, T., Rutjes, L., Sondeijker, F., Yperen, T. A. & Hageraats, R. (2018, januari). Eerste evaluatie Jeugdwet: na de transitie nu de transformatie. *Reeks evaluatie wetgeving 43,* 381-385. Den Haag, ZonMW. Geraadpleegd van: https://www.nji.nl/sites/default/files/2021-06/Rapport-Eerste-evaluatie-Jeugdwet.pdf

Gerechtshof Amsterdam (2021, juli). ECLI:NL:GHAMS:2021:2010. Geraadpleegd op 1 maart 2022 van https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHAMS:2021:2010&showbutton=true&keyword=whatsappfraude

Graham, R. & Triplett, R. (2017, december). Capable Guardians in the Digital Environment: The Role of Digital Literacy in Reducing Phishing Victimization. *Deviant Behavior*, *38*(12), 1371–1382. https://doi.org/10.1080/01639625.2016.1254980

Hennink, M., Hutter, I. & Bailey, A., (2010). *Qualitative Research Methods* (1e editie). Sage Publications Inc.

Hirsch Ballin, M. F. H. (2019). 'Overbrugging van procedurele breuklijnen bij een integrale aanpak van criminaliteit', *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 163-172. doi:10.5553/TBSenH/229567002019005003007

Hulsse, R. (2017, oktober). The Money Mule: Its Discursive Construction and the Implications. *Vanderbilt Journal of Transnational Law 50* (4). Geraadpleegd van: https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1145&context=vjtl

Hutchings, A. & Hayes, H. (2009, maart). Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the "Net"? *Current Issues in Criminal Justice, 20*(3), 433–451. https://doi-org.proxy-ub.rug.nl/10.1080/10345329.2009.12035821

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

Huygen, A. & De Meere, F. (2008, april). De invloed en effecten van sociale samenhang. Verslag van een literatuurverkenning. Verwey-Jonker Instituut. Geraadpleegd van: https://www.verwey-jonker.nl/doc/vitaliteit/De%20invloed%20en%20effecten%20van%20sociale%20samenhang_1169.pdf

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime & Justice*, *47*, 44–57. https://doi-org.proxy-ub.rug.nl/10.1016/j.ijlcj.2016.07.002

Jansen, J. & Leukfeldt, R. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice and Criminology*, *6(*2), 205-228.

Johnston, L. & Shearing, C. (2003). *Governing Security. Explorations in policing and justice*. London/NewYork: Routledge.

Kerstens, J. & Jansen, J. (2016). The Victim–Perpetrator Overlap in Financial Cybercrime: Evidence and Reflection on the Overlap of Youth's On-Line Victimization and Perpetration. *Deviant Behavior*, *37*(5), 585–600. https://doi-org.proxy-ub.rug.nl/10.1080/01639625.2015.1060796

Koops, E. J. (2014). Cybercriminaliteit. In S. van der Hof, A. R. Lodder, & G. J. Zwenne (Eds.), *Recht en computer, zesde druk* (pp. 213-241). (Recht en praktijk: Informatie- en communicatietechnologie; No. 4). Kluwer.

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 & Justice*, *42*(5), 569–581. https://doi-org.proxy-ub.rug.nl/10.1080/0735648X.2019.1692420

Kruisbergen, E., Haas, M., van Es, L. & Snijders, J. (2021, september). De pandemie als criminologisch experiment. De ontwikkeling van de criminaliteit tijdens een jaar coronamaatregelen. *Justitiële verkenningen 47* (3). doi: 10.5553/JV/016758502021047003002

Lastdrager, E. E. H. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science, 3* (9), 1–6.

Leukfeldt, E.R., (2014, december). Cybercrime and social ties. *Trends in Organised Crime 17*, 231–249. https://doi.org/10.1007/s12117-014-9229-5

Leukfeldt, E., Kleemans, E. & Stol, W. (2017a, februari). A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists. *Crime, Law & 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, mei). Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and

Malware Networks. *British Journal of Criminology*, *57* (3), 704–722. https://doi.org/10.1093/bjc/azw009

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

Leukfeldt, E., Kleemans, E. & Stol, W. (2017d). A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists. *Crime, Law & Social Change*, *67*(1), 21–37. https://doi-org.proxy-ub.rug.nl/10.1007/s10611-016-9662-2

Leukfeldt, E. R. & Kleemans, E. R. (2019). Cybercrime, money mules and situational crime prevention: Recruitment, motives and involvement mechanisms. In S. Hufnagel & A. Moiseienko (Eds.), *Criminal Networks and Law Enforcement: Global Perspectives on Illegal Enterprise* (pp. 75-89). Routledge.

Leukfeldt, E. R. & Roks, R. A. (2020, april). Cybercrimes on the Streets of the Netherlands?An Exploraton of the Intersection of Cybercrimes and Street Crimes. *Deviant Behavior 42* (11). https://doi.org/10.1080/01639625.2020.1755587

Levi, M. (2017a). Assessing the trends, scale and nature of economic cybercrimes: overview and Issues. *Crime, Law & Social Change*, *67*(1), 3–20. https://doi-org.proxy-ub.rug.nl/10.1007/s10611-016-9645-3

Levi, M., Doig, A., Gundur, R., Wall, D. & Williams, M. (2017b). Cyberfraud and the implications for effective risk-based responses: themes from UK research. *Crime, Law & Social Change*, *67*(1), 77–96. https://doi-org.proxy-ub.rug.nl/10.1007/s10611-016-9648-0

Loggen, J. & Leukfeldt, E. R. (2022, februari). Unraveling the crime scripts of phishing networks: an analysis of 45 court cases in the Netherlands. *Trends in organised crime 25*. https://doi.org/10.1007/s12117-022-09448-z

Macdonald, M. & Frank, R. (2017). Shuffle Up and Deal: Use of a Capture–Recapture Method to Estimate the Size of Stolen Data Markets. *American Behavioral Scientist*, *61*(11), 1313–1340. https://doi-org.proxy-ub.rug.nl/10.1177/0002764217734262

Maimon, D., Santos, M. & Park, Y. (2019). Online deception and situations conducive to the progression of non-payment fraud. *Journal of Crime & Justice*, *42*(5), 516–535. https://doi-org.proxy-ub.rug.nl/10.1080/0735648X.2019.1691857

Moffitt, T. E. (1993). Adolescence-limited and life-course-persistent antisocial behavior: A developmental taxonomy. *Psychological Review, 100*, 674-701.

