rijksuniversiteit groningen / faculteit gedrags- en maatschappijwetenschappen

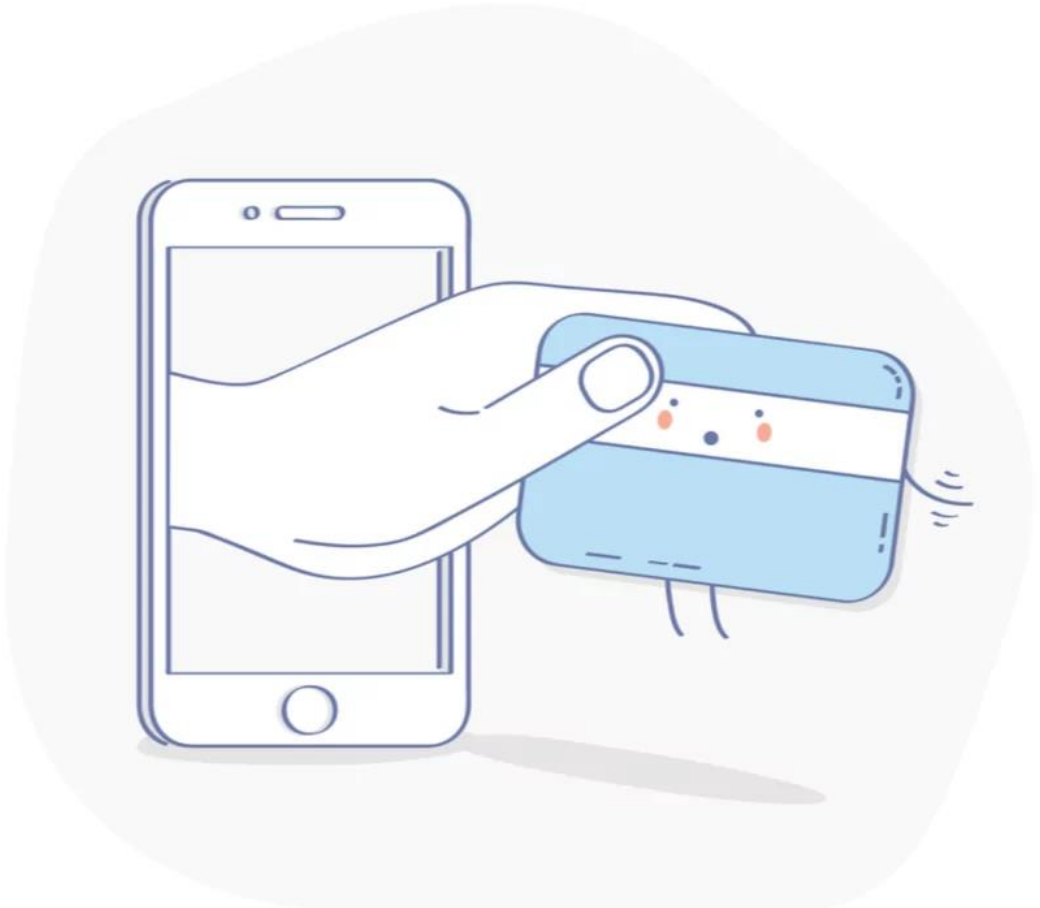
POLITIE

Inzicht in het web van bankhelpdeskfraude

Een exploratief onderzoek naar netwerken van bankhelpdeskfraudeurs

Understanding the web of bankhelpdesk fraud

Masterscriptie



Jitske Lanser
S3816176
Juli 2023
Begeleider: Prof. Dr. René Veenstra
Referent: Dr. Gert Stulp
Master Sociologie van Criminaliteit & Veiligheid

Voorwoord

Dit onderzoek is tot stand gekomen in samenwerking met het cybercrimeteam van de Dienst Regionale Recherche, politie eenheid Noord-Nederland. Ik heb met veel plezier aan dit onderzoek gewerkt en ik ben dankbaar voor de begeleiding die ik gedurende dit proces heb ontvangen.

Allereerst wil ik graag mijn dank uitspreken aan mijn begeleider vanuit de Rijksuniversiteit Groningen, René Veenstra. Uw betrokkenheid, begeleiding en inspirerende inzichten hebben een belangrijke rol gespeeld bij het schrijven van deze masterthesis. Mijn oprechte dank gaat ook uit naar mijn tweede lezer, Gert Stulp, voor de waardevolle feedback en constructieve suggesties die hebben bijgedragen aan de kwaliteit van mijn scriptie.

Daarnaast zou ik graag mijn waardering willen uiten aan mijn begeleiders vanuit de politie: Jildau Borwell, Martijn Krijnsen en Gerard Wolters. Jullie hebben me verwelkomd in jullie team en me de gelegenheid gegeven om uit eerste hand te ervaren hoe de praktijk van het veldwerk eruitziet. Ik heb, mede dankzij jullie, mijn afstudeerperiode als zeer prettig ervaren.

Samenvatting

Dit onderzoek had tot doel meer inzicht te verkrijgen in criminele netwerken die betrokken zijn bij bankhelpdeskfraude. Verschillende aspecten zijn onderzocht, waaronder het aandeel buitenlandse verdachten, de kenmerken van bankhelpdeskfraudeurs, de rollen binnen het crimescript van bankhelpdeskfraude, het verschil tussen *lone wolves* en verdachten in grotere netwerken, en de verdachten die essentieel zijn in termen van sociaal en menselijk kapitaal. Voor dit onderzoek is gebruik gemaakt van een volledige lijst met alle registraties van bankhelpdeskfraude in 2022, verkregen uit de politiesystemen. Uit de analyses bleek dat 10,9% van de verdachten buitenlands was en dat zij allemaal de rol van geldezel vervulden. Het belang van buitenlandse verdachten ligt in hun vermogen om grote geldbedragen naar het buitenland weg te sluizen en hun moeilijke opspoorbaarheid voor de Nederlandse politie. Verder kwam naar voren dat de gemiddelde leeftijd van de verdachten 28,3 jaar was en dat het merendeel van de verdachten uit mannen bestond. Bovendien had een meerderheid van de verdachten geen delictverleden of een traditioneel delictverleden, wat betekent dat zij eerder alleen traditionele delicten hebben gepleegd. Er werd een netwerkanalyse uitgevoerd waarbij alle 802 verdachten van bankhelpdeskfraude in kaart werden gebracht. Het netwerkbeeld toonde meer onderlinge verbindingen wanneer ook de verbindingen van registraties van (bankhelpdeskfraude) delicten van 2017 tot en met 2022 werden meegenomen. Binnen de drie grootste netwerken werden de essentiële actoren in termen van sociaal en menselijk kapitaal geanalyseerd, waarbij enkele actoren naar voren kwamen die cruciaal waren voor het functioneren van het crimescript. Deze actoren vervulden rollen als dienstverleners en bezaten specifieke kennis en vaardigheden die moeilijk te vervangen waren. Een crimescript voor bankhelpdeskfraude, ontworpen op basis van wetenschappelijke literatuur en data uit de politiesystemen, werd gebruikt om de verschillende rollen te identificeren. Uit de analyse bleek dat *lone wolves* zonder delictverleden geldezels vertegenwoordigden, terwijl *lone wolves* met een gemengd delictverleden, (zowel een delictverleden in de traditionele als digitale criminaliteit), vaak dienstverleners waren. Kernleden bleken minder zichtbaar voor de politie vanwege hun beperkte verbindingen met andere actoren in het netwerk. Dit onderzoek biedt nieuwe inzichten in de netwerken van bankhelpdeskfraude, een crimescript voor bankhelpdeskfraude en de analyse van de verschillende rollen. Ten slotte toont het onderzoek aan dat buitenlandse verdachten moeilijker op te sporen zijn voor de Nederlandse politie, waardoor ze aantrekkelijke samenwerkingspartners kunnen vormen voor Nederlandse bankhelpdeskfraudeurs.

Inhoudsopgave

1. Inleiding

Eind vorig jaar meldde het kabinet dat er meer moet worden ingezet op digitale veiligheid en werd er een nieuwe cybersecuritystrategie gepresenteerd. Dit is hard nodig, want in de woorden van Dilan Yeşilgöz-Zegerius, minister van Justitie en Veiligheid, vormen digitale systemen "het 'zenuwstelsel' van onze maatschappij" (Ministerie van Justitie en Veiligheid, 2022). Uit cijfers van het CBS blijkt dat 89,5% van de bevolking in Nederland, vanaf de leeftijd van 12 jaar, dagelijks gebruikmaakt van internet (CBS, 2022a). Een groot deel van iemands sociale en zakelijke leven speelt zich tegenwoordig online af. Zo wordt er veel gebruikgemaakt van sociale media, communicatie via WhatsApp en worden ook bankzaken veelvuldig online geregeld (Beerthuizen, Sipma & van der Laan, 2020).

Naast de kansen die de toenemende digitalisering biedt voor de ‘gewone burger’, biedt het ook mogelijkheden voor criminelen. Onderzoek toont aan dat delicten steeds vaker een digitale component bevatten als gevolg van de digitalisering van onze samenleving (Schiks, van 't Hoff – de Goede & Leukfeldt, 2022). De politie ziet deze ontwikkeling ook terug in hun cijfers. In 2022 registreerden zij 13.949 cyberincidenten (Politie, 2023). Hoewel dit getal voor het eerst een lichte daling (2%) laat zien ten opzichte van het voorgaande jaar, is het nog steeds zorgwekkend hoog.

In de literatuur wordt doorgaans onderscheid gemaakt tussen cybercriminaliteit in ruime zin en cybercriminaliteit in enge zin. Met cybercriminaliteit in ruime zin worden alle vormen van criminaliteit bedoeld die worden uitgevoerd met ICT als middel, maar niet gericht zijn op ICT. Criminele handelingen die onder deze noemer vallen, zijn vaak traditionele misdaden die erop gericht zijn geld te verkrijgen en worden gepleegd met behulp van computers en andere technologische middelen (Odinot et al., 2018; UNODC, 2013). Cybercriminaliteit in ruime zin wordt ook wel gedigitaliseerde criminaliteit genoemd, omdat het oude vormen van criminaliteit betreft die zijn aangepast aan de moderne digitale wereld (Politie, 2015; Ministerie van Veiligheid en Justitie, 2015). Onder cybercriminaliteit in enge zin vallen delicten die gepleegd worden met ICT als middel én als doelwit. Voorbeelden hiervan zijn hacken, het verspreiden van ransomware en DDoS-aanvallen (Odinot et al., 2018). In dit onderzoek zal de term 'gedigitaliseerde criminaliteit' gebruikt worden als aanduiding voor cybercriminaliteit in ruime zin. 'Cybercriminaliteit' fungeert binnen dit onderzoek als overkoepelende term voor alle vormen van cybercriminaliteit en omvat daarmee zowel cybercriminaliteit in ruime zin als cybercriminaliteit in enge zin.

Cybercriminaliteit lijkt vooral onder jongeren 'in trek' te zijn. Zo geeft drie op de tien minderjarigen aan enige vorm van cyber- of gedigitaliseerde criminaliteit te hebben gepleegd, wat overeenkomt met de prevalentie van zelfgerapporteerde offline criminaliteit (Van der Laan & Goudriaan, 2016). Voorbeelden van cyber- of gedigitaliseerde criminaliteit in het onderzoek waren onder andere het bedreigen van iemand via sociale media, het verkopen van een artikel online maar het niet verzenden ervan, en het zich voordoen als iemand anders op internet. Het betrof dus ook relatief onschuldige varianten.

De politie merkt tevens op dat met name jongeren steeds gemakkelijker en op steeds jongere leeftijd betrokken raken bij cybercriminaliteit (Politie, 2023). Dankzij de online wereld hebben kinderen al op jonge leeftijd de mogelijkheid om buiten het zicht van hun ouders te handelen (Mesch, 2012). Dit gebeurt vaak op een leeftijd waarop kinderen nog niet voldoende begrip hebben van goed en fout, wat kan leiden tot (onbewust) strafbaar gedrag. Bovendien komen jongeren veelvuldig in aanraking met nieuwe mogelijkheden om criminele activiteiten te ondernemen en worden ze gemakkelijk verleid tot het plegen van dergelijke delicten vanwege de aard van cybercriminaliteit, waarbij de slachtoffers onzichtbaar blijven voor de dader (Holt & Bossler, 2014). De kenmerken van cybercriminaliteit, zoals de onzichtbaarheid, lage investeringskosten en de relatief lage pakkans, maken het voor jongeren aantrekkelijk om zich met deze vorm van criminaliteit bezig te houden (De Cuyper & Weijters, 2016).

Ook vanuit de 'gewone burger' klinken steeds vaker zorgen over cybercriminaliteit. In 2022 werd 19,5% van de bevolking getroffen door deze vorm van criminaliteit, wat een stijging van 2,6 procentpunten betekent ten opzichte van 2021 (CBS, 2022b). Naast de financiële impact ervaren slachtoffers van cybercriminaliteit vaak gevoelens van schaamte en schuld, omdat er in hun sociale omgeving onbegrip heerst. Dit komt door cybercriminaliteit minder bekend en tastbaar is, waardoor de impact ervan door anderen vaak wordt onderschat. Cybercriminaliteit kan ernstige gevolgen hebben voor slachtoffers, zoals problemen met vertrouwen, depressie, stressstoornissen en angstgevoelens (Leukfeldt, Notté & Malsch, 2018).

De banksector ondervindt aanzienlijke financiële schade als gevolg van cybercriminaliteit. Marco Doeland, voorzitter van de Nederlandse Vereniging van Banken (NVB), meldt dat er in 2022 volgens de registraties bijna 61 miljoen euro aan fraude is gepleegd (Nederlandse Vereniging van Banken, 2023). Om cybercriminaliteit te voorkomen en te bestrijden, is in 2011 de Electronic Crime Taskforce (ECTF) opgericht. Dit samenwerkingsverband omvat de vier grootbanken (ABN AMRO, ING, Rabobank en SNS), het Openbaar Ministerie, de politie en de NVB. Ondanks de aandacht die banken besteden aan cybercriminaliteit, blijft de hoeveelheid cybercriminaliteit nog steeds aanzienlijk.

Een vorm van gedigitaliseerde criminaliteit die de laatste jaren sterk is toegenomen en aanzienlijke schadebedragen met zich meebrengt, is bankhelpdeskfraude (Nederlandse Vereniging van Banken, 2023; NOS, 2023). Bankhelpdeskfraude is een vorm van gedigitaliseerde criminaliteit waarbij oplichters zich voordoen als bankmedewerkers of vertegenwoordigers van frauduleuze instanties. Ze nemen telefonisch contact op met potentiële slachtoffers en maken vaak gebruik van een systeem om hun telefoonnummer te manipuleren, zodat het lijkt alsof ze bellen vanuit de bank of de fraude-instantie. Oplichters maken gebruik van 'social engineering'-technieken om het slachtoffer te misleiden en toegang te krijgen tot systemen en vertrouwelijke gegevens. *Social engineering* houdt in dat menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen of angst worden gebruikt om vertrouwelijke informatie te verkrijgen (Krombolz, Hobel, Huber & Weippl, 2015). Nadat de oplichters het slachtoffer hebben overgehaald om vertrouwelijke gegevens te delen onder het voorwendsel van een probleem met hun bankrekening, maken ze vaak gebruik van een "Remote Access Tool" zoals Anydesk, Teamviewer of LogMeIn om volledige controle over de laptop of pc van het slachtoffer te krijgen. Dit valt onder computervredebreuk. Vervolgens krijgen de oplichters vaak toegang tot de online bankrekening van het slachtoffer, waardoor ze grote geldbedragen kunnen afschrijven (Borwell, 2020).

Cybercriminele netwerken

Er is reeds onderzoek gedaan naar cybercriminele netwerken in Nederland. Onderzoek toont aan dat criminelen door gebruik te maken van online fora samenwerkingspartners kunnen vinden zonder geografische beperkingen, waardoor netwerken wereldwijd actief kunnen zijn (Leukfeldt, 2016). Het zoeken naar criminele samenwerkingspartners, het coördineren van criminele activiteiten en de samenwerking tussen criminelen op verschillende tijdstippen en vanuit verschillende locaties is mogelijk in de online wereld (Odinot et al., 2018). Gezien de mogelijkheden die deze online wereld biedt, is het aannemelijk dat er internationale samenwerkingsverbanden bestaan.

Op dit moment is echter nog weinig bekend over de invloed van buitenlandse verdachten op het Nederlandse speelveld. Er is nog onvoldoende onderzoek gedaan naar de internationale samenwerking tussen Nederlandse verdachten en één of meerdere verdachten buiten Nederland. Het is van belang het aandeel buitenlandse verdachten in de Nederlandse context van bankhelpdeskfraude te onderzoeken, omdat dit van invloed kan zijn op de aanpak van rechtshandhavingsinstanties bij deze vorm van cybercriminaliteit.

Relevantie

Er is een verschuiving waarneembaar van traditionele criminaliteit naar cybercriminaliteit. Terwijl traditionele criminaliteit al jaren afneemt, vertoont cybercriminaliteit een stijgende trend (CBS, 2022b; De Cuyper & Weijters, 2016; Europol, 2016). Criminaliteit is onwenselijk en heeft negatieve gevolgen voor onze samenleving. Ongeveer 18% van de slachtoffers van cybercriminaliteit geeft aan psychische, emotionele en financiële schade te ondervinden na een incident (CBS, 2022c). Doordat cyberdelicten zich online afspelen, vinden ze direct plaats in de persoonlijke leefomgeving van slachtoffers, wat kan leiden tot langdurige gevoelens van angst en onveiligheid. Bovendien kunnen vertrouwensproblemen ontstaan, wat leidt tot het verlies van vertrouwen in anderen, de politie en de overheid (Leukfeldt, Notté & Malsch, 2018). Gezien het toenemende belang van het internet in het leven van veel mensen, is het relevant onderzoek te doen naar mogelijkheden om cybercriminaliteit terug te dringen en de impact ervan op de samenleving te verminderen.

Beleidsrelevantie

Onderzoek naar de rol van verdachten van bankhelpdeskfraude is relevant voor beleidsvorming. Zowel in de literatuur als in de praktijk van de politie is er opmerkelijk weinig kennis over de netwerken van bankhelpdeskfraudeurs, hun werking en internationale samenwerkingspartners. Tegenwoordig zijn criminelen dankzij het internet niet meer gebonden aan een specifieke locatie, waardoor ze mogelijk een andere modus operandi hanteren dan traditionele criminelen. Dit vereist een andere aanpak dan die wordt toegepast op traditionele criminelen. Het is dan ook van belang om verdachten van bankhelpdeskfraude te onderzoeken om te begrijpen hoe een netwerk van Nederlandse en buitenlandse bankhelpdeskfraudeurs mogelijk functioneert. Een geschikte methode hiervoor is sociale-netwerkanalyse.

Sociale-netwerkanalyse, ook wel SNA genoemd, is een methode om criminele netwerken te bestuderen en inzicht te krijgen in hun werking. Door gebruik te maken van wiskundige berekeningen en algoritmen kunnen onderlinge relaties en eigenschappen van betrokken personen worden blootgelegd (Van der Hulst, 2008). Bij het ontwikkelen van interventies om een netwerk te ontmantelen, kan gekeken worden naar verschillende centraliteitsmaten (Valente, 2012). Het analyseren van de mate van centraliteit kan waardevolle informatie opleveren over de werking van het netwerk, wat van belang kan zijn bij doeltreffende ontmanteling door de politie.

Dit onderzoek maakt gebruik van gegevens van alle verdachten van bankhelpdeskfraude in 2022, verkregen van de politie, afdeling Onderzoek en Analyse, eenheid Noord-Nederland.

Het is één van de eerste studies naar netwerken van bankhelpdeskfraudeurs in Nederland, met als doel een duidelijker beeld te geven van hoe deze netwerken functioneren. Het onderzoek richt zich specifiek op de rollen die binnen deze netwerken worden vervuld, de actoren met sleutelposities en de invloed van mogelijke internationale samenwerkingen van cybercriminelen op het gebied van bankhelpdeskfraude. Om deze inzichten te verkrijgen, worden empirisch wetenschappelijk onderzoek en informatie uit opsporingsonderzoeken van de politie gecombineerd.

Dit leidt tot de onderzoeksvraag die centraal staat in dit onderzoek: *"Hoe ziet een volledig netwerkbeeld van bankhelpdeskfraudeurs eruit, hoe worden de rollen binnen deze netwerken vervuld en wat is de invloed van buitenlandse verdachten binnen deze netwerken?"*

In de volgende paragraaf wordt een theoretisch kader uiteengezet dat ten grondslag ligt aan de analyse van criminele samenwerking op het gebied van bankhelpdeskfraude. Deze paragraaf behandelt onder meer literatuur over de kenmerken van verdachten, de aanwezigheid van criminele internationale banden, de werking en het gebruik van sociale-netwerkanalyse, het concept van crimescripting en mogelijke netwerkinterventies. Vervolgens worden in de methoden de operationalisaties van de data, specificaties van de netwerkdata en de gekozen analyses beschreven. Daarna worden de onderzoeksresultaten op zowel netwerk- als actorniveau gepresenteerd en besproken. Ten slotte worden de beperkingen van dit onderzoek, beleidsimplicaties en aanbevelingen voor toekomstig onderzoek besproken.

2. Theoretisch kader

In dit hoofdstuk wordt het theoretisch kader uitgewerkt op basis van de onderzoeksvraag. Dit omvat zowel een inhoudelijke benadering als een analyse van relevante methoden, zoals sociale-netwerkanalyse en crimescripts. Om de onderzoeksvraag te beantwoorden, worden deelvragen geformuleerd.

Om inzicht te krijgen in de kenmerken van cyberverdachten op het gebied van bankhelpdeskfraude, wordt gekeken naar geslacht, leeftijd en het delictverleden van de verdachten. Het doel is om een profiel te schetsen van de *'gemiddelde bankhelpdeskfraudeur'*, aangezien hier momenteel weinig over bekend is in zowel de theorie als de praktijk van de politie. Er bestaan verschillende theorieën over het geslacht, de leeftijd en het delictverleden van cybercriminelen. Deze theorieën worden gebruikt om te beoordelen in hoeverre ze van toepassing zijn op bankhelpdeskfraudeurs.

Buitenlandse verdachten

Gezien het gebrek aan kennis over buitenlandse verdachten binnen de context van cybercriminaliteit, met name bankhelpdeskfraude, heeft de politie interesse in de rol die deze verdachten spelen in het Nederlandse speelveld van bankhelpdeskfraudeurs.

Zoals eerder benoemd, blijkt uit onderzoek dat leden van cybercriminele netwerken vaak de voorkeur geven aan samenwerking met bekenden uit de offline wereld (Leukfeldt, 2016). Er zijn echter ook netwerken die grotendeels of volledig gebaseerd zijn op het gebruik van online fora. Door gebruik te maken van deze fora kunnen criminele samenwerkingspartners worden geworven zonder geografische beperkingen, waardoor een netwerk wereldwijd actief kan zijn. Het zoeken naar criminele samenwerkingspartners, het coördineren van criminele activiteiten en de samenwerking tussen criminelen op verschillende tijdstippen en vanuit verschillende locaties is mogelijk in de online wereld (Odinot et al., 2018). Gezien de mogelijkheden die deze online wereld biedt, is het aannemelijk dat er internationale samenwerkingsverbanden bestaan. Daarom wordt er in de analyses onder andere gekeken naar het aandeel buitenlandse verdachten en de rol die zij spelen binnen bankhelpdeskfraude-netwerken.

Geslacht

Verschillende studies tonen aan dat mannen oververtegenwoordigd zijn in de cybercriminaliteit (Ruiter & Bernaards, 2013; Weulen Kranenbarg, Ruiter, Van Gelder & Bernasco, 2018).

Bovendien verschilt het type cybercriminaliteit waar mannen en vrouwen bij betrokken zijn. Mannelijke daders zijn voornamelijk betrokken bij specifieke vormen van cybercriminaliteit, zoals hacken en ransomware. Vrouwelijke daders zijn minder actief in deze vormen van cybercriminaliteit, maar vaker betrokken bij gedigitaliseerde criminaliteit zoals bankhelpdeskfraude.

Het verschil in de hoeveelheid criminaliteit die mannen en vrouwen plegen, manifesteert zich al tijdens de kindertijd. In deze periode leren mensen namelijk om te gaan met emoties en impulsen, en worden het concentratievermogen en geduld op de proef gesteld. Al deze vaardigheden hebben invloed op antisociaal gedrag. Onderzoek toont aan dat vrouwen in de kindertijd significant meer zelfcontrole hebben en minder antisociaal gedrag vertonen dan mannen. Individuen met een laag niveau van zelfcontrole hebben aantoonbaar een hoger risico op veroordeling voor crimineel gedrag dan individuen met een hoog niveau van zelfcontrole (Moffitt, Poulton & Caspi, 2013).

Leeftijd

Ten tweede worden jongeren vaker verdacht van cybercriminaliteit dan ouderen (Politie, 2023). Dit kan worden verklaard door de theorie van Moffitt over "*adolescence-limited and life-course-persistent antisocial behavior*", waarin wordt gesteld dat er twee typen criminelen zijn: personen die gedurende de adolescentie slechts een periode crimineel actief zijn en personen die langdurig crimineel actief blijven (Moffitt, 1993). Dit gedrag ontstaat als gevolg van de zogeheten *maturity gap*, een fenomeen dat veel jongvolwassenen ervaren wanneer zij vroeg biologisch volwassen worden, maar nog niet dezelfde erkenning als volwassene krijgen in sociale context. Deze discrepantie kan leiden tot gevoelens van onvrede die kunnen resulteren in crimineel gedrag. Het criminele gedrag dat voortkomt uit de *maturity gap* is meestal van tijdelijke aard en vertoont geen stabiele trend (Moffitt, 1993).

Een alternatieve verklaring is de "*age-graded theory*" (Sampson & Laub, 1993), die stelt dat crimineel gedrag veranderlijk is en kan beginnen of eindigen bij keerpunten in iemands leven, zoals het krijgen van een vaste baan, het volgen van een studie, of het stichten van een gezin.

Aangezien cyberdaders voornamelijk minderjarigen en jongvolwassenen zijn, is het mogelijk dat jonge cyberdaders vallen onder het tijdelijke antisociale gedrag dat kenmerkend is voor de adolescentie, of dat het criminele gedrag zich voordoet tot een keerpunt in het jonge leven, zoals het vinden van een baan. Bovendien hebben jongeren, vanwege hun dagelijks internetgebruik en voortdurende blootstelling aan verleidingen en nieuwe mogelijkheden,

mogelijk meer kans om betrokken te raken bij gedigitaliseerde criminaliteit dan ouderen. Deze digitale omgeving biedt hen zowel mogelijkheden voor gedigitaliseerde criminaliteit als het vergemakkelijken van traditionele vormen van criminaliteit.

Delictverleden

Het delictverleden van een cybercrimineel kan op verschillende gebieden verschillen van dat van een 'traditionele crimineel'. In het geval van cybercriminaliteit in enge zin, worden daders vaak gedreven door eigen interesse en de zoektocht naar technologische uitdagingen, in plaats van gewelddadige of financiële motieven. Dit geldt vooral voor jonge cybercriminelen, inclusief minderjarigen en jongvolwassenen. Ze beginnen veelal met het programmeren van websites om vervolgens hun vaardigheden uit te breiden naar bijvoorbeeld het ontwikkelen van hack-software. Tijdens dit proces vergroten ze niet alleen hun technologische vaardigheden, maar ook hun kennis en competentie, en streven ze naar steeds hogere persoonlijke doelen. Deze uitdagingen kunnen dienen als een welkome ontsnapping bij verveling, vooral wanneer de jonge cybercrimineel erin slaagt na veel inspanning zijn doel te bereiken (Van der Wagen, Van 't Zand, Matthijsse & Fischer, 2019).

Bij daders van gedigitaliseerde criminaliteit ligt dit anders. Zij hebben vaker een financieel motief en stappen daarom in veel gevallen over van traditionele criminaliteit naar gedigitaliseerde criminaliteit (Van der Wagen et al., 2019). Dit wordt veroorzaakt door de zogeheten "*digitale drift*". Door de digitalisering van delicten wordt het eenvoudiger om bepaalde vormen van traditionele criminaliteit te plegen en kunnen deze delicten in termen van winstgevendheid lucratiever zijn. Zo ontstaan traditionele vormen van criminaliteit die zijn aangepast aan de moderne digitale wereld. Zo kan bankhelpdeskfraude bijvoorbeeld worden gezien als een gedigitaliseerde variant van de babbeltruc (Peters, 2021). Beide delicten maken gebruik van oplichtingstechnieken, waarbij de criminelen *social engineering* toepassen om hun slachtoffers te misleiden. Het motief van de daders bij deze misdrijven is financieel, en het zijn veelal ouderen die slachtoffer worden van deze vormen van criminaliteit (Borwell, 2020).

Veel traditionele daders kiezen er dus voor zich te richten op gedigitaliseerde criminaliteit, omdat dit minder investeringskosten en een lagere pakkans biedt dan traditionele criminaliteit (De Cuyper & Weijters, 2016; Goldsmith & Brewer, 2015). Het is daarom aannemelijk dat veel daders van gedigitaliseerde criminaliteit ook actief zijn geweest of nog steeds actief zijn op andere gebieden binnen de traditionele criminaliteit. Een studie naar daders van gedigitaliseerde criminaliteit bevestigt dit (Leukfeldt, Kleemans & Stol, 2017): daders van

gedigitaliseerde criminaliteit met een financieel motief waren ook betrokken bij secundaire (traditionele) delicten.

