'*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

Dr. Inge B. Wissink

In samenwerking met:

R. Quint

Stichting Halt

In opdracht van:

Betaalvereniging Nederland (M.T. Osten)

Project Veilig Bankieren

Januari 2021

Inhoudsopgave

Introductie

In opdracht van de Betaalvereniging Nederland, en in samenwerking met de Stichting Halt is een literatuurverkenning verricht om na te gaan wat er vanuit diverse bronnen bekend is over de kenmerken van *money mules* (geldezels, katvangers). Deze informatie wordt gebruikt om te komen tot een doelgroepomschrijving voor een preventieprogramma dat ontwikkeld wordt door Halt. Er is onderzocht in welke leeftijdscategorie de *money mules* zich vooral voordoen, om wat voor een soort jongeren het gaat (bv. geslacht, SES, LVB), en welke aspecten nog meer kenmerkend zijn voor deze groep plegers.

Definitie geldezels

Er worden in de praktijk diverse termen gebruikt, zoals geldezels (*money mules*), katvangers, sprinkhanen, windhappers en stromannen. Het is niet altijd duidelijk wat er precies onder al deze termen wordt verstaan. De term 'katvangers' verwijst naar een brede categorie van personen die zichzelf beschikbaar stellen als eigenaar of registratiehouder van een voertuig, bedrijf, bankrekening of ander goed, waardoor de werkelijke eigenaar of houder zichzelf buiten het zicht van de autoriteiten kan houden (Schoenmakers, Bremmers, & van Wijk, 2012, p. 31; Versprille, 2016). Het gaat om mensen die, bewust of onbewust (ze kunnen bij rekrutering misleid worden), op allerlei manieren als dekmantel fungeren voor criminele organisaties, zonder dat zij enige expertise of vaardigheid hiervoor dienen in te zetten. Huidige literatuurverkenning richt zich echter specifiek op geldezels (vanwege de focus op geldstromen). Een 'geldezel' (oftewel *money mule*) wordt smaller gedefinieerd als '*een persoon die zijn of haar bankrekening al dan niet bewust ter beschikking stelt aan criminelen ten behoeve van het wegsluizen van frauduleus verkregen gelden*' (Oerlemans, Custers, Pool, & Cornelisse, 2016). Een enkele bron over de bredere categorie van de katvangers bleek voor de beantwoording van de onderzoeksvraag relevant omdat de resultaten de overige aanvulden. Om die reden is ervoor gekozen deze mee te nemen in de hieronder beschreven resultaten.

Methode

Via Psycinfo, EBSCO en Google Scholar is (op 21 december 2020) een literatuursearch verricht. Daarnaast zijn vijf experts (wetenschap, onderzoek en politie) gevraagd relevante bronnen te leveren. De gevonden bronnen zijn vervolgens gescand (samenvattingen, introducties, methoden en resultaten) om vast te stellen of ze daadwerkelijk relevant waren voor huidige literatuurverkenning. Tevens zijn er via de sneeuwbalmethode (door aangehaalde bronnen in relevante artikelen na te gaan) nog enkele relevante bronnen toegevoegd.

Deze zoektocht leidde in eerste instantie tot een set van 11 internationale publicaties gebaseerd op Nederlandse studies/gegevens, 14 nationale publicaties (gebaseerd op Nederlandse gegevens) en 10 internationale publicaties gebaseerd op buitenlandse studies/gegevens. Uiteindelijk is na een grondige lezing besloten om enkele studies buiten beschouwing te laten, omdat deze geen nieuwe empirische gegevens bevatten (van voor 2010; n = 2; literatuuroverzichten of opiniërende stukken; n = 10), omdat ze geen relevante informatie over jonge geldezels vermeldden (n = 2) of omdat ze geheel overlapten met een

andere geïncludeerde studie (n = 1)[1]. De overige 20 bronnen zijn opgenomen in de Overzichtstabel 1 en zullen in de Resultaten paragraaf (in chronologische volgorde) besproken worden.

