CYBER CENTRUM

CYBER CENTRE

AUTEUR: MERYEM MORI
BEGELEIDER: GIJS HUITSING
REFERENT: VINCENZ FREY

MSC. SOCIOLOGIE
RIJKSUNIVERSITEIT GRONINGEN
07 - 2022

university of groningen

POLITIE

Cyber Centrum

Een onderzoek naar online daders en online dadernetwerken

M. Mori (S4509420)

Ter afsluiting van de masteropleiding Sociologie aan de Rijksuniversiteit Groningen is dit onderzoek naar online criminaliteit verricht. Het onderzoek is tot stand gekomen in samenwerking met het cybercrimeteam van de Dienst Regionale Recherche, politie eenheid Noord-Nederland. Ik dank hierbij mijn begeleiders vanuit de politie; Jildau Borwell, Martijn Krijnsen en Gerard Wolters voor de toewijding aan dit onderzoek. Daarnaast dank ik de basisteams Groningen-Centrum en Noord-Drenthe voor de fijne afstudeerperiode. Ik dank mijn begeleider vanuit de universiteit Gijs Huitsing en mijn referent Vincenz Frey voor de ondersteuning bij dit onderzoek. Tot slot wens ik u veel leesplezier toe.

Samenvatting

Cyber Centrum: een onderzoek naar online daders en online dadernetwerken. Online criminaliteit heeft een stijgende trend waardoor onderzoek naar online daders essentieel is. De centrale vraag binnen dit onderzoek is: wat zijn de kenmerken van online daders en hoe ziet een netwerk van online daders er uit? Het onderzoek is uitgevoerd met behulp van politiesystemen en datasets die informatie bevatten over online verdachten in Noord-Nederland in 2021.

In tegenstelling tot de verwachtingen uit theorieën over adolescence-limited antisociaal gedrag, age – graded turning points, zelfcontrole, online disinhibition en digital drift, zijn verdachten van cybercriminaliteit niet significant jonger dan verdachten van gedigitaliseerde criminaliteit. De leeftijden zijn redelijk gelijk verdeeld en beide typen online verdachten zijn grotendeels volwassen. Daarnaast worden mannen niet significant vaker verdacht van cybercriminaliteit en gedigitaliseerde criminaliteit dan vrouwen. Sterker nog, de verhouding tussen mannelijke en vrouwelijke verdachten is gelijk. Verder zijn cyber verdachten niet signifcant vaker first offender dan gedigitaliseerde verdachten. Beide typen online verdachten hebben veelal een traditioneel of gemengd delictverleden.

Het online netwerk van zes geprioriteerde online verdachten is onderzocht aan de hand van welke personen deel uitmaken van het netwerk, welke personen essentieel zijn in het netwerk en wat de inhoudelijke kenmerken zijn van het netwerk. Het netwerk bestaat uit 162 personen, met een kerngroep van zes personen en twee opvallende personen die geen deel uitmaken van de kerngroep. De essentiële personen in het netwerk zijn persoon 25 en 34. De personen in het netwerk zijn vooral bezig met gedigitaliseerde criminaliteit (i.e. overige horizontale fraude, fraude met betaalproducten en online handel, witwassen). Daarnaast zijn ze actief in andere criminele markten zoals geweld, wapens en drugs. Het online netwerk neigt hierdoor meer naar een gemengd netwerk, bestaande uit gedigitaliseerde en traditionele criminaliteit.

De bevindingen uit dit onderzoek worden enigszins beperkt door limitaties in de data. De politie beschikt namelijk alleen over data van verdachten die zijn opgepakt. Hierdoor is geen zicht op personen die niet zijn opgepakt, met als gevolg dat de resultaten niet volledig representatief zijn voor alle online verdachten en dat het online netwerk gefragmenteerd is. Al met al biedt het onderzoek een helder inzicht in de kenmerken en netwerken van de onderzochte online verdachten.

Inhoud

Samenvatting **2**

1. Introductie **5**

1.1 Aanleiding **5**

1.2 Doelstelling **6**

1.3 Relevantie **7**

1.4 Indeling **8**

2. Theorie **9**

2.1 Online daderprofiel **9**

2.1.1 Leeftijd 9

2.1.2 Geslacht 11

2.1.3 Delictverleden 12

2.2 Online netwerk **14**

2.2.1 Netwerkanalyse 14

2.2.2 Crimescript 15

2.2.3 Geografische afstand 16

2.2.4 Verbintenis 17

3. Methoden **19**

3.1 Online daderprofiel **19**

3.1.1 Operationalisaties 20

3.1.2 Onderzoeksopzet 20

3.2 Online netwerk **22**

3.2.1 Onderzoeksopzet 22

4. Resultaten **23**

4.1 Online daderprofiel **23**

4.1.1 Leeftijd 24

4.1.2 Geslacht 25

4.1.3 Delictverleden 27

4.2 Online netwerk **29**

4.2.1 Netwerkbeschrijving 30

4.2.2 Netwerkanalyse 31

4.2.3 Inhoudelijk netwerk 32

5. Conclusie **33**
5.1 Online daderprofiel **33**
5.2 Online netwerk **34**

6. Discussie **36**
6.1 Sterktes en zwaktes **36**
6.2 Aanbevelingen **38**

Referenties **41**

1. Introductie

1.1 Aanleiding

Het afgelopen decennium heeft het internet een steeds prominentere rol gekregen in het dagelijks leven van personen in Nederland. Het Centraal Bureau voor de Statistiek meldt dat in 2021, 97% van alle personen ouder dan twaalf jaar toegang hebben tot het internet thuis, ten opzichte van 91,5% in 2012. In 2021 maakte 86,6% van alle personen ouder dan twaalf jaar in Nederland dagelijks gebruik van het internet. Het internetgebruik bestaat vooral uit sociale media gebruik, communicatie per e-mail en Whatsapp, informatie en vermaak met betrekking tot goederen, en dienstverlening zoals internetbankieren (CBS, 2021).

De digitalisering van het afgelopen decennium heeft in maart 2020 een stroomversnelling gekregen door de toepassing van de lockdownmaatregelen ter bestrijding van de COVID-19 pandemie. Organisaties en instanties hebben processen gedigitaliseerd om tijdens de lockdown te kunnen blijven functioneren. Dit heeft geleid tot een groot aandeel van thuiswerken, thuisonderwijs en digitale zorg. Verder zijn door de overheid digitale middelen ingezet ter bestrijding van de COVID-19 pandemie waaronder data-verzameling, informatieverspreiding en de inzet van de CoronaMelder-App en QR-code (ECP, 2020). Inmiddels zijn de digitale maatregelen ter bestrijding van de COVID-19 pandemie komen te vervallen. Echter, deze (versnelde) digitalisering kent neveneffecten voor de samenleving waarvan de gevolgen, ook na opheffing van de maatregelen, sterk merkbaar zijn.

Een neveneffect van de digitalisering van het afgelopen decennium is de toename van online criminaliteit met 22%. Het Centraal Bureau voor de Statistiek (2022) definieert online criminaliteit als delicten en incidenten die via het internet, e-mail of app plaatsvinden. Uit de Veiligheidsmonitor 2021 van het Centraal Bureau voor de Statistiek blijkt dat 17% van de personen in Nederland slachtoffer is geweest van online criminaliteit (i.e. verkoopfraude, hacken, bedreiging en intimidatie) ten opzichte van 13% in 2019. Daarnaast blijkt dat in 2021, 17% van de personen ouder dan vijftien jaar in Nederland, slachtoffer is geweest van traditionele criminaliteit (i.e. geweld- en vermogensdelicten en vernielingen) ten opzichte van 21% in 2019. Hierdoor is sprake van een toename van slachtoffers van online criminaliteit, en een afname van slachtoffers van traditionele criminaliteit (CBS, 2022).

Uit voorgaand onderzoek in opdracht van de politie eenheid Noord-Nederland naar de verhouding tussen online en traditionele criminaliteit (2022) blijkt dat 29,5% van alle aangiften en meldingen, die bij de politie binnenkomen, online criminaliteit betreffen ten opzichte van 70,5% traditionele criminaliteit. Deze verhouding schetst een algemeen beeld van het aandeel online criminaliteit binnen de politieregistraties in 2021 in Noord-Nederland. De

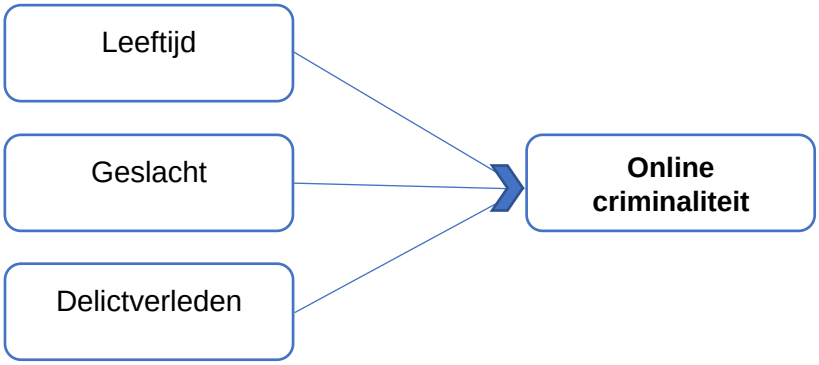
veronderstelling hierbij is dat er een groot *dark number* is bij online criminaliteit doordat uit de Veiligheidsmonitor 2021 van het Centraal Bureau voor de Statistiek is gebleken dat slechts 19% van alle slachtoffers van online criminaliteit aangifte doet bij de politie (CBS, 2022). Mogelijke verklaringen voor de lage aangiftebereidheid kunnen zijn dat slachtoffers zich schamen of zich zelf schuldig hebben gemaakt aan een ander strafbaar (online) delict. Indien er geen aangifte wordt gedaan, is er ook geen zicht op de online daders. De verwachting van de politie is daarbij dat het aandeel online criminaliteit zal blijven toenemen (Jong et al., 2018).

1.2 Doelstelling

Het doel van het onderzoek is om meer inzicht te verkrijgen in online criminaliteit zodat het effectiever bestreden kan worden. Online criminaliteit betreft delicten en incidenten die via internet plaatsvinden en is op te delen in cybercriminaliteit in enge zin en cybercriminaliteit in ruime zin (CBS, 2022). Cybercriminaliteit in enge zin omvat alle vormen van criminaliteit die gepleegd is met én gericht is op ICT (Domenie et al., 2013). Bij cybercriminaliteit in enge zin is ICT zowel het middel als het doelwit van het delict. Vormen van cybercriminaliteit in enge zin zijn hacken en het verspreiden van malware. Cybercriminaliteit in ruime zin omvat alle vormen van criminaliteit die gepleegd is met ICT als middel, maar niet als doelwit (Leukfeldt et al., 2012). Cybercriminaliteit in ruime zin wordt aangeduid als gedigitaliseerde criminaliteit en deze term wordt tevens aangehouden in dit onderzoek. Vormen van gedigitaliseerde criminaliteit zijn online fraude en stalking. De focus van dit onderzoek ligt op het verkrijgen van inzicht in de kenmerken van verdachten cybercriminaliteit en gedigitaliseerde criminaliteit, en in het verkrijgen van inzicht in het online netwerk. De onderzoeksvraag hierbij is:

“Wat zijn de kenmerken van online daders en hoe ziet een netwerk van online daders er uit?”

De onderzoeksvraag is tweeledig. Het eerste deel *“wat zijn de kenmerken van online daders”* wordt onderzocht met politiedata van verdachten van online criminaliteit. De politiedata bevat informatie over de verdachte, het slachtoffer en het delict en biedt inzicht in de kenmerken; leeftijd, geslacht en delictverleden. Deze kenmerken omvatten het online daderprofiel waaruit blijkt *wie* de personen zijn en *wat* ze doen. De verbanden worden weergegeven in het conceptueel model (figuur 1). In het tweede deel van de onderzoeksvraag *“hoe ziet een netwerk van online daders er uit”* wordt een exploratieve case study onderzoek verricht naar zes geprioriteerde online verdachten in Noord-Nederland. Hiermee wordt een specifieker inzicht verkregen in het online netwerk van de verdachten. Het online netwerk wordt in kaart gebracht met data uit verschillende politiesystemen over de geprioriteerde *Amazonegroep*, waaruit blijkt *wie* de personen in het netwerk zijn, *hoe* de personen in het netwerk met elkaar verbonden zijn en *wat* de personen in het netwerk doen.



Figuur 1: Conceptueel model online criminaliteit

1.3 Relevantie

De maatschappelijke relevantie om onderzoek te verrichten naar online criminaliteit is het feit dat online criminaliteit, net als traditionele criminaliteit, negatieve gevolgen heeft voor de samenleving. Echter, waar traditionele criminaliteit een dalende trend heeft, heeft online criminaliteit een stijgende trend met de negatieve gevolgen van dien. Uit de Veiligheidsmonitor 2021 van het Centraal Bureau voor de Statistiek (2022) is gebleken dat 18% van de slachtoffers van online criminaliteit, na het delict emotionele, psychische en/of financiële problemen ervaart. De meeste online delicten vinden plaats in de (inter)persoonlijke sfeer van het slachtoffer waardoor ze vaak gepaard gaan met emotionele en psychische schade en een onveilig gevoel in het eigen huis. De emotionele en psychische schade uit zich in schaamte, woede en stress die gedurende een langere periode doen gelden. Daarnaast verliezen slachtoffers van online criminaliteit hun vertrouwen in anderen, in de overheid en in de politie. Slachtoffers van online criminaliteit kunnen het gevoel krijgen niet serieus genomen te worden door de politie indien de aangifte of melding niet effectief wordt afgehandeld (CBS, 2022). Naast de psychische gevolgen, kan online criminaliteit zoals fraude en oplichting, ook negatieve financiële gevolgen hebben voor het slachtoffer doordat online criminelen snel al het geld van het slachtoffer kunnen bemachtigen. Daarbij kunnen online criminelen in een korte tijd meerdere slachtoffers maken. De financiële gevolgen zijn ook merkbaar voor de algehele samenleving doordat het internet traditionele criminaliteit faciliteert met bijvoorbeeld cryptocurrency en witwassen (Leukfeldt et al., 2018). Gezien het feit dat het internet een zeer prominente rol heeft in het dagelijks leven van personen in Nederland, is het relevant om online criminaliteit te onderzoeken om de impact daarvan op de samenleving te beperken. Net zoals dat er twee vormen zijn van online criminaliteit, zijn er ook twee typen online daders. Om de impact van cyber en gedigitaliseerde criminaliteit effectief te kunnen beperken, is onderzoek vereist naar de kenmerken van afzonderlijke cyber en gedigitaliseerde verdachten, en naar het functioneren van cyber en gedigitaliseerde verdachten in online netwerken.