Nederlands Jeugdinstituut, (z.d.). Transformatie jeugdhulp: Jeugdwet. Geraadpleegd op 4 maart 2022 van: https://www.nji.nl/transformatie-jeugdhulp/jeugdwet

NOS, Edwin Feldmann (2022, januari). Fraudehelpdesk ziet stijging van aantal meldingen over cybercriminaliteit. Geraadpleegd op 28 februari 2022 van https://www.nu.nl/tech/6181243/fraudehelpdesk-ziet-stijging-van-aantal-meldingen-over-cybercriminaliteit.html?_ga=2.163833791.1841654067.1646048197-1869796389.1635428663

Openbaar Ministerie (2021, augustus). Twee medeverdachten grote cybercrime-zaak Noord-Nederland aangehouden wegens betrokkenheid witwassen cryptovaluta. Geraadpleegd op 4 maart 2022 van https://www.om.nl/onderwerpen/cybercrime/nieuws/2021/08/27/twee-medeverdachten-grote-cybercrime-zaak-noord-nederland-aangehouden-vanwege-betrokkenheid-witwassen-cryptovaluta

Openbaar Ministerie, (z.d.). Fraude. Geraadpleegd op 21 februari 2022 van: https://www.om.nl/onderwerpen/fraude.

Peretti, K. K. (2008, januari). Data breaches: what the underground world of "carding" reveals. *Santa Clara Computer High-Technology Law Journal 25* (2), 345–414.

Politie.nl (2022, januari). Personeelstekort politie nog steeds hoog, neemt af na 2022. Geraadpleegd van https://www.politie.nl/nieuws/2022/januari/13/personeelstekort-politie-nog-steeds-hoog-neemt-af-na-2022.html

Politie.nl (z.d.). Wat is het Mobiel Media Lab? Geraadpleegd op 11 april 2022 van https://www.politie.nl/informatie/wat-is-het-mobiel-media-lab.html

Pröpper, I., Litjens, B. & Weststeijn, E. (2004, april). *Lokale regie uit macht of onmacht? Onderzoek naar de optimalisering van de gemeentelijke regiefunctie* [eindrapport]. Partners + Pröpper Bestuurskundig onderzoek en advies.

Rashkovski, D., Naumovski, V. & Naumovski, G. (2016). Cybercrime Tendencies and Legislation in the Republic of Macedonia. *European Journal on Criminal Policy & Research*, *22*(1), 127–151. https://doi-org.proxy-ub.rug.nl/10.1007/s10610-015-9277-7

Rathenau Instituut (2021). Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland (pp 95-126). Den Haag (auteurs: Huijstee, van, M., Nieuwenhuizen, W., Sanders, M., Masson, E., & Boheemen, van, P.).

Rechtbank Rotterdam (2022, februari). ECLI:NL:RBROT:2022:1388. Geraadpleegd op 1 maart 2022 van https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBROT:2022:1388&showbutton=true&keyword=whatsappfraude

Roks, R. A., Leukfeldt, E. R. & Densley, J. A. (2021). The Hybridization of Street Offending in the Netherlands. *British Journal of Criminology*, *61*(4), 926–945. https://doi-org.proxy-ub.rug.nl/10.1093/bjc/azaa091

Roose, H. & Meuleman, B., (2014). *Methodologie van de sociale wetenschappen: een inleiding* (1e editie). Academia Press.

Rooyakker, J. & Weulen Kranenbarg, M., (2020). Vissen met een nieuwe hengel: een onderzoek naar betaalverzoekfraude. *Justitiële verkenningen, 46* (2), 19-43. DOI: 10.5553/JV/016758502020046002003

Schilders, H. & Tops, P. (2016). Naar een meervoudige aanpak van ondermijning. Het *Tijdschrift voor de Politie 7* (16), 12-15. Geraadpleegd van https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/pdf/92747.pdf

Servaas, L., Weerman, F. & Fisher, T. (2021, maart). Risicoversterkende en -beschermende factoren voor crimineel gedrag: Een literatuuronderzoek naar de wetenschappelijke stand van zaken. [Erasmus University Rotterdam & Gemeente Rotterdam], 52-63. Geraadpleegd van: https://repub.eur.nl/pub/135248/Risico-versterkende-en-beschermende-factoren-voor-crimineel-gedrag-Servaas-Weerman-Fischer-2021-.pdf

Sheng, S., Lanyon, M. B., Kumaraguru, P. Cranor, L. & Downs, J. (2010, januari). 'Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions'. In: Mynatt, E. (red.). *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* New York: Association for Computing Machinery, p. 373-382. DOI:10.1145/1753326.1753383

Shenton, A. K. (2004). Strategies for Ensuring Trustworthiness in Qualitative Research Projects. *Education for Information, 22,* 63-75. https://doi.org/10.3233/EFI-2004-22201

Shun-Yung, K. W. & Huang, W. (2011). The Evolutional View of the Types of Identity Thefts and Online Frauds in the Era of the Internet. *Internet Journal of Criminology*, 1–21.

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

Terpstra, J. & Kouwenhoven, R. (2004). *Samenwerking en netwerken in de lokale veiligheidszorg* (IPIT Instituut voor Maatschappelijke Veiligheidsvraagstukken Universiteit Twente; Politie en Wetenschap). Uitgeverij Kerckebosch.