Resultaten

Bevindingen vanuit Nederlandse (wetenschappelijke) studies

Soudijn & Zegers (2012; internationaal)

Dit artikel schetst een goed beeld van de manier waarop geldezels online geworven kunnen worden. Voor deze studie is een kwalitatieve analyse verricht op de gegevens van een virtueel forum (wat beschouwd wordt als een online vorm van een 'offender convergence setting', oftewel, een plek waar plegers elkaar treffen; Felson, 2003). De gegevens bestaan uit meer dan 150.000 posts en 60.000 privé-berichten (in de periode 2003-2008) van 1846 leden van een forum over 'carding' (het frauduleuze gebruik van persoonlijke gegevens van betaalpassen en creditcards; Peretti, 2008). Mensen betrokken bij carding vinden elkaar via dergelijke gespecialiseerde online carding forums, waar ze informatie uitwisselen, nieuwe illegale praktijken starten of handelen in gestolen gegevens, goederen, diensten en software (Holt & Lampke, 2009). Op het forum zijn bijvoorbeeld discussies te vinden over hoe iemand het beste kan pinnen zonder herkend te worden en waar geskimd kan worden. Ook komen leden in contact met leden die tegen betaling geldtransacties kunnen verrichten. Het forum maakt tevens gebruik van een beoordelingssysteem om de betrouwbaarheid te kunnen waarborgen. Het artikel richt zich op een vorm van carding via *cashing* (d.w.z. dat via gestolen financiële gegevens cash geld wordt verkregen) en op basis van een kwalitatieve analyse van de gegevens kan een 'crime script' beschreven worden met vier fasen: de voorbereidende fase, de diefstal fase (waarin de creditcard of bankgegevens gestolen worden), de geldezel fase, en de cashing fase (waarin de hoofdverdachte het frauduleuze geld in handen krijgt). De bevindingen over de geldezel fase zijn interessant voor huidige literatuurverkenning en geven aan dat de geldezels vaak worden geworven via e-mails waarin niet wordt vermeld dat de geldezels alleen voor een korte periode kunnen worden ingezet, zoals het geval is in Nederland, maar waarin vaak titels als '*Financial Department Manager*' worden gebruikt. In een voorbeeld wervingsmail is te lezen dat de potentiële geldezels worden verleid met het vooruitzicht op een hoog regelmatig inkomen, carrière ontwikkelingsmogelijkheden, twee weken betaalde vakantie, vriendelijk team, bonussen en een loyaliteitsprogramma. Van deze aantrekkelijke voorwaarden zouden ze kunnen profiteren zonder het huis te hoeven verlaten en door slechts een paar uur per dag werk op de computer te doen. Het minimale inkomen dat genoemd wordt is 2000 dollar per maand, en 5% voor elke geldtransitie, ook zouden alle overige kosten betaald worden. Soudijn en Zegers (2012) spreken ook nog over preventiemethoden, zoals het alert maken van mogelijke slachtoffers via radio en tv en het overspoelen van de markt door nepgeldezels in te zetten (die de gevraagde diensten uiteindelijk niet leveren).

[1] Meer informatie over de methode kan opgevraagd worden bij de eerste auteur van dit rapport (I.B.Wissink@uva.nl).

Meijering (2013; internationaal)

Deze studie richt zich ook op carding (patronen) en op manieren om carding op effectieve wijze tegen te gaan. Hiervoor is gebruik gemaakt van een combinatie van informatie uit politierapporten, (wetenschappelijke) literatuur, online nieuws artikelen en andere bronnen (één *National Hi-Tech Crime Unit* expert interview). Met betrekking tot de 'cashing' fase wordt het onderwerp geldezels in grote lijnen, vanwege een gebrek aan bronnen, besproken. Geldezels zouden gerekruteerd worden via advertenties waarin mensen wordt verteld dat ze makkelijk geld kunnen verdienen. Deze mensen zouden niet weten dat het geld illegaal verkregen is (Aston, McCombie, Reardon, & Watters, 2009). Ook Meijering stelt voor dat potentiële geldezels bewust gemaakt moeten worden van het feit dat het niet winstgevend is. Het zou moeilijker gemaakt moeten worden, de risico's moeten vergroot worden en de excuses moeten onderuit gehaald worden (Clarke, 1997).