Dit onderzoek wordt uitgevoerd voor het cybercrimeteam van de politie eenheid Noord-Nederland en er wordt daarom onderscheid gemaakt tussen de districten Groningen, Friesland en Drenthe. Uit voorgaand onderzoek naar de verhouding tussen online en traditionele criminaliteit (2022) is gebleken dat, door de hoeveelheid aangiften van online criminaliteit die bij de politie binnenkomen en het gebrek aan kennis omtrent online criminaliteit, er momenteel vooral sprake is van incidentbestrijding. Rekening houdend met de capaciteiten van de politie, is dit niet de meest efficiënte manier. De politie bevindt zich in een transitie van incidentbestrijding naar fenomeenbestrijding. Bij fenomeenbestrijding is het van belang om duidelijk zicht te hebben op verdachten en trends van online criminaliteit. Zo kunnen toekomstige online daders en slachtoffers voorkomen worden. Het is daarom voor de politie relevant om de kenmerken van zowel cyber als gedigitaliseerde verdachten en hun netwerken te onderzoeken om zodoende beide vormen van online criminaliteit efficiënter te bestrijden.

De wetenschappelijke relevantie van dit onderzoek is de bijdrage aan kennis omtrent online criminaliteit waarbij onderscheid wordt gemaakt tussen cyber en gedigitaliseerde criminaliteit. Het internet is het afgelopen decennium dusdanig snel ontwikkeld, dat de tot op heden vergaarde kennis omtrent online criminaliteit niet meer toereikend is. Tot op heden is vooral onderzoek verricht naar de slachtoffers, omvang en vormen van online criminaliteit. Zowel in theorie, als bij de politie in de praktijk, ontbreekt informatie over de kenmerken en modus operandi van specifieke cyber en gedigitaliseerde verdachten. Daarnaast is er weinig informatie beschikbaar over het functioneren van online netwerken en cybercrimescripts. In het kader van fenomeenbestrijding is nader onderzoek vereist naar online verdachten en hun online netwerken. Vooralsnog worden theorieën voor betrokkenheid van traditionele verdachten toegepast op online verdachten. Echter, door het internet zijn online verdachten niet meer plaatsgebonden, wat mogelijk gepaard gaat met een andere werkwijze dan traditionele verdachten. Het is daarom voor de wetenschap relevant om kenmerken van cyber en gedigitaliseerde verdachten afzonderlijk te onderzoeken, en te onderzoeken hoe een netwerk bestaande uit cyber en gedigitaliseerde verdachten functioneert.

1.4 Indeling

Het onderzoek heeft een brede start door de kenmerken van online daders te onderzoeken en vervolgens wordt het onderzoek getrechterd tot een case study van een online netwerk. In het tweede hoofdstuk wordt het onderzoek theoretisch onderbouwd en worden toetsbare hypothesen opgesteld. In het derde hoofdstuk wordt het onderzoek geoperationaliseerd en worden de onderzoeksmethoden uitgewerkt. In het vierde hoofdstuk worden de resultaten van het online daderprofiel en de netwerkanalyse behandeld. Daarop volgen de conclusies in hoofdstuk vijf en het onderzoek wordt afgesloten met de discussie in hoofdstuk zes.

2. Theorie

In dit hoofdstuk worden de centrale concepten en theorieën nader bestudeerd. In paragraaf §2.1 wordt het online daderprofiel uiteengezet en in §2.2 wordt het online netwerk uiteengezet.

2.1 Online daderprofiel

Het online daderprofiel wordt bestudeerd aan de hand van de leeftijd, het geslacht en het delictverleden van verdachten van online criminaliteit.

2.1.1 Leeftijd

Jongeren worden over het algemeen vaker verdacht van online criminaliteit dan ouderen. Een verklaring voor online jeugdcriminaliteit is te vinden in het (cyber)psychologische domein waar de *adolescence-limited and life-course-persistent antisocial behavior* theorie van Moffitt aan ten grondslag ligt (1993). Volgens de inzichten van Mofitt zijn er twee soorten criminelen te onderscheiden; jongeren die in de adolescentie tijdelijk crimineel gedrag vertonen en jongeren die langdurig crimineel gedrag vertonen vanuit de vroege kinderjaren tot in de late volwassenheid. Echter, ten alle tijden en in alle landen, piekt jeugdcriminaliteit hierbij tijdens de adolescentie van jongeren. Aangezien minderjarigen en jongvolwassenen het grootste gedeelte van de online dadergroep omvatten, ligt de verklaring voor jeugdige online daders in *adolescence-limited antisocial behavior*, oftewel, tijdelijk crimineel gedrag in de adolescentie. De neiging tot crimineel gedrag in de adolescentie komt voort uit de *maturity gap*, de discrepantie tussen biologische en sociale volwassenheid van jongeren. Jongeren kunnen biologisch gezien steeds volwassener worden, waarbij de sociale volwassenheid uitblijft. Sociaal gezien mogen jongeren nog niet veel waardoor ze in zekere mate sociaal onderdrukt worden. Dit leidt bij jongeren tot gevoelens van onvrede, wat zich kan uiten in antisociaal en zelfs crimineel gedrag. Tijdelijk crimineel gedrag in de adolescentie heeft daarom geen pathologische basis, er lijkt geen verbinding te zijn tussen mentale stoornissen en tijdelijk crimineel gedrag. Het criminele gedrag is vaak van korte duur en houdt niet stabiel aan. Naarmate jongeren volwassen worden, dicht de kloof tussen de biologische en sociale volwassenheid waardoor het criminele gedrag ten einde komt (Moffitt, 1993).

Een andere verklaring voor het in mindere mate voorkomen van crimineel gedrag op latere leeftijd is de *age-graded theory* van Sampson en Laub (1993). Hierin wordt ten eerste verondersteld dat crimineel gedrag instabiel is, wat duidt op dat het criminele gedrag niet consistent is gedurende de hele levensloop en door bepaalde *turning points* kan beginnen of eindigen. Belangrijke turning points volgen na de adolescentie, zodra (jong)volwassenen gaan studeren, een vaste baan krijgen of gaan trouwen waardoor hun prioriteiten en doelen veranderen. Daarnaast worden de (percepties van) negatieve gevolgen van crimineel gedrag,

groter waardoor de waarschijnlijkheid van crimineel gedrag afneemt. Ten tweede is het delictverleden een belangrijk aspect in de age-graded theorie. Hierbij wordt verondersteld dat het delictverleden een voorspeller is van criminaliteit waarbij een groot delictverleden de kans verkleind om uit de criminaliteit te stappen. De dader is namelijk meer betrokken met andere criminelen en dieper genesteld in criminele netwerken. Daarnaast biedt criminaliteit meer verdienvermogen waardoor het op latere leeftijd, met een groter delictverleden, lastiger wordt om uit de criminaliteit te stappen (Weulen Kranenbarg et al., 2018).

Een belangrijk kenmerk van dit tijdperk is de sterke digitalisering en het veelvuldige internetgebruik. Het aandeel van jongeren, tussen de 12 en 25 jaar, dat dagelijks gebruik van het internet maakt, is 92,3% (CBS, 2021). Daarbij zijn jongeren opgegroeid met het internet en technologie waardoor ze daarin handiger zijn dan ouderen en ze mogelijk meer neigen tot het plegen van cybercriminaliteit in enge zin dan ouderen. Het dagelijkse internetgebruik waarin jongeren veelvuldig worden blootgesteld aan nieuwe verleidingen, en gelegenheden, kan de waarschijnlijkheid van het plegen van cybercriminaliteit vergroten. Naast de traditionele wereld, biedt de online wereld simpelweg een extra dimensie die online criminaliteit mogelijk maakt of traditionele criminaliteit faciliteert (Van der Wagen, 2019). Deze verklaring wordt ondersteund door de gelegenheidsbenadering waarin wordt verondersteld dat, indien er meer gelegenheid is om crimineel gedrag te vertonen, de kans dat iemand crimineel gedrag vertoond wordt vergroot (Cohen & Felson, 1979).

Het tijdelijke criminele gedrag op van jongeren het internet is het product van de onderlinge interactie tussen de leeftijd en het tijdperk. De eerste bevinding uit de theorie is dat online verdachten voornamelijk jongeren zijn. De tweede bevinding uit de theorie is dat er een verschil is in verdachten afhankelijk aan het type delict (cyber of gedigitaliseerd). De hypothese die hieruit voorkomt is:

[H1] Verdachten van cybercriminaliteit in enge zin zijn jonger dan verdachten van gedigitaliseerde criminaliteit.

Voorgaand empirisch onderzoek biedt ondersteuning voor deze hypothese. Zo stelt de Monitor Jeugdcriminaliteit 2020 dat het grootste gedeelte (34,5%) van de online criminaliteit wordt gepleegd door jeugdige online daders tussen de 12 en 23 jaar[1]. Dit is onderzocht aan de hand van zelfrapportages, politieregistraties en justitiestatistieken van online criminaliteit. In zelfrapportages worden jongeren geacht te rapporteren over hun eigen gedrag en handelingen. Een voordeel van zelfrapportages is dat ze inzicht bieden in niet – geregistreerde

[1] In de Monitor Jeugdcriminaliteit 2020 worden leeftijdscategorieën van 5 jaar gehanteerd waardoor de categorieën 12 – 17 jaar en 18 – 23 jaar samen het grootste gedeelte van de online daders omvatten.

online criminaliteit en een nadeel van zelfrapportages is dat ze gevoelig zijn voor contexteffecten en bias door sociaal wenselijke antwoorden. In de Monitor Jeugdcriminaliteit wordt vooral gerapporteerd over lichtere vormen van online criminaliteit. Naarmate de aard van het delict zwaarder wordt, wordt de informatie gehaald uit politieregistraties en justitiestatistieken. De politieregistraties en justitiestatistieken omvatten alleen informatie over jeugdige online daders waar de politie en justitie zicht op hebben. Hierdoor is er zowel in de zelfrapportages als in de politieregistraties en justitiestatistieken mogelijk sprake van bias waardoor geen volledig representatief beeld geschetst kan worden van alle jeugdige online daders. Uit de Monitor Jeugdcriminaliteit is gebleken dat 1 op de 10 minderjarigen tussen de 12 en 18 jaar, en 1 op de 7 jongvolwassen tussen 18 en 23 jaar, zich schuldig heeft gemaakt aan een cyberdelict in 2019. In 2020 geeft 19,5% van de minderjarigen aan zich schuldig te hebben gemaakt aan een vorm van online criminaliteit (cyber of gedigitaliseerd). Het betreft bijvoorbeeld cyberdelicten als hacken, DDoS of virus aanvallen en gedigitaliseerde delicten als fraude, sexting of stalking (Van der Laan et al., 2021).

2.1.2 Geslacht

Het merendeel van de daders van online criminaliteit is man en dit geldt zowel voor jonge als volwassene online daders (Aiken., et al 2016). Een verklaring voor de oververtegenwoordiging van mannen in online criminaliteit is te vinden in het *Dunedin* onderzoek naar de ontwikkeling van zelfcontrole in kinderen en latere criminele veroordelingen in de (jong)volwassenheid. Zelfcontrole omvat belangrijke capaciteiten, zoals het reguleren van emoties en impulsen, geduld en concentratie- en doorzettingsvermogen, die antisociaal gedrag kunnen beïnvloeden. Uit dit onderzoek is gebleken dat meiden significant meer zelfcontrole bezitten dan jongens in de kindertijd. Mensen met een lage zelfcontrole hebben meer kans (45%) om veroordeeld te worden voor criminaliteit en om een gevangenisstraf te krijgen dan mensen met een hoge zelfcontrole (15%) (Moffitt et al., 2013). Het effect van een verminderde zelfcontrole van mannen op online criminaliteit wordt versterkt door het *online disinhibition effect* (Suler, 2004). *Inhibition* treedt op wanneer gedrag wordt beïnvloed door remmende factoren zoals zelfbewustzijn, zelfcontrole en angst voor sociale afwijzing. *Disinhibition* treedt op bij een afwezigheid van deze remmende factoren. Het online disinhibition effect komt voor wanneer mensen zich online anders gedragen dan in (soortgelijke) offline situaties doordat de online omgeving anoniem kan zijn. De anonieme online omgeving vermindert de remmende factoren waardoor mensen ander, en mogelijk crimineel, gedrag vertonen (Suler, 2004). Om het online disinhibition effect te verminderen, en te voorkomen dat de remmende factoren afwezig zijn in de anonieme online omgeving, is wederom een hoge mate van zelfcontrole vereist.

Uit de theorie is gebleken dat mannen over het algemeen vaker verdacht worden van traditionele criminaliteit dan vrouwen en dat er een verschil is in het type delict (cyber of digitaal). Mannen worden hierdoor over het algemeen vaker verdacht van online criminaliteit dan vrouwen, en dit geldt nog sterker voor cybercriminaliteit in enge zin door de combinatie van een verminderde zelfcontrole bij mannen en het online disinhibition effect. De hypothese die hieruit voortkomt is:

[H2] Mannen worden vaker verdacht van online criminaliteit (cyber en gedigitaliseerd) dan vrouwen.

Voorgaand empirisch onderzoek biedt ondersteuning voor deze hypothese. Zo stelt het Centraal Bureau voor de Statistiek dat 83% van de verdachten van traditionele criminaliteit man zijn ten opzichte van 17% vrouw (CBS, 2022). Daarnaast zijn mannelijke online daders vooral actief in cybercriminaliteit in enge zin en plegen veelal delicten met een technische kant zoals hacken. Vrouwelijke cyberdaders zijn in mindere mate actief betrokken bij online criminaliteit en zijn daarbij vaker actief in gedigitaliseerde delicten zoals phishing. Gekeken naar online criminaliteit (cyber en gedigitaliseerd) is het aandeel mannelijke verdachten tussen de 78% en 95% (Weulen Kranenbarg et al., 2018).

2.1.3 Delictverleden

Verdachten van online criminaliteit hebben een beperkt delictverleden en zijn vaker first offender. Een verklaring voor het beperkte delictverleden binnen online criminaliteit is het verschil in motieven tussen cyber en gedigitaliseerde daders. Online daders hebben in eerste instantie geen gewelddadig of financieel motief om online criminaliteit te plegen. Minderjarige en (jong)volwassene daders van cybercriminaliteit in enge zin geven aan gemotiveerd te worden door nieuwsgierigheid, leergierigheid of mentale en/of technologische uitdaging (Van der Wagen, 2019). Mentale en technologische uitdaging gaat gepaard met *self challenge* waarbij cyberdaders niet alleen de technologie, maar vooral ook hun eigen kennis en expertise op de proef stellen door steeds verder te gaan en (persoonlijke) doelen te bereiken. Cyberactiviteiten kunnen een emotionele *kick* bieden bij verveling indien het (na veel moeite) toch lukt om het persoonlijke doel te bereiken. Hierbij speelt affiniteit met ICT een belangrijke rol (Aiken et al., 2016). Daarbij bevinden cyberdaders zich vaak in een grijs gebied op het internet door het online disinhibition effect. Vooral jonge cyberdaders zijn zich er hierdoor geregeld niet van bewust dat ze mogelijk strafbare feiten plegen en daardoor aangemerkt kunnen worden als cyberdader. Cyberdaders die zich wel bewust zijn van de strafbare feiten, schatten de pakkans voor zichzelf laag in. Indien een cyberdader dan toch wordt opgepakt, en vervolgd, vermindert dit de kans op recidive aanzienlijk omdat ze, ondanks hun verwachte lage

pakkans, toch zijn gepakt. De combinatie van de leeftijd van cyberdaders en de lage pakkans bij cybercriminaliteit, kan ertoe leiden dat daders van cybercriminaliteit in enge zin vaker *first offenders* zijn (Van der Wagen et al., 2019).