Terpstra, J., Van Duijneveldt, I.,Eikenaar, T. Havinga, T. &Van Stokkom, B. (2016, januari) Basisteams in de Nationale politie. Organisatie, taakuitvoering en gebiedsgebonden werk. *Politie & Wetenschap, 88*. Geraadpleegd van https://www.researchgate.net/publication/310447536_Basisteams_in_de_Nationale_Politie_Organisatie_taakuitvoering_en_gebiedsgebonden_werk

Van der Torre, E. & Tops, P. (2022). Groningse Praktijken. Een analyse van (de gemeentelijke aanpak van) ondermijning in de gemeente Groningen. Geraadpleegd op 14 april 2022 van https://hetccv.nl/fileadmin/Bestanden/Onderwerpen/Vastgoedcriminaliteit/Groningse-praktijken.pdf

Van der Wagen, W., Oerlemans, J. & Weulen Kranenbarg, M. (Eds.) (2020). *Basisboek Cybercriminaliteit: Een criminologisch overzicht voor studie en praktijk*. (Studieboeken criminologie & veiligheid). Boom Criminologie.

Van Grinsven, S. & Verwest, A. (2017). Vijf jaar aanpak Top600: waar staan we nu? *Justitiële Verkenningen, 43*, 127-141.

Weulen Kranenbarg, M., Van der Toolen, Y. & Weerman, F. (2022, januari). *Understanding cybercriminal behaviour among young people Results from a longitudinal network study among a relatively high-risk sample.* Amsterdam: VU University Amsterdam/Netherlands Institute for the Study of Crime and Law Enforcement.

Bijlage I: Interviewschema

Introductie

Goedemorgen/goedemiddag, ik ben Carmen van der Vinne en ik volg op dit moment de master sociologie van criminaliteit en veiligheid aan de universiteit in Groningen. Ter afronding van mijn master ben ik op dit moment stagiaire bij de politie in Emmen. Daar verricht ik onderzoek naar de samenwerking tussen politie, gemeente en jongerenwerkers op het gebied van online fraude door jongeren. Daarbij is het uiteindelijke doel dat er een (eerste richting naar een) integrale aanpak van online fraude door jongeren wordt gevormd. Hierbij wordt gestreefd naar een intensievere samenwerking tussen de eerdergenoemde ketenpartners van de politie.

Ethische principes

Allereerst moet ik u vragen of u toestemming geeft om de verkregen informatie uit dit interview te verwerken in mijn scriptie. Dat betekent dat mijn begeleider en referent het interview kunnen beluisteren. Buiten de studie om zullen de samenwerkingspartners, de gemeente en politie, kennisnemen van het eindwerkstuk, maar niet van de opnames. Uw gegevens blijven anoniem. Dit interview zal ongeveer een half uur duren en ik zal het opnemen zodat ik hier later aantekeningen van kan maken. De opname is nodig om de verkregen informatie te kunnen transcriberen en onderzoeken. Heeft u bezwaar tegen het opnemen van het interview? U kunt nu nog vrijwillig afzien van het onderzoek als dit u mogelijk schade zou kunnen toerekenen.

Heeft u verder nog vragen voordat we aan het interview beginnen?

Achtergrondinformatie

Naam

Functie

Opleiding

Relatie tot andere samenwerkingspartners

Interviewvragen:

Introducerende vragen

1. Wat is uw functie binnen de politie/gemeente/jongerenwerk?
- Probe: Wat houdt dat precies in?
2. Wat zijn uw dagelijkse taken?
3. Wat verbindt u met jeugd- en/of cybercriminaliteit?

Hoofdvragen

4. Hoe is uw staat van kennis omtrent jongeren die online fraude plegen in uw regio?

- Probe: De aard; omvang; gevolgen voor slachtoffers; motieven jongeren; precieze rol jongeren.

5. Hoe gaat u hier op dit moment mee om?

- Probe: Preventief of repressief; actief of passief; focus.

6. Hoe gaan andere samenwerkingspartners hiermee om?

- Probe: Gemeente; politie; jongerenwerkers.

7. Hoe ziet de huidige samenwerking tussen de verschillende samenwerkingspartners eruit?

- Actief; (gezamenlijke) doelen; uitvoering; regierol; veel/weinig; formele afspraken; informatie-uitwisseling.

8. Wat zijn de sterke en zwakke punten in de samenwerking?
9. Hoe zou dit kunnen worden veranderd?
10. Hoe ziet een ideale aanpak van online fraude door jongeren er volgens u uit?

Afsluitende vragen

11. Hoe ziet de samenwerking tussen politie, gemeenten en jongerenwerkers er over vijf jaar uit?
12. Zijn er nog belangrijke zaken onbesproken gebleven?

<u>Afsluiting</u>

Bedankt voor uw tijd. Ik zal binnenkort nog contact met u opnemen zodat u het getranscribeerde interview nog kunt nalezen en eventueel kunt voorzien van opmerkingen.

Bijlage II: Codeboek

Thema	Code	Strategie	Beschrijving	Voorbeeld
Beleid	Aantal keer overleg	Inductief	De participant geeft aan hoe vaak een overleg moet plaatsvinden.	'Dan zou het vaker moeten, maar dat zou naast het structurele overleg moeten. Het structurele overleg zou een keer in de twee maanden moeten en mocht je problematiek zien dan moet het heel makkelijk te schakelen zijn om bij elkaar te komen, omdat het een ad hoc probleem is.'
	BOB Structuur	Inductief	De participant geeft aan hoe beleid moet zou kunnen worden geformuleerd.	'Dan zou ik een BOB-structuur toepassen: beeld, oordeelsvorming en besluitvorming. Dus we gaan eerst samen een beeld vormen van wat het probleem is, hoe groot het probleem is, wie vindt het een probleem, wat maakt dit een probleem. Dan moet je vervolgens oordelen: hoe beoordelen we dit, hoe kan dit zo ontstaan en wat hebben we