De inhoudelijke deelvragen die in dit onderzoek worden behandeld, zijn als volgt:

1. Wat is het aandeel van buitenlandse verdachten in het Nederlandse beeld van bankhelpdeskfraude?
2. Wat zijn kenmerken van verdachten in het Nederlandse speelveld van bankhelpdeskfraude? Hierbij wordt er gekeken naar geslacht, leeftijd en delictverleden

Internationale sociale banden

Uit onderzoek naar Nederlandse netwerken blijkt dat veel netwerken ontstaan en groeien doordat kernleden elkaar kennen via bestaande (offline) sociale contacten (Leukfeldt, 2016). Daarnaast vormen online fora een belangrijk middel voor criminelen om geschikte netwerkrelaties te vinden in andere landen (Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, 2018). Deze fora dienen tevens als ideale platforms voor het wereldwijd delen van criminele informatie en middelen, zoals ook waargenomen wordt in de praktijk. Een recent voorbeeld hiervan is de internationale spoofingdienst 'iSpoof', die eind vorig jaar werd ontmanteld door samenwerking tussen het Cybercrimeteam van de politie Midden-Nederland en de Metropolitan Police Service in Londen. Deze dienst werd wereldwijd door criminelen gebruikt voor bankhelpdeskfraude en werd onder andere verspreid via online fora (Politie, 2022). Het internet creëert dus een geheel nieuwe manier van informatie-uitwisseling en het leggen van contacten, die mogelijk verder gaat dan traditionele sociale contacten.

In onderzoek naar verschillende soorten criminele netwerken op het gebied van phishing en banking malware is gekeken naar internationale aspecten, zoals de nationaliteit van daders en slachtoffers. De onderzoekers hebben twee typen criminaliteit kunnen onderscheiden: '*low-tech criminaliteit*' en *'high-tech criminaliteit'* (Leukfeldt, et al., 2017). Binnen low-tech criminaliteit zijn daders voornamelijk actief binnen de landsgrenzen en rekruteren ze anderen om bijvoorbeeld geld wit te wassen. In sommige gevallen onderhouden deze daders contacten met buitenlandse facilitators, bijvoorbeeld voor het creëren van phishing e-mails. High-tech criminaliteit omvat daarentegen daders die zowel in Nederland als in het buitenland actief zijn. Criminelen kopen bijvoorbeeld malware en certificaten uit het buitenland om deze vervolgens in Nederland te gebruiken. Incidenteel worden buitenlandse personen gerekruteerd voor activiteiten zoals het witwassen van geld, wat kan leiden tot gevallen van mensenhandel en fraude met valse documentatie om bankrekeningen te openen (Leukfeldt, et al., 2017). Het is

aannemelijk dat dergelijke internationale sociale banden ook bestaan in cybercriminele netwerken die gericht zijn op bankhelpdeskfraude.

Het is van belang het aandeel buitenlandse verdachten in de Nederlandse context van bankhelpdeskfraude te onderzoeken, omdat dit invloed kan hebben op de aanpak van rechtshandhavingsinstanties bij deze vorm van cybercriminaliteit. Bankhelpdeskfraude is een relatief nieuwe vorm van criminaliteit waarbij de politie nog niet exact weet hoe ermee om te gaan. Een uitdaging bij bankhelpdeskfraude is dat de dader doorgaans niet fysiek aanwezig is op de plaats van het delict, wat het lastig maakt om hen aan te houden. Het wordt nog complexer wanneer de dader zich in een ander land bevindt (Speer, 2000). Indien de politie zich alleen richt op contacten binnen het Nederlandse netwerk, omdat deze het meest zichtbaar zijn en men verwacht dat criminelen elkaar kennen via sociale connecties of de criminele onderwereld (Leukfeldt, et al., 2017), bestaat het risico dat buitenlandse verdachten over het hoofd worden gezien. Het onderzoeken van het aandeel buitenlandse verdachten biedt dus belangrijke inzichten om een compleet beeld te krijgen van de dynamiek van bankhelpdeskfraude en een effectieve aanpak te ontwikkelen.

Online ontremmingseffect

Naast het vergroten van de geografische afstand binnen een crimineel netwerk biedt digitalisering een vruchtbare omgeving voor criminelen die anoniem willen opereren. Een verklaring hiervoor is te vinden in het online ontremmingseffect (Suler, 2004). Deze theorie stelt dat de online wereld drempels kan wegnemen, omdat anonimiteit mogelijk is. Wanneer criminelen binnen hun eigen netwerk ook anoniem kunnen blijven, kan dit een aantrekkelijke factor zijn om samen te werken met online contacten. Vooral wanneer deze contacten zich geografisch ver van de crimineel bevinden, kan het gevoel van 'extra' anonimiteit nog verleidelijker zijn (Armstrong & Forde, 2003; Lusthaus, 2012).

Analyse van sociale netwerken

Sociale-netwerkanalyse is in de afgelopen decennia uitgegroeid tot een belangrijke onderzoeksmethode in de sociologie. Diverse onderzoekers, waaronder Lupsha (1983), Sparrow (1991) en Coles (2001), hebben sociale-netwerkanalyse voorgesteld als een methode om inzicht te verkrijgen in criminele samenwerkingsverbanden. Sociale wetenschappers hebben sociale netwerken sinds het begin van de twintigste eeuw gebruikt om complexe relaties weer te geven en te analyseren (Freeman, 2004). Volgens de theorie van sociale-netwerkanalyse zijn individuen, die ook wel 'actoren' worden genoemd binnen termen van sociale-

netwerkanalyse, onderdeel van een groter netwerk waarin de aard en intensiteit van hun verbindingen met anderen cruciaal zijn voor hun toegang tot informatie. Deze toegang tot informatie kan bepalend zijn voor het verkrijgen van invloed en macht binnen het netwerk (Kadushin, 2012).

Een crimineel netwerk bestaat uit verschillende elementen: (1) actoren, vaak individuen of groepen, (2) verbindingen tussen actoren (relaties) (3) de posities van actoren ten opzichte van andere actoren binnen het netwerk, en (4) het volledige netwerk. Om inzicht te krijgen in het functioneren van actoren binnen een netwerk, kunnen verschillende centraliteitsmaten worden bekeken: graad (*degree*), tussenliggendheid (*betweenness),* nabijheid (*closeness),* eigenvector en fragmentatie (*fragmentation)* (Valente, 2012). Graad geeft het aantal verbindingen van actoren in het netwerk weer. Tussenliggendheid geeft aan in hoeverre actoren een tussenpositie hebben en daarmee als cruciale schakel kunnen fungeren tussen actoren in het netwerk. Nabijheid laat zien hoeveel stappen actoren moeten nemen om bij andere actoren in het netwerk te geraken. Een lagere nabijheidsscore is gunstiger in termen van netwerkontwrichting. Eigenvector geeft aan in hoeverre actoren verbonden zijn met andere actoren die veel verbindingen hebben in het netwerk. Ten slotte verwijst fragmentatie naar de invloed op het netwerk indien een actor wegvalt (Valente, 2012). Door analyse van deze centraliteitsmaten kan inzicht worden verkregen in de structuur en dynamiek van het netwerk, wat waardevolle informatie kan bieden bij het effectief ontmantelen ervan. Actoren die bijvoorbeeld veel verbindingen hebben, bezitten in veel gevallen belangrijke informatie, genieten vertrouwen en veel aanzien van anderen. Het kan in termen van netwerkontwrichting nuttig zijn om interventies te richten op deze actoren.

Eenlingen en dyades; lone wolves

Binnen netwerkanalyse zijn verschillende soorten netwerken te onderscheiden, waaronder eenlingen (*isolates*) en dyades (*dyads*), die gekenmerkt worden door een zeer klein aantal actoren. Een eenling verwijst naar een actor die geen verbindingen heeft met andere actoren in het netwerk (Haythornthwaite, 1996). De graad van een eenling is logischerwijs gelijk aan 0. Een dyade is een netwerkrelatie met slechts twee actoren (Borgatti & Ofem, 2010). Hoewel eenlingen geen verbindingen hebben met anderen in het netwerk, betekent dit niet dat ze geen onderdeel uitmaken van het netwerk. Alle criminele actoren binnen een bepaalde geografische locatie of actief binnen een bepaalde criminele markt kunnen worden beschouwd als een crimineel netwerk, ongeacht hun connecties (Schwartz & Rouselle, 2009). Echter, eenlingen

zijn in termen van criminele netwerkanalyse niet nuttig omdat het verwijderen van eenlingen de fragmentatie in een netwerk niet vergroot (Borgatti & Ofem, 2010).

Wanneer een persoon weinig of geen verbindingen heeft met andere actoren, zoals eenlingen en actoren in dyades, wordt dit in de literatuur een *lone wolf* genoemd (Lusthaus, 2012). *Lone wolves* hebben geen sterke banden met anderen in het netwerk, hebben weinig invloed op anderen en ontvangen ook weinig informatie of ondersteuning van anderen. Sommige individuen kunnen bewust kiezen voor een beperkt aantal connecties of een meer onafhankelijke positie innemen binnen een netwerk (Lusthaus, 2019). Het kan ook voorkomen dat bepaalde groepen of individuen uitgesloten worden van het netwerk, waardoor ze als *lone wolves* worden beschouwd.

Uit verschillende studies blijkt dat cybercriminelen op grote schaal samenwerken (Leukfeldt, et al., 2017; Lusthaus, 2019). *Lone wolves* zijn ongebruikelijk in een netwerk zoals dat van bankhelpdeskfraude. Hoewel het in theorie mogelijk is om bankhelpdeskfraude individueel te plegen, is dit niet waarschijnlijk. Door *lone wolves* te identificeren, kan inzicht worden verkregen in waarom deze actoren ogenschijnlijk alleen handelen en welke kenmerken deze actoren hebben (Schwartz & Rouselle, 2009).

Crimescript

Een methode om meer inzicht te krijgen in het criminele proces van bankhelpdeskfraude is de analyse van het crimescript. Een crimescript legt de verschillende rollen, stadia en fasen van het criminele proces vast om inzicht te verkrijgen in de structuur van een criminele keten (Morselli & Roy, 2008). De analyse van crimescripts werd voor het eerst toegepast in 1994 om de opeenvolging van gebeurtenissen voor, tijdens en na het plegen van een delict te onderzoeken (Cornish, 1994). Het crimescript kan dienen als een waardevol hulpmiddel bij het opsporen van cybercriminelen en het ontwrichten van cybercriminele netwerken, omdat het inzicht kan bieden in welke rollen essentieel zijn voor het functioneren van het netwerk (Bright, Koskinen & Malm, 2019; Duijn, Kashirin & Sloot, 2014). Vanwege deze mogelijkheden wordt de analyse van crimescripts steeds vaker toegepast in onderzoek naar zowel traditionele criminaliteit als cybercriminaliteit (Dehghanniri & Borrion, 2021). Het is ook gebruikt bij de analyse van verschillende vormen van cyberfraude, zoals phishing (Leukfeldt, 2014), identiteitsfraude (Lee, 2020) en creditcardfraude (Van Hardeveld, Webber & O'Hara, 2017).

Onderzoek naar crimescripts van phishing en banking malware heeft aangetoond dat de samenstelling van de netwerken geregeld verandert, naast een min of meer vaste groep kernleden. *Kernleden* plegen zowel gezamenlijk als individueel delicten, zowel binnen als

buiten het eigen netwerk. Wanneer crimescripts veranderen als reactie op nieuwe veiligheidsmaatregelen, worden er nieuwe *dienstverleners* geworven en rekruteren kernleden ook nieuwe dienstverleners. Bovendien is er voortdurend nieuwe aanwas van *geldezels*. Ondanks al deze veranderingen kunnen binnen alle netwerken van phishing en banking malware vier posities worden onderscheiden: kernleden, professionele dienstverleners, gerekruteerde dienstverleners en geldezels (Leukfeldt, et al., 2017).

Kernleden zijn verantwoordelijk voor het initiëren en coördineren van de bankhelpdeskfraude. Ze zijn essentieel en sturen andere leden van het netwerk aan. Binnen de groep kernleden kan een hiërarchie bestaan, zoals één kernlid dat de andere kernleden aanstuurt en subgroepen van kernleden met specifieke taken. Een dergelijke hiërarchie is echter niet noodzakelijk in een netwerk gericht op bankhelpdeskfraude. Bovendien kan een kernlid ook alleen opereren; zonder andere kernleden. *Dienstverleners* bevinden zich onder de kernleden. Ze leveren diensten die nodig zijn voor het uitvoeren van bankhelpdeskfraude. Sommige dienstverleners spelen een belangrijkere rol voor de kernleden vanwege de zeldzaamheid of waarde van bepaalde diensten. Daarom kan er binnen de groep dienstverleners onderscheid worden gemaakt tussen professionele en gerekruteerde dienstverleners (Leukfeldt, et al., 2017).

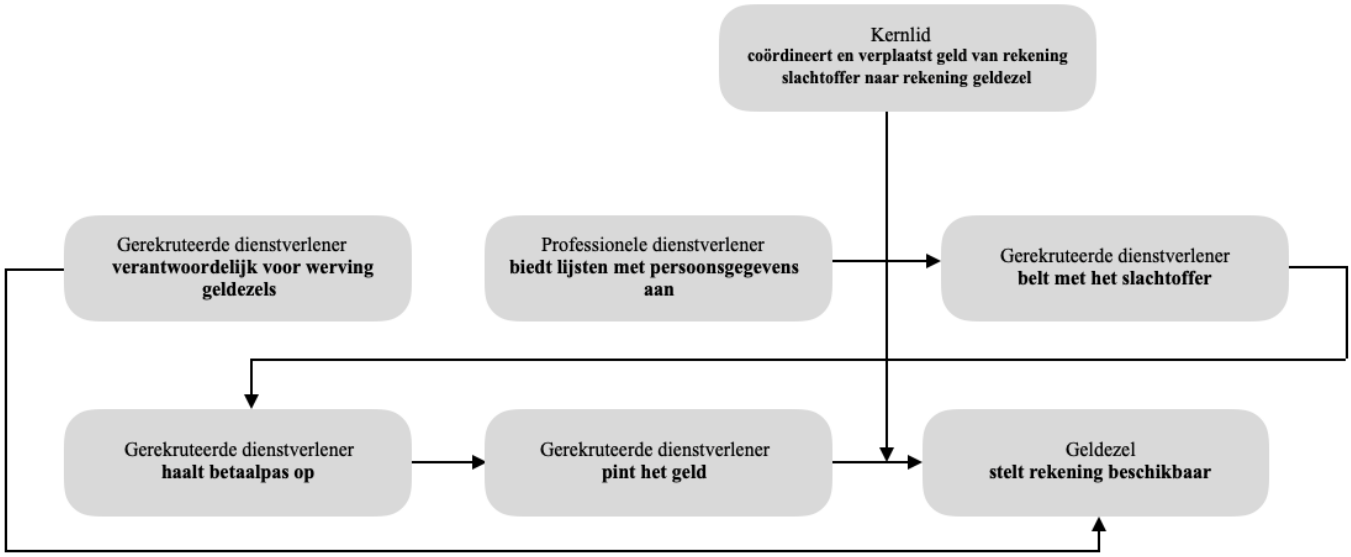
Professionele dienstverleners bieden bepaalde diensten aan de kernleden, zoals het ontwikkelen van een systeem waarmee telefoonnummers kunnen worden verborgen en de criminelen zich kunnen voordoen als officiële instanties zoals banken (Politie, 2022; Teng, 2019). Andere professionele dienstverleners bieden persoonsgegevens aan van potentiële slachtoffers die zijn verkregen uit datalekken. Dit omvat geboortedata, bankrekeningnummers en het bedrag op iemands rekening, alle gegevens die van pas komen bij bankhelpdeskfraude (Verhagen & Sabel, 2021). Deze dienstverleners worden als 'professioneel' beschouwd omdat ze op eigen initiatief hun diensten aanbieden aan de kernleden, bijvoorbeeld op online fora die door cybercriminelen worden gebruikt, of omdat ze bekende criminele dienstverleners zijn in de offline criminele wereld (Oerlemans, Custers, Pool, & Cornelisse, 2016).

Gerekruteerde dienstverleners leveren ook diensten aan de kernleden, maar zij worden aangemoedigd of gedwongen door de kernleden. Ze hebben toegang tot informatie die belangrijk is voor de kernleden of ze kunnen 'eenvoudige' diensten verlenen die de kernleden zelf zouden kunnen uitvoeren of die niet essentieel zijn voor de uitvoering van het crimescript. Voorbeelden hiervan zijn callcentermedewerkers van banken, personen die pinpassen ophalen en zich voordoen als bankmedewerkers, en medewerkers van telecommunicatiebedrijven. Net als professionele dienstverleners verlenen gerekruteerde dienstverleners diensten aan de kernleden. Het verschil tussen beide groepen is dat gerekruteerde dienstverleners minder

belangrijk zijn voor de uitvoering van het crimescript en gemakkelijker vervangen kunnen worden dan professionele dienstverleners. Gerekruteerde dienstverleners ontvangen meestal slechts een kleine vergoeding (Leukfeldt, et al., 2017).

De *geldezels*, personen die hun bankrekening beschikbaar stellen aan de kernleden om het frauduleus verkregen geld te kunnen witwassen, bevinden zich in de onderste laag van het crimescript (Oerlemans, Custers, Pool, & Cornelisse, 2016). Deze voornamelijk jonge personen, worden - bewust of onbewust - gebruikt voor hun bankrekening, zonder veel betrokkenheid bij de rest van het criminele proces. In andere netwerken worden geldezels ingezet voor het ophalen of ontvangen van producten die zijn besteld met gestolen betaalpassen, in plaats van het witwassen van geld. Vervolgens sturen de geldezels de pakketjes door naar de kernleden, wat hen de bijnaam *'shipping mules'* of *'parcel mules'* geeft (Hutchings, 2014; Van Nguyen, 2022). In deze studie wordt de term geldezel gebruikt om te verwijzen naar personen die illegaal geld of illegale producten ontvangen om deze vervolgens over te dragen. Omdat geldezels over het algemeen slechts eenmalig kunnen worden gebruikt voor het witwassen van grote geldbedragen of het doorsturen van illegale producten, is er een groot aantal geldezels nodig (Leukfeldt & Kleemans, 2019; Soudijn & Zegers, 2012). Geldezels maken geen deel uit van de groep kernleden die de illegale activiteiten coördineert. Desondanks vormen ze een cruciaal onderdeel van het crimescript, omdat ze het geldspoor onderbreken en tegelijkertijd de kernleden de mogelijkheid geven om anoniem te blijven voor de politie. Geldezels nemen een groot risico voor een relatief lage beloning en stellen cybercriminele netwerken in staat om soepel te functioneren. De persoon die de geldezels ronselt, speelt daarmee ook een belangrijke rol in het crimescript.

Figuur 1 visualiseert een crimescript van bankhelpdeskfraude. Dit voorbeeld illustreert een mogelijke structuur van een crimescript voor bankhelpdeskfraude. Aangezien er tot op heden geen exact crimescript voor bankhelpdeskfraude bekend is in de literatuur, is Figuur 1 gebaseerd op informatie uit studies over phishing en banking malware en onderzoek van analisten van de Dienst Regionale Informatie Organisatie (DRIO) van de eenheid Noord-Nederland. Zij beschreven een voorbeeld van samenwerking tussen bankhelpdeskfraudeurs in de 'Smibanese' straattaal, zie hiervoor bijlage III. Hoewel phishing- en banking malware-netwerken niet identiek zijn aan bankhelpdeskfraude-netwerken, vertonen deze vormen van cybercriminaliteit veel overeenkomsten en worden ze vaak in dezelfde context genoemd of gecombineerd.



Figuur 1. Crimescript bankhelpdeskfraude

Netwerkinterventies

Netwerkinterventies hebben tot doel gedragsverandering binnen een netwerk te bewerkstelligen door de actoren in het netwerk te beïnvloeden (Valente, 2012). Aangezien medewerking van criminelen binnen criminele netwerken onwaarschijnlijk is, zijn netwerkinterventies voor criminele netwerken voornamelijk gericht op het verwijderen van actoren uit het netwerk om het criminele netwerk te ontmantelen (Bright, Greenhill, Britz, Ritter & Morselli, 2017; Duijn, Kashirin & Sloot, 2014).

Voorgaand onderzoek heeft verschillende benaderingen opgeleverd om de relevante actoren te identificeren die nodig zijn om het netwerk te verstoren en ontmantelen. Twee benaderingen die in dit onderzoek worden belicht, zijn de sociaal-kapitaalbenadering en de menselijk-kapitaalbenadering (Hatala, 2006; Bright et al., 2017). De sociaal-kapitaalbenadering richt zich op het bepalen van de meest invloedrijke actoren binnen een netwerk door te kijken naar de verbindingen tussen de actoren (Coleman, 1988). Deze verbindingen stellen actoren in staat informatie en middelen uit te wisselen (Hatala, 2006). Netwerkinterventies gebaseerd op de sociaal-kapitaalbenadering richten zich op actoren die belangrijke posities in het netwerk bekleden (Bright et al., 2017). Deze posities omvatten actoren die directe verbindingen hebben met andere actoren en actoren die als bruggen dienen tussen kleinere groepen van actoren, ook wel bekend als clusters in termen van sociale-netwerkanalyse. Deze actoren worden vaak aangeduid als bruggenbouwers (*brokers)* (Valente, 2012). Bruggenbouwers worden beschouwd als sleutelfiguren in het netwerk vanwege hun strategische positie, waarbij zij een essentiële rol

vervullen bij zowel de verspreiding van informatie als de uitwisseling van middelen (Bright et al., 2017; Duijn et al., 2014). Binnen sociale-netwerkanalyse worden bruggenbouwers geïdentificeerd aan de hand van de centraliteitsmaat tussenliggende centraliteit (*betweenness centrality*) (Everett & Borgatti, 2010; Valente, 2012). Een andere belangrijke centraliteitsmaat binnen de sociaal-kapitaalbenadering is de nabijheidcentraliteit (*closeness centrality*). Nabijheidcentraliteit meet de afstand van een actor tot alle andere actoren in het netwerk en geeft aan hoe snel een actor informatie of invloed kan verspreiden naar andere actoren (Everett & Borgatti, 2010; Valente, 2012).

De menselijk-kapitaalbenadering kijkt niet naar de positie van actoren binnen een netwerk, maar richt zich op het identificeren van actoren met een belangrijke rol op basis van hun persoonlijke kenmerken, kennis en capaciteiten (Bright et al., 2017; Duijn et al., 2014). Hierbij wordt gekeken naar actoren die essentieel zijn voor het functioneren van het crimescript (Morselli & Roy, 2008). Actoren met veel menselijk kapitaal in het crimescript van bankhelpdeskfraude kunnen bijvoorbeeld degenen zijn die verantwoordelijk zijn voor het verstrekken van lijsten persoonsgegevens (*leads*) en de bellers. Specifieke kennis en vaardigheden zijn vereist voor deze rollen (Chiu, Leclerc & Townsley, 2011; Duijn et al., 2014; Morselli & Roy, 2008).

De volgende deelvragen met betrekking tot netwerkanalyse worden behandeld in dit onderzoek:

1. Wie zijn de essentiële personen in het netwerk? Hierbij wordt gekeken naar de centraliteitsmaten in het netwerk: graad, tussenliggende centraliteit en nabijheidcentraliteit.
2. In hoeverre verschillen *lone wolves* in geslacht, leeftijd en delictverleden van verdachten in grotere netwerken?
3. Welke rollen bekleden buitenlandse actoren?
4. Welke actoren zijn essentieel in termen van sociaal kapitaal?
5. Welke actoren zijn essentieel in termen van menselijk kapitaal? Hierbij wordt gekeken naar persoonlijke kenmerken, kennis en capaciteiten van de actoren.

3. Methoden

In deze paragraaf wordt de opzet van het onderzoek uiteengezet. Het eerste deel behandelt de verzameling en kenmerken van de data, evenals de uitgevoerde operationalisaties. Het tweede deel bespreekt de analyses die zullen worden uitgevoerd.

Data

In dit onderzoek wordt gebruikgemaakt van politiedata uit het jaar 2022. De dataset omvat een volledige lijst van alle registraties van bankhelpdeskfraude in 2022, verkregen via de Landelijke Cybercrime Query. De Landelijke Cybercrime Query is opgesteld om inzicht te verschaffen in het aandeel cyberincidenten binnen de politieregistraties (Boekhoorn, 2020). De registraties zijn afkomstig uit de Basisvoorziening Handhaving (BVH), het systeem dat de politie gebruikt voor het registreren van incidenten. Deze registraties omvatten incidenten die zich in Nederland hebben voorgedaan, maar kunnen ook niet-Nederlandse verdachten bevatten. Een verdachte wordt beschouwd als buitenlands wanneer deze een buitenlandse identiteit heeft en niet in Nederland woont (Straver, Meesters & van Duijneveldt, 2010). De gegevens die in dit onderzoek worden gebruikt, zijn verzameld in overeenstemming met artikel 8 van de Wet Politiegegevens (art. 8 Wpol, 2022). Om privacy, vertrouwelijkheid en opsporingsbelangen te waarborgen, zijn de gegevens geanonimiseerd voor publicatie in het onderzoek.

De dataset bevat in totaal 715 registraties van bankhelpdeskfraude. Binnen een registratie kunnen er verscheidene verdachten zijn. Enkele verdachten komen vaker dan eenmaal voor in de dataset, omdat zij meermaals verdacht zijn van bankhelpdeskfraude in 2022. Het aantal unieke verdachten van bankhelpdeskfraude bedraagt 824. Er zijn 22 verdachten in de data waarvan geen gegevens bekend zijn. Het is onduidelijk waarom er geen gegevens beschikbaar zijn voor deze verdachten. Deze specifieke verdachten worden niet meegenomen in de beschrijvende analyses, waardoor de uiteindelijke dataset 802 verdachten bevat (97,3%).

De informatie over de verdachten in de dataset omvat de volgende gegevens: uniek registratie- en voorvalnummer, naam, geslacht, geboortedatum, geboortegemeente, geboorteland en delictverleden. Met behulp van deze data kunnen analyses worden uitgevoerd met betrekking tot het aandeel buitenlandse verdachten binnen Nederland, de kenmerken van verdachten van bankhelpdeskfraude, de rollen binnen het crimescript, het verschil tussen *lone wolves* en verdachten in grotere netwerken, en de verdachten die essentieel zijn in termen van sociaal en menselijk kapitaal.

Operationalisaties

Om de eerste deelvraag te onderzoeken, wordt het aandeel buitenlandse verdachten in de registraties van bankhelpdeskfraude onderzocht. Alle verdachten worden gehercodeerd in een dichotome variabele bestaande uit de groepen 0 (“Nederlands”= 0) of 1 (“buitenlands”= 1). Het aantal en het percentage Nederlandse en buitenlandse verdachten van bankhelpdeskfraude worden berekend.

Om inzicht te krijgen in de kenmerken van cyberverdachten op het gebied van bankhelpdeskfraude, worden het geslacht, de leeftijd en het delictverleden van de verdachten bestudeerd. Hiervoor worden de volgende acties uitgevoerd.

Geslacht

Geslacht wordt gecodeerd als een dichotome variabele met de categorieën 'man' en 'vrouw'. Aan de hand van beschrijvende statistieken worden het aantal en het percentage mannelijke en vrouwelijke verdachten van bankhelpdeskfraude berekend.

Leeftijd

Leeftijd is een continue variabele die de leeftijd van de verdachte ten tijde van het delict weergeeft. Hierbij worden het gemiddelde, minimum, maximum en standaarddeviatie van de leeftijd berekend, en afzonderlijk voor mannelijke en vrouwelijke verdachten.

Delictverleden

Om het delictverleden van de verdachten in kaart te brengen, wordt de data geclassificeerd in de volgende categorieën: geen delictverleden, traditioneel delictverleden, digitaal delictverleden en gemengd delictverleden. De categorie ‘gemengd delictverleden’ omvat zowel een traditioneel als digitaal delictverleden. Het delictverleden van een verdachte wordt bepaald en geclassificeerd aan de hand van het unieke registratie- en voorvalnummer van de verdachte. Hiermee worden alle delicten waarvoor de persoon verdachte is geweest vóór het bankhelpdeskfraude delict, zoals geregistreerd in de *Bluespot Monitor*, in de analyse opgenomen. De Bluespot Monitor biedt op landelijk niveau inzicht in alle incidenten en acties die zijn geregistreerd in de Basisvoorziening Handhaving (BVH). Dit systeem geeft bijvoorbeeld informatie over wat er in een bepaald gebied is gebeurd en welke personen betrokken zijn bij deze incidenten (Inspectie Justitie en Veiligheid, 2021). Door het gebruik van zowel kwalitatieve data uit proces-verbaal als kwantitatieve data uit de BVH, kan er worden gesproken van methodische triangulatie.

Onderzoeksopzet

De kenmerken van bankhelpdeskfraudeurs worden beschreven aan de hand van het aandeel buitenlandse verdachten in de data, evenals het geslacht, de leeftijd en het delictverleden van de verdachten. Met behulp van beschrijvende statistieken worden deze variabelen geanalyseerd om een beeld te krijgen van de '*gemiddelde bankhelpdeskfraudeur'*. Aangezien er momenteel weinig bekend is over deze kenmerken in zowel de theoretische literatuur als de praktijk bij de politie, is het doel van deze analyse om meer inzicht te verschaffen.