Verder is een onderscheid te maken tussen motieven voor het plegen van cybercriminaliteit in enge zin en gedigitaliseerde criminaliteit, waarbij aan het laatste tevens meerdere motieven kunnen spelen. Daders van gedigitaliseerde criminaliteit kunnen in een eerder stadium vanuit traditionele criminaliteit, of in en later stadium van cybercriminaliteit in enge zin, een financieel motief ontwikkelen (Van der Wagen et al., 2019). Bij gedigitaliseerde criminaliteit kan namelijk sprake zijn van *digital drift,* door het veelvuldige gebruik van het internet en technologie worden bestaande vormen van traditionele criminaliteit gefaciliteerd en/of geïntensiveerd. Het is daarom voor traditionele daders vanuit een winstoogmerk voordelig om mee te gaan in deze digitale drift aangezien het een efficiëntere werkwijze betreft met een relatief lagere pakkans (Goldsmith & Brewer, 2015). Voor daders van gedigitaliseerde criminaliteit is het daarom aannemelijk dat ze actief zijn in andere markten. Deze veronderstelling wordt bevestigd in een onderzoek naar cybernetwerken waarbij gedigitaliseerde daders met een financieel motief ook secundaire (traditionele) criminele activiteiten hadden (Leukfeldt et al., 2017).

Het verschil in motieven tussen daders van cybercriminaliteit in enge zin en gedigitaliseerde criminaliteit, gaat gepaard met verschillen in het delictverleden. De hypothese hierbij is:

[H3] Het aantal first offenders is groter bij verdachten van cybercriminaliteit in enge zin ten opzichte van verdachten van gedigitaliseerde criminaliteit.

Voorgaand empirisch onderzoek toont aan dat jeugdcriminaliteit in Nederland in zijn geheel daalt (Van der Laan et al., 2021). Een mogelijke verklaring hiervoor is een verminderde criminaliteitsfrequentie waarbij minder jongeren, minder frequent in contact komen met justitie. De groep jongeren met een delictverleden die in contact komen met justitie wordt hierdoor kleiner en selectiever. Het delictverleden binnen online criminaliteit is beperkt in kaart te brengen aan de hand van opgespoorde online verdachten. Het schetst namelijk geen compleet beeld van alle online criminaliteit door de mogelijke oververtegenwoordiging van specifieke online daders (degenen die zowel opgespoord als veroordeeld zijn) in de politieregistraties. Daarnaast is de veronderstelling dat online daders een ander type delictverleden hebben dan traditionele daders. Het delictverleden van traditionele daders, waarover mogelijk meer informatie bekend is, kan hierdoor niet als voorspeller voor het delictverleden van online daders worden gebruikt (Boschman et al., 2022).

2.2 Online netwerk

Een online netwerk wordt bestudeerd aan de hand van netwerkanalyses, cybercrimescripts, geografische afstand en onderlinge verbintenis, waarmee inzicht wordt verkregen in het functioneren van het netwerk. Er worden hierbij deelvragen opgesteld en geen hypothesen.

2.2.1 Netwerkanalyse

Het analyseren van criminele netwerken biedt belangrijke inzichten en aanknopingspunten ter bestrijding van criminaliteit. Door het netwerk van online daders te analyseren wordt inzicht verkregen in online criminaliteit als relationeel verschijnsel, waarbij meerdere partijen bestaande uit individuele personen in hun eigen context, deel uitmaken van een groter (georganiseerd) verband. Het netwerk wordt geanalyseerd aan de hand van vier elementen: *actoren* (i.e. daders), *relaties* (verbindingen tussen de actoren), *posities* (relatieve posities van actoren) en het *functioneren* van het netwerk als geheel. Elk element uit de netwerkanalyse heeft bepaalde kenmerken. Zodra het netwerk in kaart is gebracht, kunnen kenmerken van actoren worden bestudeerd aan de hand van afzonderlijke daderkenmerken (i.e. leeftijd, geslacht, delictverleden) en sociale kenmerken. Daarna kunnen relatiekenmerken worden bestudeerd aan de hand van informele en vrijwillige relaties (i.e. vriendschap) en formele voorgeschreven relaties (i.e. taakafhankelijkheid). Vervolgens kunnen positiekenmerken worden onderzocht aan de hand van centraliteitsmaten die inzicht bieden in zogeheten *sleutelfiguren* (zie §3.2.2 Netwerkanalyse). Dit zijn cruciale individuele actoren die veel invloed hebben binnen het netwerk. Deze elementen hebben samen invloed op het functioneren van het netwerk als geheel. Dit uit zich in risico- en succesfactoren in het netwerk doordat de netwerkkenmerken van invloed zijn op de prestaties en de duurzaamheid in het samenwerkingsverband (van der Hulst, 2008).

Zodra het netwerk is geanalyseerd, kan er geïntervenieerd worden om het netwerk effectief te ontwrichten. Het effectief ontwrichten van een netwerk kan vanuit de sociaal-kapitaal benadering op vier verschillende niveaus: individueel, subgroep, peer-to-peer en netwerk. De eerste drie niveaus zijn interventies op personen. Hierbij is het van belang om de context van het netwerk in kaart te brengen door netwerkinformatie in te zetten voor gedragsverandering. Dit gebeurt aan de hand van strategische relaties en geografische afstand van het netwerk. Interventies op individueel niveau zijn het identificeren en verwijderen van strategische personen uit het netwerk. Strategische personen zijn bijvoorbeeld personen met de meeste, of de belangrijkste relaties in het netwerk. Een interventie op het niveau van subgroepen is segmentatie waarbij bepaalde personen in het netwerk op worden opgesplitst in kleinere subgroepen. Personen kunnen bijvoorbeeld worden gesegmenteerd aan de hand van hun rol in het netwerk of hun activiteit in een bepaalde criminele markt. Een interventie op het niveau

van peer-to-peer is inductie waarbij bestaande relaties tussen personen in het netwerk worden ingezet om bijvoorbeeld informatie te verspreiden of gewenst gedrag te bevorderen. Het effect van interveniëren op een persoon, gaat over op de relaties van die persoon in het netwerk. Een interventie op het niveau van het netwerk is netwerkaanpassing door bijvoorbeeld personen te verwijderen of toe te voegen aan het netwerk en relaties tussen personen te verbreken of juist mogelijk te maken, op een niveau dat de samenstelling van het gehele netwerk veranderd (Valente, 2012).

Het toepassen van een netwerkanalyse levert informatie op over interacties, activiteiten en structuren tussen personen in het netwerk. De bevindingen die hieruit voortkomen kunnen ondersteunen bij het begrijpen, en voorspellen, van gedrag van personen in het netwerk, wat vervolgens kan bijdragen aan het effectief ontwrichten van het netwerk (van der Hulst, 2008).

2.2.2 Crimescript

Crimescripting is een vorm van situationele misdaadpreventie en kan ingezet worden bij het verrichten van netwerkanalyses doordat het inzicht biedt in hoe het criminele netwerk functioneert. Met crimescripting wordt uitgewerkt welke activiteiten, door welke personen, verricht worden, en hoe de rollen, posities en processen met elkaar verbonden zijn (Reyns, 2010). Crimescripting biedt inzicht in de procedurele aspecten van een bepaalde vorm van criminaliteit door het proces stapsgewijs uit te werken. Hierdoor kan met actuele en concrete kennis en informatie criminaliteit bestreden worden (Dehghanniri & Borrion, 2019).

Een crimescript kan inzicht bieden in de modus operandi van een bepaalde vorm van criminaliteit waarbij online criminaliteit verschillende vormen kent. In een onderzoek naar de typologieën van cybernetwerken omtrent online bankieren, zijn vier typen cybercrimescripts te onderscheiden (zie tabel 1). De crimescripts van de cybernetwerken worden getypeerd op basis van de mate van technologische expertise en interactie tussen de dader en het slachtoffer. Het eerste type crimescript wordt gekenmerkt door *low-tech* criminaliteit met een hoge mate van interactie tussen de dader en het slachtoffer. Een voorbeeld hiervan is phishing met e-mails en valse linkjes waarna daders telefonisch contact opnemen met het slachtoffer. Het tweede type crimescript wordt gekenmerkt door *low-tech* criminaliteit met een *lage* mate van interactie tussen de dader en het slachtoffer. Een voorbeeld hiervan is phishing met e-mails en valse linkjes waarbij de phishing-site zeld de informatie van het slachtoffer doorspeelt naar de dader. Het derde type crimescript wordt gekenmerkt door *high-tech* criminaliteit met een *lage* mate van interactie tussen de dader en het slachtoffer. Een voorbeeld hiervan is het verspreiden van malware per mail die de computer van het slachtoffer infecteert, en de dader controle geeft over de computer, zonder dat het slachtoffer dit opmerkt. Het vierde type

crimescript wordt gekenmerkt door *high-tech* criminaliteit *zonder* interactie tussen de dader en het slachtoffer. Een voorbeeld hiervan is het infecteren van websites met verouderde beveiliging. Zodra op de website wordt geklikt, wordt de computer van het slachtoffer geïnfecteerd met malware, zonder dat het slachtoffer dit opmerkt (Leukfeldt et al., 2017).

Mate van interactie tussen dader en slachtoffer	***Low - Tech***	***High - Tech***
Geen		Type 4
Laag	Type 2	Type 3
Hoog	Type 1	

Tabel 1: Cybercrimescripts

Online criminaliteit kent verschillende crimescripts op basis van de vorm van online criminaliteit, de technische skills van de dader en de interactie met het slachtoffer. Crimescripts omvatten belangrijke elementen die inzicht bieden in de modus operandi van online daders en vullen daarmee bestaande kennis aan.

2.2.3 Geografische afstand

Het internet is continu en wereldwijd. Dit stelt personen in staat om voortdurend met elkaar in contact te zijn en dit kan bevorderend zijn voor online criminaliteit (Odinot et al., 2018). Uit de verkenning van de typologieën van cybernetwerken is gebleken dat er low-tech en high-tech criminaliteit gepleegd kan worden met weinig tot geen interactie tussen de dader en het slachtoffer. Dit stelt online daders in staat om vanuit hun eigen locatie, meerdere slachtoffers te maken op andere locaties, zonder daarvoor fysiek aanwezig te moeten zijn. Een bekend voorbeeld hiervan is de *Indian Tech Support Scams* waarin medewerkers van zogenaamde technische ondersteuningsbureaus in India, wereldwijd personen telefonisch benaderen en met listige methoden geld afhandig maken (Leukfeldt et al., 2017). De continue wereldwijde verbinding van personen stelt criminelen in staat om gedigitaliseerde criminaliteit te verrichten met het internet als facilitator. Traditionele criminaliteit gaat vaak gepaard met complexere processen waarbij toegang verkregen moet worden tot verschillende personen en verschillende locaties. Deze processen dienen in tijd en ruimte op elkaar afgestemd te worden. Het internet vereenvoudigt de processen door ze te digitaliseren en waardoor minder behoefte is aan fysieke aanwezigheid van personen. Het leggen van contacten, het coördineren van activiteiten en het samenwerken van personen op verschillende tijden en locaties, is mogelijk van achter de computer en smartphone (Odinot et al., 2018).

In het onderzoek naar de typologieën van cybernetwerken zijn internationale componenten onderzocht aan de hand van het land van herkomst van de daders en slachtoffers. Bij low-tech

criminaliteit opereren de daders voornamelijk vanuit Nederland en rekruteren ze geldezels in Nederland. In enkele gevallen is er een connectie met een facilitator in het buitenland die bijvoorbeeld phishing websites ontwikkeld. Bij high-tech criminaliteit opereren de daders zowel vanuit Nederland als vanuit het buitenland. Vanuit het buitenland worden personen, malware en certificaten ingekocht, die vervolgens in Nederland worden ingezet. In enkele gevallen worden geldezels gerekruteerd vanuit het buitenland. Dit gaat mogelijk gepaard met mensenhandel en fraude met vervalste papieren om bijvoorbeeld bankrekeningen te openen (Leukfeldt et al., 2017).

Het internet biedt de mogelijkheid om de geografische afstand van een crimineel netwerk te vergroten waardoor de geografische afstand van daders, en slachtoffers, op voorhand beperkt is in te schatten. Criminele online netwerken kunnen een groot netwerk omvatten, met een kleine geografische afstand, of een klein netwerk met een grote geografische afstand afhankelijk van het type online criminaliteit.

2.2.4 Verbintenis

Het internet stelt personen in staat om continu in contact te komen met andere personen waaronder andere online daders, oftewel personen die in de fysieke wereld lastig te bereiken zijn. Hierdoor kan er efficiënt, en mogelijk ook op grote schaal, aansluiting en verbinding gevonden worden tussen personen met gelijke waarden en interesses. Dit fenomeen wordt aangeduid als *homophily*, oftewel, soort zoekt soort. Personen zijn vaker geneigd om te gaan met gelijkgestemde personen, en het contact met gelijkgestemden kan frequenter voorkomen dan met andere personen (McPherson et al., 2001). Homophily kan online en in de fysieke wereld voorkomen waarbij het internet de mogelijkheid biedt om wereldwijd verbonden te blijven met gelijkgestemden. Een nevenwerking hiervan is dat (potentiële) online daders met elkaar in contact kunnen komen zoals is gebleken uit internationale cybernetwerken (§2.2.2).

Een verklaring hiervoor is te vinden in de *sociaal leren* theorie van Bandura (1971). De sociaal leren theorie verondersteld dat sociaal gedrag wordt aangeleerd door het gedrag van anderen te observeren en te imiteren. Sociaal leren is van significant belang voor cybercriminaliteit. Daders van cybercriminaliteit leren door andere cyberdaders te observeren en te imiteren met betrekking tot technologische vaardigheden en illegaal computergebruik. De sociaal leren theorie bevat vier componenten. Het eerste component is *differentiële associatie*. Het omvat de intensiteit, frequentie en duur van de relaties die personen hebben met andere personen die wel of geen crimineel gedrag vertonen. Indien personen omgaan met andere personen die cybercriminaliteit plegen, wordt de kans groter dat ze zelf ook cybercriminaliteit plegen. Het tweede component is *definities*. Dit omvat de houding en percepties van personen omtrent

crimineel gedrag en in hoeverre het gedrag wordt gerechtvaardigd. Hoe meer het gedrag wordt gerechtvaardigd, des te meer het gedrag wordt geaccepteerd. Het derde component is *differentiële versterking*. De waarschijnlijk van crimineel gedrag wordt vergroot als hier een positieve versterking (i.e. beloning) tegenover staat. De waarschijnlijkheid van crimineel gedrag neemt af als hier een negatieve versterking (i.e. straf) tegenover staat. Het vierde component is *imitatie*, het op een zelfde manier na doen van geobserveerd gedrag (Holt et al., 2010).