				dan te doen. Vervolgens echt naar een besluit te gaan: dit is de aanpak die we erop loslaten. Dit zouden we kunnen doen om het probleem op te lossen. Met elkaar. Dan eigenlijk iedereen binnen het eigen vakgebied.’
	Communicatie	Deductief	De participant geeft aan hoe de communicatie tussen de ketenpartners verloopt.	‘Als het nodig is dan weten we elkaar te vinden. De lijntjes zijn dan kort. We luisteren goed naar elkaar, want we nemen echt dingen van elkaar aan.’
	Consequenties	Inductief	De participant geeft aan dat jongeren moeten weten welke gevolgen voor henzelf zijn als zij worden gepakt wegens online fraude.	‘De jongeren zien ook vaak de consequenties niet in. Dus dat is vaak het probleem.’
	Convenant	Inductief	De participant geeft aan dat een convenant nodig is om vrijelijk informatie te kunnen delen met elkaar.	‘Nee, niet alles. Sociaal domein kan wel delen dat ze een inzet hebben op iemand, maar dat kan vaak niet in detail op wie ze dan inzetten. Dat doen we wel eens als het over groepen

				gaat dan wordt er via het zorg- en veiligheidshuis een overleg gepland waaronder een convenant ligt. Daardoor kan je dit informatie wel met elkaar delen. Dat is minder lastig dan het moment waarop het over individuele casussen gaat.’
	Eigen doelen organisatie	Inductief	De participant geeft aan welke doelen zijn/haar werkgever heeft bij een samenwerking tussen de ketenpartners.	‘En dan kijk je naar de daadwerkelijke taak die je hebt. Nou, welke taak heeft de politie? De politie heeft als taak natuurlijk het handhaven van de openbare orde, maar we hebben ook het signaleren en adviseren. Dat zijn hele belangrijke taken van ons. Dus op het moment dat we iets signaleren dan kunnen we daar ook adviezen in geven. Als daadwerkelijk strafrecht vervolgd moet worden is dat weer een taak voor ons. Zo heb je dus gezamenlijk één

				doel en zou je moeten kijken naar wat daadwerkelijk je taak is. Wat is de taak van de gemeente? Wat is de taak van het OM? Zo zou je het eigenlijk weg moeten zetten.'
	Einddoel	Deductief	De participant geeft een voorbeeld van een einddoel van een integrale aanpak.	'En wat doe je dan? Je doel is uiteindelijk natuurlijk om het te doen laten stoppen. Dat zou je doel zijn. Tenminste dat is in mijn gedachte het doel. Maar dan moet je in het plan van aanpak kijken en dan moet je met elkaar kijken wat het doel zou moeten zijn. Nou je wil er met elkaar voor zorgen dat er consequenties aan hangen en je wil ervoor zorgen dat de minderjarige niet nog dieper in de problemen komt. Ik denk dat dat uiteindelijk je doel is.'
	Expertise cybercrime	Inductief	De participant geeft aan dat er behoefte is aan expertise omtrent cybercriminalite	'Misschien dat er dan intern ook wel specialisten zijn op dat vlak. Zodat we intern

			it bij de organisaties.	ook weten bij wie we moeten zijn. Diegene zal ook wel de lijntjes naar buiten weten. Dat zou ook nog goed kunnen.'
	Gemaakte afspraken	Deductief	De participant geeft aan welke afspraken er worden gemaakt tijdens een overleg.	'Als we de actiepunten gaan bespreken dan zit iedereen er wel bij. Op het moment dat we het terugkoppelmoment hebben dan zit iedereen er ook bij. Maar als we elkaar in de tussentijd op de hoogte moeten houden dan gebeurt dat bij de gemeente via mij, ambtenaar openbare orde en veiligheid, en bij de politie door de operationeel expert.'
	ICT-afdeling	Inductief	De participant geeft aan dat een ICT-afdeling gewenst is binnen de organisatie.	'Als het gewenst zou zijn dan zou hier een gigantisch team zitten waarbij ik de zaak afgeef en zij er direct mee aan de slag gaan. Die alles opvragen dat nodig is qua bevoegdheden en daar direct als team mee bezig gaan. Dat

				ze dan direct op zoek kunnen naar die daders, direct oppakken en ons kunnen coachen waar we op moeten letten waar we mee bezig kunnen. Zodat we direct achter die gasten aan kunnen om ze te stoppen.’
	Informatie delen	Deductief	De participant geeft aan hoe informatie wordt gedeeld met de ketenpartners.	‘Dat bestaat uit het uitwisselen van informatie naar elkaar. Dat is wel vaak de positieve kant.’
	Kennis over andere ketenpartners	Inductief	De participant geeft aan wat ze weten over de werkzaamheden van de andere ketenpartners.	‘Nee, de politie post af en toe iets op Instagram. Ik weet verder niet wat ze doen. Van de gemeente weet ik dat ook niet.’
	Onderling contact	Inductief	De participant geeft aan hoe het onderling contact, buiten de overleggen om, tussen de ketenpartners is.	‘Kijk, er zijn wel korte lijntjes als het gaat om contact met de wijkagent. Het is wel vrij toegankelijk om contact op te nemen [...].’
	Openbare orde en veiligheid	Inductief	De participant geeft aan dat de vraag heerst of de gemeente wel een rol heeft bij cybercriminaliteit.	‘Ja, dat staat ook wel op de agenda. Dat staat op de agenda, omdat de vraag speelt of gemeentes hierin een rol spelen. Dit komt omdat het nu erg veel

				voorkomt. We staan nog aan de beginfase.'
	Overleg	Deductief	De participant vertelt over de overleggen met ketenpartners.	'We hebben verschillende overleggen per gebied. Die is eens in de vier of zes week. Dan komen we met verschillende netwerkpartners samen, dus de politie, Boa's, de gemeente, wij en vaak ook nog een collega van Sedna.'
	Prioriteiten bij partners	Inductief	De participant geeft aan wanneer een bepaald probleem prioriteit krijgt bij de ketenpartners.	'Op het moment dat we weten hoe groot de omvang is en we de impact daarvan weten dan zouden we dat wellicht moeten doen. Het is altijd een afweging welk probleem prioriteit heeft. Het zou ons wel weer alert kunnen maken.'
	Regie	Deductief	De participant geeft aan dat de regierol bij de gemeente ligt.	'Die regietaak bij de gemeente is logisch, die pak ik dan ook. Dat is op zich ook goed. Wij hebben daarin het stukje regie en dat betekent niet dat we alles doen, maar we zorgen er wel voor dat we gezamenlijk een beeld vormen