Netwerkanalyse

Hoewel in voorgaande studies enkele cybercriminele netwerken zijn onderzocht, is er weinig specifiek onderzoek gedaan naar netwerken van bankhelpdeskfraudeurs. Bovendien ontbreekt een verkennend overzicht op dit onderwerp. Daarom is ervoor gekozen om initieel het volledige beeld van bankhelpdeskfraudeurs in 2022 weer te geven in één netwerk, om zo te onderzoeken hoe dit netwerk van bankhelpdeskfraudeurs eruitziet. Hierbij wordt gebruik gemaakt van de software *Cytoscape*. Cytoscape is oorspronkelijk ontwikkeld voor systeem biologische analyses, maar wordt tegenwoordig ook gebruikt voor netwerkvisualisatie, -analyse en data-integratie (Killcoyne, Carter, Smith & Boyle, 2009).

Om te beginnen wordt gekeken naar de eenlingen en dyades in het netwerk. Hierbij wordt gekeken naar de rollen die deze actoren vervullen en waarom zij ogenschijnlijk alleen of in zeer kleine netwerken opereren. Vervolgens wordt het volledige netwerk in kaart gebracht en geanalyseerd. Hierbij worden centraliteitsmaten berekend op basis van de verbindingen tussen de actoren. Een verbinding tussen actoren bestaat wanneer ze samen voorkomen in een registratie van bankhelpdeskfraude in 2022. Deze analyse geeft inzicht in de belangrijkste actoren binnen het netwerk en hun mate van invloed en connectiviteit.

Verder wordt het netwerkbeeld onderzocht op basis van het delictverleden van de actoren. De actoren die voorkomen in het beeld van bankhelpdeskfraude in 2022 zijn in veel gevallen al eerder verdacht van bankhelpdeskfraude en/of andere delicten. Op basis van deze registraties zijn de actoren onderling meer met elkaar verbonden.

De centraliteitsmaten graad, tussenliggende centraliteit en nabijheidcentraliteit worden gebruikt om te bepalen hoe belangrijk een actor is voor het functioneren van het netwerk in termen van sociaal kapitaal. De graad geeft het totale aantal verbindingen van een actor in het netwerk. De tussenliggende centraliteit identificeert de meest cruciale schakel, ook wel bekend als de bruggenbouwer, op basis van welke actor zich op een tussenliggend pad bevindt tussen andere actoren in het netwerk. De nabijheidcentraliteit meet het aantal stappen dat een actor

moet nemen om bij andere actoren in het netwerk te komen (Valente, 2012). Deze centraliteitsmaten zijn gekozen omdat ze inzicht geven in sleutelposities, vanuit de sociaal-kapitaalbenadering.

Verder is het van belang inzicht te krijgen in de rollen die actoren bekleden en, op basis van het eerder genoemde crimescript (zie Figuur 1), in kaart te brengen in hoeverre deze rollen belangrijk zijn voor het functioneren van het netwerk. Aan de hand van de menselijk-kapitaalbenadering kunnen de essentiële rollen op basis van persoonlijke kenmerken, kennis en capaciteiten worden vastgesteld (Bright et al., 2017; Duijn et al., 2014; Hatala, 2006). Het kan waardevol zijn om netwerkanalyse te combineren met crimescripts om doelgerichte interventies toe te passen op de meest essentiële leden in het netwerk die moeilijk te vervangen zijn (Bright et al., 2017; Duijn & Klerks, 2014; Morselli & Roy, 2008).

Onderzoek naar de rollen

Om inzicht te krijgen in de rollen van actoren binnen het crimescript, is een gedetailleerde analyse van 466 registraties vereist. Deze registraties hebben betrekking op de rollen van actoren in de verschillende netwerken 1, 2 en 3 (zie Figuur 8) en eenlingen en dyades. De tijd die benodigd is om de rol van de actor te achterhalen, kan per registratie verschillen. Dankzij de digitale proces-verbalen in de politiesystemen, afkomstig uit de Basisregistraties Handhaving (BVH), kan in sommige gevallen binnen enkele minuten worden achterhaald welke rol de actor vervulde. De BVH biedt toegang tot verschillende (inter)nationale en regionale bronregisters en bevat beknopte samenvattingen van zaken (Straver, Meesters & van Duijneveldt, 2010; Politieacademie, z.d.).

In andere gevallen is het proces complexer en vereist het doorlezen van meerdere proces-verbalen, zoals proces-verbaal van bevinding en proces-verbaal van verdenking. Deze proces-verbalen bevatten bijvoorbeeld informatie over camerabeelden, identificaties door agenten en soms zelfs DNA-onderzoek.

Voor bepaalde gevallen is het nodig om de registratie en de rol te onderzoeken in een ander verwerkingsprogramma van de politie, genaamd Summ-IT. Dit komt doordat het onderzoek in dergelijke gevallen volledig is uitgewerkt in Summ-IT in plaats van in de BVH. Summ-IT wordt gebruikt voor grotere zaken waarbij de recherche betrokken is, zoals het opsporen en ontmantelen van grootschalige netwerken (Kramer, Blokland & Soudijn, 2020). De benodigde tijd om de rol te achterhalen varieert doorgaans tussen de 5 en 25 minuten, afhankelijk van de wijze waarop de informatie is verwerkt in de politiesystemen en de omvang

van het onderzoek. In enkele gevallen kan de rol van de actor niet worden achterhaald vanwege een gebrek aan informatie in de politiesystemen.

Aangezien dit onderzoek gebruikmaakt van kwalitatieve informatie uit proces-verbaal en rechercheonderzoeken, gecombineerd met netwerkanalyse, kan opnieuw worden gesproken van methodische triangulatie.

4. Resultaten

In deze paragraaf worden de resultaten van de uitgevoerde analyses behandeld, waarbij het eerste deel zich richt op de beschrijvende statistieken van de variabelen en de uitgevoerde operationalisaties, terwijl het tweede deel de netwerkanalyse behandelt.

Beschrijvende statistieken

Tabel 1 geeft de beschrijvende statistieken van de variabelen weer. Deze statistieken omvatten het gemiddelde, de standaarddeviatie, het minimum en het maximum van de variabelen. Voor de categorische variabelen (buitenlandse) afkomst, geslacht en delictverleden worden de percentages van beide groepen weergegeven in plaats van het gemiddelde. In de registraties van bankhelpdeskfraude in 2022 zijn er 925 (91,3%) Nederlandse verdachten en 88 (8,7%) buitenlandse verdachten. Aangezien sommige verdachten verschillende keren voorkomen in de dataset, wordt er ook gekeken naar het aantal unieke verdachten. Hieruit blijkt dat er 702 (89,1%) Nederlandse verdachten en 86 (10,9%) buitenlandse verdachten zijn. De gemiddelde leeftijd van bankhelpdeskfraudeurs is 28 jaar, dit geldt ook wanneer afzonderlijk gekeken wordt naar de gemiddelde leeftijd van mannen en vrouwen. Uit de statistieken blijkt dat mannen duidelijk oververtegenwoordigd zijn in het bankhelpdeskfraudebeeld van 2022, aangezien de verdeling van mannen en vrouwen in de data scheef is. De grootste groep verdachten (51%) heeft een traditioneel delictverleden en ruim een derde van de verdachten (35,4%) heeft geen delictverleden. Bijlage I bevat de volledige uitwerking van de beschrijvende statistieken.

Tabel 1. Beschrijvende statistieken van de variabelen

Variabele	***% voor categorische en M (SD) voor continue variabelen***	***Minimum***	***Maximum***	***N***
1. Afkomst (Nederlands= 0; buitenlands = 1)	89,1% Nederlands 10,9% buitenlands	0	1	788
2.Geslacht (man= 0; vrouw = 1)	80,8% man 19,2% vrouw	0	1	796
3. Leeftijd	28,3 (11,11)	13	74	676

4. Delictverleden
(geen delictverleden= 0;
traditioneel delictverleden =1;
digitaal delictverleden = 2;
gemengd delictverleden = 3)
	35,4% geen delictverleden
	51,0% traditioneel delictverleden
	4,1% digitaal delictverleden
	9,5% gemengd delictverleden
		0	3	802

Beschrijving van het netwerkbeeld uit 2022

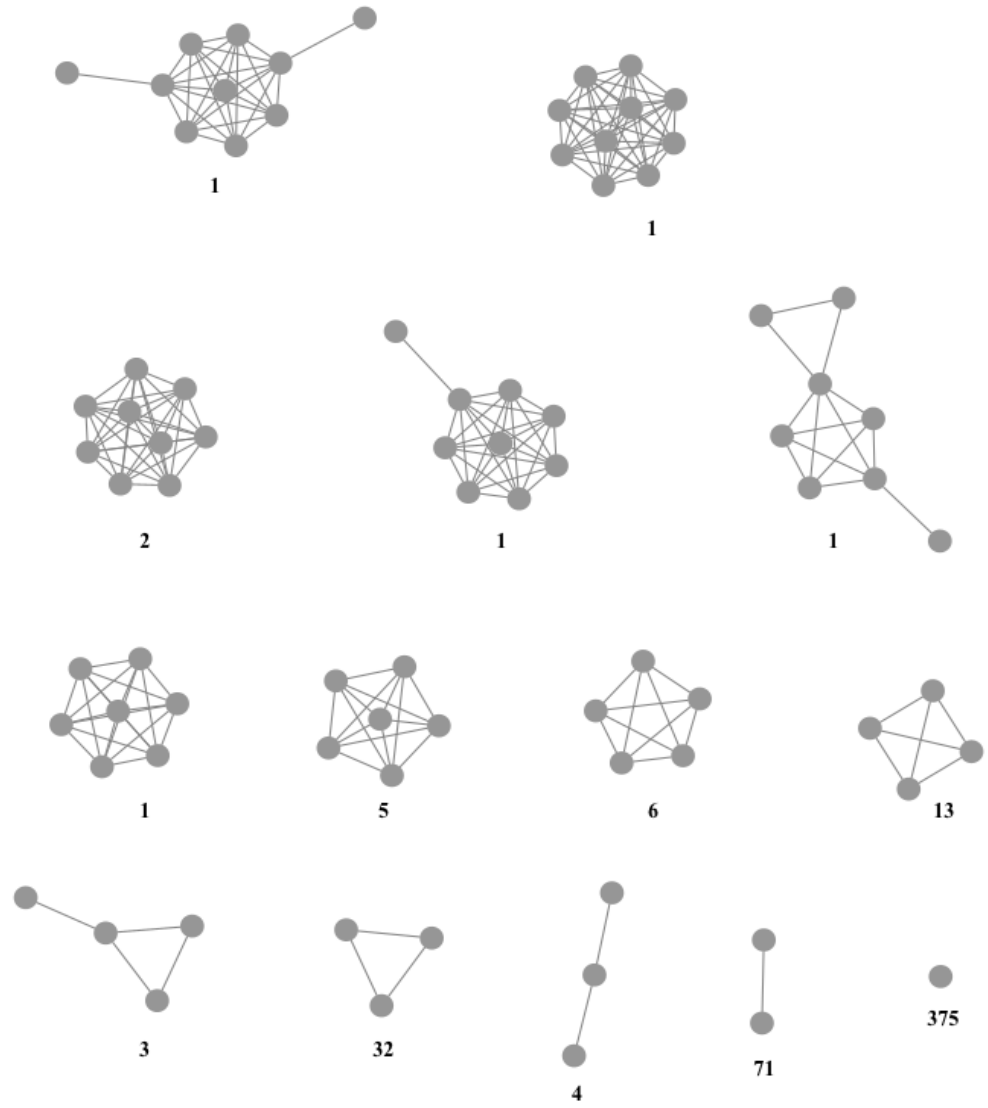
Figuur 2 toont het volledige visuele overzicht van de netwerken van alle verdachten van bankhelpdeskfraude uit 2022. Per netwerk wordt aangegeven hoe vaak deze voorkomt in het volledige netwerkbeeld. Het netwerkbeeld bestaat uit 811 actoren (*nodes*), die met elkaar verbonden zijn door 611 verbindingen (*ties)*. Actoren hebben een verbinding wanneer zij samen voorkomen in een registratie van bankhelpdeskfraude in 2022. Het aantal actoren verschilt van het eerder genoemde aantal van 802 unieke verdachten, omdat ook actoren zijn opgenomen in het netwerk waarvan geen gegevens bekend zijn, maar die wel verbindingen hebben met andere actoren. Dit is gedaan om een zo volledig mogelijk overzicht te bieden van de netwerken die verband houden met bankhelpdeskfraude, zoals bekend binnen de politiesystemen.

Op het eerste gezicht is te zien dat het netwerkbeeld bestaat uit verschillende subgroepen. Het netwerk bevat 375 eenlingen, wat bijna de helft (46,2%) van alle actoren is. Daarnaast zijn er 71 dyades (17,5%), bestaande uit in totaal 142 actoren.

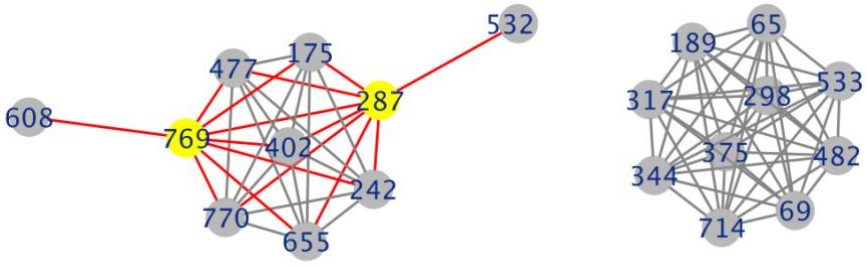
Uit de analyse van de rollen van eenlingen blijkt dat het merendeel (92,4%) van de eenlingen de rol van geldezel vervult. Het opstellen van een tabel met geanonimiseerde actoren en hun rollen zou echter niet erg informatief zijn, aangezien vrijwel elke actor de rol van geldezel heeft. Daarom is ervoor gekozen om geen tabel op te stellen. Aangezien deze actoren in termen van centraliteitsmaten minder relevant zijn voor de netwerkanalyse, worden ze niet verder in de analyse meegenomen. Hetzelfde geldt voor de dyades.

De twee grootste netwerken in het beeld van bankhelpdeskfraude uit 2022 bestaan elk uit 10 actoren. Figuur 3 geeft deze twee netwerken weer. De actoren met de hoogste graad, tussenliggende centraliteit en nabijheidcentraliteit-waarden zijn gemarkeerd in het geel. Actoren 287 en 769 hebben een graad van 8, wat betekent dat zij direct verbonden zijn met 8 andere actoren binnen het netwerk. Verder hebben ze een tussenliggende centraliteit van 0,22, wat betekent dat de betreffende actoren een redelijk goede tussenliggende positie hebben in het criminele netwerk. Ze kunnen fungeren als een verbindingspunt tussen andere individuen in het netwerk en hebben waarschijnlijk enige invloed op de informatiestroom. Op de nabijheidcentraliteit hebben ze een waarde van 0,90, wat duidt op een centrale positie binnen het netwerk. Deze actoren spelen vermoedelijk een belangrijke rol bij het faciliteren van communicatie en het verspreiden van informatie tussen verschillende groepen.

Vanwege de clustering en de relatief kleine omvang van de netwerken, is het netwerkbeeld van bankhelpdeskfraude uit 2022 beperkt in termen van sociale-netwerkanalyse. Daarom wordt het netwerk verder in kaart gebracht op basis van het delictverleden.



Figuur 2. Frequenties van de netwerken van bankhelpdeskfraude in 2022



Figuur 3. Netwerken uit het beeld van bankhelpdeskfraude met het grootste aantal verbonden actoren

Netwerk op basis van delictverleden

De actoren in het beeld van bankhelpdeskfraude in 2022 zijn in veel gevallen al eerder verdacht van bankhelpdeskfraude of andere delicten, wat resulteert in meer onderlinge verbindingen tussen de actoren. Gezien de beperkte mogelijkheden van het netwerkbeeld van alle verdachten van bankhelpdeskfraude in 2022, is het interessant om te kijken naar de netwerken op basis van het delictverleden van de verdachten. Figuur 8 toont een volledig beeld van de verdachten van bankhelpdeskfraude in 2022, inclusief de verbindingen van registraties van bankhelpdeskfraude en/of andere delicten van 5 jaar vóór 2022. Per netwerk wordt aangegeven hoe vaak deze voorkomt in het volledige netwerkbeeld op basis van het delictverleden.

Bij vergelijking van de twee netwerkbeelden valt op dat van de 375 eenlingen (zie Figuur 2) slechts 26 eenlingen (zie Figuur 8) 'overblijven' wanneer gekeken wordt naar de verbindingen op basis van delictverleden. Met andere woorden, een zeer groot deel van de eenlingen heeft in de vijf jaar vóór 2022 met één of meerdere van de andere verdachten een delict gepleegd waardoor deze eenlingen in het netwerkbeeld op basis van delictverleden geen eenling meer zijn. Hieruit kan worden geconcludeerd dat deze actoren minder geïsoleerd zijn dan op basis van het netwerkbeeld afkomstig uit enkel 2022 zou worden verwacht.

Beschrijving van de netwerken op basis van delictverleden

Zoals duidelijk te zien is in Figuur 8, bevatten de drie bovenste netwerken binnen het volledige netwerkbeeld op basis van delictverleden het grootste aantal verdachten. Deze netwerken worden daarom als meest relevant geacht in termen van sociale-netwerkanalyse en wordt binnen de netwerkanalyse specifiek gefocust op deze netwerken. De netwerken bestaan respectievelijk uit 64, 40, en 31 actoren. Verwacht wordt dat netwerk 3, vanwege het kleinere aantal actoren, vaak een hogere mate van centraliteit, dichtheid (*density*) en een kortere gemiddelde padlengte zal hebben. Tabel 2 bevat beschrijvende statistieken voor elk netwerk.

Alle drie de netwerken hebben relatief lage dichtheidswaarden. De dichtheid van een netwerk geeft aan hoeveel verbindingen er zijn in verhouding tot het totale aantal mogelijke verbindingen tussen de actoren in het netwerk (Tabassum, Pereira, Fernandes & Gama, 2018). Netwerk 3 heeft de hoogste dichtheid, namelijk 0,129. Een dichtheid van 0,129 betekent dat ongeveer 12,9% van de mogelijke verbindingen daadwerkelijk aanwezig is in het netwerk. Met andere woorden, er zijn binnen de netwerken weinig directe verbindingen tussen de actoren in vergelijking met het maximale aantal mogelijke verbindingen.

Netwerk 3 heeft een netwerkcentralisatie van 0,147, wat duidt op de hoogste centralisatie onder de netwerken. In een crimineel netwerk geeft een netwerkcentralisatie van

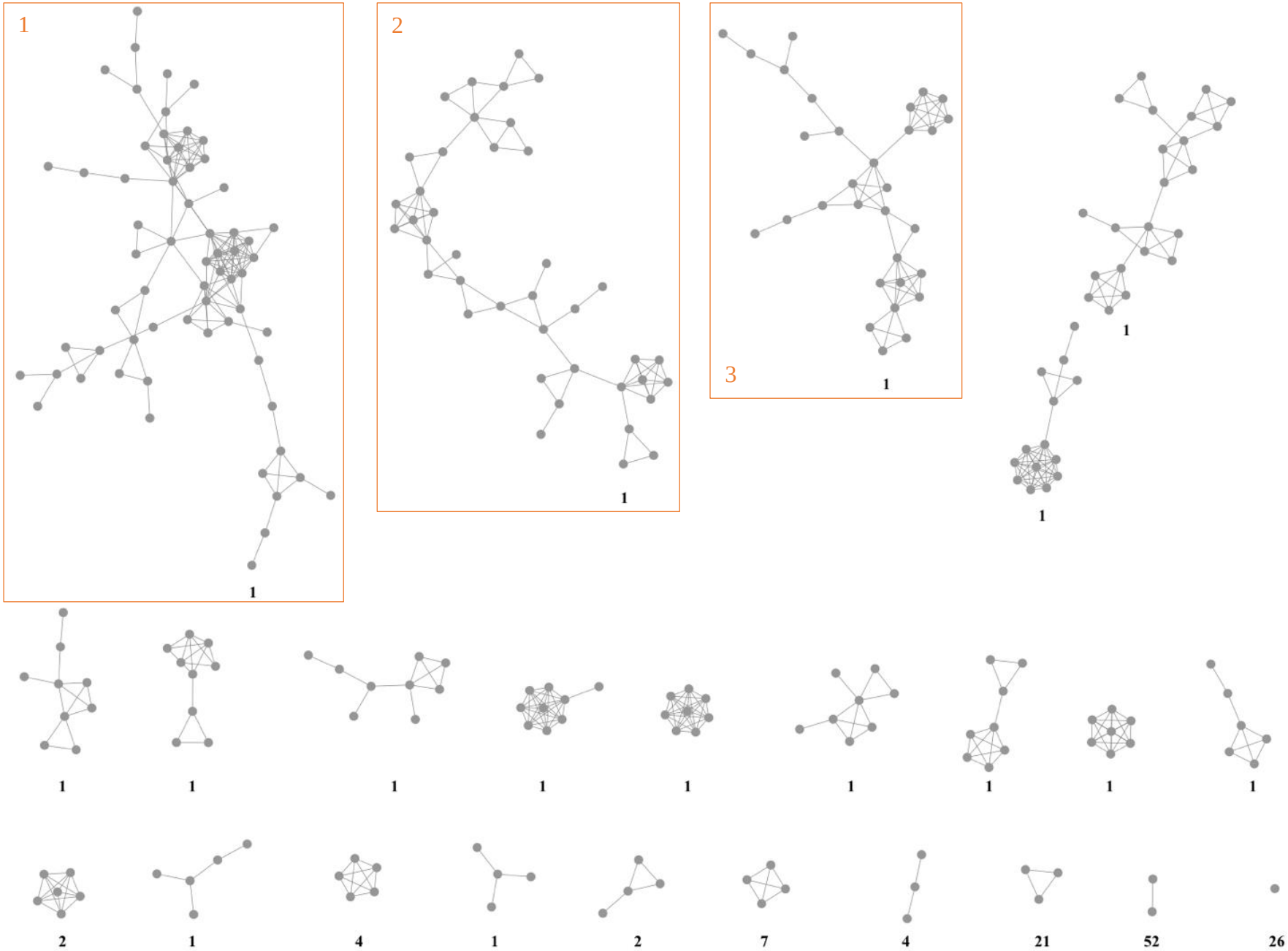
0,147 een lage centralisatie weer, wat betekent dat er weinig specifieke individuen of groepen zijn die aanzienlijk meer macht, controle of invloed hebben dan anderen in het netwerk. In plaats daarvan is de macht relatief gelijkmatig verdeeld over de actoren binnen het netwerk.

De gemiddelde padlengte van netwerk 3 is veruit het laagst, namelijk 1,688. Dit suggereert een hoge mate van directe verbindingen en nabijheid tussen individuele actoren in het criminele netwerk. Dit wijst op een sterk verbonden netwerk waarin actoren directe communicatie- en interactiemogelijkheden hebben. Netwerk 1 en netwerk 2 hebben daarentegen hogere gemiddelde padlengtes, wat duidt op gematigde afstanden tussen de actoren in het netwerk. Hoewel de afstanden niet erg kort zijn, is er nog steeds een redelijke mate van verbondenheid binnen het netwerk.

De *clusteringcoëfficiënt* van een netwerk is een maatstaf voor de mate van clustering of lokale samenhang in het netwerk. Het meet in hoeverre actoren in het netwerk de neiging hebben om verbonden te zijn met hun directe buren en of er sprake is van clustering van verbindingen tussen naburige actoren (Watts & Strogatz, 1998). Netwerk 2 heeft een clusteringcoëfficiënt van 0,618, wat wijst op een relatief hoge mate van lokale clustering en samenhang binnen het netwerk. Dit houdt in dat actoren de neiging hebben om verbindingen te hebben met hun directe buren en dat er clusters van sterk verbonden actoren kunnen bestaan. De aanwezigheid van clusters en lokale samenhang kan wijzen op een georganiseerde structuur binnen het criminele netwerk, waarin groepen actoren nauw samenwerken en gezamenlijke criminele activiteiten uitvoeren (Tabassum et al., 2018).

Tabel 2: Netwerk kenmerken

Netwerkmaten	***Netwerk 1***	***Netwerk 2***	***Netwerk 3***
Aantal actoren	64	40	31
Aantal verbindingen	151	70	60
Dichtheid	0,075	0,090	0,129
Netwerkcentralisatie	0,119	0,094	0,147
Gemiddelde padlengte	4,838	5,240	1,688
Clusteringcoëfficiënt	0,482	0,618	0,578
Gemiddelde aantal 'buren'	4,719	3,5	3,871



Figuur 8. Frequenties van de netwerken op basis van delictverleden

Lone wolves

Naast de drie grote netwerken, kent het volledige netwerkbeeld op basis van delictverleden ook eenlingen en dyades. Er zijn 26 eenlingen en 52 dyades, wat neerkomt op 104 actoren. In totaal zijn er 130 actoren die een zeer klein netwerk hebben. Deze individuen, die weinig tot geen directe verbindingen hebben met andere leden van het netwerk, worden in de sociale-netwerkanalyse *lone wolves* genoemd.

Tabel 3 toont de beschrijvende statistieken van de *lone wolves* terwijl Tabel 4 de beschrijvende statistieken van de actoren in grotere netwerken weergeeft. Bij het vergelijken van het geslacht, de leeftijd en het delictverleden van de *lone wolves* ten opzichte van de andere actoren, valt op dat er in de groep *lone wolves* in verhouding meer vrouwelijke actoren zijn dan in de groep actoren in grotere netwerken, $\chi^2(1, N = 796) = 4{,}23$, $p < {,}05$. Daarnaast is de gemiddelde leeftijd in de groep *lone wolves* ruim 2 jaar hoger dan de gemiddelde leeftijd van de groep actoren in grotere netwerken, $t(673) = 2{,}03$; $p < {,}05$). Bovendien verschilt het delictverleden van *lone wolves* van dat van actoren in grotere netwerken. Zo hebben *lone wolves* vaker geen delictverleden dan actoren in grotere netwerken en minder vaak een traditioneel, digitaal of gemengd delictverleden, $\chi^2(3, N = 802) = 43{,}63$, $p < {,}001$. Het grootste deel van de actoren in grotere netwerken (54,3%) heeft een traditioneel delictverleden.

