Criminele netwerken achter geldezels

Rapportage deel 1: verkenning

let's change
YOU. US. THE WORLD.

DE HAAGSE HOGESCHOOL

Criminele netwerken achter geldezels

Rapportage deel 1: verkenning

Een verkennend onderzoek naar de aard van cybercriminele netwerken achter geldezeldelicten en aangrijpingspunten voor de aanpak ervan

Luuk Bekkers MSc

Merel van Leuken MSc

Prof.dr. Rutger Leukfeldt

Lectoraat Cybercrime & Cybersecurity,
NSCR & De Haagse Hogeschool; in opdracht
van en in samenwerking met de regiegroep
Operatie Centurion van de Nationale Politie

POLITIE

1 Inleiding

1.1 Aanleiding

De maatschappij digitaliseert in rap tempo. Doordat het sociale en zakelijke verkeer steeds meer online plaatsvindt, ontwikkelt criminaliteit zich ook langs die weg. Steeds meer mensen worden slachtoffer van gedigitaliseerde vormen van criminaliteit, zoals hacken, phishing, en aan- en verkoopfraude, terwijl traditionele criminaliteit afneemt. In 2021 werden bijna 2,5 miljoen Nederlanders slachtoffer van cybercriminaliteit en de zelf-gerapporteerde schade loopt op tot wel honderden miljoenen euro's (CBS, 2022a; 2022b), of zelfs in de miljarden (Junger et al., 2022).

Deze trends en ontwikkelingen hebben verregaande implicaties voor de rechtshandhaving en het takenpakket van de politie. Zij hebben namelijk de uitdaging om op te treden tegen criminelen die hun activiteiten inmiddels volledig of gedeeltelijk online uitvoeren, en dat vergt soms een andere aanpak in de preventie, opsporing, en vervolging. Om de politie en diens ketenpartners te ondersteunen in die aanpak, is kennis nodig over hoe cybercriminaliteit wordt uitgevoerd.

Eerder onderzoek heeft al een aantal inzichten opgeleverd. Zo werken criminelen zelden alleen en geldt dat ook voor financieel gemotiveerde cyberdaders. Behalve personen met technische vaardigheden zijn ook personen vereist die bepaalde diensten verlenen. Bijvoorbeeld het versturen van grote hoeveelheden e-mails of het overtuigen van potentiële slachtoffers. Tevens zijn personen nodig die zich bezighouden met het cashen van crimineel verdiend geld of het verplaatsen en witwassen hiervan (Leukfeldt et al, 2017; Leukfeldt & Holt, 2019). Gezamenlijk vormen deze personen het criminele netwerk (Bekkers, Schiks & Leukfeldt, 2020).

Een belangrijke stap binnen het crime script van financieel gemotiveerde cyberdelicten is het wegsluizen en witwassen van de online verkregen illegale inkomsten. Met als doel het financiële spoor van een delict te verbergen, maken cybercriminelen vaak gebruik van geldezels – ook wel katvangers of money mules genoemd. Een geldezel is iemand die al dan niet bewust zijn of haar bankrekening laat gebruiken voor criminele doeleinden (Aston et al., 2009; Arevalo, 2015; Custers et al., 2019; Odinot et al., 2018; Oerlemans et al., 2016). Er is nog weinig onderzoek gedaan naar geldezels. Internationale literatuur ontbreekt vrijwel geheel. Het handjevol Nederlandse onderzoeken laat zien dat het een heterogene groep betreft, maar dat er personen betrokken zijn die makkelijker te beïnvloeden zijn, zoals nieuwkomers in het land, werklozen, mensen met schulden, een drugsverslaving of licht verstandelijke beperking. In sommige gevallen is ook sprake van druk, manipulatie of dreiging met geweld (Bekkers et al., 2020; Bekkers & Leukfeldt, 2022; Galdo et al., 2019; Leukfeldt, 2014).

Ondanks dat geldezels als individu wellicht minder interessant lijken dan bepaalde facilitators die de criminele netwerken van unieke diensten voorzien, zijn geldezels als groep wel degelijk van groot belang voor het functioneren van financieel gemotiveerde cyberdaders. Ze vormen een onmisbare schakel in het wegsluizen van wederrechtelijk online verkregen geld. Bijkomend voordeel is dat geldezels, in tegenstelling tot personen uit hogere lagen van het criminele netwerk, zich veelal in Nederland bevinden, en door het gebruik van hun bankrekening relatief eenvoudig op te sporen zijn.

De opsporing van criminele netwerken achter de geldezels staat echter nog in de kinderschoenen. Er is weinig zicht op het criminele netwerk dat zich achter het delict bevindt (Bekkers et al., 2020). Doordat het geld van slachtoffers meestal direct op de rekening van geldezels wordt gestort, blijven de daadwerkelijke daders uit het zicht van de politie en financiële instellingen. Voor een effectieve en integrale aanpak van cybercriminaliteit is vereist om meer zicht te krijgen op deze cybercriminele netwerken.

1.2 Het huidige onderzoek

Dit onderzoek heeft tot doel het in kaart brengen van de aard van de criminele netwerken achter geldezeldelicten, om daarmee concrete aangrijpingspunten te identificeren voor zowel de preventie, verstoring als opsporing van deze criminele netwerken. Hiermee kan worden voorzien in de behoefte aan een effectieve, integrale aanpak van zowel cybercrime als gedigitaliseerde criminaliteit.

Binnen dit onderzoek staat de volgende onderzoeksvraag centraal:

Wat kenmerkt de cybercriminele netwerken die verantwoordelijk zijn voor geldezeldelicten en wat zijn aangrijpingspunten voor de aanpak van deze cybercriminele netwerken?

Ter beantwoording van deze onderzoeksvraag zijn zes deelvragen opgesteld, te weten:

1. Bij welke vormen van cybercriminaliteit worden geldezels ingezet?
2. Wat is de aard van de delicten waarmee de cybercriminele netwerken zich bezighouden?
   a. Welke delicten plegen de leden van de cybercriminele netwerken? In hoeverre is er sprake van specialisme?
   b. Welke modus operandi hanteren de cybercriminele netwerken in de uitvoering van deze verschillende delicten? Welke crime scripts kunnen worden onderscheiden?
3. Wat zijn de kenmerken van de cybercriminele netwerken die geldezels inzetten?
   a. Uit hoeveel leden bestaan de cybercriminele netwerken?
   b. Wat zijn de kenmerken van de individuele leden van cybercriminele netwerken (demografisch, ICT kennis/vaardigheden, criminele carrières)?
   c. Welke rollen kunnen binnen de cybercriminele netwerken worden geïdentificeerd?
   d. Op welke wijze zijn de cybercriminele netwerken (hiërarchisch) georganiseerd? Op welke wijze zijn de leden aan elkaar gerelateerd?
   e. Hoe en wanneer zijn de cybercriminele netwerken ontstaan? Hoe worden nieuwe leden geworven? Van welke ontmoetingsplaatsen maken cybercriminele netwerken gebruik? Wat is de duur van de cybercriminele activiteiten?
   f. In hoeverre is sprake van contact met andere (cyber) criminele groeperingen of daders en met wettige ondernemingen, rechtspersonen, overheidsfunctionarissen en externe deskundigen/specialisten? Indien aanwezig, wat is de aard van deze contacten?
   g. In hoeverre is er sprake van geweld binnen het netwerk of andere criminele netwerken?
4. Op welke wijze worden geldezels ingezet in de cybercriminele netwerken?
   a. Welke rol spelen geldezels binnen de MO/het crime script? Bestaan hierbij verschillen tussen de delicttypen?
   b. Hoeveel geldezels worden ingezet?
   c. Wat zijn de kenmerken van de individuele geldezels (demografisch, ICT kennis/vaardigheden, criminele carrières)?
   d. Welke rollen kunnen binnen het geldezelnetwerk worden geïdentificeerd?
   e. Op welke wijze is het geldezelnetwerk (hiërarchisch) georganiseerd? Op welke wijze zijn de leden aan elkaar gerelateerd?
   f. Hoe en waar worden nieuwe geldezels geworven?
   g. In hoeverre is er sprake van geweld bij het ronselen en inzetten van geldezels?
5. Hoe ziet de aanpak van cybercriminele netwerken die geldezels inzetten er momenteel uit?
   a. Wat houdt de huidige Nederlandse aanpak van cybercriminaliteit in? In hoeverre en op welke wijze wordt ingezet op preventie, verstoring en opsporing? Wordt hierbij onderscheid gemaakt tussen geldezels en andere leden van het cybercriminele netwerk? Op welke wijze worden cyberzaken afgedaan, strafrechtelijk of anderszins?
   b. Welke actoren zijn betrokken bij de huidige aanpak van cybercriminele netwerken die geldezels inzetten en welke rol vervullen zij hierbij?
   c. Wat is bekend over de aanpak van cybercriminele netwerken die geldezels inzetten buiten Nederland?
   d. Welke *good practices* en verbetermogelijkheden kunnen geïdentificeerd worden in de (inter)nationale aanpak van cybercriminele netwerken die geldezels inzetten?
6. Waar binnen het crime script (onderzoeksvraag 1-4) zitten effectieve aangrijpingspunten voor zowel preventie, verstoring als opsporing van cybercriminele netwerken? Hoe zien deze aangrijpingspunten er uit en welke actoren zijn hiervoor verantwoordelijk?

Het onderzoek is opgedeeld in twee fasen. Een verkennende fase en een verdiepende fase. Het rapport dat voor u ligt doet verslag van de verkennende fase. In deze fase schetsen we een eerste beeld op basis van literatuuronderzoek, expertinterviews en een focusgroep. In de verdiepende fase doen we vervolgens een verdiepende kwalitatieve analyse van afgeronde opsporingsonderzoeken naar criminele netwerken die geldezels inzetten en eventuele verdiepende kwantitatieve analyses. Dit rapport geeft daarom nog niet antwoord op alle geformuleerde onderzoeksvragen.

2 Methodische verantwoording

In dit hoofdstuk beschrijven we de methoden die zijn toegepast om de onderzoeksvragen te beantwoorden. Zoals in hoofdstuk 1 al beschreven is dit onderzoek verdeeld in twee fasen en doet dit rapport verslag van de eerste verkennende fase. We hebben voor deze rapportage gebruik gemaakt van literatuuronderzoek, expertinterviews en een focusgroep. Het gebruik van verschillende methodieken (i.e. triangulatie) biedt een oplossing voor de beperkingen van de afzonderlijke methoden, en hierdoor zijn we in staat om bestaande kennis te spiegelen aan nieuwe ontwikkelingen in de praktijk.

2.1 Gehanteerde definities en categorieën

Cybercriminaliteit omvat 'alle misdrijven waarbij informatie- en communicatietechnologie (ICT) van wezenlijk belang is voor de realisatie van het delict'. Daarbinnen worden twee categorieën onderscheiden: misdrijven waarbij ICT uitsluitend het middel is ("oude wijn in nieuwe flessen", denk aan fraude via internet) en misdrijven waarbij ICT zowel het middel als het doel is (denk aan hacking en malware). De eerste categorie wordt veelal 'cybercrime in ruime zin' of 'gedigitaliseerde criminaliteit' genoemd. De tweede categorie is 'cybercrime in enge zin', maar wordt ook wel 'high tech crime' of 'cybercrime' genoemd. In dit voorstel gebruiken we cybercriminaliteit als paraplubegrip en dus niet als verwijzing naar 'cybercrime in enge zin'. Zowel cybercriminele netwerken die zich bezighouden met gedigitaliseerde criminaliteit als cybercriminele netwerken die cybercrime in enge zin plegen zijn dus onderwerp van dit onderzoek. De keuze om het begrip cybercriminaliteit te gebruiken, is gemaakt omwille van de leesbaarheid, maar ook – en belangrijker – vanwege de verwevenheid tussen de delictscategorieën. Bij online oplichting (gedigitaliseerde criminaliteit) kan bijvoorbeeld ook sprake zijn van hacken of het gebruik van malware (cybercrime in enge zin) om de fraude te kunnen plegen. Vetrekpunt binnen dit onderzoek zijn dan ook de geldezels en niet de netwerken die geldezels inzetten. Door de geldezels als vertrekpunt te nemen zullen cybercriminele netwerken die zich met diverse vormen van financieel-gemotiveerde criminaliteit bezighouden in dit onderzoek worden meegenomen.

2.2 Literatuuronderzoek

Het literatuuronderzoek is uitgevoerd in de periode april 2023 tot en met juni 2023. Er is gebruik gemaakt van een non-systematisch narratieve benadering, wat wil zeggen dat de onderzoekers zelf hebben beoordeeld welke studies werden geselecteerd en geanalyseerd. Om te beginnen is in samenspraak met het projectteam een verzameling Nederlandstalige en Engelstalige zoektermen samengesteld (zie Tabel 1). Deze zoektermen zijn in eerste instantie stapsgewijs gebruikt op Google Scholar en andere zoekmachines waar wetenschappelijke publicaties gevonden kunnen worden (e.g. PsycInfo). Daarnaast hebben de onderzoekers met de "sneeuwbalmethode" in de referentielijst van de reeds gevonden artikelen gezocht naar eventueel ontbrekende studies die aansluiten op het onderwerp. Voor sommige onderwerpen is aanvullend literatuuronderzoek verricht ter verdieping en aanvulling. Dit betreffen vooral artikelen die niet direct gerelateerd zijn aan het onderwerp geldezels of cybercriminele netwerken, maar die ondersteunend waardevolle informatie bevatten over de geïdentificeerde topics. Uiteindelijk zijn artikelen voor dit literatuuronderzoek geselecteerd op basis van de relevantie van het artikel voor de onderzoeksvragen, de empirische en methodische waarde van het onderzoek en de algemene kwaliteit.

Tabel 1. Overzicht zoektermen en aantal relevante nieuwe hits

Zoekterm	Aantal relevante nieuwe hits
Geldezels	6
Daders cybercriminaliteit	-
Witwassen cybercriminaliteit	1
Aanpak cybercriminaliteit	3
Cybercriminele netwerken	2
Money mules	28
Cybercriminal networks	7
Organised cybercrime	1
Crime script cybercrime	1
Cybercrime prevention	-
Money laundering cybercrime	1
Cybercriminal behavior	1
Andere databases	-
Snowballing	6

Het selectieproces en een eerste analyse van de gevonden artikelen wees uit dat de relevante literatuur in grofweg zes categorieën is in te delen: 1) geldezeldelicten, 2) netwerk structuur, 3) criminele activiteiten, 4) ontstaan en groei van het netwerk, 5) individuele kenmerken van netwerkleden, en 6) aanpak.

In het algemeen valt op dat de bestaande literatuur over cybercriminele netwerken en geldezels zich voornamelijk richt op de rol, positie en taken van leden van een cybercrimineel netwerk en dat dit onderzoek veelal is uitgevoerd in Nederland. Onderzoek is vooral gebaseerd op analyse van al bestaande bronnen en literatuur. Hoewel momenteel vooral (n)etnografisch onderzoek en analyse van opsporingsonderzoeken waardevolle inzichten biedt, is sprake van een gebrek aan onderzoek met een sterk empirisch karakter.

2.3 Interviews

2.3.1 Procedure

De interviews zijn afgenomen in de periode mei 2023 tot en met augustus 2023 door de eerste en/of tweede auteur van dit onderzoeksverslag. De interviews waren semigestructureerd, wat wil zeggen dat de onderzoekers op voorhand een topiclijst hebben ontwikkeld als centrale leidraad tijdens het interview, maar dat ze ook vrij waren om andere onderwerpen te verkennen die tijdens het interview aan bod kwamen. Op deze manier helpen interviews om onbekende of subjectieve fenomenen te begrijpen vanuit het perspectief van de respondent, zoals attitudes, ervaringen en gedragingen (Rowley, 2012; Kvale, 2008). Aanvullend op de interviews heeft een focusgroep plaatsgevonden met medewerkers van banken en politie die zijn aangesloten bij het publiek-private samenwerkingsverband Electronic Crimes Task Force (ECTF). Bij deze focusgroep is gebruik gemaakt van dezelfde topiclijst als bij de interviews (zie 3.1.3).

Bij aanvang van het onderzoek hebben de onderzoekers in samenspraak met het projectteam van Operatie Centurion een contactlijst opgesteld van professionals in de praktijk die vanuit verschillende invalshoeken kennis van en ervaring met geldezelproblematiek en criminele netwerken hebben. Aan de hand van deze lijst is contact gelegd met de respondenten voor dit onderzoek. Omdat de initiële werving van respondenten dus plaatsvond via het netwerk van het projectteam en de onderzoekers, is er sprake van sprake van "convenience sampling". Dit is een vorm van non-random sampling waarbij leden van een doelpopulatie worden geselecteerd omdat ze bepaalde praktische eigenschappen hebben, bijvoorbeeld met betrekking tot toegankelijkheid en beschikbaarheid (Etikan et al., 2016). Aanvullend is gebruik gemaakt van de "sneeuwbalmethode": in de interviews met de experts van de contactlijst kwamen andere experts ter sprake die nog niet waren vermeld op de initiële lijst.

Alle potentiële respondenten zijn per e-mail benaderd door de eerste of tweede auteur van dit onderzoek. Na een korte introductie en mailwisseling zijn de interviews gepland op een tijdstip en locatie naar keuze van de respondent. In drie gevallen zijn de interviews gevoerd via videobellen of telefonisch, in één geval heeft het interview fysiek op de Haagse Hogeschool plaatsgevonden, en in alle andere gevallen zijn de interviews gevoerd op de werklocatie van de respondent, evenals de focusgroep. De interviews zijn met toestemming van de respondenten opgenomen, in de meeste gevallen met een beveiligde spraakrecorder en vanwege praktische redenen in drie gevallen met een opnameapparaat zonder encryptie. De opname is naderhand uitgeschreven in de vorm van een geanonimiseerd verslag, waarna de opname direct van het opnameapparaat is verwijderd. Respondenten hebben de mogelijkheid gekregen om het interviewverslag te controleren op onjuistheden.

2.3.2 Respondenten

In navolging van het projectplan zijn in totaal 32 experts geïnterviewd in 18 interviews (n=22) en één focusgroep (n=10). Wat betreft de losse interviews waren respondent met name werkzaam bij de politie als analist, rechercheur, of teamleider (n=10) en bij het Openbaar Ministerie (n=6) als parketsecretaris, officier van justitie, of adviseur. Naast een freelance journalist, waren de overige respondenten werkzaam bij een gemeente, in de financiële sector, een gerechtsdeurwaarder, de brancheverenigingen voor bewindvoerders, en het Centrum voor Criminaliteitspreventie en Veiligheid. Binnen die organisaties vervullen de respondenten verschillende rollen, zoals beleidsadviseur, projectleider of analist. Bij de focusgroep waren in totaal 10 experts aanwezig van banken en de politie die aangesloten zijn bij de Electronic Crimes Task Force, ofwel de ECTF (de focusgroep wordt benoemd als FOCUS). Alle respondenten hebben binnen de context van hun organisatie expertise en ervaring op het gebied van geldezelproblematiek, al dan niet in combinatie met cybercriminaliteit en cybercriminele netwerken in bredere zin.

Tabel 2. Overzicht respondenten

Respondentnummer	Organisatie
RESP1	Freelancer
RESP2	Deurwaarder
RESP3	Gemeente
RESP4	Financiële sector
RESP5	Politie
RESP6	Politie
RESP7	Politie
RESP8	Politie
RESP9	Politie
RESP10	OM
RESP11	OM
RESP12	CCV
RESP13	Politie
RESP14	OM
RESP15	Politie
RESP16	Politie
RESP17	Politie
RESP18	Politie
RESP19	Bewindvoerder
RESP20	OM
RESP21	OM
RESP22	OM
FOCUS	ECTF

2.3.4 Meetinstrumenten en analyse

De onderzoekers hebben op basis van de Monitor georganiseerde criminaliteit (bijv. Kruisbergen et al., 2019), de in het onderzoeksplan geformuleerde onderzoeksvragen en de uitkomsten het literatuuronderzoek een topiclijst opgesteld dat diende als algemene leidraad tijdens het interview. De Monitor georganiseerde criminaliteit is een gevalideerd meetinstrument en wordt al jaren gebruikt om zicht te krijgen op trends en ontwikkelingen in criminaliteit dat wordt gepleegd in netwerkverband. In de topiclijst vormde de zes hoofdthema's de algemene structuur. Voorbeeldvragen betreffen *"wat is de mate van hiërarchie van criminele netwerken die geldezels gebruiken?"* en *"Bij welke vormen van cybercriminaliteit worden geldezels ingezet?"*. De volledige topiclijst is te vinden in Bijlage 1.

De analyse heeft ook plaatsgevonden aan de hand van deze zes thema's in Atlas Ti. Dit is software dat gebruikt wordt ter ondersteuning van thematische analyses. Thematische analyse wordt vaak gebruikt in kwalitatief onderzoek voor het identificeren, analyseren en rapporteren van patronen in data, en verhoogt de nauwkeurigheid van de interpretatie van de bevindingen (Braun & Clarke, 2006, 2012). Hierbij zijn de stappen gevolgd van Braun en Clarke (2006, 2012) en Vaismoradi et al. (2016). De eerste stap was om de data te coderen aan de hand van sleutelwoorden. Deze codes beschrijven kleine stukken data in de interviewtranscripten zonder directe interpretatie. In de tweede stap hebben we codes die betrekking hebben op één van de zes hoofdthema's gegroepeerd, waardoor we beter inzicht en overzicht krijgen op de data. De codes "ontmoetingsplaatsen" en "duur samenwerking" hebben bijvoorbeeld betrekking op het thema "ontstaan en groei". In de derde stap hebben auteurs onafhankelijk van elkaar gecontroleerd of er eventueel andere codes zijn die niet onder de zes thema's zijn te categoriseren, wat niet het geval was. De zes thema's dekken de data dus voldoende, en zijn gebruikt om de resultaten van dit onderzoek te beschrijven.

3 De inzet van geldezels bij verschillende vormen van cybercriminaliteit

In dit hoofdstuk komt ter sprake welke rol geldezels vervullen binnen het crime script van de verschillende delicten waarbij geldezels worden ingezet (paragraaf 3.1) en wat kenmerken zijn van de doelgroep geldezels (paragraaf 3.2). Hiermee beantwoorden we deelvraag 1 en deelvraag 4. We beschrijven de bevindingen uit het literatuuronderzoek en de interviews afzonderlijk.

3.1 De rol van geldezels in het crime script

3.1.1 Literatuuronderzoek

Het belang van geldezels (ofwel 'money mules', 'arrows', 'strawmans' en 'katvangers') voor de uitvoering van cybercriminaliteit is al vroeg erkend in de literatuur, met één van de eerste publicaties daterend uit 2006 (Dunham, 2006; Choo & Smith, 2008; Moore et al., 2009; Aston, 2009). De term geldezel verwijst naar mensen wiens bankrekening wordt gebruikt voor het wegsluizen van geld dat is verkregen door het plagen van (cyber)criminaliteit. Geld dat is gestolen door middel van financieel-gemotiveerde delicten, wordt door de daders overgemaakt van de bankrekeningen van slachtoffers naar de bankrekeningen van geldezels (Loggen & Leukfeldt, 2022; Choo, 2011; Kshetri, 2010; Smith, 2015; Raza et al., 2020; Leukfeldt et al., 2017a,b,c,d,e). Daarna wordt het geld zo snel mogelijk contant opgenomen door de kernleden, faciliteerders of geldezels zelf. In andere gevallen wordt het geld verder verhuld door bijvoorbeeld de aankoop van cryptovaluta, meerdere transacties naar andere nationale of internationale bankrekeningen, of via geldwisselkantoren (Kruisbergen et al., 2019; Smith, 2015; Sood et al., 2012; Oerlemans et al., 2016). De daders maken gebruik van deze constructie omdat zij op die manier anoniem blijven en zo uit zicht blijven van banken en opsporingsinstanties; ze gebruiken immers niet hun eigen bankrekening (Hutching, 2014). Er zijn aanwijzingen dat er tegenwoordig ook 'crypto money mules' zijn, ofwel geldezels die een cryptovaluta account onder hun beheer hebben in plaats van een eigen bankrekening. Hier is echter nog weinig wetenschappelijk onderzoek naar verricht (zie ook Kerzic, 2022; Financial Crime Academy, n.d.).