				en gezamenlijk een oplossing vinden.’
	Wensen over toekomstig beleid	Inductief	De participant vertelt welke wensen hij/zij heeft over de invulling van de integrale aanpak van online fraude.	‘Dan zou je met meer mensen onderzoek kunnen draaien, zodat het minder lang duurt. Nu duurt het best wel lang voordat alles is uitgepluisd. Dat is ook gewoon heel veel werk om te doen. Dan zit je er bovenop. Nu is het meer op de lange termijn. Dan zou je een veel kortere klap kunnen maken. Nu speelt het al dat ze heel veel tijd hebben gehad om verscheidene strafbare feiten te plegen. Je moet ervoor zorgen dat je er eerder bij bent, zodat je er eerder zicht op hebt en je eerder onderzoek kan doen.’
	Wetten	Deductief	De participant geeft aan dat de partners zich aan bepaalde wetten moeten houden.	‘De Wet op de Privacy daar moeten we ons aan houden.’
Bestrijdingsmiddelen	Beveiliging bij banken	Inductief	De participant geeft aan dat	‘Als je helemaal een ideale

			banken ook een rol zouden kunnen hebben bij de integrale aanpak.	wereld mag schetsen dan heb je een goede beveiliging vanuit banken.'
	Bijeenkomst naar aanleiding van problematiek	Inductief	De participant geeft een voorbeeld waarmee jeugdproblematiek wordt bestreden.	'Zij [gemeente] hebben die bijeenkomst eerst georganiseerd, maar op een gegeven moment kwamen er echt aangiftes binnen van bepaalde jongens tegen bepaalde jongens. Dat wij dachten dat we niet de juiste mensen hadden bereikt. Nu gaan we met de bijeenkomst vanuit ons [de politie] echt gericht enkele jongeren uitnodigen met hun ouders. Daar sluiten de gemeente, de jongerenwerkers, de Boa's en HALT bij aan.'
	Game geldezels	Inductief	De participant geeft aan dat er een game is ontwikkeld om de gevolgen voor geldezels kenbaar te maken onder de jeugd.	'Ik denk dat dat heel goed werkt en er is al wel een game, ook voor geldezels. Daar is ook een game voor. Daar kom je een stukje op de bewustwording, maar volgens mij heb je daar nog enkele

				slagen in te maken.'
	Strafrechtelijk optreden	Deductief	De participant geeft aan dat de politie een rol heeft bij het strafrechtelijk optreden bij online fraude.	'Bij ons is dat juridische gedeelte belangrijk, het strafrechtelijke.'
	Werking interventie	Inductief	De participant geeft aan welk effect de interventie heeft gehad.	'Heel positief, ja dat is heel goed ontvangen.'
Gedigitaliseerde criminaliteit	Gedigitaliseerde criminaliteit Borger-Odoorn	Inductief	De participant geeft aan of hij/zij weet of er gedigitaliseerde criminaliteit afspeelt in de gemeente Borger-Odoorn.	'Is dit ook wel iets dat zich in onze regio afspeelt? Het kan ook uit Nigeria of India komen.'
	Gedigitaliseerde criminaliteit Coevorden	Inductief	De participant geeft aan of hij/zij weet of er gedigitaliseerde criminaliteit afspeelt in de gemeente Coevorden.	'Daar kom ik wel eens mee in aanraking. We hebben wel eens zaakjes gehad op de Nieuwe Veste. Dat is een school hier in Coevorden.'
	Gedigitaliseerde criminaliteit Emmen	Inductief	De participant geeft aan of hij/zij weet of er gedigitaliseerde criminaliteit afspeelt in de gemeente Emmen.	'Maar ik zie wel veel jongeren op dit moment als slachtoffer dan als dader van online fraude.'
	Gedigitaliseerde criminaliteit Klazienaveen	Inductief	De participant geeft aan of hij/zij weet of er gedigitaliseerde criminaliteit afspeelt in Klazienaveen.	'Ja, ik kan dat niet uitsluiten. Ik kan niet zeggen dat het hier niet gebeurt. Dat is zeker niet waar, maar op

				het gebied van fraude kan ik zelf geen signalen over vinden. Nee.’
	Gedigitaliseerde criminaliteit ontwikkelt zich	Inductief	De participant geeft aan dat gedigitaliseerde criminaliteit in rap tempo ontwikkelt.	‘Het is wel zo dat op het moment dat wij er dichter op gaan zitten dat zij met vernuftige manieren om het toch voor elkaar te krijgen. Dus dat is een kat en muis spelletje.’
	Geldezels	Deductief	De participant geeft aan dat er geldezels zijn in de regio Zuidoost Drenthe.	‘Dan lopen we er wel eens tegenaan dat bijvoorbeeld een jongere allemaal bankpasjes heeft. Dat heb ik wel eens meegemaakt. Dan gaan er natuurlijk alarmbellen rinkelen. Je gaat vervolgens na wat er hier aan de hand is. Wordt hij gebruikt? Of is hij [de jongere] er zelf mee bezig? Dus op die manier loop ik er wel eens tegen aan.’
	Kennis over cyber- en gedigitaliseerde criminaliteit	Inductief	De participant geeft aan Welke kennis hij/zij heeft van cyber- en gedigitaliseerde criminaliteit.	‘Het ligt in ieder geval wel buiten onze expertise, van het team ‘Jeugd’. Dan gaan we op