Tabel 3. Beschrijvende statistieken van de lone wolves

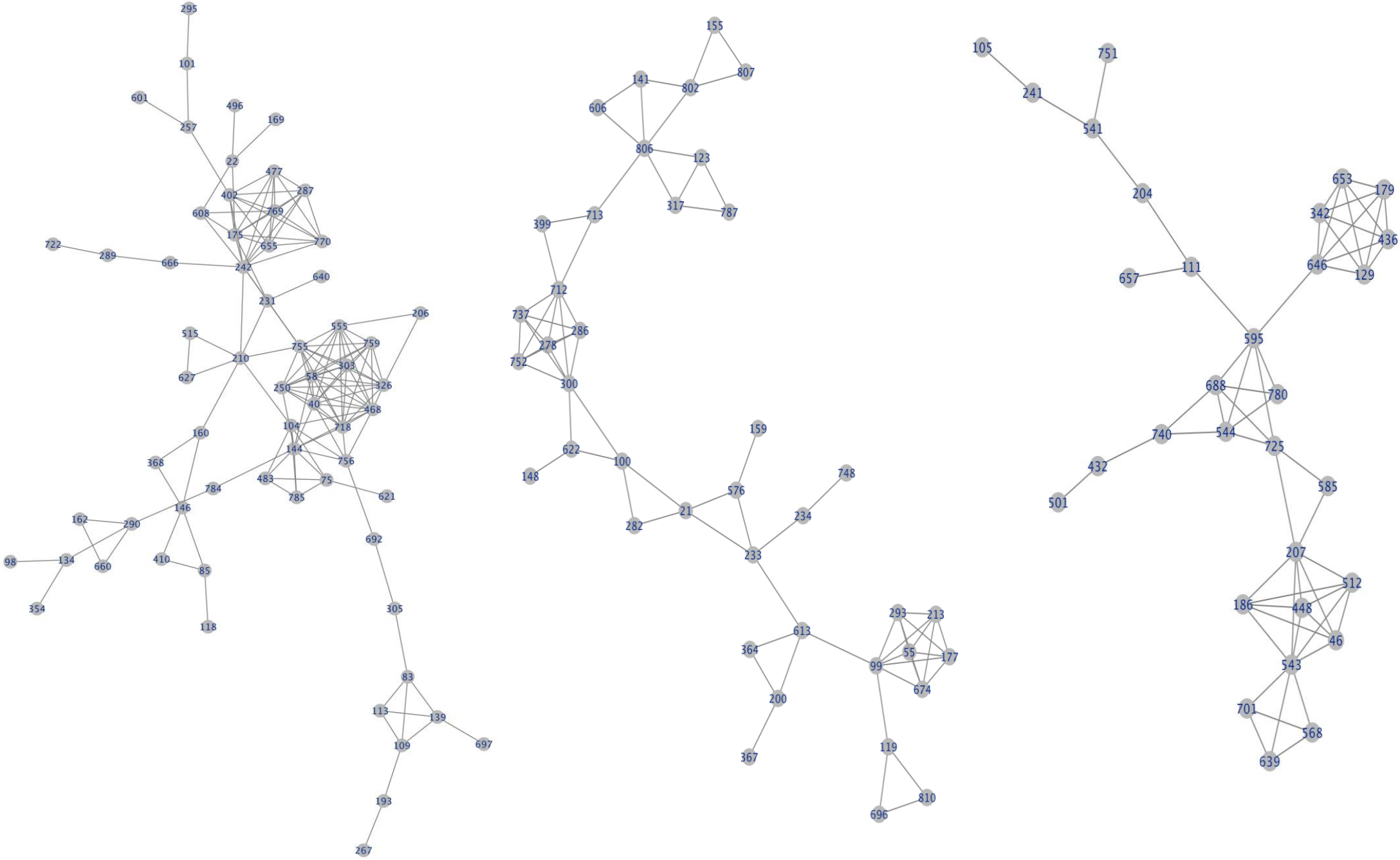
Variabele	***% voor categorische en M (SD) voor continue variabelen***	***Minimum***	***Maximum***	***N***
1. Geslacht (man= 0; vrouw = 1)	74,2% man 25,8% vrouw	0	1	128
2. Leeftijd	30,3 (12,6)	13	72	108

3. Delictverleden
(geen delictverleden= 0;
traditioneel delictverleden =1;
digitaal delictverleden = 2;
gemengd delictverleden = 3)
	60,0% geen delictverleden
	33,8% traditioneel delictverleden
	0% digitaal delictverleden
	6,2% gemengd delictverleden
		0	3	130

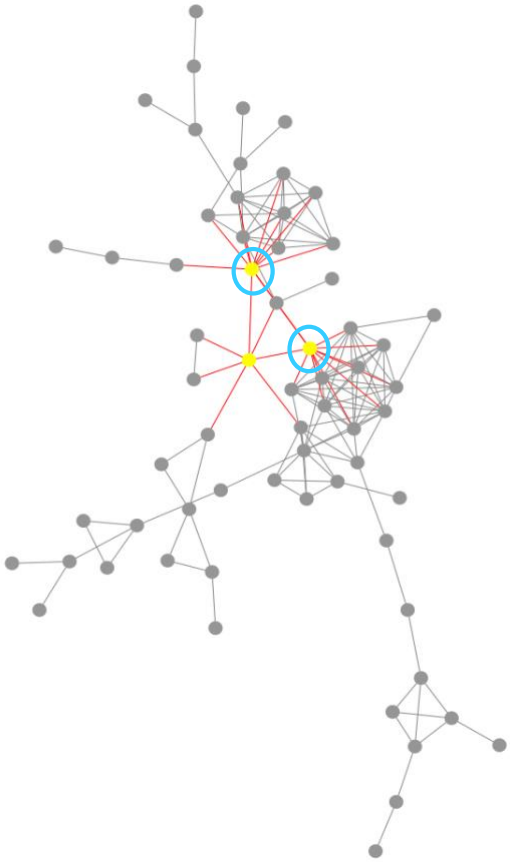
Tabel 4. Beschrijvende statistieken van de actoren in grotere netwerken

Variabele	***% voor categorische en M (SD) voor continue variabelen***	***Minimum***	***Maximum***	***N***
1. Geslacht (man= 0; vrouw = 1)	82,0% man 18,0% vrouw	0	1	668
2. Leeftijd	27,4 (10,8)	14	74	567

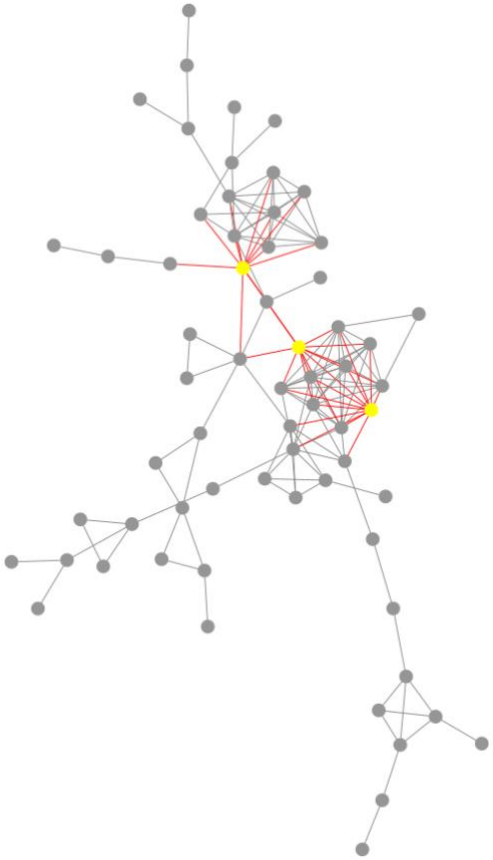
3. Delictverleden
(geen delictverleden= 0;
traditioneel delictverleden =1;
digitaal delictverleden = 2;
gemengd delictverleden = 3)
	30,7% geen delictverleden
	54,3% traditioneel delictverleden
	4,9% digitaal delictverleden
	10,1% gemengd delictverleden
		0	3	672



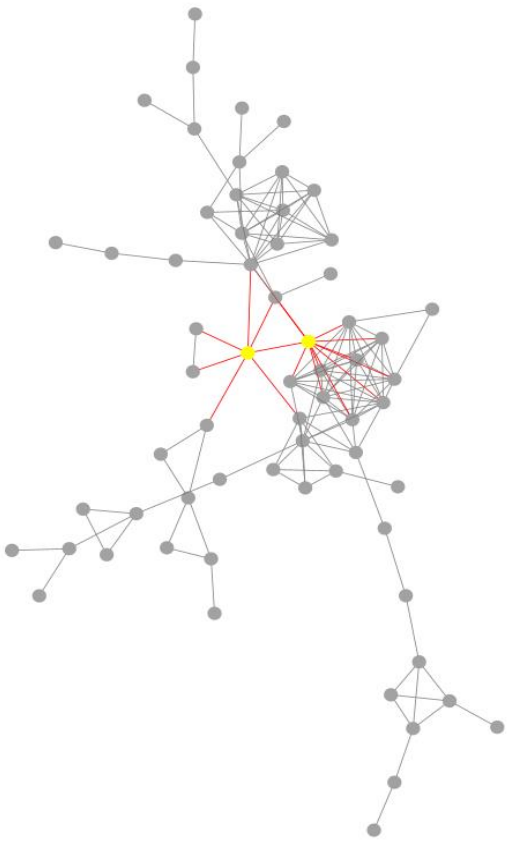
Figuur 9. Netwerken 1,2 en 3 met specificatie van de actoren



Figuur 10. Netwerk 1, de verdachten met de hoogste tussenliggende centraliteit waarden zijn aangeduid met de kleur geel en hun verbindingen zijn in het rood aangeduid. De meest essentiële actoren in termen van sociaal kapitaal binnen netwerk 1 zijn blauw omcirkeld



Figuur 11. Netwerk 1, de verdachten met de hoogste graad waarden zijn aangeduid met de kleur geel en hun verbindingen zijn in het rood aangeduid



Figuur 12. Netwerk 1, de verdachten met de hoogste nabijheidcentraliteit waarden zijn aangeduid met de kleur geel en hun verbindingen zijn in het rood aangeduid

Figuur 13. Netwerk 1, na verwijdering van actoren 242 en 755

Centraliteitsmaten

Figuur 9 toont de drie netwerken met nummers die zijn toegewezen aan de actoren. De actoren zijn geanonimiseerd en hebben allen waarden tussen 1 en 811. In de beschrijving van elk netwerk die volgt, worden de actoren genoemd aan de hand van deze nummers. Figuur 9 fungeert als een overzicht om te laten zien welke actoren aanwezig zijn in de drie netwerken.

Om de resultaten beknopt te houden, wordt in deze sectie alleen netwerk 1 volledig uitgewerkt. Voor netwerk 2 en netwerk 3 worden enkel de meest essentiële actoren in termen van sociaal kapitaal en de waarden van de buitenlandse verdachten behandeld. Gedetailleerde beschrijvingen van netwerk 2 en netwerk 3 worden weergegeven in bijlage II.

Netwerk 1

Tabel 4 geeft de centraliteitsmaten graad, nabijheidcentraliteit en tussenliggende centraliteit voor alle actoren in netwerk 1 weer. De top 5 rangen zijn weergegeven. De volledige tabellen zijn terug te vinden in bijlage II.

De actoren met de hoogste graad waarden zijn actoren 242, 755 en 468, met elk een graad waarde van 12. Dit betekent dat zij binnen het netwerk direct verbonden zijn met 12 andere actoren.

Binnen netwerk 1 kent actor 210 de hoogste nabijheidcentraliteit, namelijk 0,323. Dit geeft aan dat actor 210 een gemiddelde nabijheid heeft tot andere actoren in het netwerk. Nabijheidcentraliteit meet de afstand van een actor tot alle andere actoren in het netwerk en geeft aan hoe snel een actor informatie of invloed kan verspreiden naar andere actoren (Everett & Borgatti, 2010; Valente, 2012). Zoals te zien is in de tabel, liggen de waarden van de nabijheidcentraliteit van de actoren redelijk dicht bij elkaar. Figuur 12 toont de twee actoren met de hoogste waarden op de nabijheidcentraliteit in het geel.

In netwerk 1 hebben actoren 242 en 755 relatief hoge waarden voor tussenliggende centraliteit, wat aangeeft dat ze een tussenpositie bekleden en fungeren als schakels tussen subgroepen binnen het netwerk (Morselli & Roy, 2008). Deze tussenliggende leden zijn essentieel voor communicatie en toegang tot middelen tussen leden van verschillende subgroepen. Door gerichte interventies te richten op deze tussenliggende leden, wordt verwacht dat de criminele netwerken zullen fragmenteren, omdat de subgroepen dan niet langer met elkaar kunnen communiceren (Bouchard & Konarski, 2014; Morselli & Roy, 2008; Xu & Chen, 2003). Figuur 13 toont het netwerk nadat actoren 242 en 755 zijn verwijderd, waarbij het netwerk uiteenvalt in twee kleinere netwerken. De drie actoren aan de linkerkant komen los te staan van het grotere netwerk.

Actoren 242 en 755 tonen veruit de hoogste waarden voor de drie centraliteitsmaten. Ze hebben beiden de hoogste graad waarde en actor 242 heeft de hoogste tussenliggende centraliteit-score, terwijl actor 755 respectievelijk de tweede en derde positie inneemt op nabijheidcentraliteit en tussenliggende centraliteit. Deze actoren zijn blauw omcirkeld in Figuur 10. Het kan worden gesteld dat actoren 242 en 755 de meest essentiële actoren zijn in termen van sociaal kapitaal binnen netwerk 1. Figuur 13 laat zien hoe het netwerk eruit ziet wanneer actoren 242 en 755 worden verwijderd.

De buitenlandse actoren binnen netwerk 1, actoren 160 en 483, lijken niet essentieel te zijn in termen van sociaal kapitaal. Actor 160 scoort redelijk gemiddeld op zowel nabijheidcentraliteit als tussenliggende centraliteit, en heeft een lage graad van 3. Actor 483 heeft een nabijheidcentraliteit van 0,253 en een lage graad van 4.

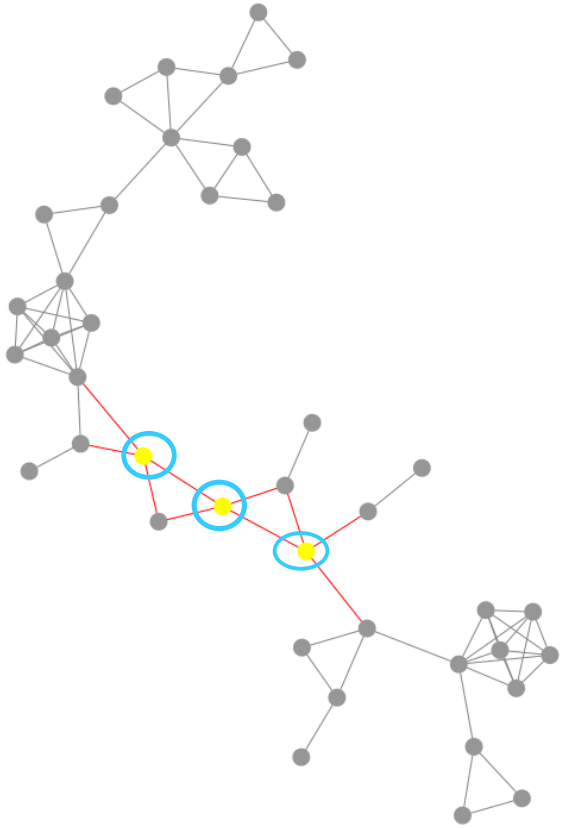
Tabel 4: centraliteitsmaten netwerk 1	**Rang**	**Actor**	**Score**
Graad	1	242, 755 en 468	12
8 – 12	2	144, 40 en 718	11
	3	58, 175, 250, 326 en 555	10
	4	303 en 759	9
	5	769 en 402	8
Nabijheidcentraliteit			
0,306 – 0,323	1	210	0,323
	2	755	0,318
	3	104	0,312
	4	468	0,307
	5	40 en 718	0,306
Tussenliggende centraliteit	1	242	0,397
0,234 – 0,397	2	210	0,327
	3	755	0,304
	4	756	0,249
	5	144	0,234

Netwerk 2

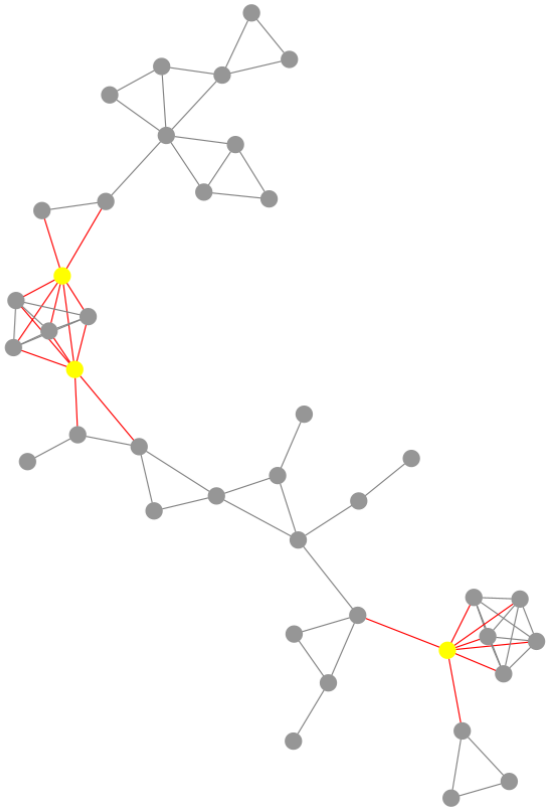
In netwerk 2 hebben actoren 233, 100 en 21 gemiddeld de hoogste waarden voor zowel de nabijheidcentraliteit als de tussenliggende centraliteit. Hoewel zij allen een gemiddelde graad van 4 hebben, kan er worden gesteld dat deze actoren in termen van sociaal kapitaal de meest essentiële actoren zijn in netwerk 2. Deze actoren zijn blauw omcirkeld in Figuur 14.

De buitenlandse actoren binnen netwerk 2, actoren 55, 213, 737 en 748, lijken niet essentieel te zijn in termen van sociaal kapitaal. Deze actoren hebben allen een waarde van 0 op de tussenliggende centraliteit, gemiddelde waarden op de nabijheidcentraliteit en een graad van 5 (actoren 55, 213, 737) of een graad van 1 (actor 748).

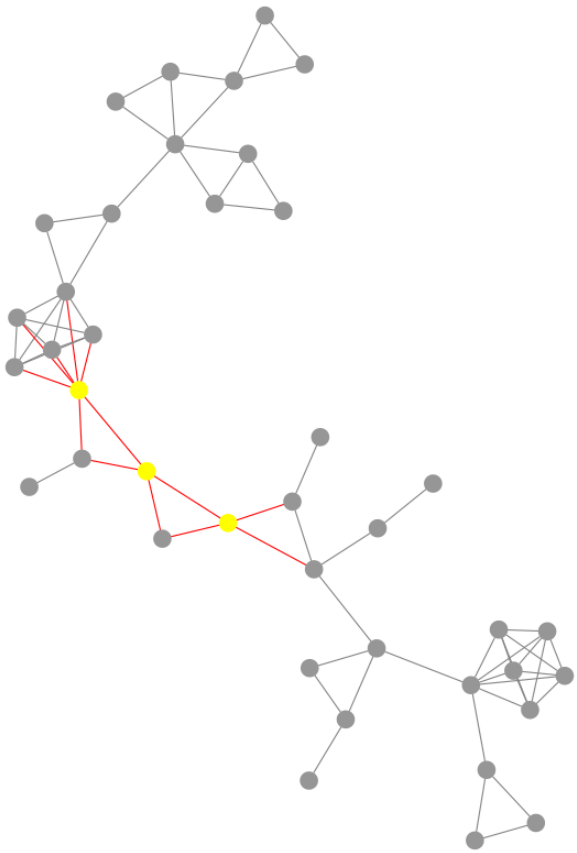
Tabel 5: centraliteitsmaten netwerk 2	**Rang**	**Actor**	**Score**
Graad	1	99, 300 en 712	7
3 – 7	2	806	6
	3	55, 177, 213, 278, 286, 293, 674, 737 en 752	5
	4	21, 100, 233, 613 en 802	4
	5	119, 123, 141, 200, 317, 576, 622 en 713	3
Nabijheidcentraliteit			
0,242 – 0,269	1	100	0,269
	2	21	0,267
	3	300	0,262
	4	233	0,257
	5	712	0,242
Tussenliggende centraliteit	1	233	0,521
0,474 – 0,521	2	100	0,513
	3	21	0,510
	4	300	0,497
	5	613	0,474



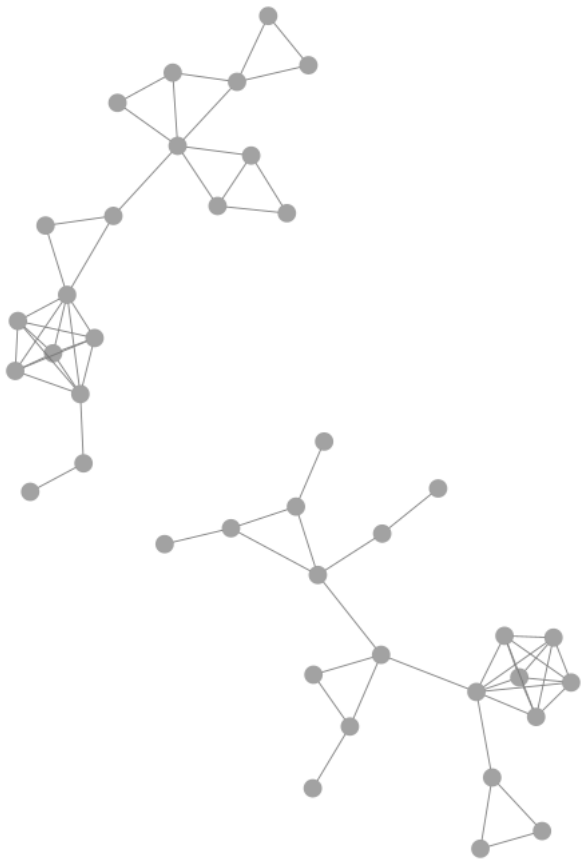
Figuur 14. Netwerk 2, de verdachten met de hoogste tussenliggende centraliteit waarden zijn aangeduid met de kleur geel en hun verbindingen zijn in het rood aangeduid



Figuur 15. Netwerk 2, de verdachten met de hoogste graad waarden aangeduid met de kleur geel en hun verbindingen zijn in het rood aangeduid



Figuur 16. Netwerk 2, de verdachten met een nabijheidcentraliteit waarde ≥ 0,262 en hoger zijn aangeduid met de kleur geel en hun verbindingen zijn in het rood aangeduid



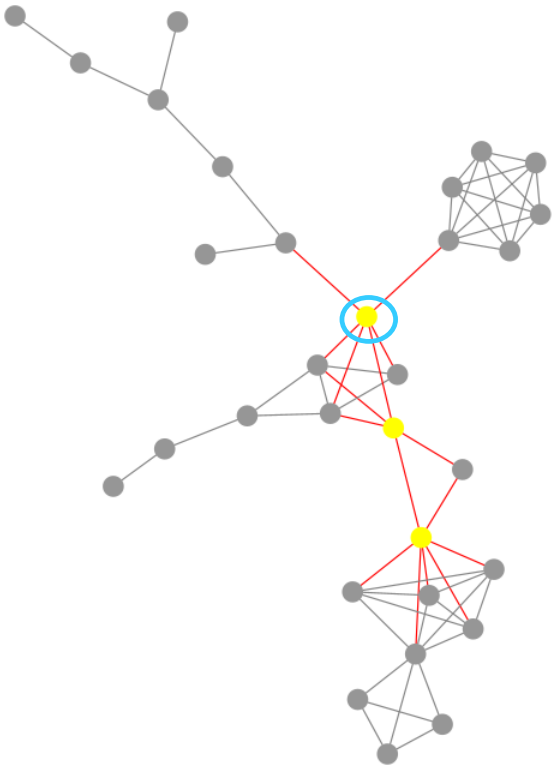
Figuur 17. Netwerk 2, na verwijdering van actor 100

Netwerk 3

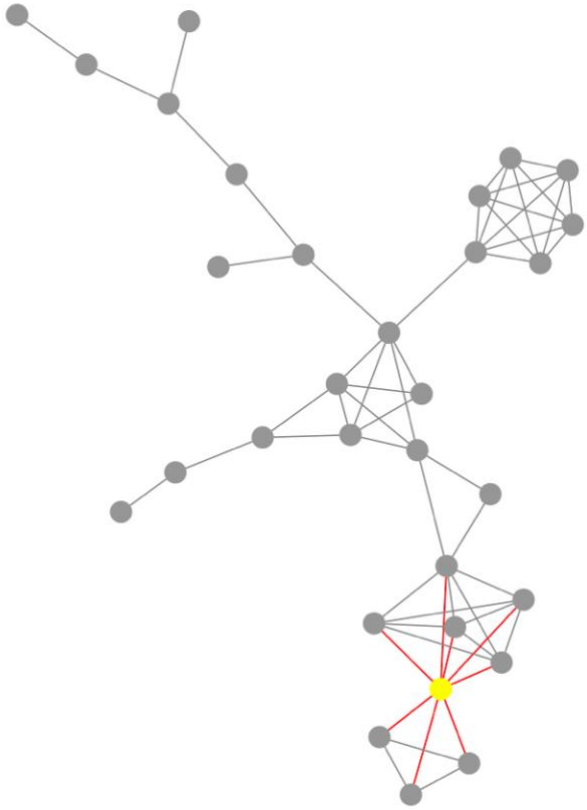
In netwerk 3 heeft actor 595 zowel de hoogste waarde op de nabijheidcentraliteit als op de tussenliggende centraliteit binnen het netwerk. Bovendien heeft deze actor een redelijk hoge graad van 6. Er kan worden gesteld dat actor 595 in termen van sociaal kapitaal de meest essentiële actor is in netwerk 3.

Ook binnen netwerk 3 lijken buitenlandse actoren niet essentieel te zijn in termen van sociaal kapitaal. Netwerk 3 heeft slechts één buitenlandse actor, actor 512, die gemiddelde scores heeft voor de graad en nabijheidcentraliteit. Daarnaast scoort deze actor 0 op de tussenliggende centraliteit.

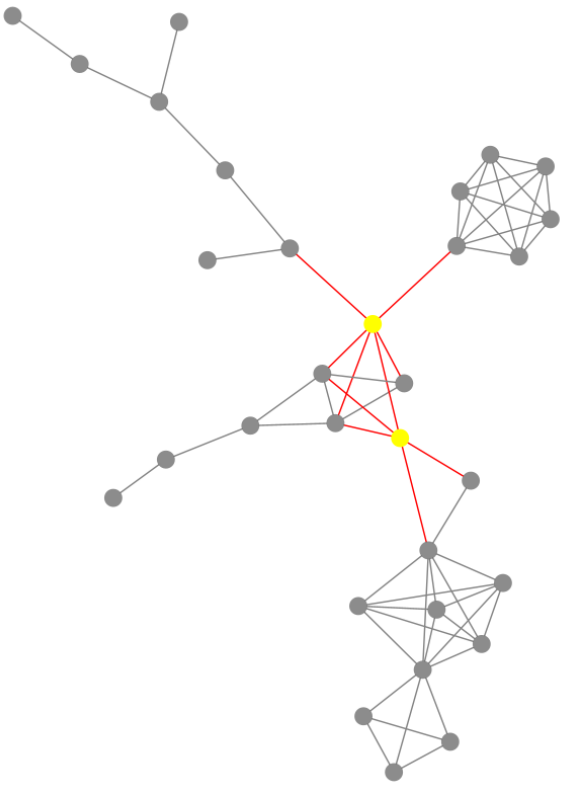
Tabel 6: centraliteitsmaten netwerk 3	**Rang**	**Actor**	**Score**
Graad	1	543	8
3 – 8	2	207	7
	3	595 en 646	6
	4	46, 129, 179, 186, 342, 436, 448, 512, 544, 653, 688 en 725	5
	5	111, 541, 568, 639, 701, 740 en 780	3
Nabijheidcentraliteit			
0,323 – 0,395	1	595	0,395
	2	725	0,375
	3	544 en 688	0,349
	4	207	0,326
	5	111	0,323
Tussenliggende centraliteit	1	595	0,613
0,287 – 0,613	2	725	0,460
	3	207	0,405
	4	111	0,343
	5	646	0,287



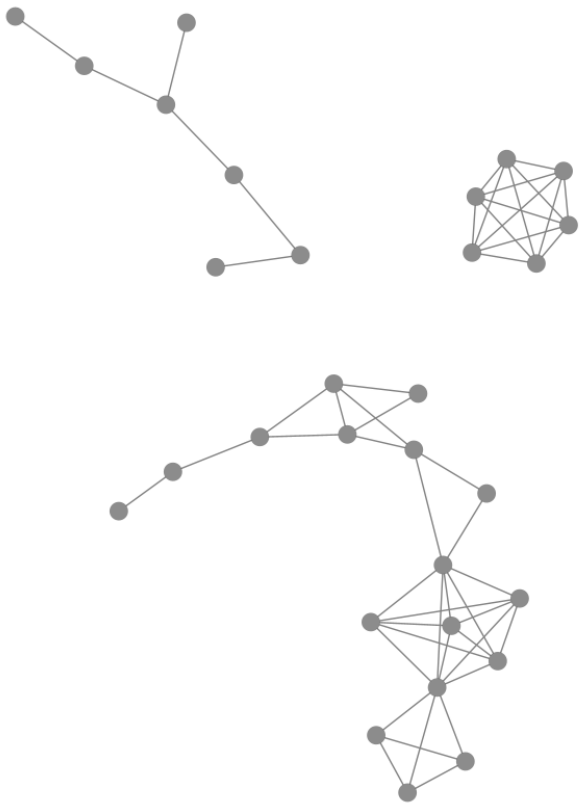
Figuur 18. Netwerk 3, de verdachten met de hoogste tussenliggende centraliteit waarden zijn aangeduid met de kleur geel en hun verbindingen zijn in het rood aangeduid. De meest essentiële actor in termen van sociaal kapitaal binnen netwerk 1 is blauw omcirkeld



Figuur 19. Netwerk 3, de verdachte met de hoogste graad waarde is aangeduid met de kleur geel en zijn verbindingen zijn in het rood aangeduid



Figuur 20. Netwerk 3, de verdachten met de hoogste nabijheidcentraliteit waarden zijn aangeduid met de kleur geel en hun verbindingen zijn in het rood aangeduid



Figuur 21. Netwerk 3, na verwijdering van actor 595

Analyse op basis van de rollen binnen het crimescript

Het kan waardevol zijn om netwerkanalyses te combineren met crimescripts om gerichte interventies binnen netwerken toe te passen op de leden die het moeilijkst te vervangen zijn (Bright et al., 2017; Duijn & Klerks, 2014; Morselli & Roy, 2008). In het crimescript van bankhelpdeskfraude spelen de kernleden een cruciale rol als voornaamste actoren. Daarnaast nemen de professionele dienstverleners een prominente positie in, gevolgd door de gerekruteerde dienstverleners en tot slot de geldezels (Leukfeldt, et al., 2017). Het is belangrijk hierbij op te merken dat niet elk netwerk van bankhelpdeskfraudeurs dezelfde rollen zal hebben zoals beschreven in het crimescript, aangezien netwerken en rollen vaak fluïde blijken te zijn. In veel netwerken komt het voor dat één persoon verschillende rollen vervult, bijvoorbeeld zowel de rol van pasjesophaler als pinner. Sommige kernleden zijn meer betrokken bij het gehele proces dan anderen. Zo werven sommigen bijvoorbeeld hun eigen geldezels, terwijl anderen dit uitbesteden. Het ontworpen crimescript kan dus worden gezien als een eerste voorbeeld in de literatuur van de rollen die over het algemeen voorkomen. Niettemin moeten de rollen van kernlid, dienstverleners en geldezel praktisch in elk netwerk aanwezig zijn.

Om de rollen te analyseren, is de rol van elke actor binnen netwerken 1, 2 en 3 onderzocht. Voor de actoren is gekeken welke rollen zij bekleden en welke kenmerken actoren met deze rollen hebben. Uit de analyse is gebleken dat sommige actoren verschillende rollen vervullen. Zo kunnen ze bijvoorbeeld zowel pasjesophaler als pinner zijn of hoofd ICT en pinner. Geldezels vervullen daarentegen uitsluitend de rol van geldezel en hebben geen andere rollen binnen het crimescript van bankhelpdeskfraude. Bijlage V bevat een overzicht van alle actoren met hun bijbehorende rol.

Binnen de netwerken zijn er relatief weinig kernleden te onderscheiden. Dit kan worden verklaard doordat kernleden vanwege hun "leidende" activiteiten minder zichtbaar zijn voor politie en justitie. De negen kernleden die geïdentificeerd kunnen worden, zijn allen man, hebben leeftijden rond de gemiddelde leeftijd van bankhelpdeskfraudeurs en hebben, op één kernlid na, een gemengd delictverleden.