Geldezels worden ingezet voor de uitvoering van sommige vormen van financieel-economische cybercriminaliteit. Dit is een categorie delicten met een winstoogmerk, die behoren tot de meest voorkomende delicten onder burgers (CBS, 2022a). Het onderzoek dat is gedaan naar geldezels en cybercriminele netwerken richt zich daarbij voornamelijk op netwerken betrokken bij phishing en bankfraude (e.g. Leukfeldt, 2014; Leukfeldt & Jansen, 2015; Oerlemans et al., 2016; Odinot et al., 2017; Lusthaus et al., 2023). Ander onderzoek noemt ook het gebruik van geldezels bij de delicten aan- en verkoopfraude en Whatsappfraude (Bekkers et al., 2020; Lusthaus et al., 2023). Bij deze delicten worden geldezels in principe op dezelfde manier gebruikt, maar het is niet duidelijk of dezelfde geldezels voor verschillende typen delicten worden ingezet en of criminele netwerken bij elk type delict in vergelijkbare mate afhankelijk zijn van het gebruik van geldezels ten opzichte van eventuele alternatieven. Denk daarbij aan het gebruik van cryptovaluta of de directe aanschaf van luxe goederen vanuit de rekening van het slachtoffer (e.g. Oerlemans et al., 2016).

Het is bekend dat sommige netwerken honderden geldezels gebruiken, aangezien banken een maximumbedrag hanteren voor geldopnames en zij bovendien de rekening van geldezels al gauw blokkeren na melding van het slachtoffer, waar het in andere gevallen niet nodig is om geldezels te gebruiken vanwege de aard van het delict (Custers et al., 2019; Leukfeldt, 2014; Oerlemans et al., 2016). In dergelijke gevallen kopen criminelen bijvoorbeeld direct luxe producten of cryptovaluta vanuit de rekening van het slachtoffer (Oerlemans et al., 2016). Er is nog weinig bekend over het specifieke bedrag dat wordt overgemaakt van het slachtoffer naar een geldezel, maar in de meeste gevallen lijkt het te gaan om bedragen boven de 1.000 euro, met uitschieters van boven de 25.000 euro (Leukfeldt & Jansen, 2015). Het feit dat vaak veel geldezels betrokken zijn bij cybercriminaliteit, impliceert ook dat er rollen en taken zijn weggelegd bij andere individuen in het netwerk om die geldezels te rekruteren en de verzameling aan geldezels te managen, coördineren en optimaliseren (Florencio & Herley, 2010, 2012; Leukfeldt & Holt, 2022).

3.1.2 Interviews

Alle respondenten benoemen dat geldezels over het algemeen betrokken zijn bij de delicten waar Operatie Centurion van de politie zich op richt. Dat betreffen phishing, hulpvraagfraude, bankhelpdeskfraude en aan- en verkoopfraude. Volgens enkele respondenten worden geldezels ook bij alle andere vormen van fraude gebruikt waarbij op een bepaald moment een bankrekening aan bod komt, zoals datingfraude, beleggingsfraude en BEC-fraude / CEO-fraude / factuurfraude (FOCUS, RESP1, RESP5). Bij datingfraude en beleggingsfraude bijvoorbeeld gaat het vaak om geld dat afkomstig is van fraude dat in het buitenland wordt gepleegd, waarbij daders vervolgens een Nederlands slachtoffer van datingsfraude gebruiken als geldezel. Maar dit soort delicten vinden plaats via meer ingewikkelde buitenlandse constructies (RESP5) waar de respondenten van dit onderzoek zich niet direct op richten, en deze delicten zijn verder dan ook niet in detail ter sprake gekomen tijdens de interviews. Bovendien zou het vanwege de hybridisatie van criminaliteit volgens respondenten denkbaar kunnen zijn dat geldezels ook voor traditionele delicten worden ingezet, waarbij criminelen bijvoorbeeld contant geld uit de drugshandel storten op de bankrekening van een geldezel (FOCUS, RESP3, RESP12).

De meeste respondenten van banken, politie, en het OM, merken op dat de "klassieke geldezel" (i.e. gebruik van een Nederlandse bankrekening bij een traditionele bank) bij het uitvoeren van cybercriminaliteit afneemt ten opzichte van een aantal jaar geleden. Daders gebruiken volgens die respondenten steeds vaker andere methoden om ongestoord gebruik te kunnen maken van gestolen geld. Respondenten noemen daarbij het gebruik van cadeaukaarten, zakelijke bankrekeningen, online buitenlandse banken (zoals Revolut), online Nederlandse banken (zoals Bunq), cryptovaluta en de directe aanschaf van producten vanuit de rekening van het slachtoffer. Deze mogelijke trend is genoemd voor alle geldezeldelicten. Ook is volgens respondenten een ontwikkeling dat geldezels niet weten dat er op hun naam een bankrekening is geopend, bijvoorbeeld omdat ze zijn misleid tot het afstaan van gegevens die nodig zijn voor het openen van een bankrekening, zoals een foto van hun paspoort (FOCUS, RESP14, RESP18).

Volgens RESP4 gaat er per maand wel 100.000 euro aan frauduleus geld naar een bepaalde buitenlandse partij. Het is bij respondenten niet bekend of de rekeninghouder in het geval van buitenlandse banken ook een geldezel is of dat daders de rekening op hun eigen naam openen. Wel zijn volgens respondenten lokaal-georiënteerde Nederlandse dadergroepen verantwoordelijk voor het beheer van de rekening en geen buitenlandse groeperingen (FOCUS, RESP5, RESP9, RESP18). Zo noemt een politiemedewerker het voorbeeld dat geldopnames van een buitenlandse bankrekening die gebruikt was voor het plegen van aan- en verkoopfraude plaatsvonden in Amsterdam (RESP18). Ook bij Nederlandse online banken is beperkt zicht op de rekeninghouder, omdat volgens respondenten geen strenge identificatie nodig is bij het openen van een bankrekening en die ook makkelijk te omzeilen is. Uit politieonderzoek komt naar voren dat het soms wel geldezels betreffen, waar in andere gevallen het mogelijk de daders zelf zijn die bijvoorbeeld onder een vals identiteitsbewijs een rekening openen (RESP15). In het geval van cryptovaluta wijst politieonderzoek ook uit dat het soms cryptowallets van de daders zelf betreffen, en in sommige gevallen cryptowallets van geldezels (RESP20, RESP21). Deze drie methodieken zijn populair omdat ze anonimiteit bieden.

Geldezels worden mogelijk ook voor verschillende delicten tegelijk ingezet, maar die constructie is tegenwoordig niet meer houdbaar volgens respondenten aangezien banken al snel ingrijpen en de rekening dus maar korte tijd gebruikt kan worden voor een klein aantal transacties (RESP1, RESP8, RESP9). RESP1 is ook nog nooit een "kruising" tegengekomen, dus dat dezelfde geldezel gekoppeld was aan twee verschillende zaken. Respondenten spreken over het algemeen dan ook niet over een netwerk aan geldezels. Ze kennen elkaar soms wel omdat ze op dezelfde locatie zijn geronseld, maar in principe zijn het losse entiteiten die worden "in- en uitgevlogen" en de geldezels zelf vormen geen netwerk (RESP5). Volgens de focusgroep zijn geldezels echter wel onderdeel van witwasnetwerken, en die netwerken zouden voor meerdere vormen van cybercriminaliteit en traditionele criminaliteit gebruikt worden. Het geld gaat dan rond over allerlei zakelijke en particuliere bankrekeningen voordat het ergens wordt gecasht. Geldezels zouden ook geronseld worden voor het witwassen van geld uit verschillende delicten.

"Ja, dus deze groep – ronselaar en de geldezel – is uiteindelijk toepasbaar op verschillende vormen van fraude. Ze kunnen makkelijk wisselen van MO, dus welke tactiek ze toepassen om dat geld binnen te halen. Uiteindelijk zijn ze verantwoordelijk voor het kunnen opnemen van het geld via een geldezelrekening. Hoe dat geld daarop komt, dat is niet zo relevant voor deze schakel in het netwerk." – RESP1

Het aantal geldezels dat wordt ingezet door criminele netwerken verschilt en zou ook afhankelijk zijn van het schadebedrag. RESP13 noemt een politieonderzoek met 18 geldezels en vijf daders hoger in het netwerk, terwijl RESP14 betrokken was bij een zaak met 133 geldezels en vijf daders, en RESP16 en RESP17 benoemen zelfs een politieonderzoek naar vier daders van phishing die bijna 400 geldezels hadden gebruikt. Ook kan het zijn dat één geldezel meerdere bankrekeningen heeft: RESP18 noemt een casus waarbij een persoon 18 bankrekeningen had bij verschillende banken, wat cybercriminaliteit faciliteert.

Bankhelpdeskfraude
Het valt respondenten op dat, rond de zomer van 2023, met name bankhelpdeskfraude op zeer grote schaal plaatsvindt in Nederland. Dit bevestigen respondenten verspreid over het hele land van verschillende organisaties. De schadebedragen zijn bij dit delict hoog, soms boven de 200.000 euro (FOCUS). Respondenten benoemen verschillende vormen van dit delict (RESP5, RESP9, RESP13, RESP10, RESP11, RESP20, RESP21), en geldezels spelen bij enkele varianten een rol; volgens een analist gaat echter het gestolen geld slechts in circa 20% van de gevallen überhaupt naar een Nederlandse bankrekening (RESP9). Het delict begint in principe met een dader die een potentieel slachtoffer opbelt en zich daarbij voordoet als een bankmedewerker. Soms praat de dader wel uren lang met het slachtoffer om diens vertrouwen te winnen en te overtuigen dat het geld niet veilig is op hun bankrekening (RESP10, RESP11).

In een eerste variant komt vervolgens een dader thuis langs bij het slachtoffer om de bankpas op te halen, waarna ze die gebruiken om geld te pinnen of luxe producten aan te schaffen. Bij deze vorm komen in principe geen geldezels aan bod (RESP5, RESP9, RESP13). Eenmaal in het huis van het slachtoffer proberen daders soms ook andere spullen te stelen (FOCUS). In een tweede vorm zorgen de daders dat het slachtoffer zelf geld overmaakt, bijvoorbeeld naar de bankrekening of cryptowallet van een geldezel.

In een derde vorm krijgen de daders op afstand via software toegang tot de rekening van het slachtoffer, en maken ze zelf geld over naar een geldezel, of kopen ze cryptovaluta of luxe goederen vanuit de rekening van het slachtoffer. RESP20 en RESP21 van het OM observeren dat het fysiek ophalen van bankpassen steeds minder vaak voorkomt omdat dat meer risico met zich meebrengt, terwijl de focusgroep benoemt dat dit momenteel wel de meest voorkomende vorm is. RESP20 en RESP21 benoemen ook dat er tijdens de uitvoering van het delict online contact blijft tussen geldezels en de dader, om te controleren of het geld al is ontvangen. Volgens de focusgroep is er soms ook sprake van slachtoffers van onder meer bankhelpdeskfraude die zelf worden ingezet als geldezel. Hierbij krijgen criminelen het slachtoffer zover dat ze een cryptowallet aanmaken of een bankrekening openen, waar de criminelen dus zelf ook toegang toe hebben. Vervolgens maakt het slachtoffer geld over naar die nieuwe rekening of cryptowallet, of gebruiken criminelen de bankrekening voor andere delicten.

Hulpvraagfraude
Hulpvraagfraude (ook wel vriend-in-nood-fraude of Whatsapp-fraude genoemd) berust volgens respondenten sterk op het gebruik van geldezels; criminelen kiezen hierbij meestal voor geldezels in plaats van andere methoden. Schadebedragen variëren hierbij van circa 1000 tot 1.500 euro per slachtoffer (RESP2).

"Whatsappfraude is de meest voorkomende vorm van geldezelproblematiek. (...). Als het Whatsappfraude is, is het aannemelijk dat er een geldezel bij betrokken is geweest. We hebben zo'n 250 zaken doorgelopen dus op een gegeven moment neem je dat aan." – RESP2

Respondenten geven aan dat doordat de overheid heeft ingezet op interventie en slachtoffers weerbaarder zijn, Nederlandse dadergroepen zich nu richten op buitenlandse slachtoffers, met name in Duitsland (RESP7, RESP8, RESP9, RESP10, RESP11, RESP15). Daar is bewijs voor aangetroffen bij in beslag genomen telefoons (RESP9), en een politiemedewerker benoemt dat ze bij huiszoekingen soms wel honderden buitenlandse SIM-kaarten en Duitse belscripts vinden (RESP15). Volgens die respondenten gebruiken daders bij dit delict vooral Bunq-rekeningen, waarbij het ook mogelijk is om een buitenlandse rekening te koppelen aan het account. Het is volgens RESP15 niet duidelijk of die op naam staat van Nederlandse of buitenlandse geldezels, maar deze respondent benoemt wel een zaak waarbij het Belgische geldezels betroffen die waren geronseld door Nederlandse dadergroepen.

"Wij zijn nu bezig, onbewust, omdat wij hier gewoon betere awareness hebben, met het pushen van criminelen naar België en Duitsland. Het zijn dezelfde gasten, dat kun je ook gewoon zien als je ze op social media volgt, waar ze op dat moment hun Snapchat-locatie delen. Die gaan dan voor midweekje naar België of Duitsland. Die vragen dan ook om Belgische en Duitse pinpassen, dus ze ronselen lokaal. (....)." – RESP1

Phishing
Hoewel phishing ook een middel kan zijn om een ander delict te plegen, zoals het verkrijgen van toegang tot computersystemen om die te infecteren met ransomware, komt slachtofferschap van phishing volgens respondenten minder voor dan voorheen, met name de vorm waarbij phishing-mails uit naam van een bank worden gestuurd (FOCUS). De focusgroep wijt dit aan verbeterde detectiesystemen van banken. Slachtofferschap van phishing namens andere partijen, zoals postkantoren, komt vaker voor. Het schadebedrag per slachtoffer is volgens respondenten bij phishing veel kleiner dan bij bankhelpdeskfraude en er worden niet altijd geldezels ingezet (FOCUS, RESP9, RESP16, RESP17). Sommige daders handelen zelfs alleen en maken geld over van het slachtoffer naar hun eigen bankrekening (RESP16, RESP17). Deze respondenten noemen het voorbeeld van een minderjarige jongen die in vakantieperiode uit verveling een phishing-kit had aangeschaft en slachtoffers geld afhandig had gemaakt. Bovendien kiezen criminelen bij phishing ook voor alternatieven voor geldezels (FOCUS, RESP9), zoals de directe aanschaf van producten, en kan het een middel zijn om persoonlijke informatie van slachtoffers te verkrijgen voor de uitvoering van een ander delict, zoals bankhelpdeskfraude (FOCUS, RESP6).

"Bij phishing gaat dat ook alle kanten op, waar het geld naartoe gaat." – RESP9

RESP16 en RESP17 benoemen wel een politieonderzoek waarbij tot wel 400 geldezels gekoppeld waren aan een dadergroep die was opgepakt voor onder meer phishing, hoewel dit wel een wat oudere zaak betrof. Ten slotte benoemt de focusgroep dat dadergroepen die zich bezig houden met phishing n zich mogelijk ook verplaatsen naar het buitenland (FOCUS).

Aan- en verkoopfraude
Dit delict bestaat volgens RESP18 van het LMIO uit drie specifieke verschijningsvormen: oplichting via handelsplaatsen, oplichting via sociale media, en webwinkelfraude. Webwinkelfraude zou volgens respondenten sterk toenemen, terwijl handelsplaatsfraude afneemt en oplichting via sociale media stabiel blijft maar relatief weinig voorkomt (RESP18). Hoewel het gemiddelde schadebedrag volgens de respondenten rond de 350 euro ligt, zijn er ook uitschieters tot wel 200.000 euro. Voor de coronaperiode, bleek uit analyse van het LMIO en uit verklaringen van verdachten dat daders van handelsplaatsfraude relatief vaak hun eigen rekening gebruiken in plaats van geldezels (RESP13, RESP18). In andere gevallen is er mogelijk wel sprake van geldezels. Volgens RESP18 is dat het geval als verschillende bankrekeningen waar aangifte tegen is gedaan voor handelsplaatsfraude geclusterd zijn binnen een bepaalde regio, wat er op zou kunnen wijzen dat daar op dezelfde locatie of in hetzelfde gebied geldezels zijn geronseld. Volgens een analist bij de politie worden bij handelsplaatsfraude zelfs bijna altijd geldezels gebruikt (RESP9). Sinds de coronaperiode is de trend echter dat daders van handelsplaatsfraude gebruik maken van buitenlandse bankrekeningen, zo benoemt een medewerker van het LMIO. Die bankrekeningen worden over langere tijd gebruikt dan het geval was bij de klassieke geldezel. Bij webwinkelfraude maken slachtoffers geld over via payment service providers (PSP's). De webwinkel is namelijk gekoppeld aan een KvK-inschrijving en dus aan zakelijke bankrekeningen, waarbij de identiteit van een katvanger wordt gebruikt in plaats van een geldezelrekening. Ook hierbij ziet het LMIO vooral het gebruik van buitenlandse PSP's, waardoor er geen zicht is op de identiteit van de katvanger. De focusgroep benoemt ook dat het gebruik van zakelijke bankrekeningen een rol speelt bij de uitvoering van cybercriminaliteit.

3.2 De kenmerken van geldezels

3.2.1 Literatuuronderzoek
Als we kijken naar individuele kenmerken van geldezels, dan is het onderzoek daarnaar helaas beperkt. Uit de onderzoeken die gedaan zijn kan wel voorzichtig worden geconcludeerd dat geldezels een zeer diverse groep betreft, waarin over het algemeen alle lagen uit de maatschappij zijn vertegenwoordigd; van jong tot oud, van een lage sociaaleconomische status tot welvarende mensen, van 'first-offenders' tot 'draaideurcriminelen'. Toch zijn er een aantal kenmerken te onderscheiden die vaker naar voren komen in de literatuur en een rode draad vormen binnen deze heterogene doelgroep (Custers et al., 2019; Bekkers et al., 2020, 2022, 2023; Europol, 2021; Arevalo, 2015; Oerlemans et al., 2016; Wissink & Quint, 2021; Aston et al., 2009; Leukfeldt & Jansen, 2015; Leukfeldt & Kleemans, 2019; Bekkers & Leukfeldt, 2023).

Ondanks dat er geen duidelijk profiel is, blijkt uit onderzoek wel dat er indicaties zijn dat het deels om kwetsbare mensen gaat die 'makkelijk' te beïnvloeden zijn. Denk aan nieuwkomers in het land, werklozen, maar ook mensen met schulden of weinig financiële middelen, drugsverslaving en psychische klachten (Custers et al., 2019; Bekkers et al., 2020; Europol, 2021; Arevalo, 2015; Oerlemans et al., 2016). Verder blijken geldezels bijvoorbeeld relatief vaak uit achterstandswijken met een lage sociaaleconomische status te komen en hebben vaker een lager opleidingsniveau (Oerlemans et al., 2016; Wissink & Quint, 2021; Arevalo, 2015; Custers et al., 2019). Dit wijst erop dat geldezels dikwijls handelen vanuit financiële motieven. Daarnaast is een vrij consistente observatie dat mannen vaker worden geronseld dan vrouwen (Bekkers et al., 2020; Wissink & Quint, 2021; Aston et al., 2009; Arevalo, 2015).

Verder valt op dat het merendeel van geldezels jongere mensen betreft (Arevalo, 2015; Aston et al., 2009; Oerlemans et al., 2016; Leukfeldt & Jansen, 2015). Onder een steekproef van 686 geïdentificeerde geldezels in Australië, was de leeftijdsgroep 15 tot 34 jaar oververtegenwoordigd (Aston et al., 2009). Vergelijkbare resultaten zijn gevonden in Nederland: geldezels zijn voornamelijk jongvolwassen tussen de 18 en 24 jaar (Oerlemans et al., 2016; Leukfeldt & Jansen, 2015). Dit komt mogelijk doordat jongeren relatief beïnvloedbaar zijn, eerder risico's nemen, gevoelig zijn voor het verdienen van geld en status en bovendien toegankelijk voor ronselaars (e.g. Boyer, 2006; Bekkers et al., 2020, 2022, 2023). Vooral personen ouder dan 18 jaar zouden in trek zijn, omdat zij over het algemeen hogere banklimieten hebben met minder restricties, waardoor ze hogere bedragen kunnen verwerken (Roks & Monshouwer, 2020; Bekkers & Leukfeldt, 2023). Uit beschrijvend onderzoek onder een grote groep Nederlandse jongeren komt naar voren dat tot wel 10% eens door ronselaars benaderd is (Bekkers et al., 2023). In totaal zegt minder dan 1% ook geldezel te zijn geweest.

Dit aantal is wat lager dan andere studies vermoeden, aangezien in het onderzoek van Bekkers et al. (2022) tot wel 3% van de Nederlandse jongeren klikt op een ronseladvertentie op Instagram en een vergelijkbaar percentage van een groep ICT-studenten in het onderzoek van Weulen-Kranenbarg et al. (2022) aangeeft geldezel te zijn geweest.

3.2.2 Interviews

Respondenten benoemen dat geldezels een heterogene doelgroep zijn, waarbij bepaalde eigenschappen of groepen mensen wel oververtegenwoordigd lijken. De rode draad hierbij is dat geldezels volgens vrijwel alle respondenten vaak kwetsbare personen betreffen, waaronder daklozen, verslaafden, mensen onder bewind, arbeidsmigranten/nieuwkomers, en mensen met schulden en lvb-problematiek, afkomstig uit wijken met een lage sociaaleconomische status en multi-problematiek. Oost-Europese arbeidsmigranten/ nieuwkomers betreffen onder meer Oekraïense vluchtelingen die de Nederlandse taal niet machtig zijn en niet goed begrijpen hoe het in Nederland werkt omtrent bankrekeningen, zo stellen respondenten (FOCUS, RESP18). Wel stellen respondenten dat het niet altijd gaat om kwetsbare personen die worden misleid, maar ook bijvoorbeeld jongeren die bewust meewerken en doorgroeien in de criminaliteit (RESP2, RESP5, RESP6)

Volgens respondenten zijn geldezels relatief vaak jonge mensen, die de consequenties van hun gedrag nog niet goed kunnen overzien (FOCUS, RESP1, RESP3, RESP4, RESP5, RESP6, RESP7, RESP8, RESP14, RESP18, RESP19). Het zijn scholieren die opportunistisch handelen om snel geld te verdienen. Soms staan de rekeningen waarmee fraude wordt gepleegd op naam van kinderen van 0 tot 12 jaar, maar dat betreffen dan ouders die de rekening van hun kind gebruiken (RESP18). Er zijn echter ook oudere geldezels, dat zijn dan bijvoorbeeld verslaafden, daklozen en/of veelplegers die al bekend zijn in het criminele circuit en ook andere delicten op hun naam hebben (RESP6). Ook mannen en laagopgeleiden lijken oververtegenwoordigd (RESP1, RESP2, RESP3, RESP5, RESP16, RESP17, RESP20, RESP21), maar vrouwen komen ook zeker voor (RESP20, RESP21). Hoewel ze niet altijd bewust zijn van wat er gebeurd met de bankrekening, handelen geldezels dus wel vaak omdat ze snel geld willen verdienen (FOCUS, RESP5, RESP7, RESP8, RESP13, RESP16, RESP17, RESP20, RESP21).

"Bij de jonge mensen zijn het toch vaak wel scholieren die dat doen. Als je kijkt naar de jonge mensen, scholieren, maakt het niet eens uit of ze schulden hebben. Die gaan echt puur af op het idee van makkelijk geld verdienen." – RESP13

Resumé

Geldezels spelen een rol bij de uitvoering van verschillende vormen van financieel-economische cybercriminaliteit. Dat betreffen de delicten bankhelpdeskfraude, hulpvraagfraude, phishing en aan- en verkoopfraude. Deze delicten vormen de afbakening van het huidige onderzoek. Ook zouden geldezels mogelijk worden ingezet voor meer complexe, internationale delicten, zoals datingfraude en CEO-fraude, maar daar is minder zicht op bij respondenten en in de literatuur. Momenteel heeft de politie vooral te maken met bankhelpdeskfraude, terwijl dat voorheen voornamelijk phishing en hulpvraagfraude waren. Mogelijk hebben Nederlandse dadergroeperingen zich hierbij verplaatst naar het buitenland. Criminelen kiezen niet alleen voor geldezels om geld weg te sluizen, maar ook voor de directe aanschaf van producten of cadeaukaarten vanuit de bankrekening van het slachtoffer, zakelijke bankrekeningen / PSP's, cryptovaluta, online buitenlandse bankrekeningen of online Nederlandse bankrekeningen. Deze witwasmethodieken zijn benoemd door respondenten en waren grotendeels eerder ook al beschreven in de literatuur, echter is er mogelijk een ontwikkeling waarbij het gebruik van geldezels afneemt en criminelen vaker toevlucht zoeken bij alternatieven. Het is mogelijk dat geldezels ook daarbij een rol spelen, omdat ze bijvoorbeeld cryptowallets of online bankrekeningen op naam hebben, maar daar is nog weinig zicht op vanwege beperkte toegang tot persoonlijke gegevens van de rekeninghouders. Hierbij onderstrepen respondenten het belang van katvangers in bredere zin, aangezien er ook mensen nodig zijn voor het bezorgen of ophalen van bestelde producten, het op naam zetten van valse webshops, en het pinnen van het gestolen geld. Verder is duidelijk dat geldezels een heterogene groep vormen wat betreft persoonlijke eigenschappen. De rode draad is dat het vaak, maar niet altijd, gaat om kwetsbare individuen die relatief makkelijk te beïnvloeden zijn. Dit betreffen jongeren die de consequenties van hun gedrag niet goed kunnen overzien, maar ook daklozen, verslaafden, en Oost-Europese arbeidsmigranten. De meeste respondenten zijn ten slotte van mening dat geldezels geen onderling netwerk vormen, en dat ze ad hoc in een netwerk terecht komen. De focusgroep benoemt echter dat geldezels wel onderdeel zijn van witwasnetwerken die voor allerlei delicten worden ingezet, zowel voor traditionele criminaliteit als cybercriminaliteit.