Leukfeldt (2014; internationaal)

De studie van Leukfeldt (2014) is de eerste studie die echt relevante resultaten biedt voor huidige literatuurverkenning. Het betreft een *case*-studie van een phishing zaak in Amsterdam (2012-2013; met daarin gegevens van verhoren, telefoontaps, internetverkeer en surveillance rapporten, aangevuld met interviews met OM, teamleider van de politie en een financiële expert van het onderzoeksteam) en hiermee wordt aangetoond dat de basis van de relaties van de phishing plegers niet wordt gelegd op online forums (zoals voorgaande literatuurbronnen van Perettie, 2008; Holt & Lampke, 2009 en Soudijn & Zegers, 2012 benadrukten), maar in offline sociale netwerken. Hiermee komen ook andere preventiemogelijkheden in beeld.

In de introductie van het artikel beschrijft Leukfeldt (2014) dat in Nederland jonge mensen op straat of via sociale media benaderd worden en gevraagd worden of ze hun betaalpassen en pincodes ter beschikking willen stellen. De resultatensectie maakt duidelijk dat, anders dan bij Soudijn en Zegers (2012), de criminelen in deze Amsterdamse zaak dus niet een forum gebruiken om geschikte medeplegers te zoeken, maar zij zoeken deze in de eigen *real-world* sociale netwerken. De pleger '*convergence settings*' zijn dus niet online te vinden, maar bestaan uit de straten van Amsterdam. Money mules worden voornamelijk via sociale contacten gevonden door *recruiters* (of: rekruteerders), en de geldezels blijken soms zelf ook vrienden in te brengen. Sommige geldezels geven ook aan dat het best normaal is om benaderd te worden door mensen die om hun bankpas vragen. In sommige gevallen zijn de geldezels benaderd via de chat functie op de telefoon (Blackberry). Vage bekenden en vrienden van vrienden komen zo ook in hun contactenlijst. Andere statements laten zien dat mensen benaderd worden op straat, op school of bij voetbalwedstrijden.

De recruiters zeggen tegen de potentiële geldezels dat het helpen zonder risico is, omdat ze niet ontdekt kunnen worden. Ze geven soms aan dat ze een vriend bij de bank hebben die het geld kan overmaken zonder dat iemand erachter kan komen. De verhoren laten echter zien dat geldezels hun bankpassen meestal niet terugkrijgen en vaak niet betaald worden. De recruiters hebben dan verschillende smoezen: de politie heeft het geld ingenomen of de bank heeft het geld niet overgemaakt. Vaak beseffen de geldezels pas na een brief van de bank dat het geld wel echt is overgemaakt. Bijna alle ondervraagde geldezels geven trouwens (in eerste instantie) aan dat ze hun bankpas verloren zijn, wat erop wijst dat ze vooraf wel geïnstrueerd zijn over wat ze moeten doen als het toch verkeerd zou gaan.

Volgens de geïnterviewden van de politie weten de geldezels ook wel dat het illegaal is wat ze doen en wordt aan hen meestal een deel van het geld beloofd.