Daarentegen is de rol van geldezel wel sterk vertegenwoordigd binnen de netwerken. Bijna de helft van de actoren binnen de netwerken vervult de rol van geldezel (48,1%). De geldezels die geïdentificeerd kunnen worden zijn zowel mannelijk als vrouwelijk, hebben doorgaans een leeftijd onder de gemiddelde leeftijd van bankhelpdeskfraudeurs en hebben veelal geen delictverleden.

Daarnaast kunnen zowel professionele als gerekruteerde dienstverleners worden onderscheiden. Met name de rollen 'pinner' en 'pasjesophaler' komen veel voor in de

onderzochte netwerken. Gerekruteerde dienstverleners worden vaak ingezet en zijn zichtbaar voor de politie door camerabeelden, getuigenverklaringen of aanhoudingen op heterdaad. De dienstverleners die geïdentificeerd kunnen worden zijn zowel mannelijk als vrouwelijk, hebben leeftijden rond de gemiddelde leeftijd van bankhelpdeskfraudeurs en hebben veelal een traditioneel delictverleden.

Lone wolves

Bij het analyseren van de rollen van de eenlingen valt op dat bijna alle eenlingen de rol van geldezel vervullen. In de dyades komt soms een andere rol naar voren, zoals gerekruteerde dienstverleners die pinnen of betaalpassen ophalen. Opvallend is dat de *lone wolves* met een gemengd delictverleden vaker de rol van dienstverlener bekleden. In Bijlage V is een volledige uitwerking te vinden van alle actoren met hun bijbehorende rollen.

Buitenlandse verdachten

Wanneer er wordt gekeken naar de buitenlandse verdachten, valt op dat alle acht buitenlandse verdachten binnen de netwerken 1, 2 en 3 de rol van geldezel bekleden. In veel gevallen wordt hun buitenlandse rekeningnummer gebruikt om geld weg te sluizen. In andere gevallen hebben de buitenlandse verdachten een Nederlands bankrekeningnummer op hun naam, waar het geld vervolgens naartoe wordt overgemaakt naar buitenlandse rekeningen. In verschillende zaken lijkt het spoor dood te lopen zodra er een buitenlands rekeningnummer of een buitenlands cryptocurrency adres in beeld komt. Een voorbeeld, zoals geciteerd uit proces verbaal: *"Wordt na hem doorgesluisd naar rekening uit land X. Om te investeren in de buitenlandse rekening en daarna de cryptocurrency te achterhalen, is m.i. kansloos, maar misschien is er iemand die dit als leerdoel graag wil doen."*

Bij het vergelijken van het geslacht, de leeftijd en het delictverleden van buitenlandse verdachten met Nederlandse verdachten, blijkt dat er geen significante verschillen zijn met betrekking tot deze drie factoren tussen buitenlandse verdachten en Nederlandse verdachten, $\chi^2(1, N = 796) = 0{,}235$, $p = {,}628$ voor geslacht, $t(673) = -1{,}536$; $p = {,}125$ voor leeftijd en $\chi^2(3, N = 802) = 4{,}892$, $p = {,}180$ voor delictverleden. Verder hebben zes van de acht buitenlandse actoren geen delictverleden, één actor heeft een traditioneel delictverleden en de andere actor heeft een digitaal delictverleden.

Sociaal en menselijk kapitaal

Wanneer er wordt gekeken naar een combinatie van sociaal en menselijk kapitaal, valt op dat in netwerk 1, waar actoren 242 en 755 de meest essentiële actoren waren in termen van sociaal kapitaal, deze actoren ook kunnen worden beschouwd in termen van menselijk kapitaal. In de menselijk-kapitaalbenadering wordt gekeken naar actoren die essentieel zijn voor het functioneren van het criminele proces, ook wel de criminele keten genoemd (Morselli & Roy, 2008). Actoren met veel menselijk kapitaal in de waardeketen van bankhelpdeskfraude kunnen bijvoorbeeld degenen zijn die verantwoordelijk zijn voor ICT en de bellers. Specifieke kennis en vaardigheden zijn vereist voor deze rollen. In netwerk 1 vervulde actor 242 de rol van professionele (technische) dienstverlener en verstrekte deze persoonsgegevens, terwijl actor 755 de rol van gerekruteerde dienstverlener had en betaalpassen ophaalde.

Een vergelijkbaar patroon doet zich voor in netwerk 3. Actor 595 is de meest essentiële actor in termen van sociaal kapitaal en vervult ook de rol van dienstverlener die betaalpassen ophaalt en geldezels rekruteert.

Netwerk 2 toont echter een enigszins ander beeld. In dit netwerk hebben actoren 233, 100 en 21 de hoogste gemiddelde centraliteitsmaten. Actoren 233 en 21 zijn geldezels, terwijl actor 100 de rol van gerekruteerde dienstverlener vervult en geld pint. Het lijkt erop dat geldezels dus een grotere rol spelen in termen van sociaal kapitaal dan verwacht wordt op basis van menselijk kapitaal.

Kernleden zijn daarentegen minder zichtbaar voor politie en justitie omdat ze minder verbindingen hebben met andere actoren in het netwerk. Ze hebben bijvoorbeeld vaker alleen direct contact met de beller, in plaats van met alle andere actoren binnen het netwerk. Hierdoor blijven kernleden buiten het zicht wanneer er wordt gekeken naar essentiële actoren in termen van sociaal kapitaal.

Schadebedragen

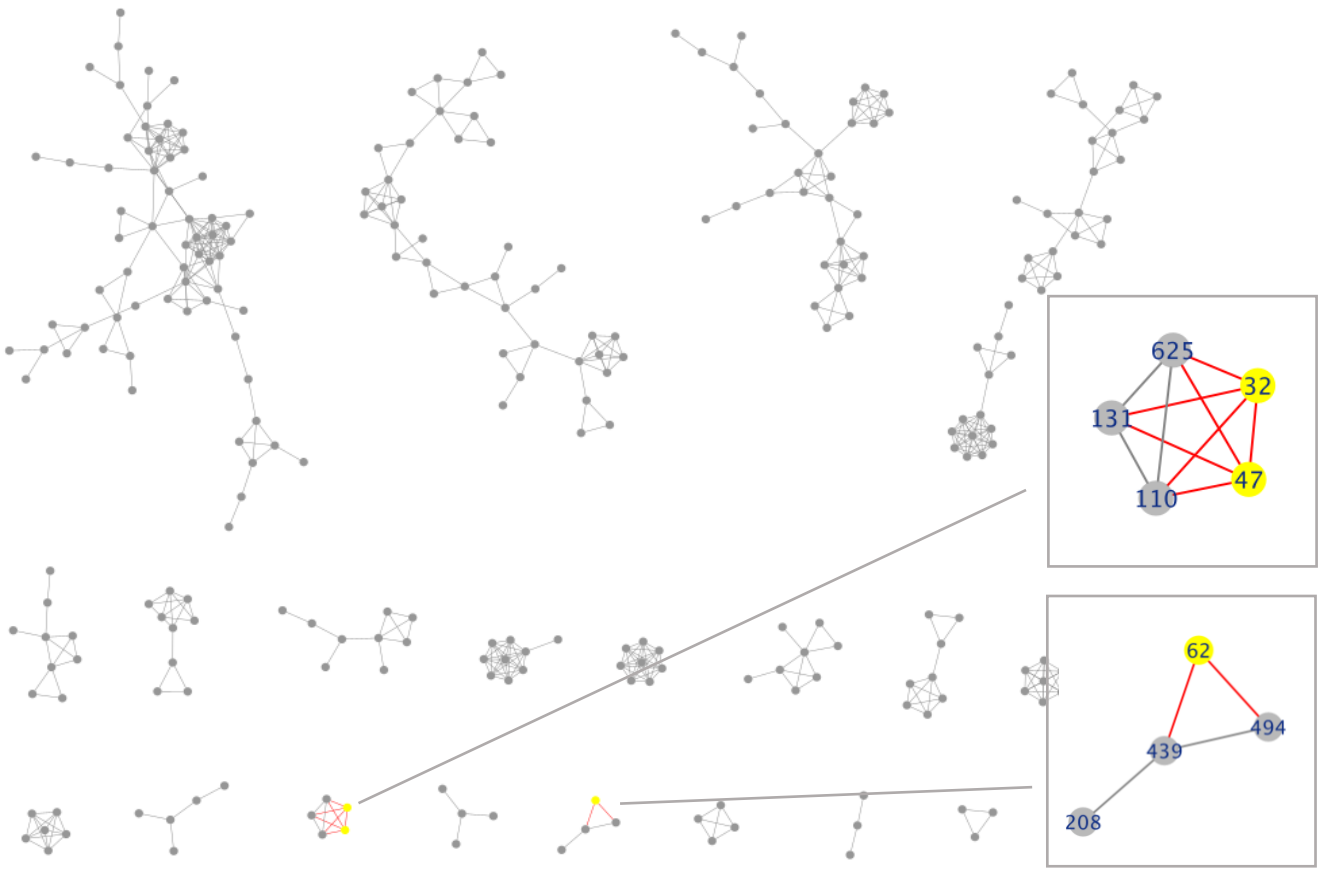
Uit de registraties van bankhelpdeskfraude blijkt dat er in totaal bijna elf miljoen euro is gefraudeerd in 2022. De drie grootste schadebedragen bedroegen elk bijna drie ton. Bij nader onderzoek van deze registraties valt op dat in twee van de drie gevallen de verantwoordelijke netwerken buitenlandse verdachten betroffen. Dit ondersteunt het vermoeden dat buitenlandse verdachten een belangrijke rol kunnen spelen bij het plegen van bankhelpdeskfraude. Hoewel buitenlandse verdachten slechts 10,9% uitmaken van de totale groep verdachten, zijn ze toch aanwezig in deze netwerken.

De betreffende buitenlandse actoren in het netwerk hebben de nummers 62, 47 en 32. Tabel 7 toont de centraliteitsmaten van deze actoren, terwijl Figuur 22 de betreffende actoren aanduidt met de kleur geel. Alle actoren binnen dit netwerk zijn direct met elkaar verbonden, waardoor de nabijheidcentraliteit-waarde voor iedereen 1 is. Bij nader onderzoek naar de rollen die deze actoren vervullen binnen het crimescript van bankhelpdeskfraude blijkt dat zij optreden als geldezels. Bovendien zijn zij allen slechts één keer verdachte geweest, enkel in de registratie waar zij allen als geldezel dienen, waardoor zij met iedereen in het netwerk een directe binding hebben. De kernleden en dienstverleners die mogelijk een rol spelen binnen het netwerk, komen niet terug in de politiesystemen en daarmee ook niet in het netwerk.

Wanneer er naar de schadebedragen per verdachte wordt gekeken, valt op dat actor 47 ruim €50.000 wegsluisde en actor 32 ‘verantwoordelijk’ was voor ruim €25.000. Het preieze geldbedrag dat actor 62 heeft kunnen wegsluizen is onbekend.

Tabel 7: centraliteitsmaten buitenlandse actoren 32, 47 en 62.

Actor	*Graad*	*Nabijheidcentraliteit*	*Tussenliggende centraliteit*
32	4	1,000	0
47	4	1,000	0
62	2	0,750	0



Figuur 22. Actoren 62, 47 en 32 binnen hun netwerk waarmee ze één van de grootste schadebedragen buitmaakten

5. Conclusie en discussie

In dit onderzoek is een exploratieve studie opgezet om meer inzicht te krijgen in criminele netwerken die actief zijn in bankhelpdeskfraude. Het onderzoek richtte zich op verschillende aspecten, waaronder het aandeel buitenlandse verdachten, de kenmerken van verdachten van bankhelpdeskfraude, de rollen binnen het crimescript van bankhelpdeskfraude, het verschil tussen *lone wolves* en verdachten in grotere netwerken, en de verdachten die essentieel zijn in termen van sociaal en menselijk kapitaal. Daarnaast is gekeken naar de schadebedragen van bankhelpdeskfraude en hoe deze kunnen bijdragen aan de identificatie van belangrijke spelers binnen het crimescript van bankhelpdeskfraude.

In deze paragraaf worden de conclusie en discussie behandeld, waarbij de belangrijkste bevindingen, sterke punten en beperkingen van dit onderzoek worden gepresenteerd. Daarnaast worden aanbevelingen voor toekomstig onderzoek en beleidsimplicaties besproken in relatie tot de sterke punten en beperkingen van het onderzoek.

Buitenlandse verdachten en kenmerken van bankhelpdeskfraudeurs

Het aandeel buitenlandse verdachten en het profiel van de *'gemiddelde bankhelpdeskfraudeur'* zijn onderzocht aan de hand van twee deelvragen. Ten eerste is geanalyseerd wat het aandeel is van buitenlandse verdachten bij bankhelpdeskfraude in Nederlands. Uit de registraties van bankhelpdeskfraude in 2022 blijkt dat 10,9% van de unieke verdachten buitenlands is. Het aandeel buitenlandse verdachten is daarmee relatief klein.

Daarnaast is het profiel van bankhelpdeskfraudeurs in Nederland onderzocht op basis van geslacht, leeftijd en delictverleden. De geslachtsverdeling en leeftijd van de verdachten komen overeen met de theorieën van zelfcontrole (Moffitt, Poulton & Caspi, 2013) en "*adolescence-limited and life-course-persistent antisocial behavior*" (Moffitt, 1993) uit eerdere studies. Volgens de zelfcontroletheorie hebben vrouwen significant meer zelfcontrole en vertonen ze tijdens de kindertijd minder antisociaal gedrag dan mannen. Individuen met een lage mate van zelfcontrole hebben een aanzienlijk hoger risico op crimineel gedrag dan individuen met een hoog niveau van zelfcontrole. Deze bevindingen worden ook weerspiegeld in de verdachten van bankhelpdeskfraude, waarbij mannen sterk oververtegenwoordigd zijn. Daarnaast ondersteunt de levenslooptheorie van Moffitt het fenomeen dat veel jongeren gedurende de adolescentie tijdelijk betrokken zijn bij crimineel gedrag, maar dit gedrag later ontgroeien (Moffitt, 1993). Deze bevindingen zijn ook van toepassing op bankhelpdeskfraude, waarbij jongvolwassenen vaker verdacht worden dan oudere personen. Verder blijkt uit de

statistieken dat de helft van de verdachten een traditioneel delictverleden heeft, terwijl een derde geen delictverleden heeft. Het hoge aantal verdachten met een traditioneel delictverleden sluit aan bij de genoemde theorie van de digitale drift, waarbij daders van bankhelpdeskfraude vaak een financieel motief hebben en daarom overstappen van traditionele criminaliteit naar gedigitaliseerde criminaliteit (Van der Wagen et al., 2019).

Netwerkanalyse

Het netwerkbeeld van bankhelpdeskfraude is onderzocht aan de hand van vijf deelvragen met betrekking tot essentiële actoren in termen van sociaal en menselijk kapitaal, kenmerken van *lone wolves* en rollen van buitenlandse verdachten. Het volledige netwerkbeeld van bankhelpdeskfraude in 2022 bestaat uit in totaal 802 personen, welke zijn geanalyseerd en in kaart zijn gebracht. Het netwerkbeeld bleek echter niet erg interessant voor analyse vanwege de relatief kleine omvang en clustering van de netwerken. Daarom is er vervolgens gekeken naar een uitgebreider netwerkbeeld van de verdachten, waarbij ook de connecties van registraties van bankhelpdeskfraude en andere delicten van 5 jaar vóór 2022 werden meegenomen. Binnen dit bredere beeld zijn er meer onderlinge verbindingen tussen de verdachten, resulterend in grotere netwerken. Desondanks zijn er nog steeds eenlingen en dyades aanwezig. Aangezien het interessant is om te onderzoeken in hoeverre deze *lone wolves* verschillen van verdachten in grotere netwerken, is hier vervolgens naar gekeken.

In totaal zijn er 130 *lone wolves* geïdentificeerd in het netwerk, waarvan 26 eenlingen en 52 dyades. Bij het vergelijken van het geslacht, de leeftijd en het delictverleden van *lone wolves* met andere actoren valt op dat er in verhouding meer vrouwelijke actoren zijn onder de *lone wolves* dan onder de actoren in grotere netwerken. Bovendien is de gemiddelde leeftijd van *lone wolves* ruim twee jaar hoger dan die van actoren in grotere netwerken. Daarnaast verschilt het delictverleden van *lone wolves* ten opzichte van dat van actoren in grotere netwerken. Het merendeel van de *lone wolves* heeft geen delictverleden, terwijl meer dan de helft van de actoren in grotere netwerken een traditioneel delictverleden heeft. De grote groep *lone wolves* zonder delictverleden bestaat bijna volledig uit geldezels die worden gerekruteerd voor hun bankrekeningen. Zij waren voorafgaand aan de bankhelpdeskfraude nog niet bekend bij de politie, maar komen direct in beeld doordat hun bankrekeningen worden gebruikt. Het bijbehorende netwerk van de geldezel blijft in dergelijke gevallen vaak buiten het zicht van politie en justitie, waardoor de *lone wolf* alleen in de politiesystemen wordt geregistreerd. Het valt verder op dat de *lone wolves* met een gemengd delictverleden vaak een rol als dienstverlener bekleden. Concluderend kan worden gesteld dat *lone wolves* zonder

delictverleden doorgaans geldezels representeren, *lone wolves* met een gemengd delictverleden voornamelijk dienstverleners zijn. *Lone wolves* met een traditioneel delictverleden laten verschillende rollen zien en zijn moeilijker te classificeren.

De buitenlandse verdachten binnen het netwerkbeeld van bankhelpdeskfraude in 2022 vervullen de rol van geldezel. In veel gevallen wordt hun buitenlandse rekeningnummer gebruikt om geld weg te sluizen, of hebben ze een Nederlands bankrekeningnummer op hun naam waarvandaan het geld naar buitenlandse rekeningen wordt overgemaakt. De opsporing van buitenlandse verdachten is vaak complex voor de politie vanwege veelal onbekende woonadressen en de vereiste samenwerking met andere (Europese) landen, wat aanzienlijke tijd kan vergen.

Wanneer de schadebedragen van de registraties in ogenschouw wordt genomen, valt op dat in twee van de drie registraties met de hoogste schadebedragen, de verantwoordelijke netwerken buitenlandse verdachten betreffen. Dit suggereert dat buitenlandse verdachten in staat zijn om grote hoeveelheden geld weg te sluizen en mogelijk een belangrijkere rol spelen dan aanvankelijk gedacht op basis van hun positie en rol in het netwerk. Aangezien buitenlandse verdachten moeilijker op te sporen zijn voor de Nederlandse politie, kunnen zij aantrekkelijke samenwerkingspartners vormen voor Nederlandse bankhelpdeskfraudeurs.

Sociaal en menselijk kapitaal

Na de analyse van essentiële actoren in termen van sociaal kapitaal blijkt dat specifieke actoren binnen de netwerken van bijzonder belang zijn. Deze actoren vertonen hoge waarden op de centraliteitsmaten, wat wijst op een hoog sociaal kapitaal. Ze nemen bruggenbouwer-posities in en spelen een centrale rol in het netwerk.

Actoren met aanzienlijk menselijk kapitaal spelen een essentiële rol in het uitvoeren van het crimescript. Ze zijn verantwoordelijk voor taken zoals het verstrekken van persoonsgegevens en het bellen van slachtoffers. Ze beschikken over specifieke kennis en vaardigheden die moeilijk te vervangen zijn. In sommige netwerken zijn deze actoren zichtbaar als dienstverleners, terwijl ze in andere netwerken juist de rol van geldezel op zich nemen. Het belang van deze actoren komt ook tot uiting in hun hoge sociaal kapitaal, dat werd gekenmerkt door hun vele verbindingen binnen het netwerk en hun frequente interactie met de politie als gevolg van hun criminele activiteiten.

Concluderend kan worden gesteld dat zowel de sociaal-kapitaalbenadering als de menselijk-kapitaalbenadering niet kunnen bepalen wie de kernleden zijn. De sociaal-kapitaalbenadering wijst vaak naar de dienstverleners, die zichtbaar zijn binnen het netwerk

vanwege hun vele verbindingen en frequente interactie met de politie. Hoewel het begrijpelijk is dat de politie de ambitie heeft zich voornamelijk te richten op de kernleden, aangezien zij degenen zijn die alles aansturen, is het ook waardevol om interventies te richten op de professionele dienstverleners, die veelal de hoogste centraliteitswaarden hebben en een essentiële rol spelen in het crimescript.

Vertaalslag naar de theorie

Wanneer er een vertaalslag naar de theorie wordt gemaakt, kan worden opgemerkt dat het concept '*low-tech'*-criminaliteit (Leukfeldt, et al., 2017) deels van toepassing is op bankhelpdeskfraude. Bij low-tech criminaliteit zijn de daders voornamelijk actief binnen de landsgrenzen en rekruteren ze anderen om bijvoorbeeld geld wit te wassen. Dit lijkt ook het geval te zijn bij bankhelpdeskfraude, waarbij in sommige gevallen echter ook geldezels uit andere landen worden gebruikt. Het lijkt erop dat er geen buitenlandse verdachten met technische vaardigheden worden gerekruteerd of zich op eigen initiatief aansluiten bij een Nederlands netwerk. De vereiste technische kennis voor het plegen van bankhelpdeskfraude lijkt voornamelijk binnenlands, vaak regionaal, te worden verworven.

Verder zijn er in de onderzochte data veel verdachten met een traditioneel of gemengd delictverleden. Dit kan worden verklaard vanuit de theorie dat traditionele daders ervoor kiezen zich te richten op gedigitaliseerde criminaliteit omdat dit lagere investeringskosten en een lagere pakkans biedt dan traditionele criminaliteit.

Sterke punten

Het eerste sterke punt van dit onderzoek zijn de nieuwe inzichten die zijn verkregen in netwerken van bankhelpdeskfraude. Er is nog niet eerder een volledig beeld van deze netwerken in Nederland in kaart gebracht en geanalyseerd. Bovendien zijn de verschillende rollen binnen het crimescript van bankhelpdeskfraude blootgelegd en vastgelegd. Crimescript analyse is een geschikte methode om criminaliteit te onderzoeken (Bright, Koskinen & Malm, 2019; Dehghanniri & Borrion, 2021; Duijn, Kashirin & Sloot, 2014). Tot op heden ontbrak echter een crimescript dat specifiek gericht is op bankhelpdeskfraude. Dit onderzoek, inclusief het ontworpen crimescript en de analyse van de rollen, draagt daarom bij aan het wetenschappelijk begrip van bankhelpdeskfraude. Dit onderzoek toont aan dat buitenlandse verdachten moeilijker op te sporen zijn voor de Nederlandse politie en in staat zijn zeer grote geldbedragen weg te sluizen, waardoor ze aantrekkelijke samenwerkingspartners kunnen vormen voor Nederlandse bankhelpdeskfraudeurs.

Het tweede sterke punt is dat dit onderzoek zich richt op verdachten die ingebed zijn in hun netwerk, waarbij niet alleen wordt gekeken naar hun delictverleden en de connecties op het gebied van bankhelpdeskfraude, maar ook breder. Veel bankhelpdeskfraudeurs hebben een traditioneel of gemengd delictverleden en hebben ook connecties in deze andere delicten. Veel criminele connecties ontstaan vaak uit contacten in het criminele circuit, bijvoorbeeld bij andere traditionele delicten. Dit onderzoek toont aan dat het waardevol kan zijn om deze connecties ook mee te nemen in de analyse. Een aanbeveling voor de politie en toekomstig onderzoek is om niet alleen naar verdachten binnen één specifiek jaar te kijken, maar om een breder tijdframe te hanteren. Zoals dit onderzoek heeft aangetoond, lijken er veel eenlingen te zijn, maar wanneer gegevens van meerdere jaren worden geanalyseerd, blijkt dat veel van hen toch verbindingen hebben met andere verdachten. Dit biedt waardevolle informatie voor opsporingsdoeleinden en voor het onderzoeken van de rol van de verdachten.

Het derde sterk punt van dit onderzoek is de beschikbaarheid van een grote hoeveelheid data binnen de politiesystemen. Voor dit onderzoek is uitsluitend gebruikgemaakt van data die valt onder Artikel 8 van de Wet Politiegegevens (WPG). Deze informatie is oorspronkelijk bedoeld voor de dagelijkse operationele taken van de politie (Overheid, 2022). Hoewel deze data een relatief laag veiligheidsniveau heeft, biedt het een aanzienlijke hoeveelheid informatie over verdachten en hun onderlinge netwerkrelaties.

Ten slotte is in dit onderzoek de sociaal- en menselijk-kapitaalbenadering gecombineerd om de meest essentiële actoren binnen de netwerken aan te wijzen. De eerste aanbeveling is gericht op het ontmantelen van deze netwerken door de actoren met het hoogste sociaal kapitaal uit het netwerk te verwijderen. Deze actoren bekleden allen belangrijke posities als bruggenbouwers in het netwerk en hebben gedurende meerdere jaren actief deelgenomen aan zowel online als traditionele criminaliteit.

Beperkingen

Eén van de beperkingen van dit onderzoek is het bestaan van het *dark number*, oftewel de niet-geregistreerde criminaliteit (Smit, et al., 2018). Aangezien de dataset enkel verdachten omvat die door de politie zijn opgepakt, is deze niet representatief. Het is bekend dat er (nog) niet-ontdekte verdachten zijn die buiten het zicht van de politie blijven en daardoor niet worden opgenomen in de data. Het is waarschijnlijk dat er een verschil bestaat tussen de verdachten die zichtbaar zijn en degenen die onzichtbaar blijven voor de politie. Bij het interpreteren van de sociale-netwerkanalyse is het belangrijk om rekening te houden met de beperking van het *dark*

number. Het ontbreken van bepaalde verdachten kan mogelijk leiden tot onjuiste conclusies over verbindingen en centraliteitsmaten.

Een tweede beperking van dit onderzoek is dat alle verdachten zonder Nederlandse nationaliteit en zonder Nederlands woonadres als buitenlands worden beschouwd. Er kan echter geen garantie worden gegeven dat deze personen zich niet illegaal in Nederland bevinden. In de politiesystemen worden dergelijke verdachten vaak geregistreerd zonder woonadres vanwege gebrek aan informatie. Hierdoor kan het voorkomen dat sommige verdachten ten onrechte als buitenlands worden beschouwd, terwijl ze mogelijk illegaal in Nederland verblijven en geen daadwerkelijke transnationale criminaliteit plegen. De bevindingen met betrekking tot buitenlandse verdachten moeten daarom met de nodige voorzichtigheid worden geïnterpreteerd.

Een derde beperking van dit onderzoek is dat de onderzochte data uitsluitend afkomstig zijn van registraties in Nederland, waardoor mogelijke criminele banden op internationaal niveau niet bekend zijn in de Nederlandse registraties (Europol, 2021). In veel gevallen waarbij buitenlandse verdachten betrokken waren, werd de zaak deels overgedragen aan het land van de verdachte en ontbrak verdere informatie in de Nederlandse politiesystemen. Om dergelijke verdachten gericht te onderzoeken, zou een rechtshulpverzoek in andere landen moeten worden ingediend, wat veel tijd in beslag kan nemen. Het gebruik van informatie uit internationale registraties kan mogelijk meer (inter)nationale verbindingen met andere actoren of netwerken aan het licht brengen, wat de netwerkstructuur aanzienlijk kan veranderen. Binnen het netwerk kunnen actoren die ogenschijnlijk aan de randen van het netwerk opereren, fungeren als verbindende schakels tussen verschillende gebieden, zoals bijvoorbeeld landen (Boivin, 2014). Toekomstig onderzoek zou zich dan ook moeten richten op het verkrijgen van gegevens uit politiesystemen van andere landen in Europa en mogelijk daarbuiten.

De buitenlandse actoren binnen deze studie tonen aan dat er mogelijkheden zijn om grote geldbedragen naar het buitenland weg te sluizen, en dat buitenlandse actoren lastiger op te sporen zijn vanwege hun woonplaats elders in de wereld. Uit verschillende proces-verbalen blijkt dat het onderzoek van de politie veelal vastloopt zodra er buitenlandse rekeningnummers of cryptocurrency-adressen opduiken. Dit brengt uitdagingen met zich mee bij het traceren van het geld en het achterhalen van de verantwoordelijke criminelen. Deze bevindingen benadrukken de noodzaak om de modus operandi van transnationale bankhelpdeskfraudeurs verder te onderzoeken, zodat rechtshandhavingsinstanties de middelen krijgen om deze vorm van cybercriminaliteit aan te pakken.

Een vierde mogelijke beperking betreft de gekozen centraliteitsmaten (graad, tussenliggende centraliteit en nabijheidcentraliteit) voor de netwerkanalyse. Deze maten zijn gekozen omdat ze centraal staan binnen de sociaal-kapitaalbenadering. Er zijn echter ook bronnen die aangeven dat deze centraliteitsmaten mogelijk eerder het perspectief van politieonderzoek dan de werkelijke verbindingen tussen de actoren blootleggen (Duijn, et al., 2014). In het geval van bankhelpdeskfraude zijn geldezels bijvoorbeeld zeer zichtbaar omdat het rekeningnummer vrijwel altijd bekend is na de fraude. Dit is duidelijk merkbaar in netwerk 2, waar twee van de drie actoren die het meest essentieel zijn in termen van sociaal kapitaal, niet het meest essentieel lijken te zijn in het netwerk.