4 De aard van de delicten waarmee cybercriminele netwerken zich bezighouden

In dit hoofdstuk staat deelvraag 2 centraal, namelijk de aard van de delicten waar cybercriminele netwerken zich op richten. Meer specifiek gaan we in op de activiteiten en modus operandi van criminele netwerken, criminele carrières van leden, en de mate van specialisme en diversiteit in het plegen van delicten.

4.1 Literatuuronderzoek

De literatuur maakt duidelijk dat cybercriminele netwerken verschillen in hun specifieke activiteiten, criminele carrières en delictspecialisaties. Wat betreft de mate van technologische volwassenheid bij het plegen van delicten, wordt ook wel gesproken van "low-tech allrounders", ofwel netwerken die bij een grote variatie aan delicten betrokken zijn en weinig technologische middelen gebruiken en dus ook weinig kennis hebben van of affiniteit hebben met IT, tegenover "high-tech specialists", refererend naar netwerken die door middel van een specifieke handelswijze, zoals hackers of complexe malware, slachtoffers geld afhandig maken (Leukfeldt et al., 2019; Leukfeldt et al., 2017b; Leukfeldt & Jansen, 2015). Zo bleek uit politiegegevens dat een cybercrimineel netwerk in Engeland bestond uit voornamelijk hackers onder de 18 jaar (Lusthaus et al., 2023). Een andere zaak betrof juist een netwerk die de auteurs karakteriseren als onprofessioneel en van een laag niveau. Het is dan ook niet nodig dat criminele netwerken die technische kennis zelf in huis hebben om een delict uit te voeren, aangezien deze kennis ook online kan worden ingekocht (Leukfeldt et al., 2019), buiten dat cybercriminaliteit mogelijk sowieso minder technisch wordt in uitvoering (Loggen & Leukfeldt, 2022).

Sommige netwerken richten dus zich enkel op het plegen van cybercriminaliteit, waar andere netwerken zich generaliseren naar zowel cybercriminaliteit als traditionele criminaliteit zoals inbraken en drugshandel (Leukfeldt & Holt, 2022; Leukfeldt, 2014). Hierbij lijken daders vooral opportunistisch te handelen: mensen die al betrokken zijn bij offline criminaliteit maken gebruik van gelegenheden en criminele kansen om online delicten te plegen, zoals phishing en malware, en daarom wordt er ook wel naar ze verwezen als "cafeteria-style offenders" (Leukfeldt & Holt, 2022). Veel kernleden lijken dan ook al in aanraking te zijn geweest met de politie, of in ieder geval bekend te zijn met het plegen van delicten, ook in de offline wereld (Leukfeldt et al., 2017a,b,c,d,e; Leukfeldt & Holt, 2022). In het onderzoek van Leukfeldt en Holt (2022), gebaseerd op analyse van opsporingsonderzoeken, werden de helft van de 37 criminele netwerken geclassificeerd als cybercrime specialisten, omdat ze enkel betrokken waren bij specifieke delictsvormen en het netwerk bestond uit individuen met hun eigen specifieke rol, zoals het schrijven van malware. De andere helft was geclassificeerd als cybercrime generalisten; sommige netwerken waren betrokken bij malware maar pleegde ook andere vormen van online fraude, en sommige leden van phishing netwerken waren ook actief in de drugshandel.

Wat betreft de criminele carrière van geldezels, wijst onderzoek uit dat 40% geen bekend voorafgaand contact had met de politie (Oerlemans et al., 2016). De auteurs hadden beschikking over informatie over frauduleuze rekeninghouders versterkt door het ECTF, en hebben vervolgens van circa 600 geldezels gezocht naar antecedenten in politiesystemen. In andere gevallen waren relatief lichte vergrijpen zoals diefstal het meest prevalent. Dit wijst erop dat geldezelen mogelijk een eerste stap vormt in de criminele loopbaan (e.g. Bekkers et al., 2020), hoewel er nog weinig bekend is over het pad dat geldezels verder bewandelen in het criminele milieu, over recidive en over *desistance*. Oerlemans et al. (2016) onderscheiden op basis van hun analyse over delictgeschiedenis vier groepen geldezels: 1) geldezels zonder antecedenten, 2) geldezels ouder dan 20 jaar met één of twee antecedenten, 3) geldezels die vanaf 15-jarige leeftijd al met de politie in aanraking kwamen en vier tot acht antecedenten hebben en 4) tot slot een groep veelplegers.

4.2 Interviews

Respondenten verschillen in hun uitspraken wat betreft de activiteiten van criminele netwerken, en ook hier is beperkt zicht op. Duidelijk is wel dat daders achter geldezeldelicten zich volgens de meeste respondenten vaak met meerdere vormen van cybercriminaliteit bezig houden (FOCUS, RESP1, RESP5, RESP6, RESP7, RESP8, RESP9, RESP10, RESP11, RESP13, RESP14, RESP16, RESP17, RESP20, RESP21). Daar is bijvoorbeeld bewijs voor gevonden op in beslag genomen telefoons van verdachten. Het is niet duidelijk of dadergroepen zich op een bepaald moment dan enkel richten op één delict of op verschillende delicten tegelijk. Gearresteerde daders van bankhelpdeskfraude, het delict dat momenteel veel voorkomt volgens respondenten, hebben vaak voorheen ook phishing, Whatsappfraude, of aan- en verkoopfraude gepleegd (RESP2, RES6, RESP7, RESP8, RESP9, RESP13, RESP20, RESP21). Uit analyse van het LMIO blijkt bovendien dat circa 10% van de bankrekeningnummers die bij hulpvraagfraude is gebruikt, ook is gebruikt voor het plegen van aan- en verkoopfraude (RESP18). Een voorbeeld van een crimineel pad is dat daders van phishing of hulpvraagfraude zijn overgestapt naar bankhelpdeskfraude, en daarvoor eventueel nog aan- en verkoopfraude hebben gepleegd (RESP2, RESP6, RESP13).

Uiteindelijk gaat het daders volgens respondenten om het verdienen van geld en status, en lijken cybercriminele netwerken dus opportunistisch te handelen: ze kiezen voor het delict waar op dat moment het meeste geld mee te verdienen is, de meeste kans van slagen biedt, en/of de laagste pakkans heeft (FOCUS, RESP5, RESP7, RESP8, RESP10, RESP11, RESP13, RESP16, RESP17). Wel benoemt de focusgroep dat er naast dit soort generalistische netwerken ook netwerken zijn die zich wel specifiek richten op één soort delict, bijvoorbeeld bankhelpdeskfraude.

"Iemand die begint met zijn criminele carrière, kijkt gewoon waar kan ik status en geld mee verdienen." – RESP16

"Wat we nu soms wel terug zien in daders van bankhelpdeskfraude is dat ze wel een verleden hebben in iets wat een paar jaar geleden trending was. Je ziet dus dat ze zich aanpassen in het criminele domein." (...)."Ik heb wel voorbij zien komen dat iemand eerst een laptop via aan- en verkoopfraude heeft gekregen, en die laptop later heeft gebruikt voor bankhelpdeskfraude." – RESP7

Volgens de meeste respondenten die zicht hebben op de netwerken hebben de daders achter geldezeldelicten eerdere antecedenten, en zijn ze met de politie in aanraking gekomen voor bijvoorbeeld straatroven, vernieling, geweldpleging en vuurwapen gebruik (RESP9, RESP13, RESP15, RESP16, RESP17). Ronselaars blijken vaak ook al in beeld te zijn geweest als geldezel, of hebben andere delicten op hun naam, zoals lichte drugscriminaliteit of inbraken. Er is volgens respondenten weinig doorgroei van leden in hetzelfde netwerk, bijvoorbeeld van pasophaler naar beller (RESP1, RESP20, RESP21). Het daadwerkelijk uitvoeren van sommige delicten vraagt ook een bepaalde mate van intelligentie en vaardigheid (RESP1). Wel zou het mogelijk zijn dat netwerkleden soms onafhankelijk van het netwerk fraudes gaan plegen (RESP20, RESP21). Over het algemeen is er weinig zicht onder de respondenten op criminele carrières.

Wat betreft geldezels stellen een aantal respondenten dat er bij een merendeel geen sprake is van een criminele carrière (RESP10, RESP11, RESP5). Een klein aantal geldezels groeien mogelijk echter wel door naar ronselaar en gaan zelf nieuwe geldezels rekruteren in hun omgeving (RESP5, RESP13, RESP15). Eén respondent benoemt dat daders van Whatsappfraude in enkele gevallen ook zijn begonnen met geldezelen (RESP15). Sommige geldezels hebben volgens respondenten bovendien al eerdere antecedenten, zoals straatroven, geweldpleging en inbraken, of overlast, winkeldiefstal en kleinschalige drugshandel (RESP3, RESP5, RESP7, RESP8, RESP16, RESP17). Dit zouden mensen in slechte omstandigheden zijn die geld willen verdienen om hun situatie te verbeteren (RESP16, RESP17). Geldezelen is in sommige gevallen ook een soort opstapdelict richting zwaardere criminaliteit, bijvoorbeeld naar ronselaar, dat zou dan vooral gaan om de "kruimeldieven" die ook al andere delicten plegen en meer bewust meewerken aan de criminele activiteiten (RESP5). Maar over het algemeen schrikken geldezels vaak van de gevolgen en doen het daarna niet nog een keer, aldus RESP5, en andere geldezels hebben dan ook geen bekend delictgeschiedenis en observeren respondenten daarbij ook weinig doorgroei naar andere rollen binnen hetzelfde netwerk (RESP5, RESP20, RESP21).

Verder signaleren een aantal respondenten overlap van cybercriminaliteit met traditionele criminaliteit. Ten eerste hebben daders soms een verleden van financieel-gemotiveerde delicten zoals diefstal, inbraken, overvallen en drugshandel (RESP3, RESP5, RESP6, RESP9, RESP14, RESP16, RESP17), maar ook van mishandeling en vernieling (RESP9). Deze daders stappen dan over op cybercriminaliteit, mogelijk vanwege lagere pakkans en meer winst. Het is bij respondenten niet geheel duidelijk of ze vorige activiteiten dan stoppen of dat ze op hetzelfde moment betrokken blijven beide vormen van criminaliteit. In genoemde voorbeelden was bijvoorbeeld een ronselaar van geldezels ook actief in de drugshandel (RESP3), waren daders van bankhelpdeskfraude al eerder veroordeeld voor overvallen (RESP9), en was een cybercrimineel ook lid van een Outlaw Motorcycle Gang (RESP16, RESP17).

"En er wordt wel eens geript, en dat gaat ook wel eens fout, veel geweld. Het risico op escalatie is groter nu, omdat de toegang tot wapens makkelijker is geworden en sprake is van een kruisbestuiving met de iets georganiseerdere misdaad." – RESP1

Ten tweede zouden sommige criminelen hun winsten mogelijk investeren in mensenhandel of grootschalige drugshandel, zoals het opzetten van een drugslijn of drugslab (FOCUS, RESP5, RESP7, RESP8, RESP10, RESP11, RESP16, RESP17, RESP20, RESP21, RESP22). Cybercriminaliteit wordt dan gepleegd om vermogen op te bouwen. Hier zijn echter nog weinig concrete voorbeelden van, en het blijft bij respondenten over het algemeen bij vermoedens zonder hard bewijs, die bijvoorbeeld zijn gebaseerd op geluiden vanuit politieonderzoek. Respondenten van het OM vragen zich ook af waarom criminelen zouden overstappen op een minder lucratief verdienmodel (RESP20, RESP21). Volgens die respondenten is het logischer dat criminele netwerken al in de drugshandel zitten en dan bankhelpdeskfraude erbij doen omdat het lucratief is. Het hoeft volgens respondenten ook niet zo te zijn dat de daders achter geldezeldelicten al een delictverleden hebben, dan is bankhelpdeskfraude bijvoorbeeld juist het instapdelict.

"Dat is wel echt iets dat ik geleerd heb. In het veiligheidsveld zijn we heel erg geneigd om te denken in clusters. Cyber, ondermijning, woninginbraak. Maar ja, daders van dit soort delicten zijn heel opportunistisch en schakelen gewoon. De ene keer levert dit meer op, de andere keer levert dat meer op." – RESP3

"We hebben hier onderzoeken bij de DR gehad, dat ze serieus aan het typen waren van 'doen we vanavond een ov'tje [overval] of gaan we vissen [phishing plegen]?'" – RESP9

Ten derde lijkt er sprake van geweld en bezit van vuurwapens onder financieel-gemotiveerde daders van cybercriminaliteit, mogelijk ook in toenemende mate (RESP6, RESP7, RESP8, RESP9, RESP13, RESP14, RESP15, RESP16, RESP17). Een voorbeeld is een zaak waarbij er tijdens een cash-out van bankhelpdeskfraude bij een pinautomaat een schietpartij plaatsvond, waarbij een verdachte was overleden (RESP16, RESP17). In een ander voorbeeld hadden alle vijf de verdachten van hulpvraagfraude schotwonden en waren dus betrokken bij eerdere schietpartijen (RESP15). De focusgroep benoemt ook dat er geweld heeft plaatsgevonden tussen *drill*-rappers[1] die betrokken waren bij cybercriminaliteit, en dat cybercriminelen elkaar soms beroven of rippen. Echter lijken dit soort daadwerkelijke conflicten met vuurwapens gerelateerd aan cybercriminaliteit over het algemeen nog zeldzaam of beperkt aan het licht te komen (RESP7, RESP8, RESP14).

Er worden volgens respondenten geregeld vuurwapens aangetroffen bij huiszoekingen van cybercriminelen of bij heterdaadsituaties waarbij cybercriminelen per toeval in een auto staande worden gehouden met vuurwapens in bezit, en bovendien zijn vuurwapens ook prominent onderdeel van video's op sociale media gerelateerd aan de "*f-game*"[2].

1 Drillrap is een muziekstijl met vaak donkere en gewelddadige teksten dat geweld verheerlijkt.

2 De term f-game refereert naar het plegen van online fraudes, waarbij zich een subcultuur heeft gevormd op sociale media waarin jongeren pronken met dure spullen en geld en nieuwe leden werven.

Er zijn verschillende redenen genoemd waarom cybercriminelen vuurwapens in bezit hebben. RESP13 van de politie heeft zaken gehad waarbij verschillende dadergroepen conflict hadden en daarom dreigen met gebruik met vuurwapens. Ook andere respondenten wijten het bezit van vuurwapens aan het feit dat er veel geld omgaat in cybercriminaliteit en daders daarom de behoefte hebben zichzelf te beschermen, vergelijkbaar met de drugshandel (RESP7, RESP8). Maar – mede vanwege het uitblijven van daadwerkelijke conflicten – denken respondenten ook dat daders simpelweg willen pronken met status (RESP9, RESP14).

"Ze schromen ook niet om een wapen aan te schaffen en de mensen die uit het netwerk willen stappen fors te bedreigen, of mensen die de boel verlinken hun eigen graf te laten graven. Het is een hele criminele bende." – RESP10

"Als je überhaupt kijkt naar jeugdgroepen, hebben ze eigenlijk altijd wapens, maar die vinden we nooit. (...). Maar ze staan op afbeeldingen wel met wapens maar je ziet ze toch eigenlijk weinig (...). En waarom hebben ze deze? Het zal wel stoerdoenerij zijn." – RESP14

Resumé

Cybercriminele netwerken verschillen in hun specifieke activiteiten. De literatuur maakt duidelijk dat de delictstijl van sommige groeperingen wordt gekarakteriseerd als "cafeteria-style", waarbij ze opportunistisch handelen en betrokken zijn bij delictsvormen waar op dat moment veel geld mee te verdienen is. Deze bevindingen worden bevestigd door respondenten in de interviews. Daders die zich nu met bankhelpdeskfraude bezig houden hebben volgens respondenten in het verleden Whatsappfraude, phishing of aan- en verkoopfraude gepleegd, of waren al bekend bij de politie vanwege inbraken, drugshandel of overvallen. Sommigen groepen verplaatsen hun activiteiten volgens respondenten zelfs naar het buitenland omdat Nederlandse burgers weerbaar zijn geworden. Daartegenover wijst literatuur uit dat er groeperingen zijn die zich specialiseren in een bepaalde vorm van cybercriminaliteit, vaak met een sterk technisch en internationaal component. Dergelijke netwerken zijn bij de interviews echter minder ter sprake gekomen, mogelijk ook vanwege de lokale focus van de respondenten. De activiteiten van lokale cybercriminele netwerken achter geldezeldelicten lijken dus vooral opportunistisch van aard, waarbij er sprake is van overlap tussen verschillende vormen van cybercriminaliteit en van cybercriminaliteit met traditionele criminaliteit. Hierbij observeren respondenten in toenemende mate gebruik van geweld en bezit van vuurwapens, hoewel daadwerkelijke incidenten nog niet systematisch plaatsvinden. Wat betreft geldezels lijkt bij een deel sprake van een delictgeschiedenis, mogelijk vooral voor lichte vergrijpen. Geldezelen is in sommige gevallen ook een soort opstapdelict richting zwaardere criminaliteit, bijvoorbeeld naar ronselaar, hoewel er onder respondenten beperkt zicht is op de criminele carrière van geldezels.

5 De kenmerken van de cybercriminele netwerken die geldezels inzetten

In dit hoofdstuk beschrijven we de resultaten die betrekking hebben op deelvraag 3, namelijk de kenmerken van de cybercriminele netwerken die geldezels inzetten. Hierbij maken we een onderscheid tussen bevindingen gerelateerd aan de structuur van de netwerken (paragraaf 5.1) en het ontstaan en groei van de netwerken (paragraaf 5.2).

5.1 Netwerkstructuur

5.1.1 Literatuuronderzoek

In tegenstelling tot wat de publieke perceptie doet vermoeden, werken cyberdaders zelden alleen. "*Many hands make light work*", zoals een dader benoemt in het onderzoek van Hutchings (2014, pp. 13). Zowel nationale als internationale literatuur wijst namelijk uit dat er vaak een netwerk van verschillende personen verantwoordelijk is voor de uitvoering van cybercriminaliteit, hoewel de precieze samenstelling en de kenmerken van zo'n netwerk kunnen verschillen (Hutchings, 2014; Leukfeldt & Holt, 2020, 2022; Leukfeldt et al., 2017a,b,c,d,e; Odinot et al., 2017; Leukfeldt et al., 2019; Lusthaus et al., 2023; Roks et al., 2021; Bulanova-Hristova et al., 2016). Wel is duidelijk dat vrijwel alle netwerken een bepaalde hiërarchie hebben, er sprake is van een verdeling van taken en verantwoordelijkheden en dat ze bestaan over een langere periode (Leukfeldt & Holt, 2020; Leukfeldt et al., 2017a,b,c,d,e; Leukfeldt et al., 2019). Verschillen zijn te vinden in onder meer het aantal leden (i.e. variërend van een handjevol tot meer dan 20 leden) en de mate van stabiliteit van het netwerk over de tijd heen (i.e. dezelfde compositie).

Over het algemeen kunnen rollen en taken in een cybercrimineel netwerk opgedeeld worden in drie categorieën (Leukfeldt et al., 2017a,b,c,d,e; Leukfeldt, 2014; Odinot et al., 2017; Lusthaus et al., 2023): kernleden, faciliteerders en geldezels. Kernleden zijn degenen die een cyberdelict initiëren en coördineren. Ze hebben controle over de rest van het netwerk en zijn betrokken bij bijvoorbeeld het overmaken van het geld van een slachtoffer naar geldezels. Kernleden lijken ook vaak samen te werken met criminelen uit andere netwerken en zijn al langer actief in het criminele milieu (Leukfeldt et al., 2017e). Soms zijn de kennis en vaardigheden van kernleden niet voldoende om een delict succesvol uit te voeren. In dat geval gebruiken ze faciliteerders, die zijn gespecialiseerd in bijvoorbeeld het ontwikkelen van kwaadaardige software, het stelen van data, het verbergen van illegaal verkregen geld, het falsificeren van identiteitsdocumenten en het bouwen van phishing websites. Dit zijn dus mensen die diensten verlenen aan het criminele netwerk. Ze adverteren deze diensten online, bijvoorbeeld op fora of het

Dark Web, of zijn bekenden van de kernleden in de fysieke wereld, en werken meestal voor meerdere netwerken tegelijk. Hiërarchisch gezien staan geldezels ten slotte onderaan het criminele netwerk. Geldezels stellen de kernleden in staat om ongehinderd gebruik te maken van het gestolen geld, en zijn daarmee een essentiële schakel in het financieel-gemotiveerde cybercriminele ecosysteem.

5.1.2 Interviews

Over het algemeen is er nog weinig zicht op de hogere lagen van het netwerk achter geldezels (RESP5). Wel is duidelijk dat de structuur van het netwerk achter geldezeldelicten verschilt, waarbij sommige netwerken zeer hecht zijn en andere meer fluïde (FOCUS, RESP10, RESP11). Respondenten herkennen wel eerder de notie van fluïde netwerken dan strikt hiërarchische netwerken (FOCUS, RESP1, RESP6, RESP10, RESP11, RESP15, RESP20, RESP21). De netwerken opereren volgens respondenten op basis van gelegenheid en hebben weinig vaste vormen, en de term "netwerk" refereert ook niet naar een piramidevorm (RESP20, RESP21). Over het algemeen zijn er wel rollen te onderscheiden bij zowel fluïde als hechte netwerken, waarbij respondenten refereren naar een vaste kern van één of meerdere uitvoerders/leiders in een netwerk en leden daaronder die specifieke taken hebben en die vaak slechts tijdelijk aan het netwerk verbonden zijn (FOCUS, RESP5, RESP6, RESP20, RESP21). Bovendien is duidelijk dat de mensen in een netwerk nauw samenwerken, en het is daarom belangrijk dat de leden elkaar kunnen vertrouwen, aldus een aantal respondenten (RESP1, RESP13).

"We moeten niet onderschatten dat er uiteindelijk binnen die criminele netwerken een soort vertrouwen moet zijn onderling. Ik kan wel zeggen ga jij even die 1000 euro pinnen, maar dan moet ik wel zeker weten dat jij er niet vandoor gaat met dat geld." – RESP13

"Een van de belangrijkste indicatoren dat cybercrime zo hard groeit, is gewoon die taakspecialisatie. (…). Omdat je gewoon voor alle kleine onderdelen, waar je zelf geen verstand van hebt, iemand kan inhuren die dat even voor je doet. En niet eens zo duur." – RESP1

Opvallend is dat de leiders in een netwerk druk zouden uitoefenen op geldezelronselaars om een bepaald quotum aan bankrekeningen aan te leveren (RESP5), wat mogelijk ook kan verklaren waarom ronselaars soms geweld toepassen of daarmee dreigen (RESP5). De ronselaar is genoemd als specifieke rol in het netwerk en dat betreft dan iemand die zich alleen bezighoudt met ronselen (RESP1).

"De druk bij dat soort gasten ligt best wel hoog. We weten uit een bepaald onderzoek bijvoorbeeld dat ze twee bankpassen per dag moesten leveren. Zo niet, dan heb je gewoon een probleem." – RESP5

Een andere belangrijke rol in het netwerk is weggelegd voor degenen die de leads aanleveren. Zij zouden zich actief bezig houden met het maken van datalekken of stelen van persoonlijke gegevens, bijvoorbeeld via phishing, of gebruiken al bestaande datalekken (FOCUS, RESP1, RESP7, RESP8, RESP13, RESP16, RESP17, RESP20, RESP21). Meerdere respondenten benoemen dat persoonlijke informatie van potentiële slachtoffers soms ook wordt doorverkocht door werknemers van callcenters (FOCUS, RESP13, RESP16, RESP17). Het is niet bekend of zij al bij het callcenter werkte voordat ze werden geronseld, of daar doelgericht zijn gaan werken om fraudes te faciliteren. In de studie van Leukfeldt et al. (2017b) bleek dat dit geronselde individuen zijn. Iemand die leads aanlevert, verleent deze diensten in principe niet voor slechts één specifiek netwerk (RESP20, RESP21), hoewel deze respondenten een zaak benoemen waarbij een bankmedewerker wel informatie doorspeelde aan maar één bepaalde dader.