				zoek naar de plek waar we die kennis kunnen halen.’
	Meldpunt online fraude	Inductief	De participant vraagt zich af of er een meldpunt voor online fraude is.	‘Ja, ik weet niet hoe de meldingen binnenkomen en waar. Waar komen de meldingen terecht en wie gaat er eigenlijk mee aan de slag? Is het meer het strafrecht dat gaat spelen of niet? Ik denk dat er vanuit de zorgkant ook moeten inspelen.’
	Onderschatting van gedigitaliseerde criminaliteit	Deductief	De participant geeft aan dat het aantal gevallen van daderschap van online fraude niet goed in beeld is.	‘Ik denk dat we heel veel niet in beeld hebben. Ik ben ook wel benieuwd wat scholen in beeld hebben, want deze jongeren vinden elkaar op school. Op school hebben ze ook hun laptop en zijn ze met van alles bezig.’
Knelpunten	Afstand tussen politie en burgers	Inductief	De participant geeft aan dat het contact tussen de politie en burgers de laatste jaren is verminderd.	‘De dingen worden dan niet zo snel opgepakt als dat ze gewend zijn. Dus krijg je, als je niet snel je verhaal kwijt kan, dat mensen niet meer bellen. Er

				ontstaat dan een afstand.’
	Afstemming met ketenpartners	Inductief	De participant geeft aan dat de ketenpartners niet bewust zijn van elkaars taken en bevoegdheden (op het gebied van online fraude).	‘Dat weet ik ook niet. De integrale lijnen zijn nog niet zo ver dat we precies weten wat de jongerenwerkers op het gebied van online fraude of cybercriminaliteit doen. Dat vormt nog niet een punt van gesprek op dit moment.’
	Financieel	Deductief	De participant geeft aan dat een gebrek aan financiële middelen leidt tot een knelpunt in de samenwerking.	‘Als wij geen geld beschikbaar maken dan heb je financieel wel een knelpunt. Als we niet meer geld beschikbaar stellen voor het team gebiedsdoorzoeking, waar de Boa’s onder vallen, dan kunnen we niet meer personeel aannemen. Het hangt vooral vast aan het wel of niet beschikbaar krijgen van capaciteit, want dat kost natuurlijk het meeste geld.’
	Onregelmatigheid werk politie	Inductief	De participant geeft aan dat het soms lastig is om te	‘Wij zijn niet altijd even betrouwbaar met wanneer je

			overleggen en communiceren met agenten, omdat zij onregelmatige diensten draaien.	er bent. Dat is het lastige. Jij vindt dat je redelijk snel een afspraak met mij hebt gemaakt, maar dit is echt zoeken qua diensten. Het is niet dat we een baan hebben van maandag tot vrijdag.'
	Ontbreken cijfers/data	Inductief	De participant geeft aan dat de data niet altijd wordt aangeleverd door de politie.	'Nou, ik merk vaak dat wij rondom jongeren en criminaliteit van jongeren eigenlijk niet echt goede data hebben. Ik ben bezig met het opstellen van een dashboard waar alle cijfers van de politie in komen. Maar er wordt eigenlijk niet echt een onderscheid gemaakt, althans die wordt mij niet aangeleverd van 23-minners en 23-plussers.'
	Personeelstekort	Deductief	De participant geeft aan dat sprake is van een personeelstekort (bij een van de ketenpartners).	'Overal, op alle niveaus. Het is echt heel erg lastig: bij de Boa's, bij de politie en op beleidsniveau zie ik het. Bij de jongerenwerkers ook. We hebben voor

				heel Emmen: je ziet hoe groot het hier is [de kaart van Emmen hangt achter haar], drie. Drie jongerenwerkers op meer dan 100.000 inwoners.'
	Tijd	Deductief	De participant geeft aan dat er niet altijd tijd is om integraal samen te werken.	'Anderzijds kan het je soms ook aan tijd ontbreken of moet je contact met een ander zoeken die niet reageert. Dan ligt het bij de ketenpartner.'
	Traagheid gemeente	Inductief	De participant geeft aan dat de gemeente traag reageert op problematiek die speelt.	'De gemeente gaat nog altijd zo traag als dat het altijd heeft gedaan. [...] Dat is dus wat het zo ingewikkeld maakt. Je moet eigenlijk snel schakelen, terwijl het systeem niet daartoe in staat is. Althans voor de partner met wie wij samenwerken is dat echt wel een uitdaging.'
	Verloop personeel	Deductief	De participant geeft aan dat veel personeel vertrekt en start bij alle ketenpartners.	'Er zijn ontzettend veel nieuwe mensen gekomen.'
	Verschillen tussen gemeenten	Inductief	De participant geeft aan dat elke gemeente	'Dat is ook heel erg lastig, want elke gemeente

			anders te werk gaat.	heeft ook de hulpverlening heel erg anders weggezet met betrekking tot minderjarigen. Dus je kunt niet een format maken waar het en voor de gemeente Emmen, gemeente Coevorden en gemeente Borger-Odoorn werkt. En dat is heel erg lastig binnen het hele stelsel in Nederland. Elke gemeente werkt weer anders.'
	Ziekteverzuim	Deductief	De participant geeft aan dat ziekteverzuim ook een knelpunt is tijdens samenwerkinge n.	'Ik weet dat er iemand vanuit openbare orde dit zou oppakken en dat diegene ziek is uitgevallen. Dan worden de taken niet uitgevoerd in de tijd zoals je dat hebt besproken met elkaar.'
Motieven	Consequenties onbekend	Deductief	De participant denkt dat sommige jongeren niet door hebben dat ze strafbaar bezig zijn.	'Ze zien er ook geen kwaad in.'
	Erbij horen	Deductief	De participant denkt dat een mogelijk motief is dat jongeren erbij willen horen.	'Als je kijkt naar de gevoeligheid voor groepsdruk op jonge leeftijd en dat