Kernboodschap

Bankhelpdeskfraude is een groeiend maatschappelijk probleem met grote financiële schade tot gevolg. Dit onderzoek dient als een eerste stap om het wetenschappelijke veld inzicht te geven in de aard van deze vorm van fraude, de werking van netwerken van bankhelpdeskfraudeurs, de kenmerken van het crimescript en een algemeen beeld van de rollen en hun eigenschappen. Gezien de samenwerking tussen Nederlandse en buitenlandse verdachten vereist deze vorm van cybercriminaliteit een totaalaanpak waarbij de politie zich niet mag beperken tot nationale grenzen. De bevindingen in deze studie benadrukken de noodzaak van internationale samenwerking en een gecoördineerde aanpak om bankhelpdeskfraude effectief te bestrijden en de maatschappij te beschermen tegen deze toenemende bedreiging.

6. Literatuur

Armstrong, H. L., & Forde, P. J. (2003). Internet anonymity practices in computer crime. *Information management & computer security*, *11*(5), 209-215.

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

Boekhoorn, P. (2020). De aanpak van cybercrime door regionale eenheden van de politie.

Boivin, R. (2014). Macrosocial network analysis: The case of transnational drug trafficking. In Masys, A. (Eds.), *Networks and network analysis for defence and security*, (pp. 49-61). Springer, Cham. doi: 10.1007/978-3-319-04147-6_3

Borgatti, S. P., & Ofem, B. (2010). Social network theory and analysis. *Social network theory and educational change*, *17*, 29.

Borwell, J. (2020). Helpdeskfraude in Nederland. *Justitiële verkenningen*, *46*(2). https://doi.org/10.5553/JV/016758502020046002005

Bouchard, M., & Konarski, R. (2014). Assessing the core membership of a youth gang from its co-offending network. *Crime and networks*, 81-96.

Bright, D., Greenhill, C., Britz, T., Ritter, A., & Morselli, C. (2017). Criminal network vulnerabilities and adaptations. *Global Crime*, *18*(4), 424-441. doi:10.1080/17440572.2017.1377614

Bright, D., Koskinen, J., & Malm, A., (2019). Illicit network dynamics: The formation and evolution of a drug trafficking network. *Journal of Quantitative Criminology*, *35*(2), 237-258. doi:10.1007/s10940-018-9379-8

Centraal Bureau voor de Statistiek. (2022a). *Internettoegang en internetactiviteiten; persoonskenmerken.* Geraadpleegd op 7 april 2023, van https://www.cbs.nl/nl-nl/cijfers/detail/84888NED

Centraal Bureau voor de Statistiek. (2022b). *Hoeveel slachtoffers maakt online criminaliteit? - Nederland in cijfers 2022*. Hoeveel slachtoffers maakt online criminaliteit? - Nederland in cijfers 2022 | CBS. Geraadpleegd op 4 april 2023, van https://longreads.cbs.nl/nederland-in-cijfers-2022/hoeveel-slachtoffers-maakt-online-criminaliteit/

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

Chiu, Y.N., Leclerc, B., & Townsley, M. (2011). Crime script analysis of drug manufacturing in clandestine laboratories: Implications for prevention. The British Journal of Criminology, 51(2), 355-374. doi: 10.1093/bjc/azr005

Coleman, J. S. (1988). Social capital in the creation of human capital. American Journal of Sociology,94, S95-S120.

Coles, N. (2001). It's not what you know - it's who you know that counts: Analyzing serious crime groups as social networks. British Journal of Criminology, 41 (4), 580–594.

Cornish, D. B. (1994). Crimes as scripts. In *Proceedings of the international seminar on environmental criminology and crime analysis* (Volume 1, pp. 30-45). Tallahassee, Florida Criminal Justice Executive Institute.

Cuyper, R.H. de & G. Weijters (2016). Cybercrime in cijfers: Een verkenning van de mogelijkheden om cybercrime op te nemen in de Nationale Veiligheidsindices. Memorandum 2016-1. WODC, Den Haag.

Dehghanniri, H., & Borrion, H. (2021). Crime scripting: A systematic review. *European Journal of Criminology*, *18*(4), 504–525. doi:10.1177/1477370819850943

Duijn, P.A.C., Kashirin, V., & Sloot, P.M.A. (2014). The relative ineffectiveness of criminal network disruption. *Scientific reports, 4*, 4238. doi: 10.1038/srep04238

Duijn, P. A., & Klerks, P. P. (2014). Social network analysis applied to criminal networks: recent developments in Dutch law enforcement. *Networks and network analysis for defense and security*, 121-159. doi:10.1007/978-3-319-04147-6_6

Europol (2016). Internet organised crime threat assessment (IOCTA). Den Haag: European police office.

Europol (2021). European Union serious and organised crime threat assessment, A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime. Publications Office of the European Union, Luxembourg. Geraadpleegd op 20 juni 2023, van https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime- threat-assessment

Everett, M. G., & Borgatti, S. P. (2010). Induced, Endogenous and Exogenous Centrality. Social Networks, 32, 339-344. doi:10.1016/j.socnet.2010.06.004

Freeman, L. (2004). The development of social network analysis. *A Study in the Sociology of Science, 1*(687), 159-167.

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

Hatala, J. P. (2006). Social network analysis in human resource development: A new methodology. *Human Resource Development Review*, *5*(1), 45-71. doi: 10.1177/1534484305284318

Haythornthwaite, C. (1996). Social network analysis: An approach and technique for the study of information exchange. *Library & information science research*, *18*(4), 323-342.

Holt, T.J., & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20-40.

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

Inspectie Justitie en Veiligheid. (2021). Een kwetsbaar recht: Een onderzoek naar de toepassing van de Individuele Beoordeling van slachtoffers door de politie. In *https://www.rijksoverheid.nl/*. Ministerie van Justitie en Veiligheid. Geraadpleegd op 11 mei 2023, van https://open.overheid.nl/repository/ronl-0370d9bf-8bd6-4495-bd6a-eda505268f19/1/pdf/tk-bijlage-themaonderzoek-ib.pdf

Kadushin, C. (2012). *Understanding social networks. Theories, concepts and findings.* New York: Oxford University Press.

Killcoyne, S., Carter, G. W., Smith, J., & Boyle, J. (2009). Cytoscape: a community-based framework for network modeling. *Methods in molecular biology (Clifton, N.J.)*, *563*, 219–239. doi:10.1007/978-1-60761-175-2_12

Kramer, J. A., Blokland, A., & Soudijn, M. (2020). Witwassen als bedrijfsmatige activiteit: de verborgen netwerken van witwassers. *Tijdschrift voor Criminologie*, *62*(4), 365. doi: 10.5553/TvC/0165182X2020062004001

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122.

Laub, J. H., & Sampson, R. J. (1993). Turning points in the life course: Why change matters to the study of crime. *Criminology*, *31*(3), 301-325.

Lee, C.S. (2020). A crime script analysis of transnational identity fraud: migrant offenders' use of technology in South Korea. *Crime Law Social Change 74*, 201–218. doi:10.1007/s10611-020-09885-3

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

Leukfeldt, E. R. (2016). Cybercriminal networks Origin, growth and criminal capabilities.

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

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

Leukfeldt, E. R., Notté, R., & Malsch, M. (2018). *Slachtofferschap van online criminaliteit: Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit*. Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving. Geraadpleegd op 4 april 2023, van https://repository.wodc.nl/bitstream/handle/20.500.12832/2355/2839_Volledige_Tekst_tcm28-368216.pdf?sequence=1&isAllowed=y

Lupsha, P. A. (1983). Networks versus networking: analysis of an organized crime group. *Career criminals*, 59-87.

Lusthaus, J. (2012). Trust in the world of cybercrime. *Global crime*, *13*(2), 71-94.

Lusthaus, J. (2019). Beneath the dark web: Excavating the layers of cybercrime's underground economy. *Institute of Electrical and Electronics Engineers, European symposium on security and privacy workshops*, 474-480. doi: 10.1109/EuroSPW.2019.00059

Mesch, G. S. (2012). Technology and youth. *New directions for youth development, 2012*(135), 97-105.

Morselli, C., & Roy, J. (2008). Brokerage qualifications in ringing operations. *Criminology, 46*(1), 71- 98. doi: 10.1111/j.1745-9125.2008.00103.x

Ministerie van Justitie en Veiligheid. (2022, 10 oktober). Kabinet presenteert nieuwe cybersecuritystrategie. Nieuwsbericht | Rijksoverheid.nl. Geraadpleegd op 24 maart 2023, van https://www.rijksoverheid.nl/actueel/nieuws/2022/10/10/kabinet-presenteert-nieuwe-cybersecuritystrategie

Moffitt, T.E. (1993). Adolescence-Limited and Life-Course-Persistent Antisocial Behavior: A Developmental Taxonomy. *Psychological Review, 100(4),* 674 – 701. doi: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 adult quality of life. *American Scientist, 101*, 352-359.

Nederlandse Vereniging van Banken. (2023, 30 maart). *Schade door fraude in 2022 bijna 61 miljoen euro: deel nooit je bankgegevens. - Veilig Bankieren*. Veilig Bankieren. Geraadpleegd op 4 april 2023, van https://www.veiligbankieren.nl/actueel/schade-door-fraude-in-2022-bijna-61-miljoen-euro-deel-nooit-je-bankgegevens/

NOS. (2023, 31 maart). Acht mensen opgepakt in groot onderzoek bankhelpdeskfraude. *NOS.nl*. Geraadpleegd op 11 mei 2023, van https://nos.nl/artikel/2469584-acht-mensen-opgepakt-in-groot-onderzoek-bankhelpdeskfraude

Odinot, G., Poot, C. D., Verhoeven, M., Kruisbergen, E., Leukfeldt, R., Kleemans, E., Rok, R., van der Bruggen, M., van der Wagen, W., Bernaards, F., Verburgh, T., Smits, E., van Wegberg, R. Oerlemans, J. J., & Custers, B. (2018). De digitalisering van georganiseerde misdaad. Den Haag: WODC

Oerlemans, J.J., Custers, B.H.M., Pool, R.L.D., & Cornelisse, R. (2016). Cybercrime en witwassen: Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware. Den Haag: WODC

Peters, R. J. (2021). *Veiliger offline dan online?* [Masterscriptie]. Vrije Universiteit Amsterdam. Geraadpleegd op 10 maart 2023 van https://cybersciencecenter.nl/media/1284/masterthesis-rj-peters.pdf

Politie. (2015). Cybercrime. Geraadpleegd op 8 maart 2023, van https://www.politie.nl/themas/cybercrime.html

Politie. (2022, 24 november). Grote spoofingdienst uit de lucht gehaald door internationale samenwerking. *politie.nl*. Geraadpleegd op 8 maart 2023, van https://www.politie.nl/nieuws/2022/november/23/03-grote-spoofingdienst-uit-de-lucht-gehaald-door-internationale-samenwerking.html

Politie. (2023). *Impact en schade cybercrime onverminderd groot*. politie.nl. Geraadpleegd op 2 april 2023, van https://www.politie.nl/nieuws/2023/januari/19/politie-registreert-minder-cybercrime.html

Ruiter, S., & Bernaards, F. (2013). Verschillen crackers van andere criminelen? Een vergelijking op basis van Nederlandse verdachtenregistraties. *Tijdschrift voor Criminologie, 55*(4), 342-359.

Schiks, J., van ’t Hoff - de Goede, S., & Leukfeldt, R. (2022). *Op zoek naar de parels bij de lokale aanpak van cybercriminaliteit en gedigitaliseerde criminaliteit: Een*

verkennend onderzoek. De Haagse Hogeschool, Centre of Expertise Cybersecurity, lectoraat Cybercrime and Cybersecurity, Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving (NSCR). Geraadpleegd op 8 maart 2023, van https://securitydelta.nl/media/com_hsd/report/535/document/cyberparels-rapport-vk89.pdf

Schwartz, D. M., & Rouselle, T. (2009). Using social network analysis to target criminal networks. *Trends in Organized Crime*, *12*(2), 188-207.

Sintenie, M. (2019, 4 november). *Een lesje Smibanese: 'Je bent niet gaande'*. parool.nl. Geraadpleegd op 15 juni 2023, van https://www.parool.nl/amsterdam/een-lesje-smibanese-je-bent-niet-gaande~bf93b668/

Smit, P. R., Ghauharali, R., van der Veen, H. C. J., Willemsen, F., Steur, J., te Velde, R. A., van der Vorst, T., Bongers F., Kabki A., & Zaitch, D. (2018). *Tasten in het duister*. Wetenschappelijk Onderzoek- en Documentatiecentrum. Geraadpleegd op 18 juni 2023, van http://hdl.handle.net/20.500.12832/217https://download.cbs.nl/pdf/cahier-2016-1-monitor-jeugdcriminaliteit.pdf

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

Sparrow, M. K. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. *Social networks*, *13*(3), 251-274.

Speer, D.L. (2000). Redefining borders: The challenges of cybercrime. *Crime, Law and Social Change 34*, 259–273. doi:10.1023/A:1008332132218

Straver, M. A., Meesters, P. M. A., & van Duijneveldt, I. M. (2010). Informatiegestuurde politie van en met blauw: Het Frontoffice/Backoffice-concept in politieregio Hollands Midden. In *politieacademie.nl*. Politieacademie. Geraadpleegd op 8 mei 2023, van https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/79352.pdf

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & behavior*, *7*(3), 321-326.

Tabassum, S., Pereira, F. S., Fernandes, S., & Gama, J. (2018). Social network analysis: An overview. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *8*(5), e1256. doi:10.1002/widm.1256

Teng, K. (2019). Unmasking the Villain: Exposing Scammers' Identities to Defeat Harmful Calls. *Brook. J. Corporate Finance & Commercial Law*, *14*, 367.

United Nations Office on Drugs and Crime. (2013). *Comprehensive Study on Cybercrime. Draft 2013.* New York: United Nations.

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

Van der Hulst, R. C. (2008). Sociale-netwerkanalyse en de bestrijding van criminaliteit en terrorisme. *Justitiële verkenningen, 6*(5), 1.

Van der Laan, A. M., & Goudriaan, H. (2016). *Monitor Jeugdcriminaliteit*. Wetenschappelijk Onderzoek- en Documentatiecentrum. Geraadpleegd op 3 april 2023, van https://download.cbs.nl/pdf/cahier-2016-1-monitor-jeugdcriminaliteit.pdf

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

Van Hardeveld, G. J., Webber, C., & O'Hara, K. (2017). Deviating From the Cybercriminal Script: Exploring Tools of Anonymity (Mis)Used by Carders on Cryptomarkets. *American Behavioral Scientist, 61*(11), 1244-1266. doi10.1177/0002764217734271

Van Nguyen, T. (2022) The modus operandi of transnational computer fraud: a crime script analysis in Vietnam. *Trends Organized Crime 25*, 226–247. doi:10.1007/s12117-021-09422-1

Verhagen, L., & Sabel, P. (2021, 20 mei). Waarom al die datalekken ons toch echt zorgen moeten baren en wat ertegen te doen is. *www.volkskrant.nl*. Geraadpleegd op 3 mei 2023, van https://www.volkskrant.nl/wetenschap/waarom-al-die-data-lekken-ons-toch-echt-zorgen-moeten-baren-en-wat-ertegen-te-doen-is~beeebcba/?referrer=https%3A%2F%2Fwww.google.com%2F

Overheid. (2022). *Wet politiegegevens.* Geraadpleegd op 8 mei 2023, van https://wetten.overheid.nl/BWBR0022463/2022-10-01

Watts, D. J., & Strogatz, S. H. (1998). Collective dynamics of 'small-world' networks. *Nature, 393*(6684), 440-442. doi:10.1038/30918

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.

Xu, J., & Chen, H. (2003). Untangling criminal networks: A case study. In *Intelligence and Security Informatics: First NSF/NIJ Symposium, ISI 2003, Tucson, AZ, USA, Proceedings 1*, 232-248. doi:10.1007/3-540-44853-5_18

Bijlagen

Bijlage I

De gekoppelde verdachten per registratie van bankhelpdeskfraude zijn opgehaald uit alle BHF-registraties van 2022 uit de Landelijke Cybercrime Query. Hiervoor is de volgende code gebruikt:

```
library(dplyr)
library(readxl)
library(WriteXLS)

# dataset BI zonder personen
bhf <- read_excel('/home/jovyan/data/cct/studenten/Jitske/BHF.xlsx')

# lijst voorvallen
voorvallen <- bhf %>% distinct(identificatie) %>% .$identificatie

# connectie Blueintel/Cybersubset DMIB
bi <- pool::dbPool(drv = RPostgreSQL::PostgreSQL(),
                   dbname = '<dbname>',
                   host = '<host>,
                   port = '5432',
                   user = '<usr>',
                   password = '<pwd>')

# functie voor tabellen lezen
get_table <- function(table_name){
  bi %>%
    tbl(table_name)
}
```

```
# joins voor de juiste dataset
df <- get_table('dmib_voorval') %>%
  filter(VOORVAL %in% voorvallen) %>%
  select(ID, VOORVAL, OMSCHRIJVING = SRT_OMSCHR) %>%
  left_join(get_table('dmib_hoedanigheid'), by=c('ID'='VOORVAL_ID')) %>%
  select(VOORVAL, OMSCHRIJVING, HOEDANIGHEID=SRT_OMSCHR,
NAT_PERS_ID) %>%
  left_join(get_table('dmib_nat_pers'), by = c('NAT_PERS_ID'='ID')) %>%
  filter(!is.na(KENO_SL_UITGEBREID) & HOEDANIGHEID ==
'VERDACHTE') %>%
  collect()

# registraties koppelen aan df
df <- bhf %>%
  select(registratie, VOORVAL=identificatie) %>%
  inner_join(df) %>%
  distinct()

# wegschrijven
WriteXLS(df, '/home/jovyan/data/cct/studenten/Jitske/bhf_verdachten.xlsx')
```

UNIEKE VERDACHTEN

De data omvat 1050 voorvallen binnen 715 registraties van bankhelpdeskfraude. Enkele verdachten komen vaker dan eenmaal in de dataset voor omdat zij meermaals verdachte zijn van bankhelpdeskfraude in 2022. Omdat sommige verdachten meermaals voorkomen in de dataset, is de onderstaande syntax uitgevoerd om een dateset van unieke verdachten te verkrijgen. Het aantal unieke verdachten van bankhelpdeskfraude is 824. Er zijn 22 verdachten in de data waarvan geen gegevens bekend zijn. Het is onduidelijk waarom er van deze verdachten geen gegevens bekend zijn. De betreffende verdachten worden niet meegenomen in de analyses, waardoor de uiteindelijke dataset 802 verdachten telt (97.3%).

Zie *Lanser_SPSS_file _unieke_verdachten.sav*

```
SYNTAX
*Identify Duplicate Cases.
SORT CASES BY KENO_SL_UITGEBREID(A).
MATCH FILES
  /FILE=*
  /BY KENO_SL_UITGEBREID
  /FIRST=PrimaryFirst
  /LAST=PrimaryLast.
DO IF (PrimaryFirst).
COMPUTE  MatchSequence=1-PrimaryLast.
ELSE.
COMPUTE  MatchSequence=MatchSequence+1.
END IF.
LEAVE  MatchSequence.
FORMATS  MatchSequence (f7).
COMPUTE  InDupGrp=MatchSequence>0.
SORT CASES InDupGrp(D).
MATCH FILES
  /FILE=*
  /DROP=PrimaryFirst InDupGrp MatchSequence.
VARIABLE LABELS  PrimaryLast 'Indicator of each last matching case as Primary'.
VALUE LABELS  PrimaryLast 0 'Duplicate Case' 1 'Primary Case'.
VARIABLE LEVEL  PrimaryLast (ORDINAL).
FREQUENCIES VARIABLES=PrimaryLast.
EXECUTE.
```

AANDEEL BUITENLANDSE VERDACHTEN

Om het aandeel buitenlandse verdachten binnen de registraties van bankhelpdeskfraude in 2022 te berekenen, is om te beginnen de variabele GEBOORTE_LAND gehercodeerd in de dichotome variabele afkomst_binair. Hiervoor is de volgende syntax gebruikt:

```
SYNTAX
RECODE GEBOORTE_LAND ('ONBEKEND'=SYSMIS) ('NEDERLAND'=0) (ELSE=1)
INTO afkomst_binair.
VARIABLE LABELS  afkomst_binair 'Afkomst'.
EXECUTE.

FREQUENCIES VARIABLES=afkomst_binair
  /ORDER=ANALYSIS.
```

Aangezien deze variabele enkel het geboorteland van de verdachte weergeeft en niet de huidige woonsituatie, is er handmatig gekeken naar de huidige woonsituatie binnen de verdachten met een buitenlands geboorteland. Dit, omdat deze niet in de data van de verdachten terugkwam. Indien een verdachte geen woonadres/leefadres had in Nederland, is deze aangeduid met een 1. Alle andere verdachten kregen de waarde 0. Vervolgens is er een frequentietabel uitgedraaid om het aandeel buitenlandse en Nederlandse verdachten in het bankhelpdeskfraude beeld te bepalen. Dit is zowel uitgevoerd voor de dataset met het

volledige beeld van de registraties van bankhelpdeskfraude als voor de dataset van de unieke verdachten van bankhelpdeskfraude.

Zie *Lanser_SPSS_file _unieke_verdachten.sav*

Statistics

Afkomst

N	Valid	1013
	Missing	15

Afkomst

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	,00	925	90,0	91,3	91,3
	1,00	88	8,6	8,7	100,0
	Total	1013	98,5	100,0	
Missing	System	15	1,5		
Total		1028	100,0		

Statistics

Afkomst

N	Valid	788
	Missing	14

Afkomst

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	,00	702	87,5	89,1	89,1
	1,00	86	10,7	10,9	100,0
	Total	788	98,3	100,0	
Missing	System	14	1,7		
Total		802	100,0		

GESLACHT

Om de verdeling van het geslacht van de verdachten weer te geven, is de variabele geslacht gecodeerd als een dichotome variabele met de categorieën 'man' en 'vrouw'. Met de volgende syntax is het aantal en het percentage mannelijke en vrouwelijke verdachten van bankhelpdeskfraude berekend.

Zie *Lanser_SPSS_file _unieke_verdachten.sav*

SYNTAX
```
*Frequentietabel geslacht
RECODE GESLACHT ('Man'=0) ('Vro'=1) INTO Geslacht_code.
VARIABLE LABELS  Geslacht_code 'Geslacht'.
EXECUTE.

FREQUENCIES VARIABLES=Geslacht_code
  /STATISTICS=STDDEV MINIMUM MAXIMUM MEAN MEDIAN
  /ORDER=ANALYSIS.
```

Geslacht

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	,00	643	80,2	80,8	80,8
	1,00	153	19,1	19,2	100,0
	Total	796	99,3	100,0	
Missing	System	6	,7		
Total		802	100,0		

LEEFTIJD

Leeftijd is een continue variabele waarvan het gemiddelde, het minimum, de maximum en de standaarddeviatie is berekend. Om de variabele leeftijd te creëren, is de volgende syntax gebruikt. Hiervoor is de geboortedatum en de datum van het delict gebruikt, om de leeftijd van de verdachte ten tijde van het delict te berekenen.

Zie *Lanser_SPSS_file _unieke_verdachten.sav*

SYNTAX
```
* Date and Time Wizard: Leeftijd.
COMPUTE  Leeftijd=DATEDIF(begin_datum_incident, GEBOORTE_DAT,
"years").
VARIABLE LABELS  Leeftijd "Leeftijd_verdachten".
VARIABLE LEVEL  Leeftijd (SCALE).
FORMATS  Leeftijd (F5.0).
VARIABLE WIDTH  Leeftijd(5).
EXECUTE.
```

SYNTAX
```
DESCRIPTIVES VARIABLES=Leeftijd
  /STATISTICS=MEAN STDDEV MIN MAX.
```

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Leeftijd_verdachten	676	13	74	28,29	11,110
Valid N (listwise)	676				

Om de gemiddelde leeftijd voor mannen en vrouwen afzonderlijk te berekenen, is de volgende syntax gebruikt.

Mannen

```
SYNTAX
USE ALL.
COMPUTE filter_$=(Geslacht_code = 0).
VARIABLE LABELS filter_$ 'Geslacht_code = 0 (FILTER)'.
VALUE LABELS filter_$ 0 'Not Selected' 1 'Selected'.
FORMATS filter_$ (f1.0).
FILTER BY filter_$.
EXECUTE.

DESCRIPTIVES VARIABLES=Leeftijd
  /STATISTICS=MEAN STDDEV MIN MAX.
```

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Leeftijd_verdachten	538	13	72	28,37	11,074
Valid N (listwise)	538				

Vrouwen

```
SYNTAX
FILTER OFF.
USE ALL.
EXECUTE.

USE ALL.
COMPUTE filter_$=(Geslacht_code = 1).
VARIABLE LABELS filter_$ 'Geslacht_code = 1 (FILTER)'.
VALUE LABELS filter_$ 0 'Not Selected' 1 'Selected'.
FORMATS filter_$ (f1.0).
FILTER BY filter_$.
EXECUTE.

DESCRIPTIVES VARIABLES=Leeftijd
  /STATISTICS=MEAN STDDEV MIN MAX.
```

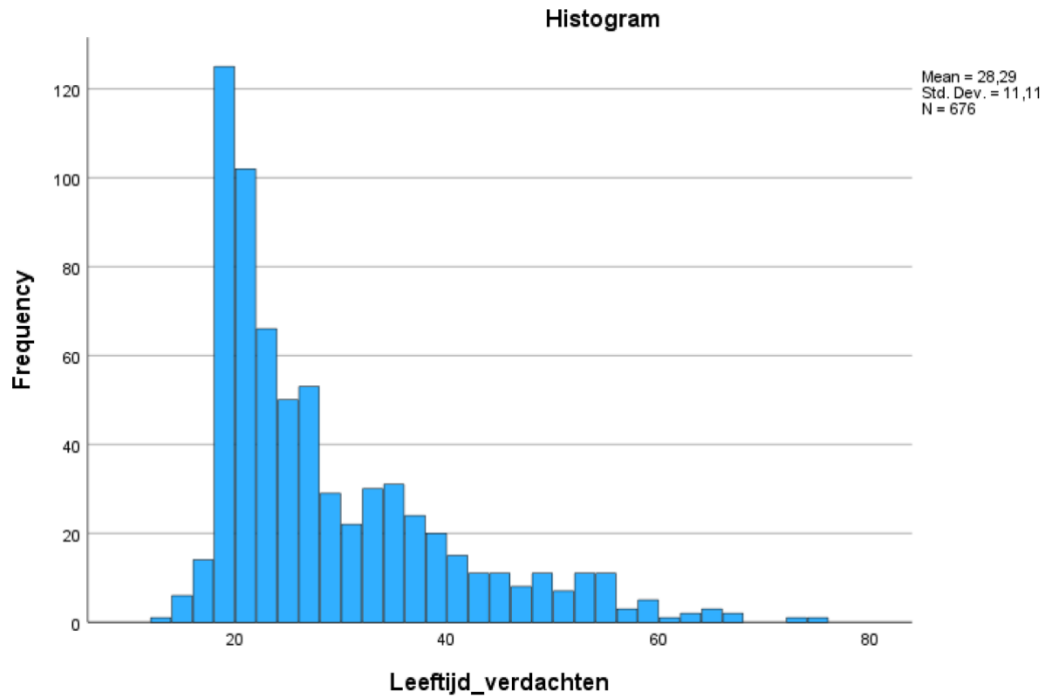
Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Leeftijd_verdachten	133	15	74	28,07	11,443
Valid N (listwise)	133				

Histogram

Om een visueel beeld te schetsen van de verdeling van leeftijd is de volgende syntax gebruikt om een histogram te creëren.

```
SYNTAX
FREQUENCIES VARIABLES=Leeftijd
  /STATISTICS=MEAN
  /HISTOGRAM
  /ORDER=ANALYSIS.
```



DELICTVERLEDEN

Het delictverleden van de verdachten bankhelpdeskfraude is terug te vinden in dataset: *Lanser_SPSS_file _unieke_verdachten.sav*

Het delictverleden van de 802 verdachten van bankhelpdeskfraude is geclassificeerd. Het BSN-nummer van elke persoon is gebruikt om het delictverleden op te vragen in de Bluespot Monitor. Bij het invoeren van het BSN-nummer worden alle persoonlijke gegevens van de persoon weergegeven, evenals alle incidenten, meldingen, activiteiten en antecedenten die aan die persoon zijn gekoppeld. Het onderzoek richtte zich op alle delicten waarvan de verdachten werden verdacht vóór de bankhelpdeskfraude waarvoor ze in de dataset worden vermeld. Op basis hiervan zijn lijsten opgesteld van verdachten die zowel vóór 2022 als in 2022 betrokken waren bij een cyberdelict, evenals een lijst van verdachten die vóór 2022 of voor hun bankhelpdeskfraude betrokken waren bij een traditioneel delict. Deze lijsten zijn met elkaar vergeleken, waarbij actoren die in beide lijsten voorkwamen werden geclassificeerd als verdachten met een gemengd delictverleden. Verdachten die alleen in de lijst van cyberdelicten voorkwamen, werden geclassificeerd als verdachten met een digitaal delictverleden. Verdachten die alleen in de lijst van traditionele delicten voorkwamen, werden geclassificeerd als verdachten met een traditioneel delictverleden. Ten slotte werden verdachten die in geen van beide lijsten voorkwamen, geclassificeerd als verdachten zonder delictverleden.