Wat betreft individuele kenmerken van daders blijkt uit interviews dat de netwerken achter de geldezeldelicten een heterogene groep betreft, en dat het lastig is om gegeneraliseerde uitspraken te doen. Wel gaat het volgens respondenten vaak om jonge mannen die in bezit zijn van Nederlands staatsburgerschap (FOCUS, RESP9, RESP14, RESP15, RESP16, RESP17, RESP20, RESP21). RESP15 van de politie noemt vijf verdachten van Whatsappfraude die op één na allemaal minderjarig waren, wat volgens respondent geen uitzondering is. Deze respondent ziet bij de meer technische delicten wel oudere mensen. Ook volgens RESP16 en RESP17 zijn daders over het algemeen jonger dan 30 jaar. Ze zijn volgens die respondenten onderdeel van gezinnen uit achterstandswijken met multi-problematiek. Opvallend is dat RESP16 en RESP17 al een aantal keer een huiszoeking hebben gedaan bij daders die nog bij hun ouders woonden, waarbij de ouders in sommige gevallen ook gebruik maakten van de illegale winsten, volgens RESP16 en REP17 vaak mensen met een migratieachtergrond.

"Dit zijn niet de onschuldige 'pubers op zolder'. Dit zijn de jongens en meisjes van de straat, die dit als een verdienmodel erbij zien. Alles wat geld oplevert voor die gasten is prima." – RESP13

"Maar omdat er toch nog steeds meer misdrijven worden gepleegd dan dat we er verdachten voor oppakken, weet ik niet of je wat [over de kenmerken] kan zeggen. Omdat je vaak bij toeval op dit soort misdrijven stuit. (…). Daar zit natuurlijk wel een bepaald type verdachte op, die je meer ziet dan andere typen verdachten." – RESP14

Bovendien hebben de daders volgens respondenten vaak een laag opleidingsniveau of geen opleiding afgerond, behalve de ICT-specialisten (RESP9, RESP16, RESP17). Een aantal daders hebben kennis van ICT omdat dat nodig is voor het plegen van delicten, bijvoorbeeld het hacken van cryptowallets, wat een ander type dader is dan degenen betrokken bij bankhelpdeskfraude (RESP9). Bij financieel-gemotiveerde cybercriminaliteit speelt het verkrijgen van status een belangrijke rol, waarbij daders binnen de rapcultuur en op sociale media pronken met dure spullen, i.e. de *f-game* (FOCUS). Ze zijn gericht op het verdienen van geld en status, en bij huiszoekingen kom je dan ook altijd dure spullen tegen, aldus RESP16 en RESP17.

"Bijna iedereen die erbij betrokken is, weet eigenlijk wel dat-ie met iets frauduleus bezig is. Het probleem is denk ik ook hier in Nederland, en ook in België en Engeland bijvoorbeeld, dat het lang niet meer gezien wordt als iets kwalijks, als je mensen oplicht. Binnen die gemeenschappen wordt het vooral gezien als iets slims. Dat zien we ook terug in de popcultuur, de jeugdcultuur. Dat er gewoon openlijk over wordt gerapt." – RESP1

Hierna zoomen we in op de specifieke geldezeldelicten en de kenmerken van de netwerken die zich daarmee bezighouden.

Bankhelpdeskfraude

De netwerkstructuur achter geldezeldelicten is met name ter sprake gekomen bij bankhelpdeskfraude. Dat komt omdat daar de aandacht van de politie momenteel naar toe gaat, maar ook omdat voor succesvolle uitvoering meer taken nodig zijn vergeleken met de andere geldezeldelicten. Respondenten onderscheiden zeker acht rollen (FOCUS, RESP7, RESP8, RESP9, RESP13): 1) de bonker (degene die nieuwe leden ronselt en bij elkaar brengt), 2) iemand die de persoonlijke informatie van potentie slachtoffers aanlevert, i.e. de leads/bellijsten, 3) een beller / "lebber", ofwel degene die het slachtoffer opbelt, 4) de ophaler, i.e. de persoon die bankpassen ophalen bij het slachtoffer, 5) de chauffeur, i.e. degene die de pasophaler naar het slachtoffer brengt en daar ophaalt, 6) iemand die het geld veilig stelt via een bankrekening, dat kan een geldezel zijn, een 7) pinner / "nipper", ofwel degene die het geld pint bij een pinautomaat, en 8) in specifieke gevallen iemand die de computerbesturing overneemt van het slachtoffer.

Die rollen komen niet in alle zaken voor en soms zijn het ook gecombineerde rollen (RESP7, RESP8, RESP10, RESP11, RESP20, RESP21), waarbij de bonker ook de beller is of de pinner ook de pasophaler, bijvoorbeeld. RESP9 benoemt een groot onderzoek naar bankhelpdeskfraude, waarbij er één hoofddader was die wel tien bellers onder zich had. Die hoofddader bepaalde ook hoeveel procent van de opbrengsten iedereen kreeg en bracht de rest van het netwerk bij elkaar, aldus RESP9. RESP22, officier van justitie, was inderdaad betrokken bij een zaak waarbij één iemand de hoofddader was en daar het gestolen geld uiteindelijk naartoe ging. Volgens RESP20 en RESP21 is de beller wel vaak ook de bedenken en initiator, en werken zij soms samen met andere daders die ook bankhelpdeskfraude plegen. Soms bellen ze wel 300 mensen per uur (RESP9), en de bellers huren dan voor een aantal dagen huisjes in vakantieparken of Airbnb's om de gehele dag slachtoffers te bellen (RESP6). Daar zijn wel eens politie-invallen geweest. Uit onderlinge communicatie zeggen de daders dat ze dan 'gewoon aan het werk' zijn, aldus RESP10 en RESP11.

"Verdachten maken gebruik van een bepaalde locatie huren, dat kan een vakantiehuisje of Airbnb zijn met Wifi, en dan zeggen ze we zijn nu twee dagen onderweg het is tijd om door te gaan naar de volgende anders staat de politie op de stoep." – RESP16

Phishing

Bij phishing is er volgens respondenten minder zicht op de netwerken omdat de uitvoering daarvan geheel online plaatsvindt en een netwerk ook niet nodig is om het delict uit te voeren. In principe gaat het hierbij om vraag en aanbod, waarbij iemand een phishing website bouwt en iemand anders dat gebruikt (RESP7, RESP8). RESP1 beschrijft de netwerken echter wel uitvoerig op basis van gesprekken met een aantal leden van een phishing netwerk. Er is sprake van een 'operator', op sociale media ook wel naar gerefereerd als 'visser'. Dit is de persoon die een phishing panel beheert, en dat kan volgens de respondent ook net zo goed een Whatsappfraudeur of handelsplaatsfraudeur zijn. Naast de operator is er een ronselaar en/of pinner: deze persoon ronselt een geldezel, aan wie de geldezel diens bankpas afgeeft. De operator contacteert de pinner wanneer het geld eraan komt, en de pinner staat dan al klaar bij bijvoorbeeld luxe warenhuizen om het geld op een cadeaukaart te zetten of het geld te pinnen. Hoewel operators de technische benodigdheden voor phishing tegenwoordig makkelijk kunnen inkopen via sociale media, is de kennis soms wel in huis: RESP16 en RESP17 halen het voorbeeld aan van een dadergroep met een IT-specialist die hielp met het bouwen van phishing websites. RESP1 heeft bovendien de hypothese dat er soms nog iemand achter het netwerk zit die de operatie in gang zet; een investeerder of iemand uit het criminele milieu die het netwerk aanspoort/betaald om de delicten uit te voeren.

Hulpvraagfraude en aan- en verkoopfraude

Bij hulpvraagfraude is het netwerk ook relatief klein, zo stellen respondenten (RESP7, RESP8, RESP14), hoewel er wel een variatie aan rollen en taken zijn genoemd. RESP15 onderscheidt in het netwerk 1) ronselaars, 2) geldezels, 3) iemand die appt/contact heeft met het slachtoffer, 4) iemand die het geld pint, en 5) iemand die telefoonnummers en persoonlijke informatie van slachtoffers, i.e. leads, verzamelt. Mogelijk bepaalt ook nog iemand welke geldezels voor welk delict worden ingezet (RESP15).

Bij aan- en verkoopfraude gebruiken criminelen soms hun eigen bankrekening, terwijl in andere gevallen er mogelijk wel sprake is van een klein netwerk (RESP7, RESP8, RESP18). Het gaat daarbij dan om een ronselaar, geldezel (katvanger in het geval van webwinkelfraude), de daadwerkelijke oplichter, en soms iemand het geld pint (RESP18). Hierbij wordt op sociale media ook wel gesproken van een 'schetser', ofwel iemand die het verhaal achter de oplichting bedenkt.

5.2 Ontstaan en groei van cybercriminele netwerken die geldezels inzetten

5.2.1 Literatuuronderzoek

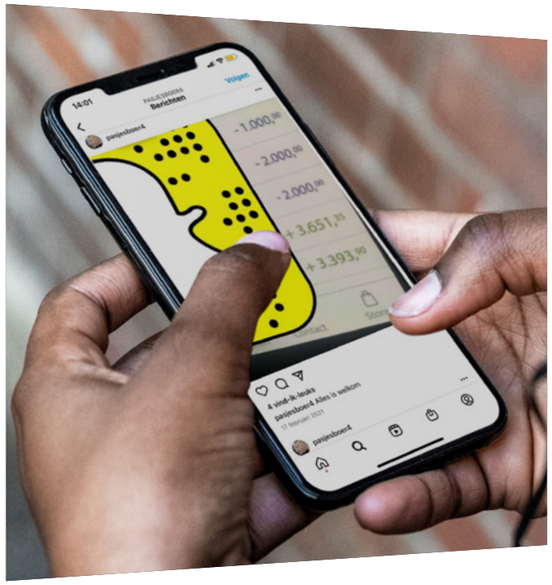
Een aantal studies richt zich op hoe een cybercrimineel netwerk ontstaat en groeit, en hoe geldezels en andere leden van het netwerk betrokken raken bij een netwerk. Dit soort kennis is belangrijk, omdat het aanknopingspunten biedt voor interventie van daderschap van cybercriminaliteit, en daarmee ook tot preventie van slachtofferschap. In het algemeen kan gesteld worden dat onderzoek al jaren lang laat zien dat sociale relaties een centrale rol spelen bij de betrokkenheid van mensen bij vormen van traditionele georganiseerde criminaliteit (Kleemans & Van de Bunt, 1999; Kleemans & Van Koppen, 2020; Kleemans & De Poot, 2008). Sociale banden zoals familie of vrienden bieden namelijk toegang tot andere daders en tot mensen wiens banen, kennis of vaardigheden worden gebruikt om het misdrijf te plegen. Aan de hand van die contacten ontstaan er dus nieuwe criminele kansen en gelegenheden om een bepaald delict te plegen. Via-via in contact komen met elkaar zorgt bovendien voor een bepaalde mate van vertrouwen onder criminelen, iets dat inherent ontbreekt in risicovolle criminele omgevingen. In andere gevallen hebben criminelen juist voordeel om mensen buiten hun initiële sociale kringen te ontmoeten, omdat geclusterde groepen zoals families, vrienden en bekenden vaak vergelijkbare achtergronden, kennis, of toegang tot criminele kansen hebben (Van Koppen, 2013). Daarom zijn 'offender convergence settings' ook van belang bij de groei van criminele netwerken, ofwel fysieke locaties zoals een café waar criminelen elkaar ontmoeten en nieuwe mensen leren kennen (Felson, 2003).

Tegenwoordig bevinden deze *offender convergence settings* zich niet alleen in de offline wereld, maar ook op internet. In dit geval worden ze ook wel aangeduid als "online/virtual offender convergence settings" (Soudijn & Zegers, 2012). Voorbeelden hiervan zijn forums en markten op het Dark Web, maar ook groepen en kanalen op Telegram en Instagram (e.g. Bekkers et al., 2020). Hier kunnen kernleden informatie uitwisselen en in contact komen met nieuwe leden wiens vaardigheden of kennis nodig is om een delict te plegen, waardoor dergelijke platformen een belangrijke rol spelen in het ontstaan en groei van cybercriminele netwerken (Soudijn & Zegers, 2012; Leukfeldt et al., 2017c; Leukfeldt et al., 2019; Roks & Monshouwer, 2020; Bekkers & Leukfeldt, 2023). Het biedt de kernleden een groot bereik onder mensen buiten hun initiële sociale cluster, en stelt ze in staat om ad hoc mensen te ronselen die nodig zijn om een delict te plegen, zoals geldezels of pinners, wat bijdraagt aan de fluïditeit van het netwerk. De online omgeving vormt daarmee een oplossing voor een aantal beperkingen van de fysieke wereld, in termen van toegankelijkheid en bereik (e.g. Leukfeldt et al., 2017a). Dit werkt mogelijk ook in de hand dat de kernleden en de netwerkleden daaromheen elkaar niet of minder goed kennen.

Ook bij cybercriminaliteit wijst onderzoek uit dat het ontstaan en de groei van criminele netwerken nog steeds sterk verankerd is in al bestaande sociale banden in de fysieke wereld, maar waarbij er ook sprake is van nieuwe relaties die ontstaan op internet (Leukfeldt & Holt, 2022; Arevalo, 2015; Leukfeldt et al., 2017c,d; Bekkers & Leukfeldt, 2023; Bekkers et al., 2023). Zo krijgen kernleden die al betrokken waren bij offline criminaliteit via mensen in hun sociale cluster de kans om ook cybercriminaliteit te plegen (Leukfeldt & Holt, 2022). Ook potentiële geldezels worden benaderd op school tijdens de pauze, op sportclubs of op feestjes, en door vrienden-van-vrienden op straat (Bekkers et al., 2023; Leukfeldt et al., 2017a; Roks et al., 2021a; Leukfeldt & Holt, 2022). Rondom die plekken wordt dan op den duur bekend dat er makkelijk geld te verdienen valt met het uitlenen van bankpassen, waardoor mensen op een gegeven moment zelf naar de ronselaars stappen of geldezels in hun eigen omgeving nieuwe geldezels ronselen, waardoor een soort 'sociaal sneeuwbal effect' ontstaat (Leukfeldt et al., 2017c; Kleemans & Van Koppen, 2020). Vaak worden geldezels onder valse voorwendselen geronseld of is er mogelijk zelfs sprake van bedreiging met geweld (Leukfeldt et al., 2017e; Bekkers & Leukfeldt, 2023; Soudijn & Zegers, 2012). Sommige cybercriminele netwerken zijn lokaal geworteld en hebben daarom een voorkeur voor geldezels uit hun eigen omgeving, wat ze een hogere mate van controle over het netwerk biedt, waar andere netwerken internationaal opereren en ook buitenlandse geldezels gebruiken (Kshetri, 2010; Arevalo, 2015; Leukfeldt & Jansen, 2015; Lusthaus & Varese, 2021; Custers et al., 2019).

Vanwege nieuwe criminele kansen en de gelegenheid om delen van het crime script te verbeteren die traditioneel in de offline wereld plaatsvonden, verplaatsen criminelen bepaalde activiteiten steeds meer naar de digitale omgeving (Roks et al., 2021; Moule et al., 2013; Maimon & Louderback, 2019; Hutchings & Holt, 2015; Leukfeldt et al., 2019). Dit refereert naar de hybridisatie van criminaliteit; ook traditionele vormen van georganiseerde criminaliteit krijgen steeds meer een cyber-element. Zo kennen kernleden elkaar dus vaak al vanuit de fysieke wereld, maar rekruteren dan geldezels of faciliteerders via internet indien dat nodig is voor de uitvoering van het delict (Leukfeldt et al., 2017c,d,e). Daders zoeken op forums naar medeplegers die helpen bij de technische aspecten van phishing of een malware aanval, en ook delictplegers betrokken bij traditionele criminaliteit gebruiken online ontmoetingsplaatsen om in contact te komen met medeplegers, zoals mensen met IT-kennis die kunnen zorgen dat drugscontainers niet geselecteerd worden voor controle in de haven (Leukfeldt et al., 2019; Leukfeldt et al., 2017c,d,e).

Geldezels komen dus zowel online als in de fysieke wereld in een crimineel netwerk terecht. Hierbij spelen verschillende onderliggende mechanismen een rol. Zo bevinden geldezels zich soms in een subcultuur waarin het geaccepteerd is om deel te nemen aan deze criminele activiteiten voor het verkrijgen van geld en status (Leukfeldt & Kleemans, 2019; Bekkers & Leukfeldt, 2023). Zo blijkt uit politieverhoren dat sommige geldezels het normaal vinden dat ze worden benaderd voor hun bankpas, soms wel op dagelijkse basis (Leukfeldt & Kleemans, 2019). Ook in algemene jongerenpopulaties geven respondenten aan dat ze hun bankpas wel zouden uitlenen aan bekenden wanneer hen daarom gevraagd wordt (Bekkers et al., 2023). Ronselaars proberen het gedrag op sociale media ook te normaliseren, aangezien ze geldezelen adverteren als 'eerlijk werk' en claimen dat veel andere mensen hieraan ook al hebben deelgenomen (Bekkers & Leukfeldt, 2023; Bekkers et al., 2022). Deze subcultuur draait om het verdienen van geld en het verkrijgen van status; geldezels kijken op naar de luxe levensstijl van criminelen, aangezien zij dure kleren dragen en veel geld uitgeven in het nachtleven (Leukfeldt & Kleemans, 2019; Bekkers et al., 2020).



De meeste ronseladvertenties op sociale media stellen dan ook dat er veel geld te verdienen is, tot wel duizenden euro's, en quasi-experimenteel onderzoek wijst uit dat dit een effectieve strategie is om jongeren te overtuigen (Bekkers et al., 2023; Bekkers & Leukfeldt, 2023). Er is echter nog weinig bekend over welke financiële vergoeding geldezels precies krijgen, als de beloning al daadwerkelijk wordt uitbetaald (Kruisbergen et al., 2019). Een ronselaar gaf in een politieverhoor aan dat geldezels zo'n 30% van het gestolen geld ontvangen, en diens ronselaar zo'n 10% (Leukfeldt & Holt, 2022). Ander onderzoek meldt beloningen van circa 5% (Oerlemans et al., 2016; Arevalo, 2015). Een gevolg van deze subcultuur is dat potentiële geldezels op eigen initiatief hun bankrekening aanbieden aan ronselaars, bijvoorbeeld omdat zij in hun omgeving zien dat andere geldezels succesvol waren en geld of status verwierven, of dat ze zelf actief andere geldezels gaan rekruteren (Leukfeldt, 2014; Leukfeldt & Kleemans, 2019).

Hierbij speelt een rol dat jonge geldezels een vertekend beeld hebben van de daadwerkelijke situatie. Ze hebben slecht zicht op de consequenties van hun gedrag, en zijn zich nauwelijks bewust van de consequenties die het kan hebben als ze als geldezel zouden worden gepakt door hun bank of door de politie. Minder dan de helft van de respondenten uit een grote steekproef onder jongeren wist überhaupt wat de term 'geldezel' inhoudt (Bekkers et al., 2023; Spithoven et al., 2021). Dit past bij het feit dat cognitieve en emotionele risicoschattingen zich nog ontwikkelen gedurende de kindertijd tot in de adolescentie en volwassenheid (Boyer, 2006; Arnett, 1992; Lavery et al., 1993; Gardner & Steinberg, 2005).

5.2.2 Interviews

In lijn met de literatuur benoemen een aantal respondenten dat de daders achter geldezeldelicten elkaar vaak al kennen uit de fysieke wereld en dus lokaal zijn ingebed, en samen bijvoorbeeld al eerder criminaliteit pleegde (RESP1, RESP5, RESP9, RESP10, RESP11, RESP13, RESP14, RESP15, RESP16, RESP17, RESP22). Dit betreffen dan familierelaties of kennissen uit de buurt.

"Ze kennen elkaar wel altijd allemaal. Dus het is echt een groep die dat doet. Dus eigenlijk wat je ook hebt met woninginbraken of zo, met een groep die dat doen (...). Gewoon van de straat. Of uit de buurt." – RESP13

Een aantal respondenten wijt dit aan het belang van onderling vertrouwen (RESP13, RESP20, RESP21). Volgens RESP7 en RESP8 komen netwerken tot stand vanuit het initiatief van één of enkele hoofddaders, die mensen erbij zoeken voor specifieke klussen, bijvoorbeeld via advertenties op Telegram of via fysieke kringen. Zo is bij webwinkelfraude al jaren een sterke herleidbaarheid naar Oost-Nederland, wat de aanwezigheid van lokale dadergroepen impliceert (RESP18). Ook volgens RESP10, RESP11 en RESP15 kennen de hoofddaders elkaar vaak al wel, en wordt een netwerk opportunistisch samengesteld, waarbij bijvoorbeeld geldezels, pinners, pasophalers en bellers worden geronseld op het moment dat het nodig is. Dat gebeurt via sociale kringen in de fysieke wereld, maar ook online. Zo benoemen RESP7 en RESP8 het voorbeeld dat een chauffeur en pasophaler die ze per toeval in een auto hadden aangehouden elkaar niet kenden. Er zijn qua geografische kenmerken van dadergroepen dan ook opvallende combinaties, aldus RESP7, RESP8 en RESP13, waarbij de netwerkleden allemaal uit verschillende plaatsen in het land komen. RESP20 en RESP21 stellen dat daders elkaar leren kennen via Telegram en dat er veel onderling contact wordt gezocht via de f-game groepen. RESP9 kan zo "*vijftien onderzoeken uit het land noemen*" waarbij de leden elkaar alleen of voornamelijk online hebben gekend. Ook in online omgevingen is vertrouwen en reputatie belangrijk (RESP1, RESP22), want voor hetzelfde geld doe je zaken met een politieagent, aldus RESP22.

"Telegram is super toegankelijk geworden om te beginnen als cybercrimineel. Je hoeft niet te kunnen hacken, je hoeft niet te kunnen programmeren, ik zou prima aan de slag kunnen als bankhelpdeskfraudeur. Of als ronselaar." – RESP1

RESP9 benadrukt dat netwerkvorming wel zeer afhankelijk is van het specifieke delict. Bij bankhelpdeskfraude zoeken de daders juist bellers in hun fysieke omgeving, terwijl de kennis en componenten voor phishing vrijwel uitsluitend online worden gevonden, aldus RESP9. Ook RESP10 en RESP11 van het OM benadrukken dat er soms wel sprake is van een vaste kern, en soms ook helemaal niet. Kortom, afhankelijk van het delict, 1) ontstaan netwerken offline en groeien ze online, 2) ontstaan ze offline en groeien ze offline, 3) ontstaan ze offline en groeien ze zowel online als offline, en 4) soms ontstaan en groeien ze volledig online.

"Van oudsher waren er vaste criminele netwerken, dat is veel meer fluïde geworden." – RESP10

Duidelijk is dat geldezels volgens alle respondenten zowel online als offline worden geronseld. Criminele netwerken zijn volgens respondenten actief op sociale media en proberen onder valse voorwendselen mensen zover te krijgen dat ze hun bankpas afstaan, vaak onder het mom van 'snel geld verdienen', waarbij voornamelijk wordt gevraagd naar Bunq-rekeningen (RESP1, RESP2, RESP3, RESP5, RESP13). Dit lijkt momenteel vooral op Telegram en Snapchat plaats te vinden, en in mindere mate op Instagram, TikTok en zelfs Tinder (RESP1, RESP13, RESP15). De ronselaars maken accounts aan zodat potentiële geldezels vanuit eigen initiatief contact kunnen opnemen, of ze gaan zelf actief willekeurige mensen benaderen (RESP5). Soms zijn dit accounts van bijvoorbeeld influencers of rappers die wel duizenden volgers hebben, waardoor het bereik onder de doelgroep groot is (RESP1). Online ronselaars lijken ook lokaal georiënteerd, aangezien er bijvoorbeeld wordt geadverteerd met specifieke postcodes (RESP5). Verschillende respondenten benoemen echter dat ronselaars ook het hele land doorreizen om een bankpas op te halen (RESP5, RESP13, RESP16, RESP17, RESP18).