				ze op zo'n manier echt wel het criminele pad op gaan door bijvoorbeeld verkeerde vrienden te maken. Ze zijn beïnvloedbaar. Ze kunnen dan zo worden binnengehaald.
	Geld verdienen	Deductief	De participant denkt dat jongeren door middel van online fraude gemakkelijk geld kunnen verdienen.	‘In eerste instantie zal het te maken hebben met een gebrek aan geld. Het is een makkelijke manier.’
	Groepsdruk	Deductief	De participant denkt dat jongeren mogelijk onder groepsdruk lijden en daarom het criminele pad op gaan.	‘Het kan ook zijn dat ze onder druk staan van iemand anders waardoor ze dat moeten doen. We hebben het hier wel over een kwetsbare doelgroep. Het betreffen ook wel veel jongeren van praktijkonderwijs, dus die jongeren zijn best wel beïnvloedbaar en worden ook wel eens voor het karretje gespannen.’
	Lage pakkans; anonimiteit	Deductief	De participant denkt dat jongeren online fraude plegen, omdat er een lage pakkans is	‘Nu heerst het idee dat de politie er toch niks mee doet en kunnen ze

			en een hoge mate van anonimiteit is.	lekker doorgaan.’
	Status	Deductief	De participant denkt dat jongeren status nastreven en dit bereiken door middel van online fraude.	‘Ze krijgen heel snel geld en lopen allemaal in hele dure kleding, zoals dure jassen en schoenen. Dat geeft hun status. Dan denken anderen ook dat ze zo'n jas willen. Dan krijg je het sneeuwbaleffect.’
	Stoerdoenerij	Inductief	De participant denkt dat jongeren stoer willen doen door middel van het versturen van oplichting berichten.	‘Jongeren willen er natuurlijk graag bij horen, dus ik denk dat ze het interessant of stoer vinden.’
Preventie	Gesprekken jongeren	Inductief	De participant voert gesprekken met jongeren.	‘Kijk op het moment dat er signalen zijn dat het hier afspeelt dan zou dat zeker gespreksstof zijn. Daarin is het wel een beetje zoeken naar wat voor jongeren je voor je hebt. Ik zou het niet als rode draad in mijn gesprekken plaatsen.’
	Informeren via sociale media	Deductief	De participant geeft aan dat sociale media geschikt zijn om mensen te	‘Dan moeten we inzetten op campagne. Via Instagram zijn we ook veel bezig om

			informeren over online fraude.	bepaalde thema's aan te halen. Dat is wel een platform waar ik zelf gebruik van zou maken om jongeren te informeren over de gevolgen zouden kunnen zijn als je je daarmee bezighoudt.’
	Nut preventieve maatregelen	Inductief	De participant geeft aan dat het nut van preventieve maatregelen nog wordt onderschat.	‘Ik denk dat het soms onderschat wordt hoe belangrijk het is om preventief te werk te gaan. Ik denk dat het in de hele jeugdzorg nog veel brandjes blussen is. Het zou mooi zijn als het meer op voorliggend vlak zou zijn.’
	Overige preventieve maatregelen	Inductief	De participant geeft andere voorbeelden van preventieve maatregelen.	‘We hebben ook de mobiele media bus. […] Die hebben we nu een keer gebruikt. De andere keer was het door corona afgezegd. Dat we daar mensen in gaan uitnodigen. Dat we die bus hier twee of drie dagen achter elkaar laten komen. Zodat je de jongeren weer naar je toe krijgt en dat je

				weer die voorlichting kunt geven.’
	School Preventieplan	Inductief	De participant geeft aan dat ze een school preventieplan hebben ontwikkeld voor scholen.	‘We bieden op basisscholen school preventieplannen aan waar financiën en online gedrag ook naar voren komen. Dat is preventief.’
	Voorlichting	Deductief	De participant geeft voorlichtingen over online fraude als voorbeeld van een preventieve maatregel.	‘Daar wordt voorlichting gegeven over geldezels: wat het inhoudt, welke consequenties er zijn als je daarmee aan de slag gaat.’
Problematiek	Aandragen problematiek anderen	Inductief	De participant geeft aan welke partners problematiek aankaarten bij de partners.	‘Maar het komt wel op basis van een bevinding van ons [jongerenwerk] of een wijkagent waarop wij aansturen dat het goed is om weer bij elkaar te komen.’
	Ad hoc problematiek	Inductief	De participant geeft aan dat de focus van het huidige beleid vooral ligt op ad hoc problematiek.	‘Het gaat veel over de waan van de dag. Er gebeurt nu iets, er zijn nu jongeren en die zijn nu overlast gevend, en daar moeten we nu op acteren.’
	Jeugdcriminaliteit ontwikkeling	Inductief	De participant vertelt over de	‘Signalen over jeugdoverlast

			ontwikkelingen omtrent jeugdcriminaliteit.	komen wél op een punt binnen en we vinden elkaar nu wel.’
	Signaleren problematiek	Inductief	De participant geeft aan wie problematiek signaleert.	‘Ja dat zou ook wel kunnen. We zijn breed, want we hebben Boa’s en we hebben buurtsportcoaches die komen ook jongeren tegen. In principe wel, alleen het is wel versnipperde informatie. Soms is één signaal, geen signaal. Als het op tien verschillende plekken ligt dan wordt het ineens wel iets belangrijks. Het doel daarvan is, is dat het juist gebundeld wordt.’
Samenwerking	Actief samen optreden	Deductief	De participant geeft aan dat actief de samenwerking wordt gezocht met partners wanneer problemen opspelen.	‘Er wordt als eerst een samenwerking gezocht met de wijkagenten. Vanuit dat kader wordt dan een plan opgesteld.’
	Samenwerken met jongerenwerkers	Inductief	De participant geeft aan wanneer de ketenpartners samenwerken met jongerenwerk.	‘Het is nog moeilijk om iets over jongerenwerkers te zeggen, want het is een hartstikke positieve ontwikkeling. Het is positief