Hieruit zijn de volgende categorieën voortgekomen:

0 = geen delictverleden, wat betekent dat de persoon niet eerder als verdachte van een delict geregistreerd staat. Dit betekent niet noodzakelijkerwijs dat de persoon niet bekend is bij de politie. Het merendeel van de personen in de data zonder delictverleden is al wel eerder in contact geweest met de politie, bijvoorbeeld als slachtoffer of getuige van een ander delict, of voor een overtreding zoals een verkeersongeval of geluidsoverlast waarvoor een waarschuwing is gegeven. Een klein aantal personen in deze categorie is niet eerder bekend geweest bij de politie voordat ze het delict pleegden.

1 = traditioneel delictverleden, wat betekent dat de persoon eerder verdachte is geweest van één of meerdere traditionele delict(en).

2 = digitaal delictverleden, wat betekent dat de persoon eerder verdachte is geweest van één of meerdere bankhelpdeskfraude zaken.

3 = mengvorm, wat betekent dat de persoon eerder verdachte is geweest van meerdere delicten die zowel bankhelpdeskfraude als een vorm van traditionele criminaliteit inhielden. Deze persoon wordt daarom geclassificeerd als een verdachte met een gemengd delictverleden.

In de onderstaande tabel worden de codes en maatschappelijke klassen weergegeven voor bankhelpdeskfraude en traditionele criminaliteit. Deze codes en klassen zijn afkomstig uit de Landelijk Query Cybercrime. Deze query is ontwikkeld om aangiften en incidenten op een correcte manier te classificeren en om misinterpretatie en verkeerde classificatie te voorkomen.

Type criminaliteit	Code	Maatschappelijke Klasse
Bankhelpdeskfraude	F90	Cybercrime
	A95	Overig gekwalificeerde diefstal
	F614	Fraude met betaalproducten
	F620	Overige horizontale fraude
	F636	Fraude met online handel
	F94	Witwassen
	F649	Overige verticale fraude
Traditionele criminaliteit	A10	Diefstal uit/vanaf personenauto
	A11	Diefstal uit/vanaf vaartuig
	A12	Diefstal uit/vanaf andere vervoermiddelen
	A20	Gekwal. Diefstal in/uit woning
	A21	Gekwal. Diefstal in/uit box/garage/schuur
	A22	Gekwal. Diefstal in/uit winkel
	A23	Gekwal. Diefstal in/uit bedrijf/kantoor
	A25	Gekwal. Diefstal in/uit hotel/pension
	A26	Gekwal. Diefstal in/uit school
	A27	Gekwal. Diefstal in/uit andere gebouwen
	A30	Diefstal in/uit woning (niet gekwal.)
	A32	Diefstal in/uit bedrijf/kantoor (niet gekwal.)
	A34	Diefstal in/uit box/garage/schuur/erf (niet gekwal.)
	A36	Diefstal in/uit andere gebouwen (niet gekwal.)
	A40	Zakkenrollerij/tassenrollerij
	A50	Winkeldiefstal
	A70	Diefstal personenauto
	A71	Diefstal motor
	A72	Diefstal fiets
	A73	Diefstal bromfiets/snorfiets
	A74	Diefstal ander vervoersmiddel
	A76	Diefstal vrachtauto/bestelauto
	A80	Verduistering (evt. in dienstbetrekking)
	A81	Heling
	A82	Chantage/afpersing
	A90	Overige (eenvoudige) diefstal
	B10	Diefstal met geweld uit/vanaf personenauto
	B20	Gekwal. Diefstal met geweld in/uit woning
	B22	Gekwal. Diefstal met geweld in/uit winkel
	B25	Gekwal. Diefstal met geweld in/uit hotel/pension
	B27	Gekwal. Diefstal met geweld in/uit andere gebouwen
	B32	Diefstal met geweld in/uit bedrijf/kantoor (niet gekwal.)
	B33	Diefstal met geweld in/uit hotel/pension (niet gekwal.)
	B34	Diefstal met geweld in/uit box/garage//schuur (niet gekwal.)
	B50	Winkeldiefstal met geweld
	B62	Diefstal met geweld fiets
	B63	Diefstal met geweld bromfiets/snorfiets
	B70	Straatroof
	B72	Overval in woning
	B73	Overval op overige objecten
	B74	Overval op geld- en waardetransport
	B95	Overige diefstallen met geweld
	C10	Vernieling van/aan auto
	C30	Vernieling van/aan openbaar gebouw
	C40	Vernieling overige objecten
	C50	Vandalisme/baldadigheid
	D10	Verkeersongeval met uitsluitend materiele schade
	D11	Verkeersongeval met letsel
	D12	Verkeersongeval met dodelijke afloop
	D13	Verlaten plaats na verkeersongeval

D20	Rijden onder invloed drugs/geneesmiddel (al dan niet i.c.m. alcohol)
D21	Rijden onder invloed (uitsluitend alcohol)
D40	Rijden tijdens rijverbod
D41	Rijden terwijl rijbewijs is ingevorderd
D42	Rijden tijdens ontzegging rijbevoegdheid
D43	Rijden zonder rijbewijs
D44	Rijden met ongeldig verklaard rijbewijs
D45	Rijden met geschorst rijbewijs
D50	Joyriding
D52	Overig verkeersmisdrijf
D70	Agressief/onveilig rijgedrag
E45	Gevarenclassificatie
F11	Openlijk geweldpleging tegen goederen
F12	Openlijk geweldpleging tegen personen
F13	Brandstichting
F15	Huisvredebreuk
F16	Lokaalvredebreuk
F17	Wederspannigheid (verzet)
F18	Niet voldoen aan bevel/vordering
F19	Overige misdrijven tegen het openbaar gezag
F30	Valse identiteit opgeven
F40	Bezit harddrugs (lijst i)
F41	Bezit softdrugs (lijst ii)
F42	Handel e.d. harddrugs (lijst i)
F43	Handel e.d. softdrugs (lijst ii)
F45	Vervaardigen softdrugs (lijst ii)
F47	Overige drugsdelicten
F50	Discriminatie
F51	Belediging
F520	Openbare schennis der eerbaarheid
F521	Verkrachting
F522	Aanranding
F526	Seksueel misbruik (incest) afh. relatie/wilsonbekwame
F527	Seksueel misbruik kinderen (geen incest)
F529	Overige meldingen zeden
F5291	Kinderpornografie
F5295	Sexting
F530	Bedreiging
F531	Overige misdrijven tegen de persoonlijke vrijheid
F532	Gijzeling/ontvoering
F533	Stalking
F540	Doodslag/moord
F550	Eenvoudige mishandeling
F551	Zware mishandeling
F561	Mensenhandel seksuele uitbuiting
F610	Vals geld aanmaken
F611	Vals geld uitgeven
F616	Ie-fraude/namaakgoederen
F617	Identiteitsfraude
F631	Krediet-, hypotheek- en depotfraude
F638	Telecomfraude
F70	Bezit vuurwapens
F71	Handel vuurwapens
F72	Bezit overige wapens
F93	Misdrijven anders
F94	Witwassen
F95	Overtreding huisverbod
M011	Op/in bodem brengen afvalstoffen
M071	Transport gevaarlijke stoffen over de weg

Tabel 1: Maatschappelijke klassen

SYNTAX

```
FREQUENCIES VARIABLES=Delictverleden
  /STATISTICS=STDDEV MINIMUM MAXIMUM MEAN MEDIAN
  /ORDER=ANALYSIS.
```

Delictverleden

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	geen delictverleden	284	35,4	35,4	35,4
	traditioneel delictverleden	409	51,0	51,0	86,4
	digitaal delictverleden	33	4,1	4,1	90,5
	gemengd delictverleden	76	9,5	9,5	100,0
	Total	802	100,0	100,0	

Bijlage II - Netwerkanalyse

De netwerkmaten van de netwerken zijn berekend met Cytoscape. Cytoscape gaf de volgende output:

Netwerk_1 (undirected)

Summary Statistics

Number of nodes	64
Number of edges	151
Avg. number of neighbors	4,719
Network diameter	13
Network radius	7
Characteristic path length	4,838
Clustering coefficient	0,482
Network density	0,075
Network heterogeneity	0,748
Network centralization	0,119
Connected components	1
Analysis time (sec)	0,026

Netwerk_2 (undirected)

Summary Statistics

Number of nodes	40
Number of edges	70
Avg. number of neighbors	3,500
Network diameter	12
Network radius	6
Characteristic path length	5,240
Clustering coefficient	0,618
Network density	0,090
Network heterogeneity	0,482
Network centralization	0,094
Connected components	1
Analysis time (sec)	0,011

Netwerk_3 (undirected)

Summary Statistics

Number of nodes	31
Number of edges	60
Avg. number of neighbors	3,871
Network diameter	9
Network radius	5
Characteristic path length	3,976
Clustering coefficient	0,578
Network density	0,129
Network heterogeneity	0,472
Network centralization	0,147
Connected components	1
Analysis time (sec)	0,008

In Cytoscape zijn de nabijheidcentraliteit, graad en tussenliggende centraliteit van alle actoren berekend. Bijbehorende output is weergegeven.

Actor	Nabijheidcentraliteit	Graad	Tussenliggende centraliteit
2	0.000	0	0.000
8	0.304	4	0.074
11	1.000	1	0.000
12	0.421	1	0.000
13	1.000	2	0.000
15	1.000	1	0.000
18	1.000	1	0.000
19	1.000	2	0.000
20	1.000	1	0.000
21	0.267	4	0.510
22	0.205	4	0.063
23	0.438	2	0.000
24	1.000	1	0.000
25	0.000	0	0.000
26	1.000	1	0.000
27	1.000	2	0.000
29	1.000	1	0.000
30	0.625	3	0.000
31	0.583	4	0.000
32	1.000	4	0.000
34	0.000	0	0.000
35	0.32	1	0.000

36	0.438	2	0.000
37	0.000	0	0.000
39	1.000	2	0.000
40	0.306	11	0.061
41	0.348	1	0.000
42	1.000	5	0.000
44	0.000	0	0.000
46	0.263	5	0.000
47	1.000	4	0.000
48	0.778	5	0.571
49	1.000	6	0.000
51	1.000	2	0.000
53	0.471	3	0.000
55	0.176	5	0.000
57	0.000	0	0.000
58	0.292	10	0.021
60	1.000	2	0.000
62	0.750	2	0.000
64	1.000	6	0.000
65	0.565	8	0.000
66	1.000	1	0.000
68	1.000	7	0.000
69	0.565	8	0.000
71	0.445	3	0.000
73	1.000	1	0.000
75	0.254	5	0.032
77	0.600	1	0.000
78	0.000	0	0.000
83	0.171	4	0.175
84	1.000	1	0.000
85	0.175	3	0.032
89	1.000	2	0.000
93	0.400	1	0.000
95	1.000	1	0.000
97	0.538	2	0.000
98	0.142	1	0.000
99	0.207	7	0.355
100	0.269	4	0.513
101	0.171	2	0.032
102	0.667	1	0.000
103	0.667	5	0.679
104	0.312	7	0.201
105	0.155	1	0.000

106	1.000	2	0.000
108	1.000	1	0.000
109	0.149	4	0.062
110	1.000	4	0.000
111	0.323	3	0.343
112	0.500	1	0.000
113	0.148	3	0.000
115	0.889	7	0.000
117	0.295	1	0.000
118	0.149	1	0.000
119	0.176	3	0.100
120	1.000	3	0.000
121	0.636	3	0.000
122	1.000	1	0.000
123	0.165	3	0.025
124	1.000	1	0.000
126	0.356	5	0.324
127	1.000	2	0.000
128	1.000	7	0.000
129	0.250	5	0.000
131	1.000	4	0.000
132	1.000	2	1.000
133	1.000	1	0.000
134	0.165	3	0.063
135	1.000	2	0.000
137	1.000	1	0.000
138	1.000	2	0.000
139	0.148	4	0.032
140	1.000	1	0.000
141	0.165	3	0.002
143	1.000	3	0.000
144	0.285	11	0.234
145	0.417	1	0.000
146	0.209	4	0.092
148	0.193	1	0.000
150	1.000	1	0.000
151	1.000	1	0.000
153	0.615	3	0.607
154	1.000	1	0.000
155	0.143	2	0.000
157	1.000	2	0.000
159	0.191	1	0.000
160	0.255	3	0.148

162	0.164	2	0.000
169	0.170	1	0.000
173	1.000	2	0.000
174	1.000	2	0.000
175	0.251	10	0.072
177	0.176	5	0.000
178	0.500	2	0.250
179	0.250	5	0.000
181	1.000	2	0.000
184	1.000	2	0.000
186	0.263	5	0.000
187	1.000	5	0.000
188	1.000	5	0.000
189	0.565	8	0.000
190	0.636	3	0.476
191	0.406	2	0.154
192	0.382	4	0.133
193	0.130	2	0.032
194	1.000	2	0.000
195	0.447	4	0.524
196	0.667	1	0.000
197	1.000	3	0.000
198	1.000	1	0.000
200	0.194	3	0.051
204	0.263	2	0.240
205	1.000	2	0.000
206	0.219	2	0.000
207	0.326	7	0.405
208	0.600	1	0.000
210	0.323	7	0.327
211	1.000	1	0.000
212	1.000	1	0.000
213	0.176	5	0.000
214	1.000	1	0.000
217	0.253	3	0.000
218	0.889	7	0.000
219	0.625	3	0.000
221	1.000	1	0.000
223	0.667	1	0.000
225	1.000	1	0.000
226	0.615	5	0.179
227	1.000	3	0.000
230	0.667	1	0.000

231	0.285	5	0.065
233	0.257	4	0.521
234	0.207	2	0.051
235	1.000	1	0.000
237	1.000	2	0.000
238	1.000	1	0.000
240	1.000	4	0.000
241	0.183	2	0.067
242	0.303	12	0.397
243	1.000	6	0.000
244	1.000	6	0.000
245	1.000	1	0.000
246	1.000	1	0.000
247	1.000	2	0.000
249	1.000	3	0.000
250	0.292	10	0.0213
251	1.000	2	0.000
253	1.000	2	1.000
255	1.000	1	0.000
257	0.204	3	0.093
258	1.000	1	0.000
259	0.444	3	0.000
263	1.000	0	0.000
267	0.115	1	0.000
268	1.000	1	0.000
270	1.000	4	0.000
272	0.000	0	0.000
273	1.000	1	0.000
276	0.591	4	0.513
277	1.000	1	0.000
278	0.227	5	0.000
279	0.323	3	0.000
281	1.000	3	0.000
282	0.238	2	0.000
286	0.227	5	0.000
287	0.245	7	0.000
288	1.000	4	0.000
289	0.193	2	0.032
290	0.195	4	0.152
293	0.176	5	0.000
294	1.000	3	0.000
295	0.146	1	0.000
297	0.404	5	0.383

298	0.565	8	0.000
299	1.000	3	0.000
300	0.262	7	0.497
302	0.444	2	0.000
303	0.276	9	0.000
305	0.197	2	0.201
306	1.000	1	0.000
307	1.000	1	0.000
309	0.667	4	0.536
310	0.700	4	0.286
311	0.000	0	0.000
314	0.444	2	0.250
316	1.000	3	0.000
317	0.165	3	0.025
318	1.000	2	0.000
319	0.583	4	0.000
320	1.000	7	0.000
321	1.000	1	0.000
322	1.000	5	0.000
323	1.000	5	0.000
326	0.278	10	0.016
327	1.000	1	0.000
328	0.889	7	0.000
330	1.000	3	0.000
332	1.000	2	0.000
333	1.000	2	0.000
334	1.000	1	0.000
335	1.000	3	0.000
336	1.000	2	0.000
337	1.000	3	0.000
338	0.471	3	0.000
339	1.000	1	0.000
342	0.250	5	0.000
343	1.000	1	0.000
344	0.565	8	0.000
345	1.000	1	0.000
348	1.000	2	0.000
350	1.000	1	0.000
351	0.533	1	0.000
352	0.667	1	0.000
354	0.142	1	0.000
356	1.000	4	0.000
358	0.833	4	0.600

359	1.000	2	0.000
361	1.000	1	0.000
363	1.000	2	0.000
364	0.193	2	0.000
365	0.600	1	0.000
366	0.625	2	0.000
367	0.163	1	0.000
368	0.207	2	0.000
369	1.000	1	0.000
371	0.565	8	0.000
372	0.000	0	0.000
374	0.000	0	0.000
375	0.565	8	0.000
376	0.000	0	0.000
377	1.000	1	0.000
381	1.000	2	0.000
382	1.000	5	0.000
383	0.381	2	0.000
385	1.000	1	0.000
388	0.500	1	0.000
389	0.000	0	0.000
390	1.000	2	0.000
391	1.000	4	0.000
393	1.000	2	0.000
395	0.444	1	0.000
396	1.000	1	0.000
398	1.000	1	0.000
399	0.206	2	0.000
401	1.000	4	0.000
402	0.249	8	0.121
405	0.000	0	0.000
406	0.500	1	0.000
410	0.174	2	0.000
411	0.276	4	0.000
413	0.276	4	0.000
414	1.000	5	0.000
415	1.000	2	0.000
416	1.000	7	0.000
417	1.000	1	0.000
420	1.000	1	0.000
421	1.000	4	0.000
422	1.000	1	0.000
424	1.000	1	0.000

425	1.000	2	0.000
426	1.000	7	0.000
428	1.000	1	0.000
429	1.000	3	0.000
432	0.219	2	0.067
436	0.25	5	0.000
437	1.000	2	0.000
439	1.000	3	0.667
441	0.889	7	0.000
442	1.000	2	0.000
443	1.000	2	1.000
444	1.000	5	0.000
445	1.000	1	0.000
446	0.444	2	0.000
447	1.000	8	0.25
448	0.263	5	0.000
449	1.000	4	0.000
450	0.394	2	0.000
455	1.000	2	0.000
456	0.328	3	0.095
458	0.636	3	0.000
459	1.000	2	0.000
463	1.000	5	0.000
466	1.000	1	0.000
467	1.000	6	0.000
468	0.307	12	0.067
470	1.000	2	0.000
471	0.000	0	0.000
473	1.000	2	0.000
474	1.000	1	0.000
475	1.000	2	0.000
476	1.000	1	0.000
477	0.245	7	0.000
479	0.889	7	0.000
481	1.000	2	0.000
482	0.722	9	0.513
483	0.253	4	0.000
484	0.889	7	0.000
485	1.000	4	0.000
486	1.000	3	0.000
488	1.000	1	0.000
490	1.000	1	0.000
491	0.000	0	0.000

492	0.276	4	0.000
494	0.750	2	0.000
496	0.170	1	0.000
497	1.000	3	0.667
498	1.000	2	0.000
499	1.000	2	0.000
501	0.181	1	0.000
502	1.000	2	0.000
503	1.000	5	0.000
505	1.000	2	0.000
506	1.000	1	0.000
508	0.381	2	0.000
510	1.000	1	0.000
512	0.263	5	0.000
513	1.000	1	0.000
514	1.000	2	1.000
515	0.246	2	0.000
516	1.000	2	0.000
520	1.000	1	0.000
521	1.000	1	0.000
524	1.000	1	0.000
525	0.471	3	0.000
526	1.000	4	0.000
537	0.000	0	0.000
540	0.444	1	0.000
541	0.219	3	0.191
542	1.000	1	0.000
543	0.270	8	0.186
544	0.349	5	0.100
546	0.875	6	0.667
547	1.000	1	0.000
549	0.615	5	0.179
550	0.583	4	0.000
552	0.667	1	0.000
553	0.600	1	0.000
554	1.000	3	0.000
555	0.278	10	0.015
556	1.000	1	0.000
558	1.000	1	0.000
560	1.000	2	0.000
561	1.000	1	0.000
562	0.276	4	0.000
565	1.000	3	0.000

566	0.800	3	0.833
567	1.000	3	0.000
568	0.217	3	0.000
572	0.323	3	0.000
573	1.000	1	0.000
574	0.667	1	0.000
576	0.235	3	0.051
577	1.000	3	0.000
581	1.000	3	0.000
582	1.000	1	0.000
585	0.300	2	0.000
588	1.000	2	0.000
590	0.571	3	0.000
592	1.000	4	0.000
593	0.583	4	0.000
594	0.000	0	0.000
595	0.395	6	0.613
596	0.750	2	0.000
597	0.727	5	0.607
599	1.000	2	0.000
601	0.170	1	0.000
603	1.000	7	0.000
604	1.000	2	0.000
606	0.163	2	0.000
607	1.000	1	0.000
608	0.240	4	0.026
609	0.447	6	0.652
610	0.333	4	0.010
611	1.000	2	0.000
612	1.000	2	0.000
613	0.235	4	0.474
614	1.000	1	0.000
615	0.667	5	0.429
616	1.000	4	0.000
617	1.000	2	0.000
620	1.000	1	0.000
621	0.203	1	0.000
622	0.237	3	0.051
625	1.000	4	0.000
627	0.246	2	0.000
630	0.750	2	0.000
632	1.000	1	0.000
633	1.000	3	0.000

634	0.000	0	0.000
636	0.667	1	0.000
637	1.000	6	0.000
639	0.217	3	0.000
640	0.223	1	0.000
641	0.241	2	0.000
642	1.000	1	0.000
643	1.000	2	0.000
645	0.600	1	0.000
646	0.316	6	0.287
649	1.000	1	0.000
653	0.25	5	0.000
655	0.245	7	0.000
656	1.000	3	0.000
657	0.246	1	0.000
658	0.533	3	0.000
659	0.667	2	0.000
660	0.164	2	0.000
662	1.000	1	0.000
666	0.237	2	0.062
667	1.000	7	0.000
668	1.000	2	0.000
670	1.000	2	0.000
672	1.000	1	0.000
674	0.176	5	0.000
678	1.000	4	0.000
679	1.000	1	0.000
680	1.000	2	0.000
683	0.000	0	0.000
687	1.000	3	0.000
688	0.349	5	0.098
689	1.000	1	0.000
692	0.232	2	0.225
693	0.571	3	0.000
694	1.000	1	0.000
696	0.151	2	0.000
697	0.129	1	0.000
698	1.000	1	0.000
699	1.000	1	0.000
700	0.438	1	0.000
701	0.217	3	0.000
702	1.000	3	0.000
703	0.538	2	0.000

704	1.000	1	0.000
705	1.000	1	0.000
709	1.000	4	0.000
710	1.000	1	0.000
711	1.000	1	0.000
712	0.242	7	0.416
713	0.217	3	0.364
714	0.565	8	0.000
715	1.000	2	0.000
716	1.000	4	0.000
718	0.306	11	0.061
720	1.000	1	0.000
721	0.309	3	0.181
722	0.162	1	0.000
723	1.000	1	0.000
724	1.000	7	0.000
725	0.375	5	0.460
726	0.25	1	0.000
727	0.000	0	0.000
729	1.000	1	0.000
732	1.000	2	0.000
733	0.000	0	0.000
734	1.000	1	0.000
735	0.625	3	0.000
736	0.889	7	0.000
737	0.227	5	0.000
738	1.000	3	0.000
739	1.000	1	0.000
740	0.273	3	0.129
741	0.362	3	0.000
747	1.000	2	0.000
748	0.173	1	0.000
749	1.000	1	0.000
751	0.181	1	0.000
752	0.227	5	0.000
753	1.000	3	0.000
754	1.000	6	0.000
755	0.318	12	0.304
756	0.280	6	0.249
759	0.276	9	0.000
760	1.000	2	0.000
761	1.000	2	0.000
764	1.000	1	0.000

765	1.000	1	0.000
766	0.533	3	0.429
767	0.000	0	0.000
768	1.000	1	0.000
769	0.246	8	0.002
770	0.245	7	0.000
773	1.000	1	0.000
774	0.241	2	0.000
776	1.000	3	0.000
778	1.000	1	0.000
779	1.000	3	0.000
780	0.300	3	0.000
782	0.253	3	0.000
784	0.232	2	0.175
785	0.253	4	0.000
786	1.000	3	0.000
787	0.142	2	0.000
788	0.318	4	0.110
790	1.000	2	0.000
791	1.000	5	0.000
794	1.000	5	0.000
796	0.000	0	0.000
797	1.000	1	0.000
801	1.000	1	0.000
802	0.166	4	0.100
805	0.000	0	0.000
806	0.193	6	0.357
807	0.143	2	0.000
808	0.394	2	0.000
809	1.000	3	0.000
810	0.151	2	0.000

Volledige uitwerking centraliteitsmaten

Netwerk 1

Netwerk 1 is volledig uitgewerkt in de resultatensectie. In Tabel 2 zijn alle centraliteitsmaten van de actoren van netwerk 1 uitgewerkt. Enkele actoren hebben een waarde van 0 voor de tussenliggende centraliteit en zijn daarom niet opgenomen in de tabel.

Tabel 2: centraliteitsmaten netwerk 1	**Rang**	**Node**	**Score**
Graad	1	242, 755 en 468	12
1 – 12	2	144, 40 en 718	11
	3	58, 175, 250, 326 en 555	10
	4	303 en 759	9
	5	769 en 402	8
	6	210, 104, 770, 655, 477 en 287	7
	7	756	6
	8	231 en 75	5
	9	22, 139, 83, 290, 785, 146, 483, 608 en 109	4
	10	160, 85, 257, 113 en 134	3
	11	101, 162, 193, 206, 289, 305, 368, 410, 515, 627, 660, 666, 692 en 784	2
	12	98, 118, 169, 267, 295, 354, 496, 601, 621, 640, 697 en 722	1
Nabijheidcentraliteit	1	210	0,323
0,115 – 0,323			
	2	755	0,318
	3	104	0,312
	4	468	0,307
	5	40 en 718	0,306
	6	242	0,303
	7	58 en 250	0,292
	8	144 en 231	0,285
	9	756	0,280
	10	326 en 555	0,278
	11	303 en 759	0,276
	12	160	0,255
	13	75	0,254
	14	483 en 785	0,253
	15	175	0,251
	16	402	0,249
	17	515, 627 en 769	0,246
	18	287, 477, 655 en 770	0,245
	19	608	0,240
	20	666	0,237
	21	692 en 784	0,232
	22	640	0,223
	23	206	0,219
	24	146	0,209
	25	368	0,207
	26	22	0,205
	27	257	0,204
	28	62	0,203
	29	305	0,197
	30	290	0,195
	31	289	0,193
	32	85	0,175

	33	410	0,174
	34	83 en 101	0,171
	35	169, 496 en 601	0,170
	36	134	0,165
	37	162 en 660	0,164
	38	722	0,162
	39	118 en 109	0,149
	42	139 en 113	0,148
	44	295	0,146
	45	98 en 354	0,142
	46	193	0,130
	47	697	0,129
	48	267	0,115
Tussenliggende centraliteit	1	242	0,397
0,002 – 0,397	2	210	0,327
	3	755	0,304
	4	756	0,249
	5	144	0,234
	6	692	0,225
	7	104 en 305	0,201
	8	83 en 784	0,175
	9	290	0,152
	10	160	0,148
	11	402	0,121
	12	257	0,093
	13	146	0,092
	14	175	0,072
	15	468	0,067
	16	231	0,065
	17	22 en 134	0,063
	18	109 en 666	0,062
	19	40 en 718	0,061
	20	75, 85, 101, 139, 193 en 289	0,032
	21	608	0,026
	22	58 en 250	0,021
	23	326 en 555	0,016
	24	769	0,002

Netwerk 2

Tabel 3 geeft de centraliteitsmaten graad, nabijheidcentraliteit en tussenliggende centraliteit voor alle actoren in netwerk 2 weer. De top 5 rangen zijn weergegeven. De volledige tabellen zijn terug te vinden in bijlage II. Actoren die een score van 0 hebben op de tussenliggende centraliteit zijn niet opgenomen in de tabel.

De actoren met de hoogste graad waarden zijn actoren 99, 300 en 712, met elk een graad waarde van 7. Dit betekent dat zij elk 7 directe verbindingen hebben met andere actoren in het netwerk.

In netwerk 2 heeft actor 100 de hoogste nabijheidcentraliteit met een waarde van 0,269. Actoren 21 en 300 hebben echter waarden die zeer dicht bij die van actor 100 liggen, wat betekent dat ze zeer vergelijkbaar zijn op dit gebied. Actoren 100, 21 en 300 hebben allemaal een gemiddelde nabijheid tot andere actoren in het netwerk. Zoals te zien is in de tabel, liggen de waarden van de nabijheidcentraliteit van de actoren opnieuw dicht bij elkaar. De actoren met waarden van 0,262 en hoger zijn geel gemarkeerd in Figuur 16.

Actoren 233, 100 en 21 laten allen hoge waarden voor tussenliggende centraliteit zien. Deze actoren hebben aanzienlijke controle over de communicatiestromen tussen andere actoren in het netwerk. Ze kunnen fungeren als belangrijke tussenpersonen en invloed uitoefenen op de verspreiding van informatie binnen het netwerk. Ze hebben een sterke invloed op de dynamiek en activiteiten van het netwerk, waaronder besluitvorming en coördinatie van acties. Figuur 17 laat zien hoe het netwerk eruit ziet wanneer actor 100 wordt verwijderd. Het netwerk valt uiteen in 2 kleinere netwerken. Wanneer actoren 233 en 21 ook uit het netwerk worden verwijderd, fragmenteert deze verder. Actor 100 lijkt echter in termen van netwerkontmanteling het meest essentieel.