Homophily en de sociaal leren theorie kunnen van invloed zijn op het verbinden van personen binnen zowel cybercriminaliteit in enge zin als gedigitaliseerde criminaliteit. Echter, aan gedigitaliseerde criminaliteit kunnen meerdere motieven ten grondslag liggen, waaronder een financieel motief. Daarom is sociaal leren geen vereiste voor het verbinden van verschillende personen in gedigitaliseerde criminaliteit aangezien contacten ook gelegd kunnen worden op basis van de behoeften van het netwerk. Zo bestaan criminele netwerken uit vaste kernelementen en vervangbare elementen. Een voorbeeld van een vervangbaar element is een geldezel bij bankfraude. De geldezel maakt geen onderdeel uit van de vaste kernelementen en is daardoor niet volledig verbonden met het netwerk. Geldezels worden via bekenden van het kernelement, of via advertenties op sociale media, geronseld. Hierbij speelt sociaal leren een beperkte, tot zelfs geen, rol (Leukfeldt et al., 2017).

3. Methoden

In dit hoofdstuk worden de mixed-methods onderzoeksmethoden uitgewerkt. In §3.1 wordt behandeld hoe het online daderprofiel wordt geschetst en §3.2 behandeld hoe het online netwerk in kaart wordt gebracht.

3.1 Online daderprofiel

Het eerste deel van de onderzoeksvraag: “wat zijn de kenmerken van online daders” wordt beantwoord met een online daderprofiel voor verdachten van online criminaliteit in Noord-Nederland in 2021. De data hiervoor is verkregen via het cybercrimeteam van de politie. Binnen de politie wordt de Basis Voorziening Handhaving (BVH) gebruikt om aangiften te registreren en af te handelen en om informatie op te vragen over aangiften, incidenten en antecedenten van verdachten. De BVH bevat ook een lijst met maatschappelijke klassen (MK) waaronder de aangiften en incidenten worden geclassificeerd door de politie. De dataset genaamd *Kopie van verdachten online criminaliteit uit Eenheid Noord-Nederland (ENN) kennisnamedatum 2021 – BlueIntel* omvat alle verdachten van cyber en gedigitaliseerde criminaliteit in 2021. De selectie van verdachten is gemaakt aan de hand van de Landelijke Query Cybercrime. Een query wordt gebruikt om misinterpretatie en misclassificatie, van aangiften en incidenten binnen de politie te voorkomen. De cybercrimequery geeft aan wat wordt aangemerkt als cybercriminaliteit in enge zin en wat wordt aangemerkt als gedigitaliseerde criminaliteit op basis van vooraf vastgestelde zoektermen en criteria. De Landelijke Query Cybercrime bevat verschillende maatschappelijke klassen (zie tabel 2).

Online criminaliteit	Code	Maatschappelijke Klasse
Cybercriminaliteit in enge zin	F90	Cybercrime
Gedigitaliseerde criminaliteit	A81	Heling
	A82	Chantage/afpersing
	A95	Overig gekwalificeerde diefstal
	F51	Belediging
	F522	Aanranding
	F530	Bedreiging
	F531	Overige misdrijven tegen de persoonlijke vrijheid
	F533	Stalking
	F550	Eenvoudige mishandeling
	F561	Mensenhandel seksuele uitbuiting
	F614	Fraude met betaalproducten
	F617	Identiteitsfraude
	F620	Overige horizontale fraude
	F636	Fraude met online handel
	F94	Witwassen
Overig	D43	Rijden zonder rijbewijs
	G44	Onderzoek overig

Tabel 2: Maatschappelijke klassen uit de Landelijke Query Cybercrime

De dataset bevat in totaal 286 verdachten inclusief informatie over de verdachten en het delict. Enkele verdachten worden vaker in de dataset vermeld omdat ze meermaals een online delict hebben gepleegd in 2021. Het aantal unieke online verdachten is berekend en de variabelen leeftijd, geslacht en delictverleden zijn geoperationaliseerd. Vervolgens is met kwantitatieve onderzoeksmethoden een profiel opgesteld voor cyber en gedigitaliseerde verdachten.

3.1.1 Operationalisaties

De variabele leeftijd wordt gemeten aan de hand van *leeftijd* in de dataset. Leeftijd is een continue variabele en toont de leeftijd van de verdachten op het moment dat het delict werd gepleegd. Aan de hand van beschrijvende statistieken wordt het: gemiddelde, minimum, maximum, modus en mediaan van de leeftijd berekend voor alle online verdachten en afzonderlijk voor cyberverdachten en gedigitaliseerde verdachten.

De variabele geslacht wordt gemeten aan de hand van *geslacht_binair* in de dataset. Geslacht is een binaire variabele bestaande uit de scoremogelijkheden man (0) en vrouw (1). Met behulp van beschrijvende statistieken wordt het aantal en het percentage mannelijke en vrouwelijke online verdachten berekend, waarbij onderscheid wordt gemaakt tussen cyberverdachten en gedigitaliseerde verdachten.

De variabele delictverleden wordt gemeten aan de hand de variabele *delictverleden_cat*, deze categorische variabele wordt gebruikt voor de beschrijvende statistieken en bestaat uit vijf mogelijke categorieën: geen (0), cybercrime (1), gedigitaliseerd (2), traditioneel (3) en gemengd (4) delictverleden. Het gemengde delictverleden beschrijft een delictenverleden bestaande uit delicten van zowel online als traditionele aard. Voor de categorisering van maatschappelijke klassen wordt de Landelijke Query Cybercrime aangehouden (zie tabel 2). Om het delictverleden van een verdachte te kunnen categoriseren is het BSN-nummer en het delict registratienummer gebruikt om in *Bluespot Monitor* alle strafbare feiten waarvan de persoon verdacht is geweest te bekijken, vóór de kennisname van het delict uit de dataset. Hierbij is sprake van triangulatie doordat kwantitatieve informatie uit de BVH en kwalitatieve informatie uit proces verbaal worden gebruikt om het delictverleden te onderzoeken. Vervolgens wordt voor de hypothesetoetsing de binaire variabele *delictverleden_type* gebruikt met first offenders (0) en non first offenders (1).

3.1.2 Onderzoeksopzet

De kenmerken van de data (verhouding cyber en gedigitaliseerde verdachten, districten en maatschappelijke klassen) en van de leeftijd, het geslacht en het delictverleden worden beschreven aan de hand van beschrijvende statistieken. Vervolgens worden de hypothesen getoetst voor cyberverdachten en gedigitaliseerde verdachten met een significantieniveau van

α = 0,05. Hierbij wordt ook gekeken naar de verschillen tussen afzonderlijke maatschappelijke klassen om een gedetailleerder beeld te schetsen. Er worden in dit onderzoek univariate en bivariate analyses uitgevoerd en geen regressieanalyse doordat de variabelen afzonderlijk worden getoetst voor cyber en gedigitaliseerde verdachten ten opzichte van elkaar. Er wordt hierbij niet gekeken naar de waarschijnlijkheid van het zijn van een cyber of gedigitaliseerde verdachte, ten opzichte van personen die geen verdachte zijn. Personen die geen verdachte zijn, bevinden zich ook niet in de politiedata. Daarbij voldoet de politiedata niet altijd aan de assumpties van een regressieanalyse.

[H1] Verdachten van cybercriminaliteit in enge zin zijn jonger dan verdachten van gedigitaliseerde criminaliteit. Ten eerste worden beschrijvende statistieken berekend van de variabele *leeftijd* voor alle online verdachten. Vervolgens wordt de hypothese getoetst met een T – toets voor het vergelijken van gemiddelden van onafhankelijke groepen om de gemiddelde leeftijd van cyberverdachten en gedigitaliseerde verdachten te vergelijken, waarbij de standaardfout voor ongelijke variatie wordt gebruikt. Daarnaast wordt met een eenweg ANOVA getoetst of er verschillen zijn in gemiddelde leeftijd tussen de afzonderlijke maatschappelijke klassen van online criminaliteit.

[H2] Mannen worden vaker verdacht van online criminaliteit (cyber en gedigitaliseerd) dan vrouwen. Ten eerste worden beschrijvende statistieken en proporties berekend van de variabele *geslacht_binair* voor alle online verdachten. Daarna wordt de gemiddelde leeftijd van mannen en vrouwen getoetst aan de hand van een T – toets voor het vergelijken van gemiddelden van onafhankelijke groepen. Ten tweede wordt de hypothese getoetst met een tweezijdige Chi-kwadraattoets om de samenhang tussen geslacht en online criminaliteit te toetsen voor de onafhankelijke proporties cyberverdachte en gedigitaliseerde verdachten.

[H3] Het aantal first offenders is groter bij verdachten van cybercriminaliteit in enge zin ten opzichte van verdachten van gedigitaliseerde criminaliteit. Ten eerste worden beschrijvende statistieken van de variabele *delictverleden_cat* gegeven voor alle online verdachten en afzonderlijk voor mannen en vrouwen. Vervolgens wordt de hypothese getoetst aan de hand van de variabele *delictverleden_type* (first offender = 0, non first offender = 1), met een Chi-kwadraattoets om de samenhang tussen het delictverleden en online criminaliteit te toetsen voor cyberverdachten en gedigitaliseerde verdachten. Indien er sprake is van afhankelijkheid tussen het delictverleden en online criminaliteit, worden de gestandaardiseerde residuen gebruikt om te berekenen waar (in welke MK) de samenhang tussen het delictverleden en online daderschap ligt.

3.2 Online netwerk

Het tweede deel van de onderzoeksvraag: “hoe ziet een netwerk van online daders er uit” wordt beantwoord door het online netwerk in kaart te brengen aan de hand van politiedata voor een groep van zes geprioriteerde online verdachten in Noord-Nederland.

3.2.1 Onderzoeksopzet

Het netwerk wordt geanalyseerd aan de hand van de centraliteitsmaten die worden berekend met edgelist en nodelist data in UCINet, en de informatie uit de BVH en BVI. De centraliteitsmaten zijn: degree, closeness, betweenness, eigenvector en fragmentation. De *degree* is het aantal connecties van een persoon in het netwerk. De *closeness* geeft aan hoeveel stappen iemand dient te zetten om andere personen in het netwerk te bereiken. De laagste closeness score is hierbij de beste score. De *betweenness* geeft aan welke persoon de meest cruciale schakel is doordat deze persoon op een tussenpad ligt met andere personen in het netwerk. De *eigenvector* geeft aan welke persoon de meeste connecties heeft met andere personen die veel connecties hebben in het netwerk. De *fragmentation* duidt op de impact op het netwerk, in het geval dat een persoon uit het netwerk wegvalt. Het analyseren van de centraliteitsmaten biedt inzicht in het functioneren van het netwerk wat kan ondersteunen bij het effectief ontwrichten van het netwerk door de politie.

Zodra de centraliteitsmaten zijn geanalyseerd, kunnen de kenmerken van de actoren worden geanalyseerd. De kenmerken (leeftijd, geslacht en delictverleden) worden opgevraagd in *BVI Bluespot Monitor* en vervolgens op dezelfde manier geoperationaliseerd als het online daderprofiel (zie §3.1.1 Operationalisaties). Hierbij is wederom sprake van triangulatie door het combineren van kwantitatieve data uit de BVH en kwalitatieve data uit de BVI en proces verbaal. De netwerkanalyse biedt ondersteuning bij bestaand onderzoek van de politie eenheid Noord-Nederland naar online criminaliteit. Het doel hiervan is om inzicht te krijgen in de kern van deze groep zodat de politie zich essentiële personen kan sporen. De netwerkanalyse is een exploratieve case study dat wordt onderzocht aan de hand van de volgende deelvragen:

1. Welke personen maken deel uit van het netwerk? Hiermee wordt inzicht verkregen in *wie* de personen zijn aan de hand van de leeftijd, geslacht en woonplaats voor het hele netwerk.

2. Welke personen zijn de essentiële personen in het netwerk? Hiermee wordt inzicht verkregen in *wat* de positie van deze personen essentieel maakt voor het netwerk aan de hand van de centraliteitsmaten.

3. Wat zijn de inhoudelijke kenmerken van het netwerk? Hiermee wordt inzicht verkregen in het delictverleden, de activiteiten en de verbindingen van de Amazonegroep in het netwerk.

4. Resultaten

In dit hoofdstuk worden de resultaten behandeld. In §4.1 wordt het online daderprofiel uitgewerkt aan de hand van beschrijvende statistieken en hypothesetoetsing van de leeftijd, het geslacht en het delictverleden van online verdachten. In §4.2 wordt het online netwerk behandeld aan de hand van een netwerkanalyse.

4.1 Online daderprofiel

De dataset bevat 286 online delicten in Noord-Nederland in 2021. Het aantal unieke online verdachten is berekend aan de hand van het BSN-nummer. Van de BSN-nummers die meermaals voorkwamen in de dataset, werd één vermelding behouden en zijn de rest verwijderd uit de dataset omdat dit aantoont dat een verdachte meerdere online delicten heeft gepleegd in 2021. Het meest recente online delict uit 2021 werd behouden en de delicten die daarvoor zijn gepleegd, zijn verwijderd uit de dataset omdat deze delicten behoren tot het delictverleden. De dataset bestaat uit 255 unieke online verdachten waarvan 67 personen (26,3%) verdacht worden van cybercriminaliteit in enge zin en 188 personen (73,7%) verdacht worden van gedigitaliseerde criminaliteit. De online verdachten zijn woonachtig in Noord-Nederland waaronder de districten Groningen (114), Drenthe (74) en Friesland (67) vallen (zie bijlage 1.1).