				dat ze er nu zijn en als er dan al een probleem moet zijn dan is het dat ze niet genoeg tijd krijgen. Er is altijd extra gewenst. Maar we zijn nog niet zo lang bezig dat ik dat soort dingen kan benoemen. Het is al mooi dat we elkaar vinden. Dat was zelfs een jaar, en sowieso twee jaar geleden, wel anders. Toen waren ze helemaal weinig in beeld. Nu kun je ze benaderen en ervoor gebruiken, dus dat is hartstikke fijn.'
	Verwijzen naar andere partners	Inductief	De participant geeft aan dat zaken worden doorverwezen wanneer zij zelf niks kunnen doen aan het probleem.	'Op het moment dat het daadwerkelijk voorkomt dan kunnen we het alleen melden. Dan is de handhaving aan de beurt.'
Taken	Groepsscan	Inductief	De participant vertelt over de groepsscan die de politie maakt van jeugdgroepen.	'Nee, de groepsscan is eigenlijk gemaakt om de jeugdgroep in beeld te krijgen. En als een jeugdgroep zich ook bezighoudt met online

				fraude dan zou je daar met elkaar een plan van aanpak voor kunnen maken.’
	Politietaak	Inductief	De participant geeft aan welke taken de politie heeft.	‘Wij, als politie, zullen dan vaak ook een stukje van de opsporing moeten doen. Die voorbeelden zijn er wel en bij dat soort overleggen heb ik me ook wel eens bij aangesloten.’
	Proces taakverdeling	Deductief	De participant geeft aan hoe de taken worden verdeeld bij een integrale samenwerking.	‘Er wordt dan een actiepuntenlijst gemaakt, waarbij iedereen een actie krijgt toebedeeld. We spreken dan ook een moment af waarop de actie moet zijn uitgevoerd.’
	Proces van taakuitoefening	Deductief	De participant geeft aan hoe de taken worden uitgevoerd.	‘Ja meestal wel. Het kan altijd voorkomen dat er iets niet gebeurt, maar daar is altijd een reden voor. We bespreken dat wel altijd als we afspraken hebben gemaakt of het is uitgevoerd. Maar ook wat er wel of niet is uitgekomen. Of waarom het niet is gelukt.’

	Taak jongerenwerk	Inductief	De participant geeft aan welke taken jongerenwerkers hebben.	‘Dan zijn de jongerenwerkers een uitstekende bron van informatie. Jongerenwerkers die met jongerengroepen werken kunnen je vertellen of het hier speelt.’
	Taak van collega's	Inductief	De participant geeft aan wanneer hij taken doorspeelt aan zijn/haar collega's.	‘Uiteindelijk wel, want daarin hebben ze ook veiligheid overleggen. Mijn collega uit Angelslo is vanuit daar ook aangesloten.’
	Taak van overige partners	Inductief	De participant geeft aan wanneer een taak moet worden uitgevoerd door andere partners (geen politie, jongerenwerk of gemeente).	‘Als er geen aangifte gedaan wordt, zou het bijvoorbeeld ook mogelijk een HALT-feit kunnen zijn. Dat de HALT-medewerker het gesprek aangaat en dat er minder consequenties zijn, maar zover is het nog niet helaas. Het blijft het strafrecht.’
	Taken graag oppakken	Inductief	De participant geeft aan dat sommige taken enthousiast worden opgepakt.	‘We zijn allemaal, Boa, politie en wij [jongerenwerk], zijn allemaal erg fanatiek in het werk dat we doen. We willen het graag

				allemaal goed doen. Dat maakt ook dat het enthousiasme er altijd wel is. Waar het ook overgaat worden de schouders altijd wel eronder gezet.'
Werkzaamheden	Dagelijkse werkzaamheden	Inductief	De participant vertelt hoe een werkdag er voor hem/haar uitziet.	'Vanmiddag heb ik een inloopspreekuur waar jongeren terecht kunnen met allerlei vragen. Dat kunnen vragen zijn over persoonlijke dingen van jongeren die niet lekker in hun vel zetten of problemen hebben met de ouders. Of ze hebben problemen met school. Daar ga ik met de jongeren in gesprek zodat ik kan vaststellen wat ik voor ze kan betekenen en waar ik ze mee kan helpen. Kan ik iets met ze doen waardoor er passende hulp wordt ingezet. […] We gaan regelmatig het gesprek aan met de jongeren.

				Vanmiddag tijdens zo'n spreekuur kunnen de jongeren zelf naar ons toekomen met dat soort ideeën of vragen. Straatwerk staat ook op de planning. Dan gaan we de wijk in, zodat we in hun leefomgeving komen. Dan sluiten we aan op wat er daar speelt. Dat kan van alles zijn.'
	Functie	Inductief	De participant vertelt over zijn/haar functie.	'Mijn functie heet beleidsadviseur Openbare Orde en Veiligheid. Dat betekent eigenlijk dat ik de burgemeester advies geef over zijn portefeuille openbare orde. Daarin heeft hij ook bevoegdheden om de openbare orde te kunnen handhaven.'
	Motto jongerenwerk	Inductief	De participant geeft aan het motto van jongerenwerkers aan.	'Onze visie bestaat eigenlijk uit twee woorden en dat is positief contact. Wij blijven zo veel mogelijk weg van handhaving en dingen die niet mogen, want dat horen

				ze al vaak genoeg van de politie, Boa of school. “Dit mag niet". Bij ons krijg je altijd een nieuwe kans en gaan we kijken naar de dingen die wel kunnen. Dus wij werken echt aan een vertrouwensband.’
	Neventaken werk	Inductief	De participant vertelt over zijn/haar nevenwerkzaamheden.	‘[…] ik zit in het netwerk divers vakmanschap. Ik doe eer gerelateerd geweld en ik ben explosievenverkenner.’
	Verbinding gedigitaliseerde criminalieit	Inductief	De participant geeft aan wat hem/haar verbindt met gedigitaliseerde criminaliteit in zijn/haar werkzaamheden.	‘Er is wel aandacht voor, maar er komen niet specifiek hulpvragen binnen die te maken hebben met cybercriminaliteit.’
	Verbinding jeugdcriminaliteit	Inductief	De participant geeft aan wat hem/haar verbindt met jeugdcriminaliteit in zijn/haar werkzaamheden	‘Ja, die komen wel regelmatig voor. Dat er hangjongeren gesignaleerd worden in de wijk en dat dat bepaalde overlast geeft. Daarbij zit ook een stukje drugs. Dat is vaak wel een combinatie van elkaar.’