Tabel 3: centraliteitsmaten netwerk 2	**Rang**	**Node**	**Score**
Graad	1	99, 300 en 712	7
1 – 7	2	806	6
	3	55, 177, 213, 278, 286, 293, 674, 737 en 752	5
	4	21, 100, 233, 613 en 802	4
	5	119, 123, 141, 200, 317, 576, 622 en 713	3
	6	155, 234, 282, 364, 399, 606, 696, 787, 807 en 810	2
	7	148, 159, 367 en 748	1
Nabijheidcentraliteit	1	100	0,269
0,142 – 0,269			
	2	21	0,267
	3	300	0,262
	4	233	0,257
	5	712	0,242
	6	282 en 622	0,238

	7	576 en 613	0,235
	8	278, 286, 737 en 752	0,227
	9	713	0,217
	10	99 en 243	0,207
	11	399	0,206
	12	200	0,194
	13	148, 364 en 806	0,193
	14	159	0,191
	15	55, 119, 177, 213, 293 en 674	0,176
	16	748	0,173
	17	802	0,166
	18	123, 141 en 317	0,165
	19	367 en 606	0,163
	20	696 en 810	0,151
	21	155 en 807	0,143
	22	787	0,142
Tussenliggende centraliteit	1	233	0,521
0,002 – 0,521	2	100	0,513
	3	21	0,510
	4	300	0,497
	5	613	0,474
	6	712	0,416
	7	713	0,364
	8	806	0,357
	9	99	0,355
	10	119 en 802	0,100
	11	200, 234, 576 en 622	0,051
	12	123 en 317	0,025
	13	141	0,002

Netwerk 3

Tabel 4 geeft de centraliteitsmaten graad, nabijheidcentraliteit en tussenliggende centraliteit voor alle actoren in netwerk 3 weer. De top 5 rangen zijn weergegeven. De volledige tabellen zijn terug te vinden in bijlage II. Actoren die een score van 0 hebben op de tussenliggende centraliteit zijn opnieuw niet opgenomen in de tabel.

De actor met de hoogste graad waarde is actor 543 (zie figuur 19) met een graad waarde van 8. Dit betekent dat deze actor 8 directe verbindingen heeft met andere actoren in het netwerk.

Binnen netwerk 3 heeft actor 595 veruit de hoogste nabijheidcentraliteit. Dit duidt er op dat deze actor een bovengemiddelde nabijheid heeft tot andere actoren in het netwerk. Met de hoogste waarde voor nabijheidcentraliteit in het netwerk kan deze actor waarschijnlijk het meeste invloed uitoefenen en een zeer centrale positie innemen. Daarnaast hebben actoren 544, 688, 207, 111, 646, 585 en 780 ook allen een relatief hoge nabijheidcentraliteit, met een waarde van 0,300 of hoger. Deze actoren zijn in Figuur 20 aangeduid met de kleur geel.

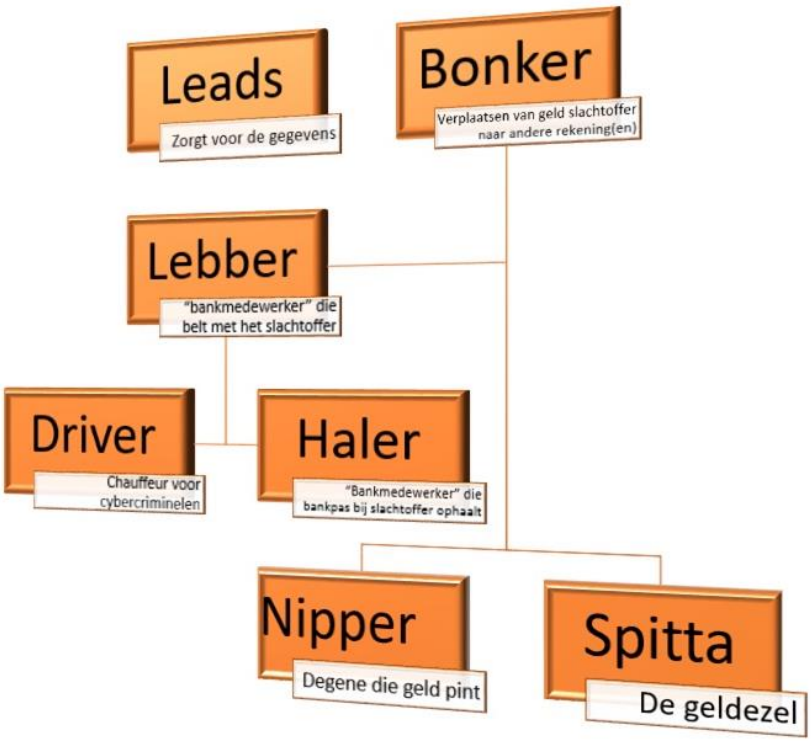
Bovendien heeft actor 595 ook veruit de hoogste tussenliggende centraliteit waarde. Actoren 725 en 207 hebben een tussenliggende centraliteit van boven de 0,4 en hebben daarmee ook een relatief hoge tussenliggende centraliteit waarde. Deze drie actoren zijn geel gemarkeerd in Figuur 18. Figuur 21 laat zien hoe het netwerk eruit ziet wanneer actor 595 wordt verwijderd. Het netwerk valt uiteen in 3 kleinere netwerken. Deze actor vervult duidelijk een belangrijke rol in termen van sociaal kapitaal.

Tabel 4: centraliteitsmaten netwerk 3	**Rang**	**Node**	**Score**
Graad	1	543	8
1 – 8	2	207	7
	3	595 en 646	6
	4	46, 129, 179, 186, 342, 436, 448, 512, 544, 653, 688 en 725	5
	5	111, 541, 568, 639, 701, 740 en 780	3
	6	204, 241, 432 en 585	2
	7	105, 501, 657 en 751	1
Nabijheidcentraliteit	1	595	0,395
0,155 – 0,395			
	2	725	0,375
	3	544 en 688	0,349
	4	207	0,326
	5	111	0,323
	6	646	0,316
	7	585 en 780	0,300
	8	740	0,273
	9	543	0,270
	10	46, 186, 204, 448 en 512	0,263
	11	129, 179, 342, 436 en 653	0,250

	12	657	0,246
	13	432 en 541	0,219
	14	568, 639 en 701	0,217
	15	241	0,183
	16	501 en 751	0.181
	17	105	0,155
Tussenliggende centraliteit	1	595	0,613
0,000 – 0,613	2	725	0,460
	3	207	0,405
	4	111	0,343
	5	646	0,287
	6	204	0,239
	7	541	0,191
	8	543	0,186
	9	740	0,129
	10	544 en 688	0,098
	12	241 en 432	0,067

Bijlage III – Smibanese straattaal

Analisten van de Dienst Regionale Informatie Organisatie (DRIO) van de eenheid Noord-Nederland hebben een voorbeeld beschreven van de samenwerking tussen bankhelpdeskfraudeurs vanuit de ‘Smibanese’ straattaal. Deze straattaal is een dialect van de straattalen in Nederland afkomstig uit de Bijlmer (Sintenie, 2019). Afbeelding 1 geeft dit voorbeeld weer. Een gerekruteerde dienstverlener, ook wel 'lebber' genoemd, belt het slachtoffer op en doet zich voor als een bankmedewerker. De zogenaamde bankmedewerker meldt dat er criminele activiteiten zijn waargenomen op de rekening en dat er een collega, de 'haler', langs zal komen om de bankpas op te halen. Deze 'haler' wordt naar het slachtoffer gebracht door een 'driver', oftewel een chauffeur. Zowel de 'driver' als de 'haler' zijn gerekruteerde dienstverleners en krijgen instructies van de 'lebber'. De bankpas (of gegevens) wordt vervolgens door de 'haler' overhandigd aan de 'bonker', het kernlid, die het geld overboekt van de rekening van het slachtoffer naar de rekening van de 'spitta' (geldezel). De 'nipper', ook een gerekruteerde dienstverlener, pint vervolgens zo snel mogelijk het geld zodra het op de rekening van de geldezel staat. Het woord 'haler' is overigens geen onderdeel van het 'Smibanese'-jargon, maar er is nog geen specifieke term voor deze rol beschikbaar.



Afbeelding 1. een voorbeeld van de samenwerking tussen bankhelpdeskfraudeurs vanuit de ‘Smibanese’ straattaal.

Bijlage IV – Lone wolves analyse

Zie *Lanser_SPSS_file_analyse_isolates&dyads.sav*

Geslacht – lone wolves

```
SYNTAX
*Analyse lone wolves.
DATASET ACTIVATE DataSet1.
RECODE GESLACHT ('Man'=0) ('Vro'=1) INTO Geslacht_code.
VARIABLE LABELS  Geslacht_code 'Geslacht'.
EXECUTE.

FREQUENCIES VARIABLES=Geslacht_code
  /STATISTICS=STDDEV MINIMUM MAXIMUM MEAN MEDIAN
  /ORDER=ANALYSIS.
```

Geslacht

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	,00	95	73,1	74,2	74,2
	1,00	33	25,4	25,8	100,0
	Total	128	98,5	100,0	
Missing	System	2	1,5		
Total		130	100,0		

Leeftijd – lone wolves

```
SYNTAX
DESCRIPTIVES VARIABLES=Leeftijd
  /STATISTICS=MEAN STDDEV MIN MAX.
```

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Leeftijd	108	13	72	30,29	12,629
Valid N (listwise)	108				

Delictverleden – lone wolves

```
SYNTAX
FREQUENCIES VARIABLES=Delictverleden
  /STATISTICS=STDDEV MINIMUM MAXIMUM MEAN MEDIAN
  /ORDER=ANALYSIS.
```

Delictverleden

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	geen delictverleden	78	60,0	60,0	60,0
	traditioneel delictverleden	44	33,8	33,8	93,8
	gemengd delictverleden	8	6,2	6,2	100,0
	Total	130	100,0	100,0	

Aandeel buitenlands – lone wolves

```
SYNTAX
FREQUENCIES VARIABLES=afkomst_binair
  /STATISTICS=STDDEV MINIMUM MAXIMUM MEAN MEDIAN
  /ORDER=ANALYSIS.
```

afkomst_binair

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	121	93,1	98,4	98,4
	1	2	1,5	1,6	100,0
	Total	123	94,6	100,0	
Missing	System	7	5,4		
Total		130	100,0		

Geslacht – overige actoren

Zie *Lanser_SPSS_file_analyse_all_but_isolates&dyads.sav*

```
SYNTAX
*Analyse all but lone wolves.
RECODE GESLACHT ('Man'=0) ('Vro'=1) INTO Geslacht_code.
VARIABLE LABELS  Geslacht_code 'Geslacht'.
EXECUTE.

FREQUENCIES VARIABLES=Geslacht_code
  /STATISTICS=STDDEV MINIMUM MAXIMUM MEAN MEDIAN
  /ORDER=ANALYSIS.
```

Geslacht

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	,00	548	81,5	82,0	82,0
	1,00	120	17,9	18,0	100,0
	Total	668	99,4	100,0	
Missing	System	4	,6		
Total		672	100,0		

Leeftijd – overige actoren

```
SYNTAX
DESCRIPTIVES VARIABLES=Leeftijd
  /STATISTICS=MEAN STDDEV MIN MAX.
```

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Leeftijd	567	14	74	27,93	10,773
Valid N (listwise)	567				

Delictverleden – overige actoren

```
SYNTAX
FREQUENCIES VARIABLES=Delictverleden
  /STATISTICS=STDDEV MINIMUM MAXIMUM MEAN MEDIAN
  /ORDER=ANALYSIS.
```

Delictverleden

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	geen delictverleden	206	30,7	30,7	30,7
	traditioneel delictverleden	365	54,3	54,3	85,0
	digitaal delictverleden	33	4,9	4,9	89,9
	gemengd delictverleden	68	10,1	10,1	100,0
	Total	672	100,0	100,0	

Aandeel buitenlands – overige actoren

```
SYNTAX
FREQUENCIES VARIABLES=afkomst_binair
  /STATISTICS=STDDEV MINIMUM MAXIMUM MEAN MEDIAN
  /ORDER=ANALYSIS.
OUTPUT MODIFY
  /SELECT TABLES
  /IF COMMANDS=["Frequencies(LAST)"] SUBTYPES="Frequencies"
  /TABLECELLS SELECT=[VALIDPERCENT CUMULATIVEPERCENT] APPLYTO=COLUMN
HIDE=YES
  /TABLECELLS SELECT=[TOTAL] SELECTCONDITION=PARENT(VALID MISSING)
APPLYTO=ROW HIDE=YES
  /TABLECELLS SELECT=[VALID] APPLYTO=ROWHEADER UNGROUP=YES
  /TABLECELLS SELECT=[PERCENT] SELECTDIMENSION=COLUMNS FORMAT="PCT"
APPLYTO=COLUMN
  /TABLECELLS SELECT=[COUNT] APPLYTO=COLUMNHEADER REPLACE="N"
  /TABLECELLS SELECT=[PERCENT] APPLYTO=COLUMNHEADER REPLACE="%".
```

afkomst_binair

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	658	97,9	99,1	99,1
	1	6	,9	,9	100,0
	Total	664	98,8	100,0	
Missing	System	8	1,2		
Total		672	100,0		

T-toets en de Pearson chikwadraatwaarde

T-toetsen

Lone wolves en leeftijd

Er is een T – toets uitgevoerd om het verschil in leeftijd tussen *lone wolfs* en actoren uit grotere netwerken te toetsen. *Lone wolves* hebben een significant hogere leeftijd (2,36 punten hoger) dan andere actoren in grotere netwerken, $t(673) = 2{,}028$; $p = 0{,}043$).

```
SYNTAX
T-TEST GROUPS=Lone_wolf(0.0 1.0)
  /MISSING=ANALYSIS
  /VARIABLES=Leeftijd
  /ES DISPLAY(TRUE)
  /CRITERIA=CI(.95).
```

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means							
						Significance				95% Confidence Interval of the Difference	
		F	Sig.	t	df	One-Sided p	Two-Sided p	Mean Difference	Std. Error Difference	Lower	Upper
Leeftijd	Equal variances assumed	7,329	,007	2,028	673	,021	,043	2,361	1,164	,075	4,647
	Equal variances not assumed			1,821	138,215	,035	,071	2,361	1,297	-,203	4,925

Afkomst en leeftijd

Er is een T – toets uitgevoerd om het verschil in leeftijd tussen buitenlandse en Nederlandse verdachten te toetsen. Er is geen significant verschil in leeftijd tussen buitenlandse en Nederlandse verdachten, $t(673) = -1{,}536$; $p = 0{,}125$).

```
SYNTAX
T-TEST GROUPS=Afkomst(0.0 1.0)
  /MISSING=ANALYSIS
  /VARIABLES=Leeftijd
  /ES DISPLAY(TRUE)
  /CRITERIA=CI(.95).
```

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means							
						Significance				95% Confidence Interval of the Difference	
		F	Sig.	t	df	One-Sided p	Two-Sided p	Mean Difference	Std. Error Difference	Lower	Upper
Leeftijd	Equal variances assumed	,333	,564	-1,536	673	,063	,125	-6,478	4,219	-14,761	1,806
	Equal variances not assumed			-1,561	6,131	,084	,168	-6,478	4,150	-16,579	3,624

Chi-kwadraattoetsen

Lone wolves en geslacht

Om te kijken naar de samenhang tussen *lone wolves* en geslacht is gebruik gemaakt van een Chi-kwadraat toets. *Lone wolves* zijn vaker vrouw dan andere actoren in grotere netwerken $\chi^2(1, N = 796) = 4{,}228$, $p = ,04$

```
SYNTAX
CROSSTABS
  /TABLES=Geslacht_code BY Lone_wolf
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ
  /CELLS=COUNT EXPECTED SRESID
  /COUNT ROUND CELL.
```

Geslacht * Lone wolf Crosstabulation

			Lone wolf		
			lone wolf	actor uit groter netwerk	Total
Geslacht	man	Count	95	548	643
		Expected Count	103,4	539,6	643,0
		Standardized Residual	-,8	,4	
	vrouw	Count	33	120	153
		Expected Count	24,6	128,4	153,0
		Standardized Residual	1,7	-,7	
Total		Count	128	668	796
		Expected Count	128,0	668,0	796,0

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	4,228[a]	1	,040		
Continuity Correction[b]	3,739	1	,053		
Likelihood Ratio	3,979	1	,046		
Fisher's Exact Test				,049	,029
Linear-by-Linear Association	4,222	1	,040		
N of Valid Cases	796				

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 24,60.

b. Computed only for a 2x2 table

Lone wolves en delictverleden

Om te kijken naar de samenhang tussen *lone wolves* en delictverleden is gebruik gemaakt van een Chi-kwadraat toets voor verschil in gemiddelden. *Lone wolves* hebben vaker geen delictverleden dan actoren in grotere netwerken $\chi^2(3, N = 802) = 43{,}63$, $p < ,001$

```
SYNTAX
CROSSTABS
  /TABLES=Lone_wolf BY Delictverleden
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ
  /CELLS=COUNT EXPECTED SRESID
  /COUNT ROUND CELL.
```

Lone wolf * Delictverleden Crosstabulation

			Delictverleden				
			geen delictverleden	traditioneel delictverleden	digitaal delictverleden	gemengd delictverleden	Total
Lone wolf	lone wolf	Count	78	44	0	8	130
		Expected Count	46,0	66,3	5,3	12,3	130,0
		Standardized Residual	4,7	-2,7	-2,3	-1,2	
	actor uit groter netwerk	Count	206	365	33	68	672
		Expected Count	238,0	342,7	27,7	63,7	672,0
		Standardized Residual	-2,1	1,2	1,0	,5	
Total		Count	284	409	33	76	802
		Expected Count	284,0	409,0	33,0	76,0	802,0

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	43,630[a]	3	<,001
Likelihood Ratio	46,458	3	<,001
Linear-by-Linear Association	25,507	1	<,001
N of Valid Cases	802		

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 5,35.

Geslacht en afkomst

Om te kijken naar de samenhang tussen afkomst en geslacht is gebruik gemaakt van een Chi-kwadraat toets voor verschil in gemiddelden. Buitenlandse verdachten verschillen niet significant in geslacht van andere actoren in grotere netwerken, $\chi^2(1, N = 796) = ,235$, $p = 0{,}628$.

```
SYNTAX
CROSSTABS
  /TABLES=Geslacht_code BY Afkomst
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ
  /CELLS=COUNT EXPECTED SRESID
  /COUNT ROUND CELL.
```

Geslacht * Afkomst Crosstabulation

			Afkomst		
			niet-buitenlands	buitenlands	Total
Geslacht	man	Count	636	7	643
		Expected Count	636,5	6,5	643,0
		Standardized Residual	,0	,2	
	vrouw	Count	152	1	153
		Expected Count	151,5	1,5	153,0
		Standardized Residual	,0	-,4	
Total		Count	788	8	796
		Expected Count	788,0	8,0	796,0

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	,235[a]	1	,628		
Continuity Correction[b]	,001	1	,973		
Likelihood Ratio	,261	1	,610		
Fisher's Exact Test				1,000	,526
Linear-by-Linear Association	,235	1	,628		
N of Valid Cases	796				

a. 1 cells (25,0%) have expected count less than 5. The minimum expected count is 1,54.

b. Computed only for a 2x2 table

Delictverleden en afkomst

Om te kijken naar de samenhang tussen afkomst en delictverleden is gebruik gemaakt van een Chi-kwadraat toets voor verschil in gemiddelden. Buitenlandse verdachten verschillen niet significant in delictverleden van Nederlandse verdachten, $\chi^2(3, N = 802) = 4{,}892$, $p = 0{,}180$.

```
SYNTAX
CROSSTABS
  /TABLES= Afkomst BY Delictverleden
  /FORMAT=AVALUE TABLES
  /STATISTICS=CHISQ
  /CELLS=COUNT EXPECTED SRESID
  /COUNT ROUND CELL.
```

Afkomst * Delictverleden Crosstabulation

			Delictverleden				
			0	1	2	3	Total
Afkomst	niet-buitenlands	Count	279	407	32	76	794
		Expected Count	281,2	404,9	32,7	75,2	794,0
		Standardized Residual	-,1	,1	-,1	,1	
	buitenlands	Count	5	2	1	0	8
		Expected Count	2,8	4,1	,3	,8	8,0
		Standardized Residual	1,3	-1,0	1,2	-,9	
Total		Count	284	409	33	76	802
		Expected Count	284,0	409,0	33,0	76,0	802,0

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	4,892[a]	3	,180
Likelihood Ratio	5,101	3	,165
Linear-by-Linear Association	1,508	1	,220
N of Valid Cases	802		

a. 4 cells (50,0%) have expected count less than 5. The minimum expected count is ,33.

Bijlage V – Analyse op basis van rollen

Wanneer een actor de rol ‘overig’ heeft, is deze actor per abuis opgenomen in het netwerk terwijl deze persoon niet in crimescript thuis hoort. Bijvoorbeeld een onterechte verdachte of een slachtoffer van bankhelpdeskfraude.

Netwerk 1 - actor	***ROL***
22	Geldezel
40	Gerekruteerde dienstverlener; pinner
58	Gerekruteerde dienstverlener
75	Overig
83	Pakketjes geldezel
85	Driver,
98	Pinner
101	Geldezel
104	Pasjesophaler en pinner
109	Pasjesophaler
113	Geldezel
118	Pasjesophaler en pinner
134	Pasjesophaler en pinner
139	Pakketjes geldezel
144	Beller
146	Geldezel
160	Geldezel
162	Geldezel
169	Geldezel
175	Pinner en professionele (technische) dienstverlener
193	Geldezel
206	Driver
210	Overig
231	Pinner
242	Professionele (technische) dienstverlener, verstrekte persoonsgegevens
250	Pasjesophaler
257	Overig
267	Geldezel
287	Geldezel
289	Kernlid
290	Geldezel
295	Geldezel
303	Kernlid
305	Kernlid en pinner
326	Overig
354	Overig
368	Geldezel

402	Werver geldezels
410	Pasjesophaler
468	Gerekruteerde dienstverlener
477	Overig
483	Geldezel
496	Geldezel
515	Passenophaler en pinner
555	Professionele dienstverlener; technisch onderlegd
601	Geldezel
608	Belle
621	Geldezel
627	Pakketjes geldezel
640	Geldezel
655	Overig
660	Geldezel
666	Geldezel
692	Pinner
697	Geldezel
718	Beller
722	Pakketjes geldezel
755	Beller
756	Beller
759	Kernlid
769	Pinner
770	Pinner
784	Pakketjes geldezel
785	Pasjesophaler
Netwerk 2 - actor	**ROL**
21	Geldezel
55	Geldezel
99	Geldezel
100	Pinner
119	Geldezel
123	Geldezel
141	Pinner en pasjesophaler
148	Geldezel
155	Pinner
159	Geldezel
177	Geldezel
200	Geldezel
213	Geldezel

233	Geldezel
234	Geldezel
278	Pinner en pasjesophaler
282	Driver
286	Geldezel
293	Geldezel
300	Driver
317	Geldezel
364	Geldezel
367	Geldezel
399	Pakketjes geldezel
576	Geldezel
606	Overig
613	Geldezel
622	Geldezel
674	Geldezel
696	Pinner
712	Pakketjes geldezel
713	Geldezel
737	Pinner
748	Pasjesophaler
752	Kernlid
787	Overig
802	Pasjesophaler
806	Pinner
807	Pinner
810	Geldezel
Netwerk 3 - actor	**ROL**
46	Geldezel
105	Pinner. Heeft ook contact met geldezels
111	Kernlid
129	Professionele dienstverlener
179	Kernlid, coördineert de bellers
186	Geldezel
204	Pasjesophaler
207	Geldezel
241	Pasjesophaler
342	Kernlid
432	Pasjesophaler
436	Beller
448	Geldezel

501	Pinner
512	Geldezel
541	Pasjesophaler en geldezel werver
543	Geldezel
544	Pinner
568	Pinner
585	Pinner
595	Pasjesophaler en rekruteerde geldezels
639	Geldezel
646	Pasjesophaler en pinner
653	Kernlid
657	Pasjesophaler
688	Beller
701	Pasjesophaler & pinner
725	Driver
740	Pinner
751	Driver
780	Pasjesophaler

Isolate - actor	***ROL***
2	Geldezel
25	Geldezel
34	Geldezel
37	Overig
44	Geldezel
57	Geldezel
78	Geldezel
263	Geldezel
272	Geldezel
311	Geldezel
372	Pasjesophaler
374	Geldezel
376	Geldezel
389	Geldezel
405	Geldezel
471	Geldezel
491	Geldezel
537	Geldezel
594	Geldezel
634	Geldezel
683	Geldezel
727	Geldezel
733	Geldezel

767	Geldezel
796	Geldezel
805	Geldezel

Dyade - actor	***ROL***
11	Geldezel
15	Geldezel
18	Pasjesophaler
20	Overig
24	Pinner
26	Geldezel
29	Geldezel
66	Geldezel
73	Geldezel
84	Pasjesophaler
95	Beller
108	Pinner en professionele (technische) dienstverlener
122	Geldezel
124	Pinner
133	Geldezel
137	Geldezel
140	Onbekend
150	Geldezel
151	Geldezel
154	Overig
198	Geldezel
211	Geldezel
212	Geldezel
214	Geldezel
221	Pinner
225	Pinner
235	Overig
238	Geldezel
245	Geldezel
246	Pasjesophaler
255	Geldezel
258	Verstrekte leads
268	Geldezel
273	Pinner
277	Overig
306	Geldezel
307	Geldezel

321	Geldezel
327	Geldezel
334	Geldezel
339	Pinner
343	Pinner
345	Verstrekte leads
350	Pasjesophaler
361	Geldezel
369	Geldezel
377	Beller
385	Geldezel
396	Geldezel
398	Geldezel
417	Geldezel
420	Geldezel
422	Pinner
424	Pasjesophaler en pinner
428	Geldezel
445	Geldezel
466	Pasjesophaler
474	Geldezel
476	Geldezel
488	Geldezel
490	Geldezel
506	Pinner
510	Pasjesophaler
513	Pasjesophaler en rekruteerde geldezels
520	Geldezel
521	Geldezel
524	Pasjesophaler
542	Geldezel
547	Overig
556	Geldezel
558	Geldezel
561	Geldezel
573	Geldezel
582	Pinner
607	Geldezel
614	Geldezel
620	Geldezel
632	Geldezel
642	Overig
649	Geldezel

662	Geldezel
672	Geldezel
679	Pinner
689	Geldezel
694	Geldezel
698	Pasjesophaler
699	Geldezel
704	Pasjesophaler
705	Geldezel
710	Geldezel
711	Geldezel
720	Beller
723	Pinner
729	Geldezel
734	Pasjesophaler
739	Pasjesophaler en rekruteerde geldezels
749	Geldezel
764	Pinner
765	Geldezel
768	Pasjesophaler
773	Pasjesophaler
778	Geldezel
797	Geldezel
801	Geldezel

Bijlage VI – Analyse kenmerken buitenlandse verdachten en Nederlandse verdachten in netwerk 1, 2 en 3

Zie *Lanser_SPSS_file _analyse_lonewolf_all_isolates_dyads&others.sav*

Leeftijd – buitenlandse verdachten

SYNTAX

```
DATASET ACTIVATE DataSet3.
USE ALL.
COMPUTE filter_$=(Afkomst = 1).
VARIABLE LABELS filter_$ 'Afkomst = 1 (FILTER)'.
VALUE LABELS filter_$ 0 'Not Selected' 1 'Selected'.
FORMATS filter_$ (f1.0).
FILTER BY filter_$.
EXECUTE.

DESCRIPTIVES VARIABLES=Leeftijd
  /STATISTICS=MEAN STDDEV MIN MAX.
```

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Leeftijd	7	25	58	34,71	10,920
Valid N (listwise)	7				

Geslacht – buitenlandse verdachten

SYNTAX

```
FREQUENCIES VARIABLES=Geslacht_code
  /STATISTICS=STDDEV MINIMUM MAXIMUM MEAN MEDIAN
  /ORDER=ANALYSIS.
```

Geslacht

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	,00	7	87,5	87,5	87,5
	1,00	1	12,5	12,5	100,0
	Total	8	100,0	100,0	

Delictverleden – buitenlandse verdachten

SYNTAX

```
FREQUENCIES VARIABLES=Delictverleden
  /STATISTICS=STDDEV MINIMUM MAXIMUM MEAN MEDIAN
  /ORDER=ANALYSIS.
```

Delictverleden

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	6	75,0	75,0	75,0
	2	1	12,5	12,5	87,5
	3	1	12,5	12,5	100,0
	Total	8	100,0	100,0	

Leeftijd – Nederlandse verdachten

SYNTAX

```
USE ALL.
COMPUTE filter_$=(Afkomst = 0).
VARIABLE LABELS filter_$ 'Afkomst = 0 (FILTER)'.
VALUE LABELS filter_$ 0 'Not Selected' 1 'Selected'.
FORMATS filter_$ (f1.0).
FILTER BY filter_$.
EXECUTE.

DESCRIPTIVES VARIABLES=Leeftijd
  /STATISTICS=MEAN STDDEV MIN MAX.
```

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Leeftijd	668	13	74	28,24	11,105
Valid N (listwise)	668				

Geslacht – Nederlandse verdachten

SYNTAX

```
FREQUENCIES VARIABLES=Geslacht_code
  /STATISTICS=STDDEV MINIMUM MAXIMUM MEAN MEDIAN
  /ORDER=ANALYSIS.
```

Geslacht

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	man	636	80,1	80,7	80,7
	vrouw	152	19,1	19,3	100,0
	Total	788	99,2	100,0	
Missing	System	6	,8		
Total		794	100,0		

Delictverleden – Nederlandse verdachten

```
SYNTAX
FREQUENCIES VARIABLES=Delictverleden
  /STATISTICS=STDDEV MINIMUM MAXIMUM MEAN MEDIAN
  /ORDER=ANALYSIS.
```

Delictverleden

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	279	35,1	35,1	35,1
	1	407	51,3	51,3	86,4
	2	32	4,0	4,0	90,4
	3	76	9,6	9,6	100,0
	Total	794	100,0	100,0	