Online criminaliteit	Code	Maatschappelijke Klasse	Frequentie	Percentage
Cybercriminaliteit in enge zin	F90	Cybercrime	67	26,3
Gedigitaliseerde criminaliteit	A81	Heling	2	0,8
	A82	Chantage/afpersing	20	7,8
	A95	Overig gekwalificeerde diefstal	2	0,8
	F51	Belediging	9	3,5
	F522	Aanranding	1	0,4
	F530	Bedreiging	3	1,4
	F531	Overige misdrijven tegen de persoonlijke vrijheid	2	0,8
	F533	Stalking	7	2,7
	F550	Eenvoudige mishandeling	3	1,2
	F561	Mensenhandel seksuele uitbuiting	5	2,0
	F614	Fraude met betaalproducten	40	15,7
	F617	Identiteitsfraude	9	3,5
	F620	Overige horizontale fraude	75	29,4
	F636	Fraude met online handel	6	2,4
	F94	Witwassen	2	0,8
Overig	D43	Rijden zonder rijbewijs	1	0,4
	G44	Onderzoek overig	1	0,4

Tabel 3: Frequentietabel maatschappelijke klassen (N = 255)

De frequenties van de maatschappelijke klassen uit de Landelijke Query Cybercrime staan vermeld in tabel 3 waarbij enkel de maatschappelijke klasse F90 cybercriminaliteit in enge zin

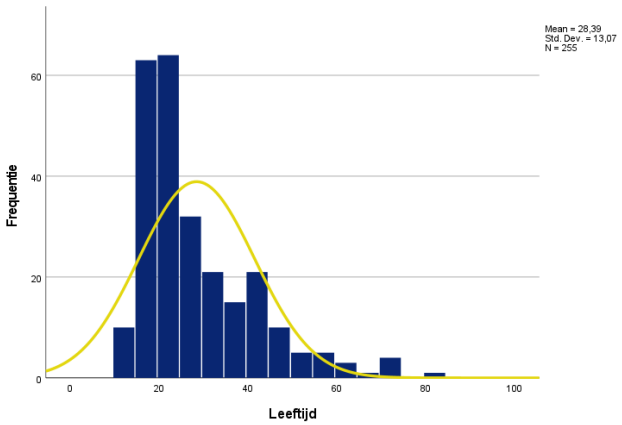
betreft. Gekeken naar gedigitaliseerde criminaliteit komen de volgende maatschappelijke klassen het meest voor: F620 overige horizontale fraude (i.e. vriend-in-nood Whatsappfraude) 29,4%, F614 fraude met betaalproducten (i.e. bankhelpdeskfraude en geldezels) 15,7% en A82 chantage/afpersing (i.e. chanteren met seksueel getinte foto's) 7,8%. De delicten zijn verder te verdelen aan de hand van hoofd- en subcategorieën. De meest voorkomende hoofdcategorieën zijn: fraude/oplichting (76,5%), afpersing/chantage (8,2%) en persoonlijke delicten gericht op de zakelijke sfeer (5,5%). De meest voorkomende subcategorieën zijn: fraude bankgegevens/internetbankieren (54,1%), vriend-in-nood Whatsappfraude (6,7%) en accountmisbruik om online bestellingen te plaatsen (5,5%). Opvallend is dat de meest voorkomende gedigitaliseerde delicten een financieel component hebben (zie bijlage 1.2).

4.1.1 Leeftijd

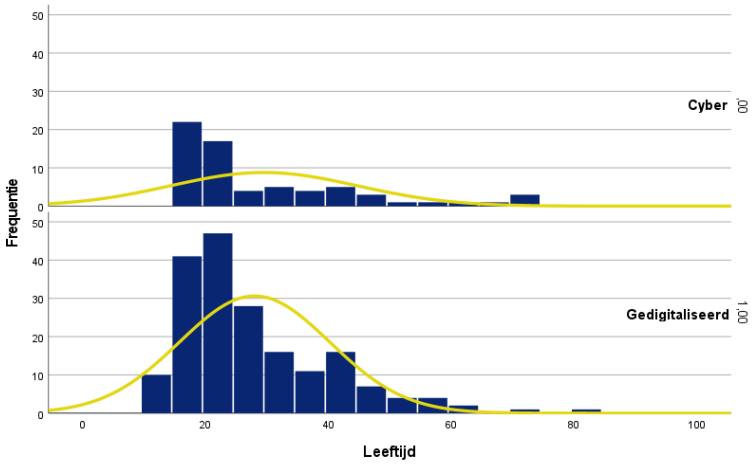
De gemiddelde leeftijd van de online verdachten is 28,39 jaar (*s* = 13,07) met een minimum leeftijd van 12 jaar en een maximum leeftijd van 81 jaar (zie tabel 4). In combinatie met de hoogste gemiddelde leeftijd van 31,61 jaar (*s* = 15,93) maakt dit district Friesland het oudste district. District Drenthe is het jongste district met leeftijden tussen de 14 en 54 jaar. Er zijn geen significante leeftijdsverschillen gevonden tussen de districten ($F(2) = 2{,}82$; $p = 0{,}61$). De meest voorkomende leeftijd is 19 jaar, deze leeftijd komt 24 keer voor. Daarop volgt 18 jaar, dit komt 22 keer voor en vervolgens 20 jaar, dit komt 16 keer voor. Van de 255 online verdachten, zijn 49 verdachten minderjarig (19,2%) met een leeftijd tussen de 12 en 18 jaar, en zijn 76 verdachten jongvolwassen (29,8%), met een leeftijd tussen de 18 en 23 jaar. In totaal zijn 125 van de 255 online verdachten minderjarig of jongvolwassen (12 t/m 23 jaar), dit is met 49,0% net minder dan de helft van alle verdachten (zie bijlage 1.3). Figuur 2 toont aan dat de leeftijd van de online verdachten rechtsscheef verdeeld is.

	Gemiddelde	Std. Deviatie	Minimum	Maximum	Mediaan
District Groningen	27,07	12,77	13,00	71,00	23,00
District Drenthe	27,51	9,97	14,00	54,00	25,00
District Friesland	31,61	15,93	12,00	81,00	24,00
Mannen	28,74	13,53	12,00	81,00	24,00
Vrouwen	27,30	11,52	13,00	64,00	23,00
Totaal online verdachten	28,39	13,07	12,00	81,00	24,00

Tabel 4: Beschrijvende statistieken leeftijd (N = 255)



Figuur 2: Histogram leeftijd online verdachten

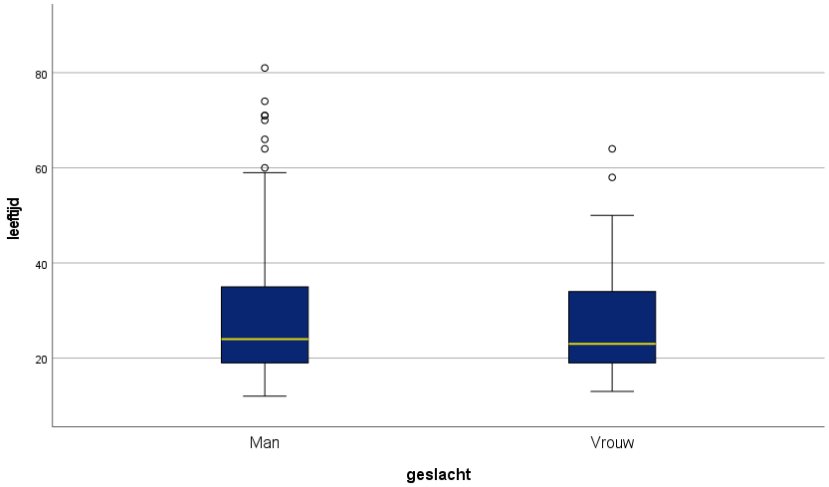


Figuur 3: Verdeling leeftijd cyber en gedigitaliseerde verdachten

De gemiddelde leeftijd van cyberverdachten is 29,51 jaar (*s* = 15,20) en van gedigitaliseerde verdachten is 27,99 jaar (*s* = 12,24). Figuur 3 toont aan dat de leeftijd tussen cyberverdachten en gedigitaliseerde verdachten redelijk gelijk is verdeeld. Er is hierbij geen significant verschil gevonden tussen de gemiddelde leeftijd van verdachten van cybercriminaliteit in enge zin en verdachten van gedigitaliseerde criminaliteit (*t*(98,2) = 0,734; *p* = 0,465). Verder is gekeken naar de verschillen in gemiddelde leeftijd op basis van de maatschappelijke klassen van online criminaliteit (zie tabel 2), waarbij wel een signifcant verschil is gevonden in de gemiddelde leeftijd (*F*(17) = 1,994; *p* = 0,012). Echter, aan de hand van gestandaardiseerde residuen is gebleken dat dit significante verschil wordt veroorzaakt door verschillen in leeftijd tussen de maatschappelijke klassen behorende tot gedigitaliseerde criminaliteit, en niet tussen cybercriminaliteit in enge zin (MK F90) en gedigitaliseerde criminaliteit (alle andere MK's). De hypothese, dat verdachten van cybercriminaliteit in enge zin jonger zijn dan verdachten van gedigitaliseerde criminaliteit, wordt hierbij verworpen (zie bijlage 2.1).

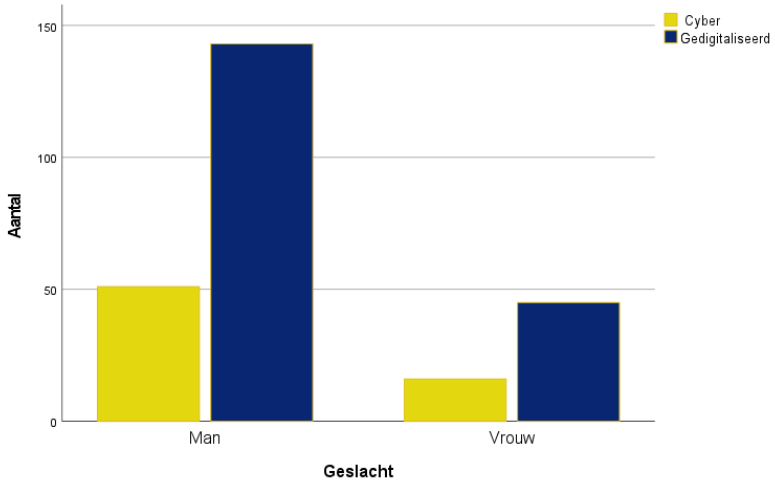
4.1.2 Geslacht

De online verdachten bestaan uit 194 mannen (76,1%) en 61 vrouwen (23,9%). Mannelijke verdachten hebben een gemiddelde leeftijd van 28,74 jaar (*s* = 13,53), een minimum leeftijd van 12 jaar en een maximum leeftijd van 81 jaar. Vrouwelijke verdachten hebben een gemiddelde leeftijd van 27,30 jaar (*s* = 11,52) (zie figuur 4). De jongste vrouwelijke verdachte is 13 jaar en de oudste vrouwelijke verdachte is 64 jaar (zie bijlage 1.4). Er is geen significant verschil gevonden tussen de gemiddelde leeftijd van mannelijke verdachten ten opzichte van vrouwelijke verdachten (*t*(117) = 0,816; *p* = 0,416). Tot slot is gekeken naar de samenhang tussen het geslacht en het district. Er is geen significante samenhang gevonden tussen het geslacht van verdachten en het district waarin hij of zij woonachtig is (X^2(2) = 0,538; *p* = 0,764).



Figuur 4: Boxplot geslacht en leeftijd online verdachten

Er zijn 67 verdachten van cybercriminaliteit in enge zin, waarvan 51 man en 16 vrouw, en 188 verdachten van gedigitaliseerde criminaliteit, waarvan 143 man en 45 vrouw (zie tabel 5). De proportie mannelijke cyberverdachten is 0,76 ten opzichte van de porportie vrouwelijke cyberverdachten 0,24. De proportie mannelijke gedigitaliseerde verdachten is 0,76 ten opzichte van de proportie vrouwelijke gedigitaliseerde verdachten 0,24. Er is geen significante samenhang gevonden tussen het geslacht van cyberverdachten en gedigitaliseerde verdachten ($X^2(1) <.001$; $p = 0{,}993$). Sterker nog, de verhouding tussen mannen en vrouwen is vrijwel gelijk (zie figuur 5). Daarnaast is gekeken naar het verschil tussen mannen en vrouwen aan de hand van de maatschappelijke klassen van online criminaliteit waarbij ook geen sprake is van een significante samenhang tussen mannelijke en vrouwelijke verdachten ($X^2(17) = 23{,}18$; $p = 0{,}145$). De hypothese, dat mannen vaker worden verdacht van cybercriminaliteit in enge zin en gedigitaliseerde criminaliteit ten opzichte van vrouwen, wordt hierbij verworpen (zie bijlage 2.2).



Figuur 5: Verdeling geslacht cyber en gedigitaliseerde verdachten

Geslacht	Cyber	π	Gedigitaliseerd	π	Totaal
Man	51	0,761	143	0,761	194
Vrouw	16	0,239	45	0,239	61
Totaal	67	1,000	188	1,000	255

Tabel 5: Kruistabel geslacht en online criminaliteit (N = 255).

4.1.3 Delictverleden

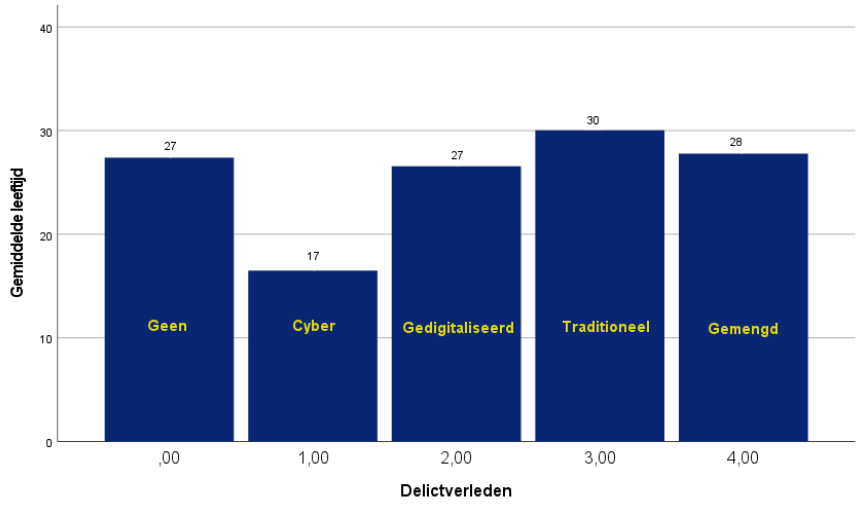
De 225 online verdachten hebben een delictverleden bestaande uit 2266 incidenten, activiteiten en antecedenten (zie bijlage 1.5). Tabel 6 toont aan dat van de 255 online verdachten, 63 verdachten (24,7%) geen delictverleden hebben en daarmee first offenders zijn. Dit houdt in dat ze niet eerder verdacht zijn geweest van een strafbaar delict. Echter, dit betekent niet altijd dat de persoon niet bekend is bij de politie. De online verdachten zonder delictverleden kunnen bekend zijn bij de politie als betrokkene of aangever van een ander delict, of hebben een waarschuwing gekregen van de politie (i.e. geluidsoverlast, verkeersovertreding). Van de 255 online verdachten hebben 65 verdachten (25,5%) een gemengd delictverleden. Dit houdt in dat ze eerder verdacht zijn geweest van zowel een traditioneel als een online delict (cyber of gedigitaliseerd). Dit is mogelijk een verklaring voor het lage aandeel verdachten met een online delictverleden. Slechts 25 personen (9,8%) zijn eerder verdacht geweest van enkel online delicten, waarvan 23 personen eerder verdacht zijn geweest van gedigitaliseerde criminaliteit en 2 personen eerder verdacht zijn geweest van cybercriminaliteit in enge zin. Het merendeel van de online verdachten heeft een traditioneel delictverleden (40,0%).