Criminelen ronselen geldezels volgens respondenten ook in de fysieke wereld, waarbij ze via-via worden aangesproken door bekenden uit de buurt, vrienden-van-vrienden of zelfs familie. Een relatiecomponent speelt dus vaak mee. Een voorbeeld hiervan is een netwerk achter phishing waarbij een dader een Roemeense vrouw had met familiecontacten in Spanje en Duitsland, en daarbij kwamen vaak Roemeense, Spaanse en Duitse geldezels naar voren (RESP16, RESP17). Ook benoemen respondenten dat ronselaars naar fysieke locaties gaan waar kwetsbare doelgroepen te vinden zijn, zoals daklozenopvang, asielzoekerscentra, verslavingsklinieken en mbo-scholen, en daar soms wel weken lang tijd investeren om te ronselen (FOCUS, RESP3, RESP5, RESP6, RESP10, RESP11). Duidelijk is dus dat ronselaars hierbij inspelen op actualiteiten, aangezien op een gegeven moment veel seizoenarbeiders en Oekraïense vluchtelingen werden geronseld (FOCUS).

Zowel bij online als offline ronselen zou er veelal sprake zijn van misleiding en manipulatie (FOCUS, RESP1, RESP2, RESP3, RESP5, RESP7, RESP8, RESP9, RESP10, RESP11, RESP19, RESP22). Geldezels worden er vaak ingeluisd en voelen zich "gewoon genaaid", aldus RESP1. Ook RESP2 is van mening dat geldezels niet weten waar het geld daadwerkelijk vandaan komt, ondanks dat sommige geldezels waarschijnlijk wel weten dat er iets illegaals gebeurt. Ronselaars hebben allerlei smoesjes voor waarom zij de bankrekening nodig zouden hebben. Over het algemeen wordt daarbij wel een beloning in het vooruitzicht gesteld, maar die wordt in het merendeel van de gevallen niet uitbetaald volgens respondenten (FOCUS, RESP19, RESP22). Specifiek bij de daklozen en verslaafden wordt in plaats van geld ook drugs beloofd in ruil voor de bankpas (RESP5).

"Hij zei dan "ik heb heel veel geïnvesteerd in crypto en als ik dat naar mijn eigen rekening uit-cash dan moet ik er belasting over betalen, dus als jij nou jouw rekening beschikbaar stelt, leen ik even je bankpas, dan stort ik het erop. (...)." – RESP1

Geweld of bedreiging met geweld bij het ronselen van geldezels lijkt zeldzaam, hoewel er volgens sommige respondenten soms wel sprake van is (FOCUS, RESP5, RESP7, RESP8, RESP13). Zo is er een voorbeeld waarbij er een explosie was geweest voor de deur van iemand die weigerde een bankpas af te staan (RESP5), en zijn er ontvoeringen geweest waarbij mensen onder dwang een bankrekening moesten openen of hun pinpas moesten afstaan (RESP5, RESP13). Het is niet duidelijk of die werkwijze een algemene trend is of slechts gekoppeld aan een aantal specifieke dadergroepen. RESP16 en RESP17 zijn van mening dat sociale druk om mee te werken ook een vorm van dwang is.

"Hij heeft veel status hij is het baasje van de wijk hier, en hij vraagt mij of ik iets kan betekenen, nou dat wil ik wel doen want dan helpt mij dat ook weer. Dat is heel anders dan online, waar het meer financieel gewin in." – RESP16

Resumé

De structuur van het netwerk achter geldezeldelicten verschilt per delict en is ook afhankelijk van het delict. Vooral bij bankhelpdeskfraude zijn er relatief veel rollen en taken nodig, in tegenstelling tot de andere delicten waarbij geldezels worden ingezet. Respondenten beschouwen de netwerken over het algemeen als fluïde en opportunistisch, en rollen worden soms ook gecombineerd. Er lijkt wel vaak sprake van één of enkele kernleden die verantwoordelijk zijn voor de uitvoering van het delict en die gebruik maken van faciliteerders en/of geldezels indien dat nodig is, wat in lijn is met eerdere bevindingen uit de literatuur. De omvang en de mate van stabiliteit van dergelijke cybercriminele netwerken verschilt, waarbij een handjevol kernleden zijn geassocieerd met enkele tot wel honderden geldezels. Hoewel het een heterogene groep is, lijken de daders achter geldezeldelicten relatief vaak jonge mannen te zijn met een laag opleidingsniveau en eerdere antecedenten op hun naam, zoals diefstal, vernieling, en inbraken. Geld en status lijken een belangrijke rol te spelen bij het plegen van cybercriminaliteit onder deze groep. De daders pronken met dure spullen op sociale media, en zijn onderdeel van subculturen waarin frauduleuze activiteiten genormaliseerd zijn.

Criminele netwerken achter geldezeldelicten ontstaan en groeien bovendien op verschillende manieren. Zowel het literatuuronderzoek als de interviews maken wel duidelijk dat netwerken vaak lokaal geworteld zijn, waarbij de kernleden elkaar al kennen via bestaande sociale relaties. Dit biedt een bepaalde mate van vertrouwen tussen de leden. Internet speelt vervolgens een cruciale rol bij de groei van het netwerk, en mogelijk is deze rol nog belangrijker geworden in de afgelopen jaren. Soms lijkt een netwerk zelfs volledig online te ontstaan en te groeien, zo concluderen respondenten op basis van politieonderzoek. Met name Telegram zou mogelijkheden bieden om in contact te komen met mensen die nodig zijn voor het plegen van een delict. Verder zouden geldezels volgens respondenten lokaal geronseld worden, bij verslavingsklinieken, de daklozenopvang, en scholen, maar ook online op sociale media. In de meeste gevallen is er volgens respondenten sprake van misleiding en manipulatie, en zijn geldezels niet op de hoogte van wat er met hun bankrekening gebeurt. Over het gebruik van geweld en dwang bij het ronselen zijn respondenten verdeeld, en die strategie lijkt incidenteel gebruikt te worden. Wel is duidelijk dat geldezels vaak onderdeel zijn onderdeel van subculturen waarin het geaccepteerd en genormaliseerd is om deel te nemen aan criminele activiteiten voor het verkrijgen van geld en status, hoewel een beloning niet altijd daadwerkelijk uitbetaald wordt.

6 De huidige aanpak van cybercriminele netwerken die geldezels inzetten

In dit hoofdstuk behandelen we deelvraag 5, over de huidige aanpak van cybercriminele netwerken die geldezels inzetten. Belangrijk is om te benoemen dat we geen uitputtend overzicht geven van de huidige aanpak in Nederland (zie bijvoorbeeld Boekhoorn, 2019; Van den Eeden et al., 2021; Staats et al., 2021). Het doel is om op hoofdlijnen een beeld te schetsen van het beleid en de praktijk, waarbij we gebruik maken van zowel de literatuur als interviews.

6.1 Literatuuronderzoek

Het opsporen en vervolgen van daders van cybercriminaliteit is in de praktijk ingewikkeld (OM, n.d.). De aangiftebereidheid onder slachtoffers van cybercriminaliteit is relatief laag, lager nog dan bij traditionele criminaliteit, waardoor veel zaken niet in beeld komen bij de politie (Van de Weijer et al., 2020; Domenie et al., 2013). In de gevallen dat er aangifte is gedaan, worden zaken veelal geseponeerd en is het opheldering spercentage laag (Boekhoorn, 2019). Daders die wel worden vervolgd, kunnen te maken krijgen met hoge gevangenisstraffen en hoge boetes. Het is vanwege de aard van cybercriminaliteit echter lastig om zicht te krijgen op wie de daders zijn, bijvoorbeeld omdat daders anoniem zijn, het delict op afstand wordt gepleegd en er geen fysieke sporen zijn van dader-slachtoffer interactie.

De Nederlandse overheid heeft de aanpak van cybercriminaliteit geïntensiveerd en geprioriteerd binnen de politie en het Openbaar Ministerie. Zoals onder meer geformuleerd in de Veiligheidsagenda 2023-2026 (Ministerie van Justitie en Veiligheid, 2022), zet de overheid in op zowel strafrechtelijke vervolging als meer alternatieve interventies, een hogere pakkans van daders, professionalisering van de cybercrimeteams waardoor zij ook de meest complexe onderzoeken kunnen draaien, en meer kennis binnen de politie op landelijk en lokaal niveau, evenals een sterkere informatiepositie, betere aangiftebehandeling, nationale-, internationale- en publiek-private samenwerking (zoals oprichting van de ECTF en operatie Centurion), en meer wettelijke bevoegdheden voor de opsporing (Ministerie van Justitie en Veiligheid, 2022; Rijksoverheid, n.d.; Politie, n.d; Van den Eenden et al., 2021; Boekhoorn, 2019; Oerlemans et al., 2022). Dit alles moet leiden tot een verbeterde aanpak van cybercriminaliteit. Zo is het streven om in 2026 meer dan 30% meer verdachte van gedigitaliseerde criminaliteit te identificeren dan in 2023, met ieder jaar minstens vijf fenomeenonderzoeken (Ministerie van Justitie en Veiligheid, 2022). Ook in het geval van cybercrime in enge zin beoogt de overheid een toename in zowel verdachten als aangepakte criminele samenwerkingsverbanden. Er zijn nog wel stappen te zetten, omdat bijvoorbeeld de (internationale) samenwerking nog incidenteel plaatsvindt en een lange doorlooptijd heeft, een landelijke aansturing op versterking van de informatiepositie nog ontbreekt, en, zeker op lokaal niveau, er nog weinig kennis, wil, vaardigheden, motivatie, prioriteit of lef is om de aanpak van cybercriminaliteit in de praktijk vorm te geven (Boekhoorn, 2019; Schiks et al., 2022; Van den Eeden et al., 2021; Spithoven & Leukfeldt, 2023; De Paoli et al., 2021).

De Nederlandse overheid zet breed in op de preventie van cybercriminaliteit, met initiatieven zoals Hack_Right, Bl@ckmail, escaperooms, Halt-maatregelen, en online bewustwordingscampagnes, en ook voor de politie is het voorkomen en verstoren van cybercriminaliteit een belangrijke taak geworden (Oosterwijk & Fischer, 2017; Schiks et al., 2021, 2022, 2023; Boekhoorn, 2019). Juist ook een lokale benadering is daarbij belangrijk, in overeenstemming met de kerndoelen van Operatie Centurion, aangezien criminele netwerken ook lokaal georiënteerd zijn en burgers zo bereikt kunnen worden. Gemeenten kunnen onder meer inwoners stimuleren om aangiften te doen, ontwikkelingen in dader-en slachtofferschap monitoren en specifieke doelgroepen voorlichten (Spithoven & Leukfeldt, 2023; Leukfeldt et al., 2020). Er lijkt sprake van een toenemende behoefte onder gemeenten om in actie te komen, en samen met onder meer het CCV (Centrum voor Criminaliteitspreventie en Veiligheid), de VNG (Vereniging van Nederlandse Gemeenten) en verschillende kennisinstellingen, worden er ook stappen gezet richting een onderbouwde en effectieve aanpak (Spithoven & Leukfeldt, 2023; CCV, 2022). De effectiviteit van preventieve maatregelen en interventies gericht op daderschap van cybercriminaliteit is weliswaar lastig te onderzoeken, maar er zijn positieve bevindingen gerelateerd aan enkele specifieke initiatieven (e.g. Schiks et al., 2021, 2022, 2023).

Geldezels zijn in het bijzonder een belangrijke doelgroep voor preventie van cybercriminaliteit: cybercriminele netwerken zijn sterk afhankelijk van de rol en taken van deze actoren, waardoor interventie op het niveau van geldezels direct het criminele proces verstoort en dus leidt tot minder slachtofferschap van cybercriminaliteit onder burgers en bedrijven. Geldezelen specifiek wordt in de wet beschouwd als een vorm van witwassen (artikel 420 bis Wetboek van Strafrecht). Gezien de ernst van dit misdrijf gaat het gepaard met een aantal strafrechtelijke consequenties, zoals een strafblad, een taakstraf, een Halt-straf voor 'first-offenders', hoge boetes (max. € 87.000) en zelfs een gevangenisstraf ten hoogte van maximaal 4 jaar. Hierdoor hebben geldezels ook vaak geen recht meer op een VOG. In de praktijk worden zaken vooral geseponeerd, of is er sprake van een geldboete, taak- of leerstraf. Gepakte geldezels worden echter niet altijd juridisch gestraft, vooral als er weinig bewijs is. Soms vinden dan stopgesprekken plaats op het politiebureau, waarbij de politie de verdachte al dan niet in aanwezigheid van diens ouders aanspreekt op het gedrag (Bekkers et al., 2020).

Geldezels komen echter niet altijd in aanraking met de politie, omdat slachtoffers soms geen aangifte doen en de politie ook andere prioriteiten heeft. Aannemelijker is dat geldezels in beeld

komen bij de financiële instelling waar zij bankieren (Spithoven et al., 2021). Banken monitoren namelijk op verdachte transacties, zoals het storten van opvallend hoge geldbedragen, en delen bovendien persoonlijk identificeerbare informatie van geldezels met slachtoffers en andere banken (Spithoven et al., 2021; Rani et al., 2022a,b, 2023a,b). Daardoor is de kans groot dat banken geldezeltransacties snel detecteren. Omdat het gebruik van bankrekeningen voor de uitvoering van illegale activiteiten volgens de gebruikersovereenkomst van banken niet mag, worden geldezels als frauduleus geregistreerd in de centrale database (i.e. IVR en EVR) van samenwerkende banken. Hierdoor lopen geldezels het risico dat ze geen leningen meer kunnen krijgen, waaronder een hypotheek voor de aankoop van een huis, en kunnen ze voor de duur van acht jaar worden uitgesloten van het openen van een nieuwe rekening. Bovendien kunnen geldezels zelf via het civiele recht aansprakelijk gesteld worden voor het gestolen geld van het slachtoffer; geld dat niet langer in hun bezit is. Deze juridische mogelijkheid is voor slachtoffers aanzienlijk verruimd in 2021, toen de Procedure NAW-gegevens Begunstigde bij Niet-Bancaire Fraude (PNBF) in het leven werd geroepen. Deze procedure verplicht banken onder bepaalde voorwaarden de NAW-gegevens van de (vermeende) fraudeur te verstrekken aan het slachtoffer (Rijksoverheid, 2020).

In juridische zin wordt geldezelen beschouwd als een vorm van witwassen (Europol, 2021). Helaas is wetenschappelijk onderzoek en politieonderzoek naar witwassen bij cybercriminaliteit schaars (e.g. Kruisbergen et al., 2019). Het is wel opvallend dat zowel bij traditionele criminaliteit als cybercriminaliteit de daders een sterke voorkeur hebben voor cash geld (Kruisbergen et al., 2019). Dit onderstreept het belang van geldezels voor de uitvoering van cybercriminaliteit, en maakt duidelijk dat criminaliteit in de digitale omgeving sterk afhankelijk is van bronnen in de fysieke wereld. Daarom wordt ook wel gesproken van de 'hybridisatie' van criminaliteit, wat ook zichtbaar is bij bijvoorbeeld het rekruteren van geldezels op sociale media (Roks et al., 2021). In Nederland is het witwassen van illegaal verkregen geld strafbaar volgens artikel 420bis van het Wetboek van Strafrecht. Dit artikel stelt dat iemand zich schuldig maakt aan witwassen als die persoon geld ontvangt, bezit of gebruikt dat afkomstig is van een misdrijf en redelijkerwijs had kunnen vermoeden of wist dat het geld afkomstig was van illegale activiteiten (Kruisbergen & Soudijn, 2015). Het gaat dus om het uitvoeren van transacties die erop gericht zijn crimineel geld een ogenschijnlijk legale herkomst te geven, met als uiteindelijk doel de winst uit criminaliteit onontdekt te kunnen gebruiken. Dat is waar geldezels voor worden gebruikt.

Duidelijk is dat geldezels en de bredere (jongeren)populatie niet goed op de hoogte zijn van het fenomeen en de mogelijke gevolgen van dit strafbare feit (Bekkers et al., 2023; Wissink & Quint, 2021; Bekkers et al., 2020). Onderzoekers raden daarom aan dat preventieprogramma's door actoren zoals Halt, de politie, jongerenwerkers, scholen en gemeenten, de consequenties meer onder de aandacht brengen onder de doelgroep, en daarbij gebruikmaken van sociale media, rolmodellen en ervaringsdeskundigen (Bekkers et al., 2023; Wissink & Quint, 2021; Bekkers et al., 2020). Zo is er recent in gemeente Haarlem een campagne uitgevoerd, waarbij jongeren op sociale media zijn blootgesteld aan nagemaakte ronseladvertenties om ze via de advertenties te herleiden naar een waarschuwingspagina (Schiks et al., 2021; Bekkers et al., 2022). In Nederland lopen er nog andere kleinschalige initiatieven door Halt en reclassering, waaronder 'digitaal papier prikken' (i.e. nepaccounts op Instagram rapporteren), een weerbaarheidstraining en voorlichting op scholen (Bekkers et al., 2020).

6.2 Interviews

Opsporing

"Je kunt het op twee manieren benaderen. Je kunt zeggen we beginnen bij de geldezel en zo komen we op de laag erboven. Daarvan weten we inmiddels in de praktijk dat dat niet zoveel oplevert. Maar je kunt het ook omdraaien en top-down beginnen. (…). We gaan telecomsporen uitlopen, daarmee komen we bij een telefoon, via de telefoon naar andere nummers. Dan zie je dat je dat netwerk veel beter in kaart kunt brengen." – RESP10

Respondenten krijgen zicht op de netwerken achter geldezeldelicten via twee lijnen (RESP5, RESP6, RESP10, RESP11, RESP16, RESP17): verhoren van geldezels (bottom-up) of door actief politieonderzoek naar de lagen erboven (top-down). Aangiftes tegen geldezels worden tegenwoordig automatisch gerouteerd naar het politieteam waar de geldezel woonachtig is (RESP5, RESP18). Deze meldingen worden in principe afgehandeld door de VVC-teams (i.e. team veelvoorkomende criminaliteit), en de districtsteams besteden er alleen aandacht aan in het kader van een lopend onderzoek (RESP12). Maar over het algemeen heeft de politie volgens respondenten vooralsnog te weinig capaciteit, prioriteit en kennis voor het opsporen en afhandelen van aangiftes tegen geldezels (RESP3, RESP18), onder meer omdat het als relatief lichte vergrijpen worden beschouwd. "Als we landelijk vijf procent van de geldezels aanpakken, dan is dat veel", aldus RESP18. Hoewel er soms wel relevante informatie naar voren komt bij het verhoor van geldezels, leert de praktijk dat geldezels meestal weinig weten over het criminele netwerk of durven ze niet te verklaren. Bovendien wordt er volgens respondenten ook niet altijd goed uitgevraagd in het verhoor naar bijvoorbeeld accountnamen van ronselaars (RESP1, RESP7, RESP8), hoewel er nu standaard verhoorplannen zijn ontwikkeld om daarbij te ondersteunen. Daarom lukt het volgens respondenten over het algemeen niet om via deze lijn tot het netwerk erboven te komen (RESP6, RESP7, RESP8, RESP10, RESP11, RESP15). Respondenten benoemen hierbij het belang van actiedagen om toch met deze thematiek aan de slag te gaan (RESP13, RESP15, RESP17).

Bij de top-down benadering zoekt de politie vanuit een landelijke benadering naar aangrijpingspunten om leden van het criminele netwerk te identificeren, in theorie bijvoorbeeld via IP-adressen (e.g. van online accounts die geldezels ronselen), telefoonnummers, adressen van cryptowallets, communicatie tussen leden van het netwerk op sociale media, en het uitlezen van telefoons van verdachten. Daarbij wordt voornamelijk op specifieke actoren in een netwerk gefocust. Dergelijk politieonderzoek start vanuit aangiften van slachtoffers of banken, en wordt volgens respondenten al gauw zeer complex vanwege een vertakking aan namen, rekeningnummers, en andere informatie verspreid over het hele land (RESP12, RESP13, RESP16, RESP17). Effectieve opsporing vereist dus samenwerking, capaciteit en gedegen vooronderzoek van de politie. Over het algemeen werkt deze benadering volgens respondenten beter om zicht te krijgen op het netwerk dan de bottom-up benadering via geldezels, zo stellen respondenten (RESP6, RESP7, RESP8, RESP10, RESP11). In het bijzonder benoemen respondenten het belang van informatie op de telefoons van verdachten (RESP1, RESP5, RESP6, RESP7, RESP8, RESP15, RESP20, RESP21). Vaak lijkt er met behulp van die informatie goed zicht te ontstaan op het netwerk. Zo onderhouden criminelen contact met elkaar via sociale media, worden geldezels online geronseld, en bevatten telefoons van verdachten screenshots en notities die het plegen van cybercriminaliteit bewijzen, bijvoorbeeld van gesprekken met slachtoffers of van frauduleuze transacties.

"Er is altijd wel iets dat kan leiden tot meer informatie. Dat is gewoon een startpunt. Informatie opvragen over die account. (…). Het zijn vaak toch mensen die het account ooit hebben aangemaakt op het wifi-netwerk van hun ouders, en daarna voorzichter zijn geworden en een VPN zijn gaan gebruiken. Of ze vergeten het een keertje." – RESP1

Maar dit soort politieonderzoek wordt momenteel nog niet vaak gedaan vanwege gebrek aan capaciteit, kennis en prioriteit (RESP6, RESP7, RESP8, RESP12, RESP20, RESP21); er heerst "cyber-vrees" bij veel van de niet-specialistische teams die dit soort zaken nu ook moeten oppakken en deze teams kiezen daarom eerder voor traditionele zaken. Het delen van informatie tussen verschillende politieteams in het land gaat bovendien nog "stroperig" en is genoemd als verbeterpunt binnen de aanpak van criminele netwerken (RESP1, RESP7, RESP8). Verder is het gebruik van buitenlandse bankrekeningen een obstakel in de opsporing, omdat de politie geen informatie over de rekeninghouder krijgt van buitenlandse banken of pas na zeer lange tijd (RESP5, RESP6, RESP10, RESP11, RESP13). Ook bewindvoerders vinden deze ontwikkeling zorgelijk, want zij hebben ook geen toegang tot buitenlandse bankrekeningen van cliënten (RESP19). Themaspecialisatie en aanpak gericht op lokaal daderschap zijn daarnaast benoemd door respondenten als sterke punt binnen de aanpak van cybercriminaliteit binnen de politie (RESP1, RESP18).

"De basisteams komen niet eens verder meer dan de pinner. Omdat het best wel moeilijk is om achter de witwassers te komen. Achter de mensen die weer bij de deuren zijn geweest of in contact staan met oplichters, daar kom je bijna niet." – RESP12

Opvallend is dat verschillende respondenten het belang onderstrepen van heterdaadsituaties bij de opsporing van criminele netwerken (RESP12, RESP13, RESP15). Daarbij stuit de politie bijvoorbeeld bij een verkeerscontrole per toeval op personen die een groot aantal bankpassen in bezit hebben. Volgens RESP12 en RESP15 berust de aanpak van criminele netwerken nu vaak nog op dat soort toevalstreffers.

Wat betreft opsporing is het volgens vrijwel alle respondenten cruciaal dat er samenwerking plaatsvindt tussen politie en private partijen. In eerste instantie zijn dat banken. Banken delen bijvoorbeeld gegevens over de modus operandi van criminele netwerken met de politie en leveren grote dossiers met informatie

aan bij aangiftes (FOCUS). Maar een groot knelpunt voor banken is volgens respondenten dat er veel restricties zijn omtrent het delen van informatie tussen banken en met de politie (FOCUS, RESP4). Daardoor blijft er volgens respondenten veel nuttige informatie bij banken liggen. Voor individuele banken is het bijvoorbeeld praktisch onmogelijk om een netwerk in kaart te brengen omdat die netwerken zijn verspreid over meerdere banken, en banken zouden dus beter in staat moeten zijn om informatie te delen met elkaar (FOCUS, RESP4). Momenteel zijn er wel initiatieven in ontwikkeling om dat toch te kunnen doen, bijvoorbeeld door een anoniem uniek nummer te genereren voor verdachte telefoons. De politie mag ook niet zomaar zelf informatie opvragen bij banken, daar moet een opsporingsindicatie voor zijn (RESP4). Omdat de politie daarbij ook moet handelen op weinig informatie of onduidelijke informatie, is het verzoek om informatie bij banken vaak te breed of juist te specifiek (RESP4). Vanwege het toenemende gebruik van buitenlandse banken en buitenlandse service providers door criminelen beoogt de politie ook samenwerking op te zetten met dergelijke partijen (RESP13, RESP18).