Delictverleden	Frequentie	Percentage
0. Geen delictverleden	63	24,7
1. Cyber delictverleden	2	0,8
2. Gedigitaliseerd delictverleden	23	9,0
3. Traditioneel delictverleden	102	40,0
4. Gemengd delictverleden	65	25,5

Tabel 6: Beschrijvende statistieken delictverleden (N = 255).

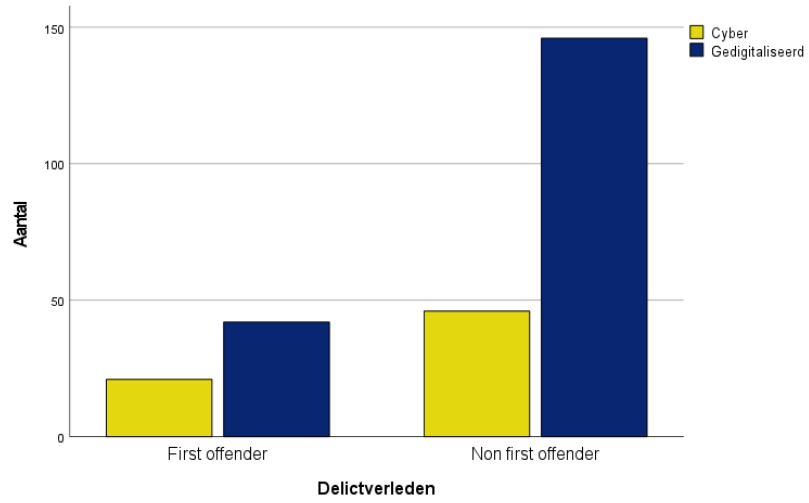
De categorieën van het delictverleden verschillen onderling signifcant van elkaar wat aantoont dat niet alle groepen even groot zijn ($t(254) = 25,59$; $p < .001$). Daarnaast is gekeken naar de verschillen in gemiddelde leeftijd tussen de categorieën van het delictverleden (zie figuur 6). Er zijn geen significante verschillen gevonden in de gemiddelde leeftijd van de verdachten met een bepaald delictverleden ($F(4) = 1,059$; $p = 0,378$). Verder is gekeken naar de afhankelijkheid tussen het geslacht en het delictverleden waarbij wel sprake is van een significante samenhang ($X^2(4) = 14,80$; $p < .01$). Aan de hand van de gestandaardiseerde

residuen is gebleken dat de samenhang lijkt te liggen tussen vrouwelijke online verdachten met een gedigitaliseerd delictverleden en vrouwelijke online verdachten met een gemengd delictverleden (zie bijlage 1.5).



Figuur 6: Staafdiagram gemiddelde leeftijd per delictverleden

Er zijn 21 first offenders van de 67 cyberverdachten (π = 0,313) en 42 first offenders van de 188 gedigitaliseerde verdachten (π = 0,223) (zie figuur 7). Cyberverdachten zijn niet vaker first offender dan gedigitaliseerde verdachten ($X^2(1) = 2{,}152$; $p = 0{,}142$). De hypothese, dat het aantal first offenders significant groter is bij verdachten van cybercriminaliteit ten opzichte van verdachten van gedigitaliseerde criminaliteit, wordt hierbij verworpen (zie bijlage 2.3).



Figuur 7: Verdeling delictverleden cyber en gedigitaliseerde verdachten

Gekeken naar de vijf categorieën van het delictverleden, zijn ook hier geen significante verschillen gevonden tussen het delictverleden van cyberverdachten en gedigitaliseerde verdachten ($X^2(4) = 3{,}025$; $p = 0{,}554$). Verder valt op dat er zowel 1 verdachte van cybercriminaliteit in enge zin, als 1 verdachte van gedigitaliseerde criminaliteit een cyber

delictverleden heeft. Daarnaast heeft zowel het hoogste aantal verdachten van cybercriminaliteit in enge zin, als van verdachten van gedigitaliseerde criminaliteit, een traditioneel delictverleden (zie tabel 7).

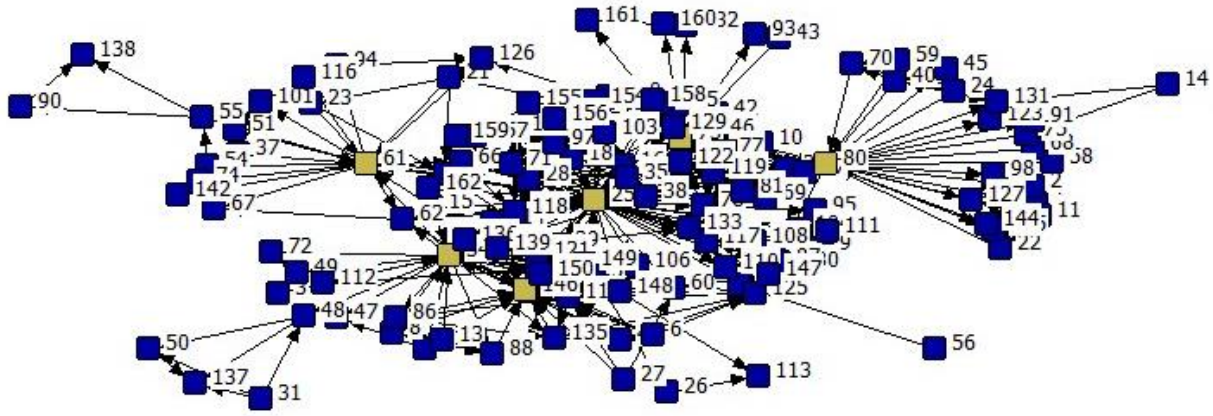
Delictverleden	Cyber	Gedigitaliseerd	Totaal
0. Geen delictverleden	21	42	63
1. Cyber delictverleden	1	1	2
2. Gedigitaliseerd delictverleden	6	17	23
3. Traditioneel delictverleden	23	79	102
4. Gemengd delictverleden	16	49	65
Totaal first offenders	21	42	63
Totaal non first offenders	46	146	192
Totaal	67	188	255

Tabel 7: Kruistabel online criminaliteit en delictverleden (N = 255).

4.2 Online netwerk

Het netwerk van de Amazonegroep is in kaart gebracht aan hand van bestaande relaties met andere personen. Dit zijn personen die elkaar kennen doordat ze samen als verdachte of betrokkene zijn aangemerkt door de politie, waarbij de delicten zijn gefilterd op maatschappelijke klasse (zie bijlage: Maatschappelijke Klassen). De verzameling is hierbij als volgt gegaan. Ten eerste is een lijst met *KenO's* (uniek kenmerk van naam en geboortedatum van de persoon) door het BVH politiesysteem gehaald. Vervolgens zijn alle voorvallen geselecteerd waarin personen de afgelopen vier jaar samen met (iemand uit) de Amazonegroep als verdachte of betrokkene zijn voorgekomen. Er is hierbij bewust voor voorvallen gekozen en niet voor registraties omdat registraties uit meerdere voorvallen kunnen bestaan. Op basis van het samen voorkomen in een voorval is de aanname gedaan dat de persoon een relatie heeft met de Amazonegroep. De personen zijn samengevoegd tot een *nodelist* bestaande uit 162 personen. Dit is de standaard werkwijze van de landelijke eenheid in het onderzoeken van fluïde netwerken. Het netwerk is gefragmenteerd doordat alleen personen met de rol verdachte en betrokkene zijn geselecteerd. Het gaat hierbij dus niet perse om een kennisrelatie en relaties op basis van andere rollen (i.e. bestuurder, getuige, slachtoffer) zijn weggelaten waardoor het netwerk in totaal uit 150 personen bestaat die (indirect) relatie hebben met de Amazonegroep. Zij vormen samen de *edgelist*. Hierbij speelt het dark number ook een rol bij de fragmentatie van het netwerk. De politie heeft alleen zicht op de personen die samen zijn gepakt. Personen die tijd met elkaar spenderen, zonder gepakt te worden, zijn in feite onzichtbaar voor de politie.

Het totale netwerk bestaat uit 162 personen (nodelist), waarvan het netwerk verder wordt gefragmenteerd in 150 personen (edgelist) die verdeeld zijn over een groot component en kleinere losse componenten (zie bijlage 3.2). Figuur 8 toont het netwerk met 129 personen die het kerncomponent van de Amazonegroep vormen (persoon 25, 34, 61, 73, 80 en 146).



Figuur 8: Kerncomponent Amazonegroep

4.2.1 Netwerkbeschrijving

De eerste deelvraag: “welke personen maken deel uit van het netwerk” wordt behandeld aan de hand van een beschrijving van het netwerk. De *KenO’s* zijn per persoon ingevoerd in *BVI Bluespot Monitor* en op basis daarvan is het geslacht, de leeftijd (in 2021) en de woonplaats geanalyseerd van alle 162 personen uit de nodelist die samen zijn voorgekomen in de BVI met (iemand uit) de Amazonegroep (zie tabel 8). De 162 personen hebben een gemiddelde leeftijd van 26,20 (*s* = 11,78), een minimum leeftijd van 15 jaar en een maximum leeftijd van 82 jaar. De meest voorkomende leeftijd is 20 jaar (17,3%), daarop volgt 22 jaar (13,0%), 19 jaar (9,9%) en 21 jaar (8,6%). Van de 162 personen zijn 124 man (76,5%) en 38 vrouw (23,5%), waarbij de Amazonegroep significant meer gelinkt is aan mannen dan aan vrouwen (Z = -6,757; *p* <.001). De gemiddelde leeftijd van mannen is 26,03 (*s* = 11,90) en de gemiddelde leeftijd van vrouwen is 26,76 (*s*= 11,49) waarbij geen sprake is van een significant verschil (*t*(63,29) = -0,340; *p* = 0,735). De personen wonen in verschillende steden zoals Groningen (69,8%), Rotterdam (3,1%) en Assen (3,1%) (zie bijlage 3.1).

Kenmerk	Man	Vrouw	Totaal
Aantal	124	38	162
Leeftijd	26,03	26,76	26,20
	(*s* = 11,90)	(*s*= 11,49)	(*s* = 11,78)

Tabel 8: Kenmerken netwerkbeschrijving (N=162)

4.2.2 Netwerkanalyse

De tweede deelvraag “welke personen zijn de essentiële personen in het netwerk” is geanalyseerd aan de hand van de centraliteitsmaten degree, closeness, betweenness, fragmentation en eigenvector, op basis van de edgelist data (zie tabel 9).

Centraliteitsmaat	Rang	Node	Score
Degree	1	25	66,000
1,000 – 66,000	2	34	36,000
	3	80	26,000
	4	146	22,000
	5	61	20,000
	6	*38	14,000
Closeness	1	34	319,000
319,000 – 1037,000	2	25	343,000
	3	80	413,000
	4	*38	414,000
	5	*35	415,000
	6	61	416,000
Eigenvector	1	25	0,488
0,000 – 0,488	2	34	0,234
	3	*38	0,188
	4	*118	0,178
	5	146	0,169
	6	*66	0,165
Betweenness	1	25	4865,602
0,000 – 4865,602	2	80	2335,833
	3	34	1943,835
	4	61	1561,775
	5	73	681,427
	6	*48	375,000
Fragmentation	1	25	0,221
-0,010 – 0,221	2	80	0,070
	3	34	0,038
	4	61	0,038
	5	73	0,020
	6	*48	0,009

*Nodes zijn opvallende personen die geen deel uitmaken van de Amazone groep.

Tabel 9: Centraliteitsmaten (N = 150)

Persoon 25 heeft de hoogste degree met 66 relaties in het netwerk, ten opzichte van een minimum van 1 relatie. Persoon 25 heeft ook de hoogste eigenvector en is daarmee het vaakst verbonden met andere personen die ook veel relaties hebben en daardoor een centrale positie hebben in het netwerk. Daarnaast heeft persoon 25 de hoogste betweenness, dit maakt persoon 25 de cruciale schakel omdat deze persoon het vaakst op het tussenpad staat van andere personen in het netwerk. Persoon 25 wederom de hoogste fragmentation waardoor deze persoon de grootste impact heeft in termen van ontmanteling van het netwerk. Doordat persoon 25 relaties heeft met 44% van het netwerk, staat deze automatisch hoog in alle

centraliteitsmaten. Daarop volgt persoon 34 met een degree van 36 wat duidt op 36 relaties in het netwerk. Persoon 34 heeft daarbij de laagste closeness, dit houdt in dat persoon 34 het meest centraal staat in het netwerk en met 319 stappen andere personen in het netwerk kan bereiken, ten opzichte van een maximum van 1037 stappen.

Alle personen uit de Amazone kerngroep komen voor in (een van) de top zes rangen van de centraliteitsmaten waarbij persoon 25 en persoon 34 in alle top-centraliteitsmaten voorkomen en daarmee de twee essentiële personen zijn in het netwerk. Verder bekleden enkele personen die geen deel uitmaken van de Amazonegroep ook belangrijke posities in het netwerk. Persoon 38 heeft met 14 relaties ook een hoge degree en een lage closeness waarbij persoon 38 met 414 stappen de andere personen in het netwerk kan bereiken. Verder heeft persoon 48 een hoge betweenness wat aantoont dat deze persoon een centrale persoon is die regelmatig op het tussenpad van anderen staat om andere personen in het netwerk te bereiken. Daarbij heeft persoon 48 een hoge fragmentation, indien persoon 48 uit het netwerk wordt gehaald, heeft dit een grote impact op de ontwrichting van het netwerk (zie bijlage 3.2).

Gekeken naar het gehele netwerk, hebben oudere personen over het algemeen een lagere degree, van tussen de 2 en 10 relaties, dan jongere personen in het netwerk. Echter, personen met de laagste degree van 1 relatie, zijn wel jong. De vrouwen in het netwerk hebben een lagere degree van tussen de 1 en 10 relaties. Mannen hebben over het algemeen een hogere eigenvector, wat aangeeft dat mannen verbonden zijn met personen die ook veel relaties hebben. Mannen met een hoge closeness, zijn vaker ouder terwijl vrouwen met een hoge closeness vaker jonger zijn. Met uitzondering van twee vrouwen, hebben alle vrouwen een betweenness van 0,000, wat aantoont dat ze geen cruciale schakels zijn in het netwerk. Daarnaast hebben alle vrouwen een lage fragmentation, indien ze uit het netwerk worden verwijderd, heeft dit weinig impact op de ontwrichting van het netwerk (zie bijlage 3.1 en 3.2).

4.2.3 Inhoudelijk netwerk

De inhoud van deze paragraaf is ter waarborging van de privacy verwijderd uit de publicatie van dit onderzoek. De paragraaf is op te vragen bij de auteur en de eerste begeleider.