Naast de banken, benoemen respondenten dat ook andere private bedrijven waardevolle informatie in huis hebben over criminele netwerken omdat criminelen gebruik maken van bepaalde diensten bij de uitvoering van het delict, zoals telecombedrijven, internet service providers, payment service providers, en remote access tool bedrijven (RESP4, RESP7, RESP8, RESP10, RESP11, RESP13, RESP16, RESP17, RESP18). Die bedrijven kunnen dan ook persoonlijke informatie verschaffen over criminelen wat kan ondersteunen in de opsporing, zoals IP-adressen en gebruikersnamen. De politie werkt al samen met een aantal van dat soort partijen, want dan pas ontstaat er zicht op een crimineel netwerk (RESP4, RESP17, RESP18), maar ook hierbij is er strenge regelgeving omtrent het delen van informatie en gaan gesprekken veelal over "hoe we überhaupt kunnen samenwerken en informatie overdragen" (RESP5), en kost het opvragen van informatie veel tijd. Volgens RESP4 hebben die partijen ook meer incentive nodig om samen te werken.

Afdoening
Wat betreft geldezels hebben vrijwel alle respondenten de voorkeur voor stopgesprekken als alternatieve afdoening voor het strafrecht, omdat het vaak kwetsbare mensen betreffen en omdat de strafbare handeling van geldezels (i.e. het overhandigen van een bankpas) juridisch gezien niet zwaar wordt aangerekend. Voor een strafrechtelijke aanpak is bovendien niet altijd capaciteit en het is bij geldezels ook lastig te bewijzen dat er sprake is van wederrechtelijkheid en opzettelijkheid (RESP5, RESP10, RESP11). Hard straffen zou de onderliggende problematiek bij geldezels ook versterken (RESP6, RESP19), en er is bij een alternatieve afdoening meer kans om zicht te krijgen op het crimineel netwerk (RESP1, RESP3). RESP13 was volgens eigen zeggen betrokken bij circa 200 stopgesprekken en daarvan hadden er twee gerecidiveerd. Respondenten benoemen aan de andere kant ook dat de afhandeling van geldezels wel maatwerk is en vooral afhankelijk is van delictgeschiedenis; geldezels die bewust meewerken en vaker de fout ingaan behoeven eerder een strafrechtelijke benadering (RESP7, RESP8, RESP17, RESP18). Hoe dan ook is het verstoren van de geldezel-laag belangrijk voor de aanpak van cybercriminaliteit, aldus verschillende respondenten (RESP12, RESP13, RESP16, RESP17).

"Je moet bij iedereen goed kijken wat z'n rol is. Als iemand 1 keer zijn pas uitleent omdat iemand zegt ja dan kan ik een rekening mee betalen en je krijgt het morgen terug (...). Als daar vervolgens het geld van 35 verschillende mensen mee wordt weggesluisd, ja dan is degene die de pas uitleende niet strafrechtelijk aansprakelijk voor de schade." – RESP10

Naast het strafrecht en andere alternatieve afdoeningen, speelt ook het civiel recht een rol bij de aanpak van geldezelproblematiek. Via het civielrecht kunnen slachtoffers het gestolen geld namelijk terugeisen bij de begunstigde rekeninghouder (de ontvanger van het geld), hetgeen veelal de geldezel betreft. Geldezels zijn in principe altijd aansprakelijk voor het gestolen geld behalve als ze niet wilsbekwaam zijn en bijvoorbeeld handelen onder doodsbedreiging (RESP2). Het civiel recht kan ook in gang gezet worden door de politie (RESP18): een vrij recente ontwikkeling is dat de politie rekeninghouders (waaronder geldezels) selecteert waartegen tenminste vijf aangiftes zijn gedaan en waarbij de persoon niet kwetsbaar is (e.g. niet dakloos). Gegevens van deze persoon verstrekt de politie aan de deurwaarder, die vervolgens de geldezel aansprakelijk kan stellen. RESP2 benadrukt ook dat aansprakelijkheid het uitgangspunt moet zijn en niet kwetsbaarheid. Andere respondenten beschouwen het civiel recht wel als een zeer ingrijpende maatregel dat vooral het belang van het slachtoffer dient (RESP1, RESP3).

"In mijn optiek moet dat geld altijd worden teruggeëist, maar moet je erover nadenken wat je dan vervolgens met deze persoon doet. Maar als je op een gegeven moment zegt 'het is een kwetsbaar persoon dus we gaan niet meer de wet handhaven', man, dat wordt echt heel ingewikkeld in een financieel systeem om dat overeind te houden." – RESP2

De laag boven geldezels behoeft zonder meer een strafrechtelijke aanpak volgens respondenten (RESP5, RESP10, RESP11, RESP16, RESP17). De vraag is wel in hoeverre dit effectief is. Zwaarder straffen werkt niet, aldus RESP16 en RESP17.

"Kijk lui die je pakt nu voor bankhelpdeskfraude, zeg dat ze 24 maanden gevangenisstraf krijgen, we zien gewoon dat die gozer vrijkomt en een week later alweer de aangiftes binnenkomen, met precies hetzelfde MO als daarvoor." – RESP16

Preventie
Alle respondenten benoemen dat in de preventie vooral scholen, ouders, jeugdwerk, en gemeente een rol hebben, maar ook meer specifieke organisaties zoals Marktplaats, het CCV en slachtofferhulp. Zij kunnen Nederlandse burgers bijvoorbeeld beter inlichten over de strafbaarheid van het uitlenen van een bankrekening en de financiële gevolgen (RESP2). Hier zijn nog stappen te zetten. Zo zijn er nog gemeenten die niemand specifiek hebben aangesteld voor het onderwerp cybercriminaliteit en cyberweerbaarheid, de focus ligt over het algemeen nog bij ondermijning (RESP3).

Verder hebben banken volgens respondenten een rol bij het detecteren en voorkomen van fraudes en geldezeltransacties. Banken hebben in het verleden allerlei maatregelen geïntroduceerd, zoals verlaagde limieten en een spaarslot waarmee mensen 24 uur moeten wachten voordat ze spaargeld van de rekening kunnen halen, en soms delen banken ook verhalen van slachtoffers waarmee ze slachtofferschap bespreekbaar willen maken (FOCUS). Een grote bottleneck is volgens respondenten dat online banken en buitenlandse banken soms geen strenge identificatieplicht hanteren en deze makkelijk te omzeilen is. Het is bijvoorbeeld wel nodig een foto van jezelf te maken met je eigen paspoort in de hand, maar dat lukt daders terwijl ze een hand voor hun ogen houden of een vals paspoort gebruiken, aldus RESP15. Vooral online banken en buitenlandse banken hebben daarom nog een belangrijke taak (RESP20, RESP21). Klanten kunnen bij online banken ook grote geldbedragen verwerken zonder dat de bank ingrijpt. Ten slotte benoemen respondenten de verantwoordelijkheid van de maatschappij in bredere zin. Het zou bijvoorbeeld niet moeten kunnen dat je nog steeds duizenden euro's kan uitgeven aan dure kleren met een doorgeknipte bankpas, zo stelt RESP5, en criminelen kunnen zonder identificatieplicht tot wel een miljoen euro op een cadeaukaart storten en dat innen (RESP1). Daar liggen nog kansen voor preventie. Slachtoffers zelf zouden beter kunnen opletten of ze bijvoorbeeld geld overmaken naar een buitenlandse bankrekening (RESP18).

Resumé
Opsporing van cybercriminele netwerken is in toenemende mate onderdeel van het takenpakket van de politie, wat zich reflecteert in de doelstellingen die zijn geformuleerd in de Veiligheidsagenda 2023-2036. Grofweg benoemen respondenten twee lijnen binnen de opsporing van die netwerken: via geldezels (bottom-up) en via aanknopingspunten gericht op de bovenste lagen (top-down). Geldezels worden relatief snel geïdentificeerd, maar die aangiften worden niet altijd opgepakt door de desbetreffende VVC-teams en ook weten geldezels over het algemeen weinig over het criminele netwerk. Criminelen zijn bovendien in staat om grensoverschrijdend te opereren, zowel nationaal als internationaal. De verhouding tussen deze grenzeloosheid en de lokale oriëntatie van gezag is een belangrijk knelpunt in de aanpak van de netwerken. Dat komt onder meer door gebrek aan capaciteit en kennis, maar ook vanwege stroeve samenwerking tussen politieteams en meer inhoudelijke factoren die opsporing belemmeren, zoals het gebruik van buitenlandse bankrekeningen door criminelen. Via het uitlezen van telefoons, IP-adressen en telecomsporen lukt het beter om tot de bovenste lagen van een netwerk te komen. Private partijen zoals banken en telecombedrijven hebben daarom essentiële informatie in huis over cybercriminele netwerken, en publiek-private samenwerking met die partijen is dan ook nodig voor succesvolle opsporing. Daar is ook al sprake van, bijvoorbeeld in de vorm van de ECTF, maar regelgeving omtrent informatiedeling is nog een belemmerende factor volgens betrokken respondenten. Ook internationale samenwerking wordt mogelijk steeds belangrijker vanwege het gebruik van internationale bankrekeningen door dadergroepen en het opereren van Nederlandse dadergroepen in het buitenland. In tegenstelling tot de hogere lagen in het netwerk, wordt bij de vervolging van geldezels ook gekozen voor een alternatieve afdoening in de vorm van stopgesprekken en/of directe aansprakelijkheid. Die keuze berust vooral op de kwetsbaarheid van geldezels en eventuele delictgeschiedenis. Bij geldezels wordt er daarnaast breed ingezet op preventie, waarbij verschillende partijen een verantwoordelijkheid hebben, zoals gemeenten die kunnen inzetten op bewustwordingscampagnes en online banken op strenge identificatieplicht. Respondenten benadrukken daarmee het belang van een integrale benadering vanuit verschillende hoeken in de maatschappij.

7 Eerste aanknopingspunten voor een effectieve aanpak van criminele netwerken

Op basis van de literatuur en de interviews zijn een aantal aanknopingspunten te destilleren voor de effectieve aanpak van criminele netwerken die gebruik maken van geldezels. In dit hoofdstuk beschrijven we die punten aan de hand van vier categorieën: 1) samenwerking, 2) preventie, 3) opsporing, en 4) afdoening. We benadrukken hierbij dat deze punten zijn genoemd door de respondenten, en dat het geen advies betreft van de onderzoekers zelf. Dit hoofdstuk heeft betrekking op deelvraag 6.

Samenwerking
Publiek-publieke samenwerking - nationaal/lokaal
De literatuur en ervaringen in de praktijk maken duidelijk dat criminaliteit hybridiseert. Er is sprake van overlap tussen traditionele criminaliteit en cybercriminaliteit, waarbij gemengde vormen ontstaan en waarbij dadergroepen delicten plegen op basis van criminele mogelijkheden die zich op dat moment voordoen. Dit betekent dat het belangrijk is om een gezamenlijke aanpak op te zetten voor verschillende vormen van financieel-gedreven criminaliteit binnen lokaal en nationaal gezag (RESP3). Zo kennen wijkagenten en jeugdwerkers de daders van cybercriminaliteit mogelijk al omdat die daders eerder betrokken waren bij kleinschalige drugshandel, inbraken of overlast in de buurt.

Naast dat criminaliteit hybridiseert, is het duidelijk dat de activiteiten van criminele netwerken de lokale en regionale grenzen overschrijden; slachtoffers gelinkt aan hetzelfde criminele netwerk komen uit het hele land, maar de netwerken zijn lokaal geaard, daders kennen elkaar uit de buurt en opereren veelal vanuit hun eigen regio (RESP1, RESP5, RESP9, RESP10, RESP11, RESP13, RESP14, RESP15, RESP16, RESP17, RESP22). Dit betekent dat de lokale overheid een belangrijke taak heeft in de aanpak van criminele netwerken en dat er samenwerking nodig is tussen lokale overheden in Nederland en de verschillende opsporingsinstanties, in lijn met de kerndoelen van Operatie Centurion. Alleen door gezamenlijk op te trekken kan er goed zicht ontstaan op het netwerk, zo is duidelijk geworden in de interviews (RESP1, RESP7, RESP8, RESP18).

Publiek-private samenwerking

Private partijen hebben volgens respondenten een sterke informatiepositie wat betreft cybercriminele netwerken, bijvoorbeeld gerelateerd aan IP-adressen, telecomsporen, en persoonsgegevens gekoppeld aan accounts die zijn gebruikt bij het plegen van delicten. Banken vormen de belangrijkste private partner van de politie op dit gebied. Echter zijn er volgens respondenten beperkingen in wet- en regelgeving nog een grote barrière bij informatiedeling, en blijft daardoor veel relevante informatie achter bij banken (FOCUS, RESP4, RESP5). Onderzocht moet daarom worden of en hoe deze informatiedeling beter kan. Ook blijkt de kwaliteit van informatieverzoeken door de politie aan banken niet altijd even goed te zijn; volgens respondenten is een dergelijk verzoek nog te breed of juist te specifiek (RESP4). Verder is vooral het gebruik van online banken en buitenlandse banken door criminele netwerken momenteel een grote bottleneck onder respondenten, en daar ligt dan ook ruimte voor een verbeterde aanpak (RESP20, RESP21) Naast banken zijn een aantal specifieke partijen aangedragen, namelijk telecombedrijven, internet service providers, remote access tool bedrijven, en payment service providers. Respondenten benadrukken daarom het belang van structurele samenwerking met die partijen (RESP4, RESP7, RESP8, RESP10, RESP11, RESP13, RESP16, RESP17, RESP18). De politie gaat die samenwerking ook aan, maar ook hierbij is wet- en regelgeving omtrent privacy volgens respondenten nog een grote barrière en bovendien hebben rechtshulpverzoeken lange doorlooptijden. Benadruk volgens RESP4 in de samenwerking het voordeel ("*incentive*") voor die bedrijven om mee te werken, zoals mogelijke reputatieschade.

Privaat-private samenwerking

Zoals respondenten adviseren, zou er een nog beterere samenwerking moeten komen tussen banken in Nederland (FOCUS, RESP4). Informatie over criminele netwerken is namelijk gefragmenteerd aanwezig binnen het bankwezen, en meer samenwerking en informatiedeling helpt netwerken in kaart te brengen. Er zijn initiatieven om deze samenwerking op te kunnen zetten binnen de heersende regelgeving, bijvoorbeeld door een anoniem uniek nummer te genereren voor verdachte telefoons die wel gedeeld mag worden. Ten slotte zouden online banken meer verantwoordelijkheid moeten nemen en een strengere identificatieplicht hanteren (RESP15). Online banken zijn volgens respondenten in trek bij criminelen, vanwege relatieve anonimiteit. Online banken zouden volgens respondenten ook beter moeten monitoren op verdachte transacties en deze sneller detecteren bij een lagere drempelwaarde (RESP15). Dit vereist scherper toezicht en wet- en regelgeving.

Internationale samenwerking

Internationale samenwerking is belangrijk vanwege mogelijke activiteiten van Nederlandse criminele groeperingen die ook actief zijn in het buitenland en het gebruik van buitenlandse bankrekeningen en buitenlandse betaaldiensten door criminelen, wat een obstakel is in de opsporing (RESP5, RESP6, RESP10, RESP11, RESP13). Zet daarom in op informatiedeling tussen nationale overheden en buitenlandse banken en buitenlandse betaaldiensten. Vooralsnog is deze samenwerking beperkt en zijn buitenlandse partijen weinig responsief.

Preventie

Verstoren laag geldezels

Duidelijk is dat geldezels een belangrijke doelgroep vormt voor preventie en interventie. Geldezels hebben een centrale rol in het crime script van diverse vormen van financieel gemotiveerde cybercrimes; criminelen zijn afhankelijk van de rol van geldezels om ongestoord gebruik te kunnen maken van het gestolen geld. Door te interveniëren op deze schakel, zijn criminelen minder goed in staat een delict succesvol uit te voeren. Hierbij is het in eerste instantie van belang om de doelgroep te kunnen bereiken. Zet daarom in op voorlichting op plekken waar geldezels worden geronseld, zoals op sociale media (zie ook Bekkers et al., 2022; Schiks et al., 2021), maar ook op fysieke plekken, waaronder scholen, daklozenopvang, verslavingsklinieken, en instellingen voor begeleid wonen. Meer specifiek blijkt uit literatuur dat het belangrijk is om deze voorlichting te focussen op het verhogen van de risicoperceptie omtrent de pakkans en de consequenties van het uitlenen van bankpassen, zowel binnen het strafrecht en civielrecht, en het de-normaliseren van het plegen van cybercriminaliteit (Bekkers et al., 2022, 2023; Bekkers & Leukfeldt, 2023). Dit zijn namelijk belangrijke factoren die bijdragen aan geldezelen. Dergelijke voorlichting is niet alleen een taak van de overheid, ook partijen als Marktplaats en slachtofferhulp zouden breder kunnen inzetten op het verstrekken van informatie over geldezelen, zoals benoemd door experts in de interviews (RESP2).

Verstoren 'hogere lagen' in criminele netwerk

Niet alleen bij geldezels, ook bij de hogere lagen in het crimineel netwerk speelt normalisatie van het plegen van cybercriminaliteit mogelijk een belangrijke rol bij daderschap, zo blijkt uit de interviews (FOCUS, RESP9, RESP17, RESP20, RESP21). Het meest prominente voorbeeld hiervan is de subcultuur rondom de f-game op sociale media. Deze term refereert naar het plegen van online fraudes, waarbij jongeren op sociale media pronken met dure spullen en geld, en proberen nieuwe leden te werven voor het plegen van delicten. Omdat criminelen actief zijn op deze platformen, zou online situationele criminaliteitspreventie ingezet kunnen worden, bijvoorbeeld door het gebruik van rolmodellen, influencers en "ervaringsdeskundigen" in zelfgemaakte video's of advertenties, om een verandering teweeg te brengen in de heersende normen en waarden op sociale media (e.g. Wissink & Quint, 2021; Bekkers et al., 2023). Deze vorm van preventie is gericht op het verminderen van de gelegenheid om criminaliteit te plegen, en wordt steeds meer toegepast in de digitale omgeving met veelbelovende resultaten (e.g. Ho et al., 2022). Het doel hierbij is met name het voorkomen van jonge aanwas.

Cybercriminaliteit als maatschappelijke verantwoordelijkheid

Verschillende respondenten onderstrepen het belang van de aanpak van cybercriminaliteit vanuit een maatschappelijke verantwoordelijkheid (RESP1, RESP5, RESP18, RESP20, RESP21). Zet bijvoorbeeld in op het verhogen van de weerbaarheid van slachtoffers. Informeer burgers over de werkwijze van criminele netwerken en verdachte situaties, bijvoorbeeld wanneer wordt gevraagd geld over te maken naar buitenlandse bankrekeningen. Met name gemeenten kunnen hier een belangrijke rol bij spelen, maar ook burgers onderling. Verder benoemen respondenten dat private partijen een meldplicht zouden moeten hebben bij bijvoorbeeld opvallende transacties of gedragingen, waaronder hoge stortingen op cadeaukaarten, en het gebruik van bankpasjes die doorgeknipt zijn (RESP1, RESP5).

Opsporing

Versterken lokale overheid

Zowel de literatuur als de interviews met experts maken het belang duidelijk van een sterke lokale aanpak van cybercriminaliteit in termen van kennis, motivatie, en prioriteit (RESP6, RESP7, RESP8, RESP12, RESP20, RESP21). Cybercriminaliteit wordt onterecht nog beschouwd als iets wat per definitie internationaal, ongrijpbaar, complex en abstract is. Gemeenten kunnen inwoners bijvoorbeeld meer stimuleren om aangiften te doen en lokale ontwikkelingen in dader- en slachtofferschap van cybercriminaliteit beter monitoren. Ook zouden gemeenten specifieke personen moeten aanstellen die zich richten op het fenomeen cybercriminaliteit en cyberweerbaarheid; volgens een respondent hebben weinig gemeenten in Nederland een medewerker in dienst die zich specifiek richt op dit thema (RESP3). Lokale politieteams zouden meer prioriteit moeten geven aan het onderwerp cybercriminaliteit, ondanks dat de aanpak van cybercriminaliteit in het algemeen is geprioriteerd in de Veiligheidsagenda. Er heerst "cyber-vrees", en de politie kiest daarom ook eerder voor zaken betreffende traditionele criminaliteit. Het is dus van belang deze angst weg te nemen. Maak daarbij gebruik van themaspecialisten en analisten die aanwezig zijn binnen of buiten de politieorganisatie (RESP1, RESP18).

Investeer ook in de "top-down" benadering

Door het gebrek aan kennis en prioriteit binnen de lokale politieorganisatie, richt de opsporing zich op individuele aangiften in plaats van de hogere lagen (de "top-down" benadering), zoals telecomsporen en IP-adressen. Respondenten geven echter aan dat op deze manier beter zicht op het netwerk ontstaat, en het zou dan ook lonen om te investeren in deze benadering (RESP6, RESP7, RESP8, RESP10, RESP11).

Geldezels in het kader van opsporing

Tegelijkertijd zou de politie ook meer aandacht dienen te besteden aan de doelgroep geldezels in het kader van effectieve opsporing, bijvoorbeeld door aangiftes tegen geldezels vaker in behandeling te nemen, de doelgroep beter te verhoren, en actiedagen te organiseren (RESP1, RESP3, RESP7, RESP8; RESP13, RESP15, RESP17, RESP18). Maak duidelijk aan de aangiftebehandelaars en verhoorders waarom ze bepaalde informatie uitvragen en wat de meerwaarde daarvan kan zijn op een later moment in de opsporing. Zo kan bewijsmateriaal in de telefoon van geldezels waardevolle informatie opleveren over het netwerk, zoals accountnamen van online ronselaars en gesprekken met die persoon, ondanks dat geldezels zelf vaak niet weten wie de ronselaars zijn. Maak daarbij gebruik van de standaardverhoorplannen die tegenwoordig beschikbaar zijn.

Digitale omgevingen en devices

Wat betreft de opsporing, is het duidelijk dat criminelen actief zijn op de openbare platformen zoals Snapchat en Telegram, zowel ter voorbereiding van het plegen van delicten, als communicatie met medeplegers tijdens de uitvoering ervan. Mogelijk bevatten die platformen daarom nuttige informatie voor de opsporing, zoals accountnamen, geografische oriëntatie van criminelen (e.g. postcodes), en de werkwijze van criminele netwerken. Respondenten adviseren daarom dat de politie inzet op het monitoren van deze platformen en bij het uitlezen van de telefoon van verdachten (pinners, geldezels, hoofddaders, etc.) specifiek aandacht besteed aan eventuele online communicatie, zoals accountnamen, ondanks dat die informatie ogenschijnlijk niet direct waarde heeft voor de opsporing; op een later moment in het onderzoek kan dat mogelijk veranderen. Uit de interviews blijkt dat het uitlezen van telefoons van verdachten essentieel is om zicht te krijgen op het criminele netwerk (RESP1, RESP5, RESP6, RESP7, RESP8, RESP15, RESP20, RESP21). Ze bevatten vaak sterk bewijsmateriaal, zoals screenshots van gesprekken met slachtoffers, en bieden inzicht in onderlinge verhoudingen en rolverdelingen in het netwerk. Zelfs tijdens het plegen van delicten spelen online omgevingen mogelijk een belangrijke rol, bijvoorbeeld voor het aansturen van medeverdachten.

Heterdaadsituaties

Zoals benoemd door respondenten, lijken heterdaadsituaties een belangrijke rol te spelen bij het inzichtelijk krijgen van criminele netwerken (RESP12, RESP13, RESP15). Zo is bij bankhelpdeskfraude opvallend dat de daders opereren vanuit recreatiewoningen, zoals AirBnb's en vakantieparken, of vanuit het huis van één van de daders. Met behulp van bijvoorbeeld telecomsporen, taps, en IP-adressen, is het mogelijk dergelijke omgevingen te identificeren tijdens het plegen van de delicten. Heterdaadsituaties zijn niet alleen direct bewijs voor illegale activiteiten, maar zo kan de politie ook in handen komen van telefoons van verdachten en ander bewijsmateriaal om zicht te krijgen op het netwerk. Andere heterdaadsituaties die zijn benoemd zijn routine verkeerscontroles; het is van belang dat de politie aandacht besteed aan objecten in de auto die mogelijk wijzen op fraudes, zoals een groot aantal simkaarten en bankpassen.

Afdoening

Stopgesprekken

Stopgesprekken zijn een interessante vorm van alternatieve afdoening voor geldezels volgens vrijwel alle respondenten. Respondenten zijn positief over deze methode, omdat 1) geldezels vaak kwetsbare mensen betreffen, 2) de strafbare handeling van geldezels in principe niet zwaar wordt aangerekend en strafrecht dus niet altijd passend is, 3) de capaciteit voor een strafrechtelijke aanpak beperkt is, 4) het überhaupt lastig te bewijzen is dat er bij geldezels sprake is van wederrechtelijkheid en opzettelijkheid, 5) hard straffen de onderliggende problematiek bij geldezels zou versterken, en 6) met stopgesprekken de kans groter is dat er zicht ontstaat op het crimineel netwerk. Wel merken we op dat dit soort interventies geëvalueerd moeten worden omdat anders onbekend is welke effect ze daadwerkelijk hebben. Ten slotte zouden geldezels die vaker de fout in gaan en een bredere delictgeschiedenis hebben, wel een strafrechtelijke benadering behoeven, zo blijkt uit de interviews.

Het civiel recht en geldezels

Duidelijk is dat ook het civiel recht een rol speelt bij de afdoening van geldezelen, en mogelijk wordt die rol groter vanwege verruimde mogelijkheden voor slachtoffers van online fraude om de ontvanger van het gefraudeerde geld direct aansprakelijk te

stellen. Deze aanpak ontlast mogelijk het strafrecht, maar kan zeer ingrijpende gevolgen hebben voor geldezels, terwijl zij niet de daadwerkelijke daders zijn en niet meer over het gestolen geld beschikken. Zo kan er beslag worden gelegd op de eigendommen van geldezels en diens familie. In het kader van interventie en preventie zouden de consequenties voor geldezels in het civiel recht een afschrikwekkende werking kunnen hebben, en het is dan ook belangrijk deze gevolgen breder onder de aandacht te brengen onder jongeren (RESP2), hoewel ook hierbij evaluatie moet plaatsvinden naar de effecten van de interventie.

Resumé

Er zijn door respondenten verschillende aanknopingspunten benoemd voor een effectieve aanpak van criminele netwerken achter geldezeldelicten. Om te beginnen lijkt het van belang om in te zetten op een verbeterde samenwerking tussen overheidsorganisaties zelf (publiek-publiek) en ook tussen overheid en private partijen (publiek-privaat). Zo benoemen respondenten dat de lokale overheid een centrale rol heeft in de aanpak van criminele netwerken en dat, vanwege de grenzeloosheid van cybercriminaliteit, samenwerking tussen de verschillende lokale overheden en opsporingsinstanties nodig is voor een effectieve aanpak. Daarnaast hebben private partijen een sterke informatiepositie en die informatie is cruciaal voor de aanpak van criminele netwerken, bijvoorbeeld gerelateerd aan IP-adressen en telecomsporen. Die partijen betreffen in eerste instantie banken, maar ook telecombedrijven, internet service providers, remote access tool bedrijven, internationale online banken, en payment service providers. Wet- en regelgeving omtrent privacy en beperkte responsiviteit vanuit de private sector zit effectieve samenwerking echter nog in de weg. Bovendien zijn respondenten het eens dat geldezels een belangrijke doelgroep vormen in het kader van preventie en interventie, gezien de essentiële rol in het crime script, waarbij al verschillende voorbeelden zijn te vinden in de literatuur. Binnen de opsporing wijst de praktijk uit dat een sterke lokale overheid in termen van kennis, motivatie, en prioriteit, bijdraagt aan een succesvolle aanpak, waarbij het loont om de opsporing te richten op de hogere lagen in het netwerk in plaats van individuele aangiften als uitgangspunt, waarbij de politie gebruik maakt van bijvoorbeeld telecomsporen en IP-adressen. Vooral het uitlezen van telefoons van verdachten levert waardevolle informatie op, zo blijkt in de praktijk. Volgens respondenten zou het ook kunnen helpen als de aanpak van geldezels wordt geïntensiveerd in het kader van opsporing, en er bijvoorbeeld meer aandacht uitgaat naar de kwaliteit van het verhoor en het aantal aangiftes tegen geldezels dat in behandeling wordt genomen. Ten slotte lijken stopgesprekken en het civiel recht interessante alternatieve afdoeningen voor geldezels, maar dergelijke interventies behoeven nog evaluatie.

8 Conclusies en aanbevelingen voor verdiepende analyse

8.1 Conclusies

Het doel van dit onderzoek was het in kaart brengen van de aard van criminele netwerken die gebruik maken van geldezels, om daarmee concrete aangrijpingspunten te identificeren voor zowel de preventie, verstoring als opsporing van deze criminele netwerken. Hiermee kan worden voorzien in de behoefte aan een effectieve, integrale aanpak van cybercriminaliteit, zowel in brede zin als in enge zin. Binnen dit onderzoek stonden zes deelvragen centraal. Om die vragen te beantwoorden zijn in de verkennende fase van het huidige project verschillende methodieken toegepast, namelijk literatuuronderzoek, semigestructureerde interviews met in totaal 22 experts uit de praktijk, en een focusgroep met 10 experts van de ECTF. Deze bevindingen vormen de basis voor de verdiepende analyse.

1. Bij welke vormen van cybercriminaliteit worden geldezels ingezet?

   Geldezels spelen een rol bij de uitvoering van verschillende vormen van financieel-economische cybercriminaliteit. In principe betreffen dat de delicten waar Operatie Centurion zich op richt, namelijk bankhelpdeskfraude, hulpvraagfraude, phishing, en aan- en verkoopfraude. Mogelijk worden geldezels ook bij andere meer internationale delicten ingezet, zoals CEO-fraude en datingfraude, maar daar is vanwege de aard van die delicten minder zicht op in de literatuur en bij de respondenten. Wat betreft de geldezeldelicten heeft de politie momenteel vooral te maken met bankhelpdeskfraude, terwijl dat voorheen voornamelijk phishing en hulpvraagfraude waren. Mogelijk zijn dit in ieder geval voor een deel wel dezelfde netwerken die overstappen op andere delicten, in lijn met nieuwe criminele mogelijkheden die ontstaan door ontwikkelingen in de maatschappij.

2. *Wat is de aard van de delicten waarmee de cybercriminele netwerken zich bezighouden?*

   Criminele netwerken verschillen in de specifieke criminele activiteiten die worden uitgevoerd. De literatuur maakt duidelijk dat de delictstijl van sommige criminele groeperingen wordt gekarakteriseerd als “cafeteria-style”, waarbij ze opportunistisch handelen en betrokken zijn bij delictsvormen waar op dat moment veel geld mee te verdienen is. Deze bevindingen worden bevestigd door respondenten in de interviews. Daders die zich nu met bankhelpdeskfraude bezig houden hebben in het verleden bijvoorbeeld Whatsappfraude, phishing of aan- en verkoopfraude gepleegd, of waren al bekend bij de politie vanwege inbraken, drugshandel of overvallen. Dit betekent ook dat er sprake is van hybridisatie en overlap tussen traditionele vormen van criminaliteit en cybercriminaliteit. Hierbij observeren respondenten bijvoorbeeld in toenemende mate gebruik van geweld en bezit van vuurwapens, hoewel daadwerkelijke incidenten nog niet systematisch lijken plaats te vinden.
   De activiteiten van lokale cybercriminele netwerken achter geldezeldelicten lijken dus in principe vooral opportunistisch van aard, waarbij ze handelen op criminele mogelijkheden die zich voordoen. Sommigen groepen verplaatsen hun activiteiten volgens respondenten zelfs naar het buitenland omdat Nederlandse burgers weerbaar zijn geworden. Daartegenover wijst literatuur uit dat er groeperingen zijn die zich specialiseren in een bepaalde vorm van cybercriminaliteit, vaak met een sterk technisch en internationaal component. Dergelijke netwerken zijn bij de interviews echter minder ter sprake gekomen, mogelijk ook vanwege de lokale focus van de respondenten. Wat betreft geldezels lijkt bij een deel ook sprake van een delictgeschiedenis, mogelijk vooral voor lichte vergrijpen, hoewel geldezels hier waarschijnlijk sterk in verschillen.
   Het optreden als geldezels kan ook een opstapdelict zijn richting zwaardere vormen van criminaliteit, maar het is onder respondenten en in de literatuur nog onduidelijk in hoeverre er sprake is van recidive en doorgroei van geldezels in criminaliteit.

3. *Wat zijn de kenmerken van de cybercriminele netwerken die geldezels inzetten?*

   Er is relatief weinig bekend over de kenmerken van cybercriminele netwerken, met name onder respondenten. Literatuuronderzoek en de interviews maken duidelijk dat bestaande sociale relaties van belang zijn bij het ontstaan van criminele netwerken, waarbij de kernleden/hoofddaders elkaar al kennen uit de buurt of als familielid. Bij de groei van het netwerk speelt zowel de fysieke omgeving als online omgevingen een belangrijke rol. Geldezels worden bijvoorbeeld lokaal geronseld bij verslavingsklinieken en de daklozenopvang, maar ook op sociale media, zoals naar voren komt in de literatuur en de interviews. Ze zijn onderdeel van subculturen waarin het plegen van fraudes genormaliseerd en geaccepteerd is, en waarbij er een lage risicoperceptie heerst omtrent de gevolgen. Met name Telegram en de f-game groepen bieden mogelijkheden om in contact te komen met de mensen en de componenten die nodig zijn voor het plegen van een delict. In een aantal gevallen ontstaat en groeit een netwerk mogelijk zelfs volledig via online contacten. De precieze samenstelling en omvang van een cybercrimineel netwerk verschilt ook en lijkt afhankelijk van het type delict. Zo zijn bij bankhelpdeskfraude relatief veel rollen en taken nodig vergeleken met de andere geldezeldelicten. Wel is er over het algemeen sprake van een vaste kern die verantwoordelijk is voor de uitvoering van het delict, die daarbij gebruik maken van andere personen indien dat nodig is. Het is nog onduidelijk hoe stabiel dergelijke netwerken zijn en hoelang ze over de tijd heen samenwerken, en waarschijnlijk verschillen netwerken daar ook in. Op basis van de beperkte kennis in de literatuur en de interviews is dus te concluderen dat criminele netwerken verschillen wat betreft structuur en ontstaan en groei.

4. *Op welke wijze worden geldezels ingezet in de cybercriminele netwerken?*

   Geld dat is gestolen door middel van financieel-gemotiveerde delicten, wordt door de daders overgemaakt van de bankrekeningen van slachtoffers naar de bankrekeningen van geldezels. Daarna wordt het geld zo snel mogelijk contant opgenomen door de kernleden, faciliteerders of geldezels zelf. In andere gevallen wordt het geld verder verhuld door bijvoorbeeld de aankoop van cryptovaluta, meerdere transacties naar andere nationale of internationale bankrekeningen, of via geldwisselkantoren. De daders maken gebruik van deze constructie omdat zij op die manier anoniem blijven en zo uit zicht blijven van banken en opsporingsinstanties; ze gebruiken immers niet hun eigen bankrekening. Criminelen kiezen bij de uitvoering van geldezeldelicten echter niet alleen voor geldezels, maar ook voor de aanschaf van producten of cadeaukaarten (vanuit de bankrekening van het slachtoffer), cryptovaluta, online buitenlandse bankrekeningen, zakelijke bankrekeningen, of online Nederlandse bankrekeningen. Deze witwasmethodieken zijn benoemd door respondenten en waren grotendeels eerder ook al beschreven in de literatuur, echter is er mogelijk een ontwikkeling waarbij het gebruik van geldezels afneemt en criminelen vaker toevlucht zoeken bij alternatieven. Het is mogelijk dat geldezels ook daarbij een rol spelen, omdat ze bijvoorbeeld cryptowallets of online bankrekeningen op naam hebben, maar daar is nog weinig zicht op vanwege beperkte toegang tot persoonlijke gegevens van de rekeninghouders. Hierbij onderstrepen respondenten het belang van katvangers in bredere zin, aangezien er ook mensen nodig zijn voor het bezorgen of ophalen van bestelde producten, het op naam zetten van valse webshops, en het pinnen van het gestolen geld.

   Verder is duidelijk dat geldezels een heterogene groep is wat betreft persoonlijke eigenschappen. De rode draad is dat het vaak, maar niet altijd, gaat om kwetsbare individuen die relatief makkelijk te beïnvloeden zijn. Dit bleek uit het literatuuronderzoek, en werd bevestigd door respondenten in de interviews. Het betreffen bijvoorbeeld jongeren die de consequenties van hun gedrag niet goed kunnen overzien, maar ook daklozen, verslaafden, en Oost-Europese arbeidsmigranten. De meeste respondenten zijn ten slotte van mening dat geldezels geen onderling netwerk vormen, en dat ze ad hoc in een netwerk terecht komen, bijvoorbeeld via digitale platformen. De focusgroep benoemt echter dat geldezels wel onderdeel zijn van witwasnetwerken die voor allerlei delicten worden ingezet, zowel voor traditionele criminaliteit als cybercriminaliteit.

5. *Hoe ziet de aanpak van cybercriminele netwerken die gelezels inzetten er momenteel uit?*

   Binnen de aanpak van cybercriminele netwerken is er een onderscheid in opsporing en vervolging, alternatieve afdoening, en preventie. De opsporing van cybercriminele netwerken door de politie verloopt grofweg via twee lijnen: via geldezels (bottom-up), en via aanknopingspunten gericht op de bovenste lagen (top-down). Geldezels worden relatief snel geïdentificeerd, maar aangiftes worden niet altijd opgepakt door de desbetreffende VVC-teams, geldezels worden niet altijd goed verhoord, en bovendien weten geldezels over het algemeen weinig over het criminele netwerk. Vooralsnog is het daarom minder succesvol om via geldezels tot het netwerk erboven te komen. Via opsporingsmogelijkheden gerelateerd aan bijvoorbeeld IP-adressen van verdachten en telecomsporen lukt dat beter volgens respondenten. Deze strategie vraagt echter gedegen politieonderzoek met een landelijke visie, en dat blijkt in de praktijk nog lastig. Dat komt onder meer door gebrek aan

capaciteit, kennis, prioriteit en landelijke aansturing, maar ook vanwege stroeve samenwerking tussen politieteams en meer inhoudelijke factoren die het onderzoek belemmeren, zoals het gebruik van buitenlandse bankrekeningen door criminelen.

In de opsporing is samenwerking met publiek-private partners essentieel; partijen zoals banken en telecombedrijven hebben cruciale informatie over het cybercriminele netwerk in huis. Deze samenwerking wordt volgens respondenten belemmerd door regelgeving omtrent privacy. Wat betreft de afdoening behoeven de daders van cybercriminaliteit volgens respondenten zonder meer een strafrechtelijke aanpak, waar vaak een aantal jaar gevangenisstraf de maat is. Bij geldezels daarentegen wordt in de meeste gevallen gekozen voor een alternatieve afdoening buiten het strafrecht, in de vorm van stopgesprekken. Deze keuze berust vooral op de kwetsbaarheid van geldezels en eventuele delictgeschiedenis, maar ook op capaciteit en prioriteit binnen de politie en OM. Mede daarom wordt er breed ingezet op preventie van geldezelen, waarbij verschillende partijen een verantwoordelijkheid hebben, zoals gemeenten die inzetten op bewustwordingscampagnes en online banken op strenge identificatieplicht. Dit onderstreept het belang van een integrale benadering vanuit verschillende hoeken in de maatschappij, waarbij de cyberweerbaarheid van burgers en bedrijven centraal staat. Het effect van preventieve maatregelen gericht op crimineel gedrag en slachtofferschap is lastig vast te stellen en er is nog weinig gedegen onderzoek verricht in het geval van cybercriminaliteit specifiek, maar voorlopige evaluaties laten een positief beeld zien.

6. *Waar binnen het crime script zitten effectieve aangrijpingspunten voor zowel preventie, verstoring als opsporing van cybercriminele netwerken?*
   Er zijn door respondenten verschillende aanknopingspunten benoemd voor een effectieve aanpak van criminele netwerken achter geldezeldelicten. Om te beginnen lijkt het van belang om in te zetten op een verbeterde samenwerking tussen overheidsorganisaties zelf (publiek-publiek) en ook tussen overheid en private partijen (publiek-privaat). Zo benoemen respondenten dat de lokale overheid een centrale rol heeft in de aanpak van criminele netwerken en dat, vanwege de grenzeloosheid van cybercriminaliteit, samenwerking en informatiedeling tussen de verschillende lokale overheden en opsporingsinstanties nodig is voor een effectieve aanpak. Daarnaast hebben private partijen een sterke informatiepositie en die informatie is cruciaal voor het inzichtelijk maken en opsporen van criminele netwerken, bijvoorbeeld gerelateerd aan IP-adressen, telecomsporen, en persoonsgegevens gekoppeld aan accounts die zijn gebruikt bij het plegen van delicten. Deze zaken spelen een rol in het crime script van de verschillende geldezeldelicten, zowel in het kader van voorbereiding als de uitvoering. Die partijen betreffen in eerste instantie banken, maar ook telecombedrijven, internet service providers, remote access tool bedrijven, internationale online banken, en payment service providers.

   Bovendien zijn respondenten het eens dat geldezels een belangrijke doelgroep vormen in het kader van preventie en interventie, gezien de essentiële rol in het crime script; het beperken van de toegang van criminelen tot bankrekeningen verstoort succesvolle uitvoering van het delict. Daarom zou het volgens respondenten ook kunnen helpen als de aanpak van geldezels wordt geïntensiveerd in het kader van opsporing, en er bijvoorbeeld meer aandacht uitgaat naar de kwaliteit van het verhoor en het aantal aangiftes tegen geldezels dat in behandeling wordt genomen. Binnen de opsporing wijst de praktijk uit dat een sterke lokale overheid in termen van kennis, motivatie, en prioriteit, bijdraagt aan een succesvolle aanpak, waarbij het loont om de opsporing te richten op de hogere lagen in het netwerk in plaats van individuele aangiften als uitgangspunt, waarbij de politie gebruik maakt van bijvoorbeeld telecomsporen en IP-adressen. Vooral het uitlezen van telefoons van verdachten levert waardevolle informatie op over het opereren van het netwerk en de onderlinge communicatie voor, tijdens, en na het plegen van delicten, zo blijkt in de praktijk.

8.2 Aanknopingspunten voor nader onderzoek

De volgende stap in dit project is verdiepende analyse op basis van afgeronde opsporingsonderzoeken van de politie. Het literatuuronderzoek en de interviews bieden houvast voor deze verdiepingsslag. Om te beginnen zou de verdieping zich primair moeten richten op het nader in kaart brengen van de aard van cybercriminele netwerken. De respondenten en de interviews bieden al waardevolle inzichten, maar over het algemeen is kennis nog beperkt en gefragmenteerd. Het is nodig uitspraken van respondenten te toetsen aan bevindingen in politieonderzoek en dit ook te vergelijken met eerdere analyses van criminele netwerken in de literatuur (e.g. Leukfeldt et al., 2017a,b,c,d,e), om zo beter zicht te krijgen op de netwerk structuur, het ontstaan en de groei van netwerken, en de activiteiten waar netwerken zich mee bezig houden. We adviseren bij nader onderzoek specifiek aandacht te besteden aan de volgende punten, omdat ze implicaties hebben voor de opsporing en er nog relatief weinig over bekend is.

a. “The online and offline side of cybercrime”
   Zowel het literatuuronderzoek als expertinterviews wijzen uit dat digitale platformen een belangrijke rol spelen bij het ontstaan en de groei van cybercriminele netwerken, en mogelijk wordt die rol ook steeds groter. Tegelijkertijd zijn netwerken afhankelijk van de fysieke wereld en al bestaande sociale relaties; daders kennen elkaar vaak al uit de buurt, en bovendien vinden delen van de uitvoering van cybercriminaliteit offline plaats, zoals het pinnen van gestolen geld en het ophalen van luxe goederen bij winkels. Deze momenten kunnen van belang zijn voor de opsporing. Het behoeft echter nog een verdiepingsslag om beter zicht te krijgen op de rol van zowel online als offline mechanismen in de groei van netwerken en de uitvoering van cybercriminaliteit, zowel voor, tijdens, en na het plegen van delicten. Zo zijn er ook aanwijzingen dat daders contact onderhouden via sociale media bij het plegen van delicten, en dat openbare berichtgeving van criminelen op bijvoorbeeld Telegram bruikbare informatie bevat, wat aanknopingspunten kan bieden voor de opsporing.

b. Witwasmethodieken en alternatieven voor geldezels
   Cybercriminaliteit is dynamisch, en dat uit zich ook in ontwikkelingen wat betreft het verbergen en wegsluizen van gestolen geld. Hoewel geldezels nog steeds nodig zijn voor de uitvoering, geven enkele respondenten aan dat de “klassieke” geldezel mogelijk een kleinere rol speelt of krijgt dit andere verschijningsvormen, waarbij criminelen bijvoorbeeld ook gebruik maken van internationale bankrekeningen, cadeaukaarten, cryptovaluta of de directe aanschaf van luxe producten. Het is daarom belangrijk goed inzicht te krijgen op hoe cybercriminelen geld wegsluizen, hoe en in welke situatie ze kiezen voor een bepaalde witwasmethode, en wat de ontwikkelingen zijn wat betreft het gebruik van geldezels.

c. Criminele carrières en ontwikkeling in modus operandi
   Er is nog relatief weinig zicht op de levensloop en criminele carrière van zowel de individuele daders van cybercriminaliteit als die van geldezels, en ook wat betreft de activiteiten van netwerken over de tijd heen. Daders lijken te schakelen tussen delicten op basis van winstmarges en pakkansen, en handelen in die zin dus opportunistisch, maar het is nog niet bekend hoe dit zich ontwikkelt in de loop van de jaren, hoe en waarom de modus operandi van een bepaald delict veranderd en hoe stabiel criminele netwerken wat betreft verschillende delictsvormen. Zo hebben ook verschillende officieren van justitie en politiemedewerkers het vermoeden dat cybercriminelen betrokken zijn bij bankhelpdeskfraude zodat ze vermogen opbouwen om te kunnen investeren in de drugshandel. Dit is echter gebaseerd op geluiden vanuit politieonderzoeken en er mist nog empirisch bewijs.

d. Evalueren alternatieve interventies
   Het blijkt dat momenteel al enkele alternatieve interventies worden ingezet gericht op geldezels, waarbij met name stopgesprekken in de praktijk vaak wordt toegepast volgens respondenten. Hierbij worden geldezels aangesproken op hun gedrag door de politie zonder juridische gevolgen. Deze afdoening zou volgens respondenten beter bij de doelgroep passen, en ervaringen in de praktijk zijn positief. Het behoeft echter nog wetenschappelijke evaluatie om inzicht te krijgen in het daadwerkelijk effect van de interventie op het gedrag van geldezels. Naast stopgesprekken, lijken civielrechtelijke afdoeningen ook van steeds groter belang, waarbij geldezels schade moeten terugbetalen na vorderingen van het slachtoffer. Ook hierbij geldt dat het nog onduidelijk is wat de gevolgen zijn en in hoeverre het een preventieve of repressieve werking heeft op delictgedrag. Tot slot lijken er andere kleinschalige interventies toegepast te worden in Nederland, zoals voorlichting door Halt en informatiecampagnes van de politie. Weinig is echter wetenschappelijk onderbouwd en geëvalueerd, dus dat is een belangrijke richting voor toekomstig onderzoek.

Referenties

Arevalo, B. C. (2015). *Money Mules: Facilitators of financial crime. An explorative research on money mules* (thesis Universiteit Utrecht).

Arnett, J. (1992). Reckless behavior in adolescence: A developmental perspective. *Developmental Review*, *12*(4), 339-373.

Bekkers, L. M. J., & Leukfeldt, E. R. (2023). Recruiting money mules on instagram: a qualitative examination of the online involvement mechanisms of cybercrime. *Deviant Behavior*, *44*(4), 603-619.

Bekkers, L. M., Moneva, A., & Leukfeldt, E. R. (2022). Understanding cybercrime involvement: a quasi-experiment on engagement with money mule recruitment ads on Instagram. *Journal of Experimental Criminology*, 1-20.

Bekkers, L., Schiks, J., & Leukfeldt, E. R. (2020). *Naar een interventie tegen geldezels. Een pilot in de gemeente Haarlem.* Den Haag: Centre of Expertise Cybersecurity, Haagse Hogeschool.

Bekkers, L., Van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (2023). Money Mules and Cybercrime Involvement Mechanisms: Exploring the Experiences and Perceptions of Young People in the Netherlands. *Deviant Behavior*, 1-18.

Boekhoorn, P. (2020). De aanpak van cybercrime door regionale eenheden van de politie. *Politie en Wetenschap*, 102.

Boyer, T. W. (2006). The development of risk-taking: A multi-perspective review. *Developmental Review*, *26*(3), 291-345.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77-101.

Braun, V., & Clarke, V. (2012). *Thematic analysis*. American Psychological Association.

Brown, C. S. D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. International Journal of Cyber Criminology, 9(1), 55–119.

Bulanova-Hristova, G., Kasper, K., Odinot, G., Verhoeven, M., Pool, R., de Poot, C., Werner, W., & Korsell, L. (2016). *Cyber-OC - scope and manifestations in selected EU member states.* Wiesbaden: Bundeskriminalamt.

CCV. (2022). *Factsheet City Deal Lokale Weerbaarheid Cybercrime.* Geraadpleegd via https://hetccv.nl/fileadmin/Bestanden/Onderwerpen/Cybercrime/Factsheet_City_Deal_Lokale_Weerbaarheid_Cybercrime.pdf.