5. Conclusie

In dit hoofdstuk worden de bevindingen geconcludeerd. In §5.1 worden de conclusies omtrent het online daderprofiel behandeld en in §5.2 worden de conclusies omtrent het online netwerk behandeld.

5.1 Online daderprofiel

Het online daderprofiel is onderzocht aan de hand van de leeftijd, het geslacht en het delictverleden van online verdachten in Noord-Nederland in 2021. Op basis van de *adolescence-limited and life-course-persistent* theorie van Moffitt (1993) en de *age-graded* theorie van Sampson en Laub (1993), is de hypothese opgesteld dat verdachten van cybercriminaliteit in enge zin jonger zijn dan verdachten van gedigitaliseerde criminaliteit. Hiervoor is geen ondersteuning gevonden in de resultaten, waarin 49% van de online verdachten minderjarig of jongvolwassen zijn (12 – 23 jaar). De leeftijden van cyberverdachten ten opzichte van gedigitaliseerde verdachten, verschillen vrijwel niet van elkaar. De leeftijden zijn daardoor voor alle online verdachten redelijk gelijk verdeeld met een gemiddelde leeftijd van 28,39 jaar (*s* = 13,07). Het eerste kenmerk van het online daderprofiel is dat verdachten van zowel cybercriminaliteit in enge zin als gedigitaliseerde criminaliteit, volwassen zijn waarbij verdachten van cybercriminaliteit in enge zin niet jonger zijn verdachten van gedigitaliseerde criminaliteit.

Op basis van de *zelfcontrole* theorie van Moffitt (1993) en de *online disinhibition* theorie van Suler (2004) is de hypothese opgesteld dat mannen vaker verdacht worden van zowel cybercriminaliteit als gedigitaliseerde criminaliteit dan vrouwen. Ook hiervoor is geen ondersteuning gevonden in de resultaten. De verhouding tussen mannelijke en vrouwelijke verdachten van zowel cybercriminaliteit als gedigitaliseerde criminaliteit, is vrijwel gelijk. Er is geen significant verschil gevonden tussen het geslacht van cyber en gedigitaliseerde verdachten, en ook niet tussen de leeftijd van mannelijke en vrouwelijke verdachten. Mannelijke en vrouwelijke verdachten van online criminaliteit verschillen op het gebied leeftijd en type online criminaliteit, vrijwel niet van elkaar. Het tweede kenmerk van het online daderprofiel is dat verdachten van cybercriminaliteit en verdachten van gedigitaliseerde criminaliteit zowel man als vrouw kunnen zijn, waarbij mannen niet vaker verdacht worden van online criminaliteit dan vrouwen.

Theorieën over *self – challenge* (Aiken, 2016), *digital drift* (Goldsmith & Brewer, 2015) en secundaire criminele activiteiten (Leukfeldt et al., 2017) tonen aan dat er een verschil is in motieven tussen cyberverdachten van gedigitaliseerde verdachten. Op basis hiervan is de hypothese opgesteld dat er een verschil is in het delictverleden van online verdachten, waarbij

verdachten van cybercriminaliteit in enge zin vaker first offender zijn dan verdachten van gedigitaliseerde criminaliteit. Ook hiervoor is geen ondersteuning gevonden in de resultaten. Cyberverdachten zijn niet vaker first offender dan gedigitaliseerde verdachten. Daarnaast zijn cyberverdachten en gedigitaliseerde verdachten voornamelijk non first offenders, waarbij ze veelal hetzelfde type delictverleden hebben bestaande uit traditionele of gemengde (traditionele en online) criminaliteit. Het derde kenmerk van het online daderprofiel is dat online verdachten over het algemeen vaker non first offenders zijn, waarbij verdachten van cybercriminaliteit in enge zin niet vaker first offender dan verdachten van gedigitaliseerde criminaliteit.

Hieruit kan geconcludeerd worden dat er geen significante verschillen zijn tussen verdachten van cybercriminaliteit in enge zin en verdachten van gedigitaliseerde criminaliteit op basis van de kenmerken leeftijd, geslacht en delictverleden. Online verdachten in Noord-Nederland in 2021 zijn volwassen, kunnen zowel man als vrouw zijn en zijn vaker non first offenders met een traditioneel of gemengd delictverleden.

5.2 Online netwerk

Het online netwerk van de Amazone kerngroep is onderzocht aan de hand van drie deelvragen omtrent welke personen deel uitmaken van het netwerk, welke personen essentieel zijn en wat de inhoudelijke kenmerken zijn van het netwerk. Het netwerk bestaat uit in totaal 162 personen, waarvan 129 personen directe relaties hebben met een persoon uit de Amazonegroep. De gemiddelde leeftijd van de personen in het netwerk is 26,20 jaar (s = 11,78) en het netwerk bestaat significant meer uit mannen dan vrouwen. Het netwerk heeft een geografische omvang die verder reikt dan Noord-Nederland met personen die onder andere woonachtig zijn in het midden en het zuiden van Nederland.

De essentiële personen in het netwerk zijn de zes personen die deel uitmaken van de Amazonegroep, waarbij persoon 25 en 34 de essentiële personen zijn. Zij hebben de meeste relaties met andere personen, bekleden belangrijke brugposities in het netwerk en zijn ook actief in verschillende criminele markten. Daarnaast vallen persoon 38 en 48 op door de belangrijke positie die ze bekleden in het netwerk en door de relaties die ze hebben met personen uit de Amazonegroep. De Amazonegroep komt vooral in beeld bij de politie voor online criminaliteit bestaande uit cybercriminaliteit, overige horizontale fraude, fraude met betaalproducten en online handel, en witwassen. Daarnaast zijn ze actief in traditionele markten zoals diefstal, wapens, drugs en verkeersdelicten.

De inhoud van deze alinea betreft §4.2.3 en is ter waarborging van de privacy verwijderd uit de publicatie van dit onderzoek. De alinea is op te vragen bij de auteur en de eerste begeleider.

Hieruit kan geconcludeerd worden dat het online netwerk bestaat uit zes kernelementen en vervangbare elementen met een grote geografische afstand. Informatie afkomstig uit de BVH en BVI tonen aan dat het crimescript van de Amazonegroep voortdurend blijft ontwikkelen waarbij ze nieuwe manieren vinden om online criminaliteit te plegen, met daarnaast nog secundaire criminele activiteiten. De Amazonegroep is actief in verschillende markten waarbij vooral vermogensdelicten de overhand hebben. Hieruit blijkt dat de online delicten veelal een financieel component hebben. Door het gebrek aan *high-tech* skills in de delicten neigt het netwerk meer naar een gemengd netwerk met traditionele en gedigitaliseerde criminaliteit, in plaats van een netwerk met cybercriminaliteit in enge zin.

6. Discussie

In dit hoofdstuk wordt gereflecteerd op het onderzoek. In §6.1 worden de sterktes en zwaktes van het onderzoek besproken. In §6.2 worden aanbevelingen gedaan voor vervolgonderzoek.

6.1 Sterktes en zwaktes

Het eerste sterke punt is de hoeveelheid data die beschikbaar is bij de politie. Er is zowel voldoende informatie over het delict als over de verdachte beschikbaar om uitgebreid onderzoek kunnen doen. In dit onderzoek is enkel gebruik gemaakt van data uit Artikel 8 van de Wet Politiegegevens (WPG). De WPG regelt de rechten en plichten van de politie met betrekking tot het verwerken van politiegegevens. Politiegegevens op basis van Artikel 8 zijn gegevens die worden verwerkt voor de uitvoering van de dagelijkse politietaak (Overheid, 2020). Ondanks dat Artikel 8 data een laag veiligheidsniveau heeft, is er veel informatie beschikbaar over verdachten, relaties en netwerken en deze informatie is ook snel toegankelijk. Dit scheelt (toekomstige) onderzoekers veel tijd doordat het niet noodzakelijk is om zelf data te verzamelen. Daarbij heeft het zelf verzamelen van politiedata ook een ethische kanttekening waarbij de privacy van verdachten en slachtoffers gewaarborgd dient te worden.

Het tweede sterke punt is de nieuwe inzichten in online criminaliteit die zijn verkregen met dit onderzoek. Het onderzoek is gebaseerd op theoretische aannames vanuit de samenleving zoals dat mannen vaker verdacht worden van online criminaliteit en dat de verdachten vaak jongeren zijn met geen of beperkte relaties met anderen. Het onderzoek heeft aangetoond dat dit niet het geval is. De verhouding tussen mannelijke en vrouwelijke online verdachten is gelijk en minder dan de helft van de online verdachten is minderjarig of jongvolwassen (12 – 23 jaar). Het onderzoek heeft hierbij tot een nieuw inzicht geleid doordat met behulp van de netwerkanalyse is aangetoond dat online criminaliteit te concretiseren is tot personen in plaats van (anonieme) computers op het internet. De verdachten zijn echte mensen, met echte relaties en woonachtig in Nederland. Deze nieuwe bevinding zou de opsporing van online criminaliteit kunnen bevorderen doordat het concreet inzicht biedt in *wie* de verdachten zijn.

Het eerste zwakte punt van dit onderzoek, en vrijwel elk onderzoek met politiegegevens, is dat de data niet representatief is door een groot dark number. Dit komt doordat de data alleen verdachten omvat, dit zijn de personen die opgepakt zijn en waar de politie zicht op heeft. Personen die niet gepakt zijn, bevinden zich ook niet in de data. De veronderstelling hierbij is dat er mogelijk een verschil is tussen daders die wel of (nog) niet opgepakt zijn door de politie. Voor het online daderprofiel is dit een mogelijke oorzaak voor het beperkte aantal cyberdaders in de dataset. De aanname hierbij is dat cyberdaders mogelijk meer kennis hebben van ICT en daardoor beter uit beeld van de politie kunnen blijven, of dat personen die zich bezig houden

met cyberzaken simpelweg minder kwade of illegale bedoelingen hebben. De bevindingen uit dit onderzoek zijn hierdoor niet representatief voor alle online daders, maar alleen voor de verdachten die zijn opgepakt door de politie. Hetzelfde geldt voor de online netwerkdata. Het analyseren van telefoondata in plaats van BVH en BVI data had een beter beeld geschetst van het netwerk en had mogelijk ook de invloed van het dark number kunnen beperken. Echter, juridisch gezien is het gebruik van telefoondata niet toegestaan zonder “PAG” goedkeuring. Dit is een verzoek dat moet worden goedgekeurd voor de start van het onderzoek om inzicht te kunnen krijgen in lopende onderzoeken en gevoelige informatie. Voor vervolgonderzoek is het waardevol om vroegtijdig een PAG goedkeuring aan te vragen en het netwerk te analyseren aan de hand van telefoondata. Zo kan er inzicht worden verkregen in de informele relaties, die anders niet geregistreerd staan in de politiesystemen.

Het tweede zwakte punt is dat de data niet consistent wordt geclassificeerd. Uit voorgaand onderzoek naar de verhouding tussen online en traditionele criminaliteit is gebleken dat de aangiften inconsistent worden geclassificeerd onder verschillende maatschappelijke klassen. Soortgelijke delicten, met dezelfde maatschappelijke klassen, worden soms als online en soms als traditionele criminaliteit geclassificeerd. Na herclassficatie tijdens het voorafgaande onderzoek is gebleken dat van alle aangiften en incidenten in Noord-Nederland in 2021, 30% online criminaliteit betreft en 70% traditionele criminaliteit. Daarnaast zijn er bepaalde maatschappelijke klassen zoals stalking waarbij het aandeel online (gedigitaliseerde) criminaliteit zelfs tot 80% kan oplopen ten opzichte van 20% traditionele stalking. Hierdoor is er mogelijk sprake van onderschatting van online delicten en online verdachten in de data omdat dergelijke delicten en maatschappelijke klassen niet zijn meegenomen. Dit zou mogelijk kunnen betekenen dat er grotere verschillen zijn tussen cyber en gedigitaliseerde verdachten als er meer traditionele maatschappelijke klassen, waar ook gedigitaliseerde criminaliteit plaatsvindt, worden meegenomen in het onderzoek.

Het derde zwakte punt betreft mogelijke verklaringen voor dat er geen ondersteuning is gevonden voor de hypothesen. Ten eerste geldt voor de hypothesen omtrent leeftijd [H1] en delictverleden [H3] dat er geen ondersteuning is gevonden. Dit komt mogelijk doordat minderjarige verdachten niet direct bij de politie terechtkomen maar bij Halt. Dit heeft ook een spillover effect op het delictverleden doordat jonge first offenders eerst een Halt straf krijgen. Ze krijgen hierbij geen strafblad en doen daarvoor in ruil onbetaald werk of krijgen een andere passende maatregel om niet direct bij de politie in beeld te komen. Bureau Halt was eerst bedoeld voor lichte delicten van jonge, first offenders, maar uit onderzoek is gebleken dat Halt ook zware delicten en recidive behandeld (ten Boom, 2007). Hierdoor zijn er zowel minder jonge verdachten, als minder first offenders, in de data. De resultaten omtrent leeftijd en

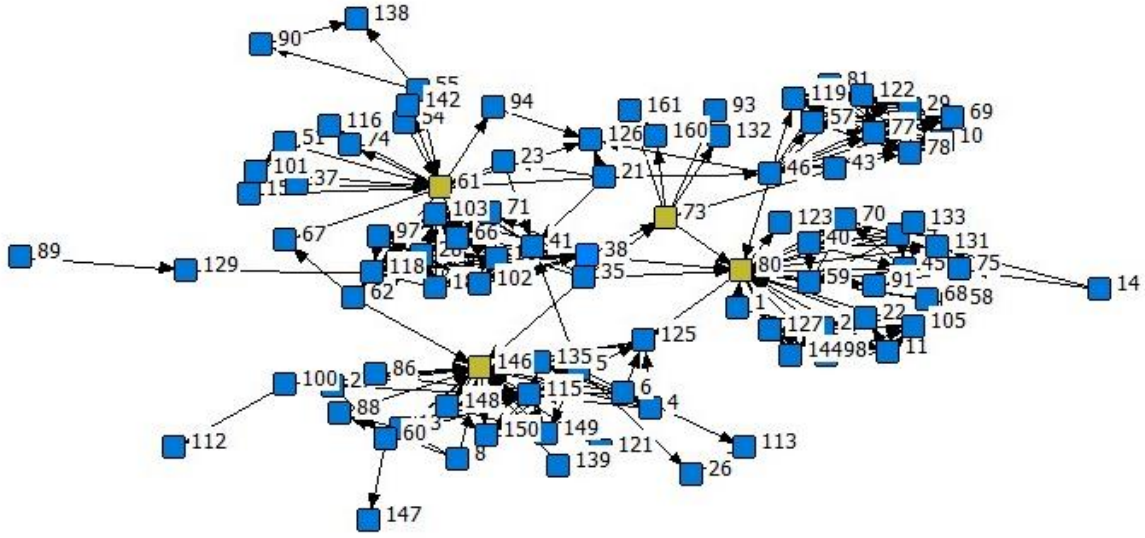
delictverleden zijn daarom mogelijk niet representatief voor alle online verdachten waarbij het voorstelbaar is dat cyberverdachten wel vaker jonger en first offenders zijn, ten opzichte van gedigitaliseerde verdachten. Ten tweede geldt voor alle hypothesen dat er geen ondersteuning is gevonden doordat de hypothesen zijn opgesteld op basis van theorieën die mogelijk niet volledig toe te passen zijn op online criminaliteit. De veronderstelling hierbij is dat de theorieën vooral gebaseerd zijn op traditionele criminaliteit. Het is hierbij voorstelbaar dat online criminaliteit dusdanig verschilt van traditionele criminaliteit, dat de (traditionele) theorieën en daaruit voortkomende hypothesen ontoereikend zijn en niet ondersteund worden met data omtrent online criminaliteit.

Het vierde zwakte punt is de hoge mate van degree voor persoon 25. Een hoge degree kan ook te maken hebben met het feit dat het netwerk is samengesteld uit *ego-netwerken*, dit zijn netwerken bestaande uit één persoon met iedereen die aan die persoon verbonden is. Hetzelfde geldt voor de bevinding dat alle personen uit de Amazonegroep hoog scoren op de centraliteitsmaten. De personen waar de politie veel focus op legt, krijgen vanzelf een centrale positie met hoge scores. Dit is overigens voor persoon 25 geen belemmering in het onderzoek aangezien deze persoon ook hoog scoort op de overige netwerkmaten en een uitgebreid delictverleden heeft, maar wel een kanttekeningen bij de netwerkresultaten.

6.2 Aanbevelingen

De eerste aanbeveling betreft de ontmanteling van het online netwerk. Het is hierbij van belang om interveniëren op individueel niveau tegen persoon 25 en 34 door ze uit het netwerk te verwijderen. Zij zijn namelijk de essentiële personen in het netwerk doordat ze beide cruciale posities bekleden en daarbij ook al enkele jaren actief betrokken zijn bij online en traditionele criminaliteit. Het verwijderen van persoon 25 en 34 uit het netwerk, is ook een interventie op het niveau van het netwerk doordat het netwerk daarmee wordt aangepast. Beide personen hebben een soort belangrijke “leidersrol”, gekeken naar het inhoudelijke netwerk, waarin ze het netwerk sturen en nieuwe personen aan het netwerk linken. Zodra persoon 25 en persoon 34 uit het netwerk worden verwijderd, wordt de samenstelling van netwerk aangepast. Figuur 9 toont aan dat de dichtheid van het netwerk verminderd en dat het netwerk verder wordt gefragmenteerd. De personen die dan de leidersrollen in het netwerk overnemen zijn persoon 61, 80 en 146 uit de Amazonegroep. Voor persoon 80 is een interventie op het niveau van subgroepen aanbevolen. Persoon 80 is vooral actief in traditionele markten en verbindt personen aan het netwerk die alleen met hem verbonden zijn. Het interveniëren op persoon 80 kan ertoe leiden dat het netwerk verder segmenteert in een subgroep met vooral traditionele delicten en een subgroep met vooral online delicten, waarna de subgroep met traditionele delicten wegvalt bij verwijdering van persoon 80 uit het netwerk (Valente, 2012). Andere

personen die geen deel uitmaken van de kerngroep, maar wel belangrijke posities bekleden in het netwerk, zijn persoon 38 en 48. Mede door hun activiteit in online criminaliteit is nuttig om ze ook te prioriteren (zie bijlage 3.4).



Figuur 9: Kerncomponent Amazonegroep zonder persoon 25 en 34

De tweede aanbeveling betreft het vervolgonderzoek waarbij onderzoek wordt gedaan naar jeugdige online daders in samenwerking met Halt. De aanname hierbij is dat er mogelijk sprake is van een onderschatting van minderjarige online daders en first offenders bij de politie, doordat ze eerder en vaker bij Halt terechtkomen dan direct bij de politie. Hierdoor is het onderzoeken van online daders met behulp van alleen politiedata niet voldoende. Het combineren van politiedata met Haltdata kan meer inzicht bieden in online criminaliteit onder minderjarigen, waarna representatievere uitspraken gedaan kunnen worden over de leeftijd en het delictverleden van online daders. Dit kan tevens ondersteunen bij het vergaren van nieuwe kennis en inzichten die bestaande theorieën over (online) criminaliteit aanpassen, of zelfs nieuwe theorieën ontwikkelen die specifiek gericht zijn op het cyber-psychologische en cyber-criminologische domein van online criminaliteit. Deze theorieën kunnen in vervolgonderzoeken verder empirisch worden onderzocht.

De derde aanbeveling betreft vervolgonderzoek naar online criminaliteit met telefoondata. Het is hierbij belangrijk dat de screening en PAG – aanvraag vroegtijdig worden afgerond om toegang te kunnen verkrijgen tot de uitgelezen telefoondata van verdachten. Telefoondata is een middel om het dark number bij criminaliteit tegen te gaan aangezien er dieper inzicht verkregen kan worden in de activiteiten en relaties van personen, waar de politie anders geen zicht op heeft. Personen die elkaar frequent treffen en spreken, maar niet samen opgepakt zijn, blijven tot op heden onzichtbaar voor de politie. Daarnaast kan het inzicht bieden in de

belangrijke “leiders” binnen het netwerk die anders onzichtbaar blijven doordat belangrijke personen geregeld geldezels en katvangers inzetten als “fysieke” link met het slachtoffer. Dit heeft als gevolg dat geldezels en katvangers worden opgepakt worden door de politie. Het voortdurend oppakken van geldezels is niet de meest efficiënte manier om online criminaliteit te bestrijden. Om het netwerk efficiënt te ontwrichten zou de focus moeten liggen op de belangrijke personen in het netwerk.

De vierde aanbeveling betreft het classificeren van online en traditionele data in de politiesystemen. In combinatie met voorgaand onderzoek naar de verhouding tussen online en traditionele criminaliteit, toont dit onderzoek aan dat de delicten regelmatig onjuist worden geclassificeerd. Online delicten worden weggeschreven als traditionele delicten waardoor er een onderschatting plaatsvindt van online delicten en online verdachten. Het advies aan de politie is daarom om nauwkeurige criteria te hanteren voor de classificatie van online en traditionele delicten in de gehele politieorganisatie. Dit zou kunnen door een optie “online of traditioneel” toe te voegen in de BVH en BVI, of door aan de voorkant bij *Intake en Service* tijdens het opnemen van de aangifte te vermelden of het online delict betreft. Dit zijn vrij simpele stappen die een grote impact kunnen hebben op de uiteindelijke aanpak van online criminaliteit want hetgeen waar de politie geen zicht op heeft, kan de politie ook niet bestrijden.

Online criminaliteit is een probleem dat de samenleving op grote schaal treft waardoor een totaalaanpak vereist is. De politie is verantwoordelijk voor de opsporing van online verdachten en het aanleveren van online verdachten bij het Openbaar Ministerie. Uit dit onderzoek is gebleken dat banken en platformen zoals Marktplaats op verschillende manieren online criminaliteit faciliteren. Deze instanties dienen ook bij te dragen aan het bestrijden van online criminaliteit door hun klanten en gebruikers strenger te controleren en tijdig informatie te delen met de politie. Het is de verantwoordelijkheid van de samenleving om weerbaarder te worden tegen online criminaliteit want er zijn geen slachtoffers zonder daders.

Referenties

Aiken, M., Davidson, J., & Amann, D. (2016). *Youth pathways into cybercrime*. Europol: European Cybercrime Centre/UCD Geary institute for public policy/ Middlesex University.

Boschman, S.E., Piersma, T.W., Weijters, G., Tollenaar, N. & Teerlink, M. (2022). *Verschil in recidivetrends onder jeugdigen. Inzicht in ontwikkelingen in recidive onder verschillende groepen jeugdige justitiabelen.* Wetenschappelijk Onderzoek en Documentatiecentrum.

Centraal Bureau voor de Statistiek. (2020). *Internet; toegang, gebruik en faciliteiten: 2012 – 2019.* Opgehaald van: https://www.cbs.nl/nl-nl/cijfers/detail/83429NED

Centraal Bureau voor de Statistiek. (2021). *Internettoegang en internetactiviteiten; persoonskenmerken.* Opgehaald van: https://www.cbs.nl/nl-nl/cijfers/detail/84888NED

Centraal Bureau voor de Statistiek. (2022). *Veiligheidsmonitor 2021*. Opgehaald van: https://www.cbs.nl/nl-nl/publicatie/2022/09/veiligheidsmonitor-2021

Centraal Bureau voor de Statistiek. (2022). *Verdachten; delictgroep, geslacht, leeftijd en migratieachtergrond*. Opgehaald van: https://opendata.cbs.nl/statline/#/CBS/nl/dataset/81947NED/table?fromstatweb

Cohen, L.E. & Felson, M. (1979). Social Change and Crime Rate Trends: A routine activity approach. *American Sociological Review, 44(4)*, 588 – 608. Doi: https://doi.org/10.2307/2094589

Dehghanniri, H. & Borrion, H. (2019). Crime scripting: A systematic review. *European Journal of Criminology, 19(1),* 1 – 14. Doi: https://doi.org/10.1177/1477370819850943

Domenie, M.M.L., Leukfeldt, E.R., van Wilsem, J.A., Jansen, J. & Stol, W.P.H. (2013). *Slachtofferschap in een gedigitaliseerde samenleving. Een onderzoek onder burgers naar e- fraude, hacken en andere veelvoorkomende criminaliteit.* Boom Lemma.

Goldsmith, A. & Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology, 19(1),* 112-130. Doi: https://10.1177/1362480614538645

Hoiting, E., Fokkema, M., Mori, M. & Van Veen, N. (2022). *De verhouding tussen traditionele en online criminaliteit.* Politie eenheid Noord-Nederland.

Holt, T.J., Burruss, G.W. & Bossler, A.M. (2010). Social Learning and Cyber Deviance: Examining the Importance of a Full Social Learning Model in the Virtual World.

Journal of Crime and Justice, 33(2), 31-61. Doi: https://doi.org/10.1080/0735648X.2010.9721287

Jong, L., Leukfeldt, E.R. & van de Weijer, S. (2018). Determinanten en motivaties voor intentie tot aangifte na slachtofferschap cybercrime. *Tijdschrift voor Veiligheid, 17(1-2),* 66 – 78. Doi: https://doi.org/10.5553/TvV/187279482018017102006

Leukfeldt, E.R., Veenstra, S., Domenie, M.M.L. & Stol, W.P.H. (2012). *De strafrechtketen in een gedigitaliseerde samenleving. Een onderzoek naar de strafrechtelijke afhandeling van cybercrime.* Programma Aanpak Cybercrime.

Leukfeldt, E.R., Notté, R. & Malsch, M. (2018). *Slachtofferschap van online criminaliteit. Een onderzoek naar de behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit.* Wetenschappelijk Onderzoek en Documentatiecentrum.

Leukfeldt, E. R., Stol, W. PH., & Kleemans, E. R. (2017). A typology of cybercriminal networks: from low-tech allrounders to high-tech specialists. *Crime, Law and Social Change, 67(1),* 21-37. Doi: https://doi.org/10.1007/s10611016-9662-2

Platform voor de Informatie Samenleving (2020). *De digitale samenleving in stroomversnelling.* Opgehaald van: https://ecp.nl/publicatie/visie-ecp-digitale-samenleving-in-stroomversnelling/

McPherson, M., Smith-Lovin, L., & Cook, J.M. (2001). Birds of a Feather: Homophily in Social Networks*. Review of Sociology, 27(1)*, 415 - 444. Doi: https://doi.org/10.1146/annurev.soc.27.1.415

Moffitt, T.E. (1993). Adolescence-Limited and Life-Course-Persistent Antisocial Behavior: A Developmental Taxonomy. *Psychological Review, 100(4),* 674 – 701. Doi: https://doi.org/10.1037/0033-295X.100.4.674

Moffitt, T.E., Poulton, R. & Caspi, A. (2013). Lifelong Impact of Early Self – Control: Childhood self – discipline predicts adults quality of life. *American Scientist, 101(5),* 352 – 359. Doi: https://doi.org/10.1511/2013.104.352

Odinot, G., de Poot, C. & Verhoeven, M. (2018). *De digitalisering van georganiseerde misdaad: De aard en aanpak van georganiseerde cybercrime.* Wetenschappelijk Onderzoek en Documentatiecentrum.

Overheid. (2020). *Wet politiegegevens.* Opgehaald van: https://wetten.overheid.nl/BWBR0022463/2020-01-01

Reyns, B. (2010). A situational crime prevention approach to cyberstalking victimization: Preventative tactics for Internet users and online place managers. *Crime Prevention and Community Safety, 12(2),* 99 – 118. Doi: https://doi.org/10.1057/cpcs.2009.22

Suler, J. (2004). The Online Disinhibition Effect. *CyberPsychology & Behavior, 7(3),* 321 – 326. Doi: https://doi.org/10.1089/1094931041291295

Ten Boom, A., Ferwerda, H. & van Leiden, I. (2007). Een pioniersstudie in justitieland: de evaluatie van Halt in een experimentele setting. *Tijdschrift voor Criminologie 49(1),* 33 – 44.

Valente, T. W. (2012). Network interventions. *Science, 337(6090)*, 49–53. Doi: https://doi.org/10.1126/science.1217330

Van der Hulst, R.C. (2008). *Sociale netwerkanalyse en de bestrijding van criminaliteit en terrorisme. Sociale netwerkanalyse; justitiële verkenningen.* Wetenschappelijk Onderzoek en Documentatiecentrum.

Van der Laan, A.M., Beerthuizen, M.G.C.J. & Boot, N.C. (2021). *Monitor Jeugdcriminaliteit 2020. Ontwikkelingen in jeugdcriminaliteit in de eerste twee decennia van de eeuw.* Wetenschappelijk Onderzoek en Documentatiecentrum.

Van der Wagen, W., van 't Zand – Kurtovic, E.G., Mathijsse, S.R. & Fischer, T.F.C. (2019). *Cyberdaders; uniek profiel, unieke aanpak?* Wetenschappelijk Onderzoek en Documentatiecentrum.

Warren, S., Oxburgh, G., Briggs, P. & Wall, D. (2017). How Might Crime-Scripts Be Used to Support the Understanding and Policing of Cloud Crime? *Human Aspects of Information Security. Lecture Notes in Computer Science, 10292,* 539 – 556. Doi: https://doi.org/10.1007/978-3-319-58460-7_38

Weulen Kranenbarg, M., Ruiter, S., Van Gelder, J. & Bernasco, W. (2018). Cyber-offending and traditional offending over the life-course: An empirical comparison. Journal of Developmental and Life Course Criminology 4(3), 343–364. Doi: https://doi.org/10.1007/s40865-018-0087-8