Centraal Bureau voor de Statistiek (CBS) (2022a). *Veiligheidsmonitor 2021*. Geraadpleegd via https://www.cbs.nl/nl-nl/publicatie/2022/09/veiligheidsmonitor-2021.

Centraal Bureau voor de Statistiek (CBS) (2022b). *2,5 miljard euro schade door criminaliteit tegen burgers.* Geraadpleegd via https://www.cbs.nl/nl-nl/nieuws/2022/38/2-5-miljard-euro-schade-door-criminaliteit-tegen-burgers.

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & security, 30*(8), 719-731.

Choo, K. K. R., & Smith, R. G. (2008). Criminal exploitation of online systems by organised crime groups. *Asian Journal of Criminology, 3*, 37-59

Custers, B. H., Pool, R. L., & Cornelisse, R. (2019). Banking malware and the laundering of its profits. *European Journal of Criminology, 16*(6), 728-745.

Dunham, K. (2006). Money mules: An investigative view. *Information Security Journal, 15*(1), 6.

Eeden, C. A. J. van den, Berkel, J. J. van, Lankhaar, C. C., & Poot, C. J. de (2021). *Opsporen, vervolgen en tegenhouden van cybercriminaliteit*. Den Haag: WODC.

Europol. (2021). *Money Muling*. Geraadpleegd via https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling.

Felson, M. (2003). The Process of Co-offending. In M. J. Smith and D.B. Cornish (Eds.), *Theory for Practice in Situational Crime Prevention* (pp. 149-168). Londen: Willan Publishing.

Financial Crime Academy (n.d.). *Methods Of Cryptocurrency Money Laundering: The 7 Additional Methods of Cryptocurrency Money Laundering.* Geraadpleegd via https://financialcrimeacademy.org/methods-of-cryptocurrency-money-laundering/.

Florencio, D., & Herley, C. (2010). *Phishing and money mules. In 2010 IEEE International Workshop on Information Forensics and Security* (pp. 1-5). Seattle, WA (USA): IEEE.

Florencio, D., & Herley, C. (2012). Is everything we know about password stealing wrong? *Security & Privacy, 10*(6), 63-69.

Gardner, M., & Steinberg, L. (2005). Peer influence on risk taking, risk preference, and risky decision making in adolescence and adulthood: an experimental study. *Developmental Psychology*, *41*(4), 625-635.

Ho, H., Ko, R., & Mazerolle, L. (2022). Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review. *Computers & Security*, *115*, 102611.

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

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55*(3), 596-614.

Junger, M., Veldkamp, B., & Koning, L. (2022). *Fraudevictimisatie in Nederland.* https://www.utwente.nl/nl/bms/fraudvic/fraudevictimisatie-in-nederland.pdf

Kerzic, K. (2022). Using predictive analytics for money mule detection on a cryptocurrency exchange (Doctoral dissertation University Nova de Lisboa). Geraadpleegd via https://run.unl.pt/bitstream/10362/145709/1/TGI1919.pdf.

Kshetri, N. (2010). Diffusion and effects of cyber-crime in developing economies. *Third World Quarterly, 31*(7), 1057-1079.

Kleemans, E. R., & De Poot, C. J. (2008). Criminal careers in organized crime and social opportunity structure. *European Journal of Criminology*, *5*(1), 69-98.

Kleemans, E., & Van Koppen, V. (2020). Organized crime and criminal careers. *Crime and Justice, 49*(1), 385-423.

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

Koppen, M. V. van (2013). Involvement mechanisms for organized crime. *Crime, Law and Social Change*, *59*, 1-20.

Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. A. (2019). Money talks money laundering choices of organized crime offenders in a digital age. *Journal of Crime and Justice, 42*(5), 569-581.

Kruisbergen, E. W., & Soudijn, M. R. J. (2015). Wat is witwassen eigenlijk?. *Justitiële verkenningen*, *41*(1), 10.

Kvale, S., & Brinkmann, S. (2009). *Interviews: Learning the craft of qualitative research interviewing*. Sage.

Lavery, B., Siegel, A. W., Cousins, J. H., & Rubovits, D. S. (1993). Adolescent risk-taking: An analysis of problem behaviors in problem children. *Journal of Experimental Child Psychology*, *55*(2), 277-294.

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

Leukfeldt, E. R., & Holt, T. J. (2020). Examining the social organization practices of cybercriminals in the Netherlands online and offline. *International Journal of Offender Therapy and Comparative Criminology, 64*(5), 522-538

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

Leukfeldt, R., & Jansen, J. (2015). Cyber Criminal Networks and Money Mules: An Analysis of Low-Tech and High-Tech Fraud Attacks in the Netherlands. *International Journal of Cyber Criminology, 9*(2).

Leukfeldt, R., & Kleemans, E. E. (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 lilegal Enterprise (pp. 75-89). Routledge.

Leukfeldt, E. R., Kleemans, E. R., Kruisbergen, E. W., & Roks, R. A. (2019). Criminal networks in a digitised world: on the nexus of borderless opportunities and local embeddedness. *Trends in Organized Crime, 22*, 324-345

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

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017b). A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change, 67*, 21-37

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

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

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017e). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research, 23*, 287-300.

Leukfeldt, E. R., & Roks, R. A. (2021). Cybercrimes on the streets of the Netherlands? An exploration of the intersection of cybercrimes and street crimes. *Deviant Behavior, 42*(11), 1458-1469.

Leukfeldt, E. R., Spithoven, R. & Misana-ter Huurne, E. F. J. (2020). De lokale aanpak van cybercrime. Risicocommunicatie als antwoord op een grenzeloos vraagstuk. In C. de Poot et al. (Eds.), *Politie en cybercriminaliteit* (pp. 203-222). Antwerpen: Gompel & Scavina.

Lusthaus, J., Kleemans, E., Leukfeldt, R., Levi, M., & Holt, T. (2023). Cybercriminal networks in the UK and Beyond: Network structure, criminal cooperation and external interactions. *Trends in Organized Crime*, 1-24.

Lusthaus, J., & Varese, F. (2021). Offline and local: The hidden face of cybercrime. *Policing: A Journal of Policy and Practice, 15*(1), 4-14.Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology*, *2*, 191-216.

Mikhaylov, A., & Frank, R. (2016). *Cards, money and two hacking forums: An analysis of online money laundering schemes.* In 2016 European intelligence and security informatics conference (EISIC) (pp. 80-83). Seattle, WA (USA): IEEE.

Ministerie van Justitie en Veiligheid. (2022). *Veiligheidsagenda 2023-2026.* https://www.rijksoverheid.nl/documenten/rapporten/2022/12/15/tk-bijlage-8-veiligheidsagenda-2023-2026

Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *Journal of Economic Perspectives, 23*(3), 3-20

Moule Jr, R. K., Pyrooz, D. C., & Decker, S. H. (2013). From 'What the F#@% is a Facebook?' to 'Who Doesn't Use Facebook?': The role of criminal lifestyles in the adoption and use of the Internet. *Social Science Research*, *42*(6), 1411-1421.

Odinot, G., Verhoeven, M. A., Pool, R. L. D., & Poot, C. J. de (2017). *Organised cybercrime in the Netherlands. Empirical findings and implications for law enforcement*. Den haag: WODC.

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

Oerlemans, J. J., & Toor, D. van (2022). *Strafrechtelijke aspecten van cybercriminaliteit en digitale opsporing*. Boom Juridisch Uitgevers.

OM. (n.d.). *Aanpak cybercrime*. Geraadpleegd via https://www.om.nl/onderwerpen/cybercrime/aanpak-cybercrime.

Oosterwijk, K., & Fischer, T. F. C. (2017). Interventies jeugdige daders cybercrime. Den Haag: WODC.

Politie. (n.d.). *Wat doet de politie tegen cybercrime?* Geraadpleegd via https://www.politie.nl/informatie/wat-doet-de-politie-tegen-cybercrime.html.

Rani, M. I. A., Zolkaflil, S., & Nazri, S. N. F. S. M. (2022a). The money mule red flags in anti-money laundering transaction monitoring investigation. *International Journal of Business and Economy, 4*(1), 150-163.

Rani, M. I. A., Zolkaflil, S., & Nazri, S. N. F. S. M. (2022b). Money mule risk assessment: an introductory guidance for financial crime compliance officers. *Asian Journal of Research in Business and Management, 4*(1), 208-217.

Rani, M. I. A., Zolkaflil, S., & Nazri, S. N. F. S. M. (2023a). The trends and challenges of money mule investigation by Malaysian enforcement agency. *International Journal of Business and Technopreneurship, 13*(1), 37-50.

Rani, M. I. A., Zolkaflil, S., & Nazri, S. N. F. S. M. (2023b). Estimating reliability of scale development in money mule risk assessment among financial crime compliance officers. *International Journal of Asian Social Science, 13*(3), 101-111

Raza, M. S., Zhan, Q., & Rubab, S. (2020). Role of money mules in money laundering and financial crimes a discussion through case studies. *Journal of Financial Crime, 27*(3), 911-931.

Rijksoverheid. (n.d.). *Cybercrime bestrijden.* Geraadpleegd via https://www.rijksoverheid.nl/onderwerpen/cybercrime-en-cybersecurity/cybercriminaliteit-bestrijden.

Rijksoverheid. (2020). *Kamerbrief over voortgang samenwerking banken en politie bij de aanpak van Internetoplichting.* Geraadpleegd via https://www.rijksoverheid.nl/documenten/kamerstukken/2020/11/17/tk-voortgang-samenwerking-

banken-en-politie-bij-de-aanpak-van-internetoplichting.
Roks, R. A., Leukfeldt, E. R., & Densley, J. A. (2021). The hybridization of street offending in the Netherlands. *The British Journal of Criminology*, *61*(4), 926-945.
Roks, R., & Monshouwer, N. H. (2020). F-gamers die 'mapsen','swipen'en 'bonken': een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger. *Justitiële Verkenningen, 46*(2), 44-58.
Rowley, J. (2012). Conducting research interviews. *Management research review*, *35*(3/4), 260-271.
Schiks, J., Bekkers, L., & Leukfeldt, R. (2021). Naar een interventie tegen geldezels. Den Haag: De Haagse Hogeschool.
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. *Politie & Wetenschap, 89.*
Schiks, J. A. M., van't Hoff-de Goede, S., & Leukfeldt, R. E. (2023). An alternative intervention for juvenile hackers? A qualitative evaluation of the Hack_Right intervention. *Journal of Crime and Justice*, 1-19.
Smith, G. S. (2015). Management models for international cybercrime. *Journal of Financial Crime, 22*(1), 104-125
Staats, W., Meerts, C., & Kleemans, E. R. (2021). *Nieuwe manieren van samenwerken. Een systematische literatuurreview naar (de effectiviteit van) publiek-private samenwerkingsverbanden op het gebied van financieel-economische criminaliteit en cybercrime*. Vrije Universiteit Amsterdam | Nationale Politie.
Sood, A. K., Bansal, R., & Enbody, R. J. (2012). Cybercrime: Dissecting the state of underground enterprise. *IEEE internet computing, 17*(1), 60-68
Soudijn, M. R., & Zegers, B. C. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime, 15*(2-3), 111-129
Spithoven, R., & Leukfeldt, R. (2023). *Gemeenten lijden aan digitale koudwatervrees*. Secondant. https://ccv-secondant.nl/platform/article/gemeenten-lijden-aan-digitale-koudwatervrees
Spithoven, R., Van Ee, H., & Van Houten, Y. H. (2021). Zorg voor kwetsbare geldezels. *Tijdschrift voor de Politie, 3*, 48-53.
Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & health sciences*, *15*(3), 398-405.
Weulen-Kranenbarg, M., Van der Toolen, Y., & Weerman, F. (2022). *Understanding cybercriminal behaviour among young people: Results from a longitudinal network study among a relatively high-risk sample*. Amsterdam: VU University Amsterdam/ Netherlands Institute for the Study of Crime and Law Enforcement.
Wissink, I., & Quint, R. (2021). *'If it's too good to be true, it's too good to be true': Een verkenning van de literatuur over de kenmerken van jonge geldezels.* Stichting Halt.

Bijlage 1: interviewprotocol

Hartelijk dank voor deelname aan ons onderzoek. Dit interview is onderdeel van een onderzoek naar de criminele netwerken achter geldezeldelicten en aangrijpingspunten voor de aanpak hiervan. Het lectoraat Cybercrime & Cybersecurity van de Haagse Hogeschool voert dit onderzoek uit in opdracht van en in samenwerking met de regiegroep Operatie Centurion van de Nationale Politie.

Uit onderzoek blijkt dat financieel gemotiveerde cybercriminelen vaak gebruikmaken van geldezels met als doel het financiële spoor van gepleegde delicten te verbergen. Geldezels zijn personen die al dan niet bewust hun bankrekening voor criminele doeleinden laten gebruiken. Zij vormen een belangrijke schakel in het wegsluizen van wederrechtelijk verkregen geld. In tegenstelling tot personen uit hogere lagen van het criminele netwerk zijn geldezels relatief eenvoudig op te sporen. Opsporingsinstanties en financiële instellingen hebben vaak echter weinig zicht op het criminele netwerk dat zich achter de geldezels bevindt. Dit vormt dan ook de aanleiding voor dit onderzoek.

Vertrekpunt zijn de geldezels en niet de cybercriminele netwerken die geldezels inzetten. Hierdoor zullen criminele netwerken die zich met diverse vormen van cybercriminaliteit bezighouden in dit onderzoek worden meegenomen. We richten ons dus niet op slechts één specifieke vorm van cybercriminaliteit, maar op alle vormen van cybercriminaliteit waarbij geldezels worden ingezet.

Wij zijn voor dit interview niet geïnteresseerd in namen of andere tot personen herleidbare informatie. Het interview zal ongeveer 90 minuten in beslag nemen. Alles wat u met ons deelt, is vertrouwelijk en is alleen voor ons, de onderzoekers, toegankelijk. De gedeelde informatie wordt gepseudonimiseerd en versleuteld opgeslagen op een beveiligde locatie. Wij zorgen ervoor dat uw antwoorden niet naar u te herleiden zijn.

1 Algemeen

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

- Wat is uw geslacht?
- Wat is uw leeftijd?
- Bij welke organisatie bent u werkzaam [naam organisatie, afdeling]?
- Wat is uw functie?
- Op welke wijze bent u betrokken bij de aanpak van cybercrime en/of geldezel-/cybercriminele netwerken?
- Hoe lang houdt u zich al bezig met de aanpak van cybercrime en/of geldezel-/cybercriminele netwerken?

2 Cyberdelicten waarbij geldezels worden ingezet

Graag stellen wij u een aantal specifieke vragen om meer inzicht te krijgen in (de aard van) de delicten waarbij geldezels worden ingezet.

Soorten delicten waarbij geldezels worden ingezet

- Bij welke vormen van cybercriminaliteit worden geldezels ingezet?
- Kunt u een beschrijving van deze criminaliteitsvormen geven?

De volgende vragen per genoemde vorm van cybercriminaliteit langslopen. Expliciet vragen naar eventuele verschillen met andere vormen van cybercriminaliteit.

De aard van delicten waarbij geldezels worden ingezet

- Welke modus operandi (MO) hanteren cybercriminele netwerken die geldezels inzetten in de uitvoering van deze delicten?
- Welke stappen worden genomen in de uitvoering van deze delicten? Welke crime scripts kunnen worden onderscheiden?
- Is bij het plegen van deze delicten sprake van specialisme? Zo nee, welke andere delicten en MO's zijn er?
- Welke rol speelt ICT in deze MO?
- Welke rol speelt geweld in deze MO?
- Wat is de mate van verwevenheid tussen deze cyberdelicten en traditionele delicten?
- Op welke schaal worden deze delicten gepleegd? Hoe vaak? Wat is de duur hiervan?
- In hoeverre is sprake van internationale aspecten bij de uitvoering van deze delicten?
- Hoe heeft u zicht gekregen op de aard van deze delicten?

3 Cybercriminele netwerken achter geldezeldelicten

Dit onderdeel heeft betrekking op de cybercriminele netwerken die gebruikmaken van geldezels om het financiële spoor van de gepleegde delicten te verbergen. Graag stellen wij u een aantal specifieke vragen om meer inzicht te krijgen in de kenmerken van de netwerken die geldezels inzetten en kenmerken van individuele leden uit deze netwerken.

Kenmerken van de cybercriminele netwerken

- Wat zijn kenmerken van cybercriminele netwerken die geldezels inzetten?
  Structuur:
  - Aantal leden?
  - Rollen en taken?
  - Mate van hiërarchie?
  - Hoe zijn leden aan elkaar gerelateerd (soort relaties)?
  - Mate van dynamiek van het netwerk?
  - Stabiliteit/flexibiliteit van groep kernleden?
  - Aanwezigheid van conflicten binnen het netwerk?
  - Contact met andere (cyber)criminele netwerken? Sprake van conflicten?
  - Contact met wettige ondernemingen, rechtspersonen, overheidsfunctionarissen, externe deskundigen/ specialisten? Aard van deze contacten?

  Ontstaan en groei:
  - Hoe zijn deze netwerken ontstaan?
  - Wanneer zijn deze netwerken ontstaan?
  - Wat is de duur van de cybercriminele samenwerking?
  - Hoe worden nieuwe leden geworven?
  - Ontmoetingsplaatsen (offline/online, welke kanalen)
  - Communicatie (offline/online, welke kanalen)
- Hoe heeft u zicht gekregen op de kenmerken van deze cybercriminele netwerken?

Kenmerken van individuele leden

- Wat zijn kenmerken van de individuele leden van deze cybercriminele netwerken?
  Demografische kenmerken:
  - Leeftijd
  - Geslacht
  - (Etnische) achtergrond
  - Opleiding/werk
  - Sociaaleconomische status
  - Thuissituatie (alleenstaand, samenwonend, thuiswonend, probleemgezin)

  Kennis en vaardigheden:
  - Intelligentie
  - (ICT) kennis en vaardigheden

  Criminele carrière:
  - Zijn de leden first offenders? Zo niet, met welke delicten hebben ze zich dan voorafgaand aan het plegen van cybercriminaliteit beziggehouden?
  - Hoe zijn deze individuen betrokken geraakt bij cybercriminaliteit?
  - Wat zijn de motivaties van deze individuen om cybercriminaliteit te plegen?
- Hoe heeft u zicht gekregen op de kenmerken van deze individuele leden?

4 Geldezelnetwerken

Dit onderdeel heeft betrekking op geldezelnetwerken, ofwel het netwerk van de geldezels zelf. Graag stellen wij u een aantal vragen om meer inzicht te krijgen in de kenmerken van deze netwerken en individuele leden. Tevens vragen we naar de wijze waarop geldezels geworven en ingezet worden.

Kenmerken van de geldezelnetwerken

- Wat zijn de kenmerken van geldezelnetwerken?
  Structuur:
  - Aantal leden?
  - Rollen en taken?
  - Mate van hiërarchie?
  - Hoe zijn leden aan elkaar gerelateerd (soort relaties)?
  - Mate van dynamiek van het netwerk?
  - Stabiliteit/flexibiliteit van groep kernleden?
  - Aanwezigheid van conflicten binnen het netwerk?
  - Contact met andere geldezelnetwerken? Sprake van conflicten?
  - Contact met wettige ondernemingen, rechtspersonen, overheidsfunctionarissen, externe deskundigen/ specialisten? Aard van deze contacten?

  Ontstaan en groei:
  - Hoe zijn deze netwerken ontstaan?
  - Wanneer zijn deze netwerken ontstaan?
  - Wat is de duur van de samenwerking?
  - Hoe worden nieuwe leden geworven?
  - Ontmoetingsplaatsen (offline/online, welke kanalen)
  - Communicatie (offline/online, welke kanalen)
- Hoe heeft u zicht gekregen op de kenmerken van deze geldezelnetwerken?

Kenmerken van individuele geldezels

- Wat zijn kenmerken van individuele geldezels?
  Demografische kenmerken:
  - Leeftijd
  - Geslacht
  - (Etnische) achtergrond
  - Opleiding/werk
  - Sociaaleconomische status
  - Thuissituatie (alleenstaand, samenwonend, thuiswonend, probleemgezin)

  Kennis en vaardigheden:
  - Intelligentie
  - (ICT) kennis en vaardigheden

  Criminele carrière:
  - Zijn de geldezels first offenders? Zo niet, met welke delicten hebben ze zich hieraan voorafgaand dan beziggehouden?
  - Hoe zijn deze geldezels betrokken geraakt bij cybercriminaliteit?
  - Wat zijn de motieven van deze geldezels om hun bankrekening uit te lenen?
- Hoe heeft u zicht gekregen op de kenmerken van deze individuele geldezels?

Het ronselen en inzetten van geldezels

- Op welke wijze worden geldezels geronseld door cybercriminele netwerken? En op welke wijze worden zij ingezet door deze netwerken?
  Ronselen:
  - Online/offline sociale contacten
  - Online/offline ontmoetingsplaatsen (welke kanalen)
  - In hoeverre speelt dwang een rol? En geweld?

  Inzetten:
  - Rol/functie binnen het crime script
  - Hoeveel geldezels zijn nodig voor de uitvoering per delict?
  - Hoeveel geldezels worden ingezet door cybercriminele netwerken?
- Hoe heeft u zicht gekregen op de processen van het ronselen en inzetten van geldezels door cybercriminele netwerken? PPS LIMBURG!

5 Aangrijpingspunten voor de aanpak van zowel de criminele netwerken achter geldezeldelicten als van geldezelnetwerken

Tot slot zijn we geïnteresseerd in de aanpak van cybercriminele netwerken achter geldezeldelicten en van geldezelnetwerken. We stellen u vragen over zowel de huidige aanpak als mogelijkheden voor de aanpak in de toekomst. Ook gaan wij in op uw mening over zowel de sterke punten als verbeterpunten van deze aanpak.

De volgende vragen nogmaals per vorm van cybercriminaliteit langslopen. Expliciet vragen naar eventuele verschillen met andere vormen van cybercriminaliteit. Daarnaast blijven vragen naar het onderscheid tussen de aanpak van geldezelnetwerken en de criminele netwerken hierachter.

Aanpak van cybercriminele netwerken achter geldezels en geldezelnetwerken

- Huidige aanpak cybercriminele netwerken achter geldezels
  - Hoe ziet bij uw organisatie de aanpak van cybercriminele netwerken die geldezels inzetten er momenteel uit?Ligt hierbij de focus op individuele daders, het gehele netwerk of beide? Waarom?
  - In hoeverre wordt hierbij ingezet op a) preventie, b) verstoring en c) opsporing? Op welke manier en waarom?
  - Indien opsporing: op welke wijze worden deze zaken afgedaan, strafrechtelijk of anderszins?
- Huidige aanpak van geldezelnetwerken
  - Hoe ziet bij uw organisatie de aanpak van geldezelnetwerken er uit?
  - ligt hierbij de focus op individuele daders, het gehele netwerk of beide? Waarom?
  - in hoeverre wordt hierbij ingezet op a) preventie, b) verstoring en c) opsporing? Op welke manier en waarom?
  - Indien opsporing: op welke wijze worden deze zaken afgedaan, strafrechtelijk of anderszins?
- Effectieve aangrijpingspunten
  - Waar binnen het crimescript zitten volgens u effectieve aangrijpingspunten voor preventie, verstoring en opsporing? Waarom?
  - Hoe zien deze aangrijpingspunten er uit en welke actoren zijn hiervoor verantwoordelijk?

- In hoeverre is sprake van een integrale aanpak van deze cybercriminele netwerken en geldezelnetwerken?
  - Met welke actor(en) werkt u samen in deze aanpak?
  - Welke rol vervullen betrokken organisaties in deze aanpak?
  - Hoe ziet deze aanpak er precies uit?
  - Is deze aanpak delictspecifiek?
  - Is deze aanpak geëvalueerd? Hoe effectief is deze aanpak volgens u?
- Wat zijn naar uw mening de sterke punten van de huidig aanpak?
- Wat zijn naar uw mening verbeterpunten van de huidige aanpak?
- In hoeverre zijn er bij uw organisatie interventies nog in ontwikkeling? Hoe zien deze eruit?
- Bent u bekend met de aanpak van cybercriminele netwerken en/ of geldezelnetwerken buiten Nederland?

Dit is het einde van het interview. Heeft u nog opmerkingen of dingen die u wil toevoegen?

We zullen het interview niet woord voor woord uitwerken, maar op grote lijnen samenvatten, om zo de onderzoeksvragen te beantwoorden. Wilt u het transcript inzien? En wilt u het (concept) onderzoeksrapport inzien?

Adresgegevens

Johanna Westerdijkplein 75
2521 EN Den Haag

cybersecurity@hhs.nl

dehaagsehogeschool.nl