In het artikel beschrijft Leukfeldt (2014) dat de resultaten erop duiden dat de belangrijkste doelwitten van recruiters jonge mensen zijn die snel geld willen verdienen. De benadering vindt meestal plaats via de telefoon, op straat, school of de sportschool en het blijkt dus best normaal om dergelijke (openlijke) verzoeken te ontvangen. Meer onderzoek is volgens Leukfeldt (2014) nodig om vast te stellen of er een specifieke risicogroep van potentiële geldezels geïdentificeerd kan worden en campagnes ontwikkeld kunnen worden om hen te informeren (over dat ze gebruikt en waarschijnlijk niet beloond worden). Hierbij is het volgens Leukfeldt (2014) van belang de motivaties van geldezels beter te begrijpen om zo vast te kunnen stellen of bewustzijnscampagnes mogelijk bruikbaar zijn (bv. bij een goed afgebakende groep onbewuste geldezels) of dat andere maatregelen nodig zijn (bv. berechting van geldezels). Ten slotte, terwijl Soudijn en Zegers (2012) voor interventiedoeleinden online forums voor ogen hebben (verbonden aan een lokaal dan wel een internationaal netwerk), adviseert Leukfeldt (2014) dat men zich op de sociale banden in netwerken richt (naast technologische maatregelen gericht op de forums).

Leukfeldt & Jansen (2015; internationaal)

In het volgende jaar publiceren Leukfeldt en Jansen een studie waarvoor de bankgegevens van 600 fraude incidenten zijn bestudeerd (van de jaren 2011, 2012 en 2013), bestaande uit gegevens van 1005 frauduleuze transacties en 967 money mules. Leukfeldt en Jansen (2015) benadrukken de verschillen tussen Nederland en andere landen: in tegenstelling tot de Nederlandse cybercriminele netwerken lijkt de structuur van de geanalyseerde netwerken in andere landen meer divers, soms zonder kernleden, *enablers* (oftewel, ondersteuners) of geldezels. Soms voeren de kernleden alles zelf uit.

Leukfeldt en Jansen passen het *social opportunity structure perspective* toe en geven aan dat criminele netwerken ontstaan en groeien op basis van bestaande sociale netwerken en contacten (Kleemans & De Poot, 2008). Om echter uit te kunnen breiden buiten dit initiële sociale netwerk moeten contacten met outsiders gelegd worden. Daarbij is een onderscheid te maken tussen low-tech lokale groepen en high-tech internationale specialisten. Bij low-tech groepen gaat het om groepen die aanvallen plegen waarbij het gebruik van technologie beperkt is (bv. bij phishing waarbij e-mails verstuurd worden, nep-websites van banken worden ingezet en telefoontjes gepleegd worden om gegevens te stelen), terwijl high-tech groepen (bv. bij malware) vaak systemen van slachtoffers aanvallen (met daarvoor ontwikkelde software) en vervolgens overnemen, inclusief bankgegevens en overboekingen. En dit onderscheid hangt dus ook samen met de manier waarop geldezels benaderd worden: bij low-tech gebeurt dit meer lokaal en offline (‘op straat’) en bij high-tech meer internationaal en online.

De resultaten laten in de eerste plaats zien dat er minder geld wordt overgemaakt aan de geldezels in de high-tech zaken (32% kreeg minder dan 1000,- tegenover 9.9% in de low-tech zaken). Ook worden er aanwijzingen gevonden dat de jongeren in Nederland vooral voor de low-tech attacks gebruikt worden (phishing), omdat de meeste geldezels in die zaken Nederlandse bankrekeningen gebruiken (bijna 90%). Bij de high-tech zaken komen ook veel Oost-Europese bankrekeningen voor.

Leukfeldt en Jansen hebben daarnaast naar de achtergrondinformatie van de money mules met Nederlandse bankrekeningen gekeken (hierbij zijn overigens wel veel missende

waarden). Geldezels blijken vaker van het mannelijke dan van het vrouwelijke geslacht. Verder wordt er een significant verschil tussen de geldezels van de low-tech en de high-tech zaken gevonden in leeftijd: 56% van de geldezels in low-tech zaken is jonger dan 25 jaar, terwijl dat aandeel in de high-tech zaken slechts 29% is. Leukfeldt en Jansen (2015) benadrukken en dat naast internationaal opererende netwerken (online), in Nederland lokale criminele netwerken een grote rol spelen en dat leden daarvan via bestaande sociale netwerken zoals scholen en sportclubs jonge mensen overtuigen om hun bankgegevens te geven in ruil voor een klein bedrag.

Arevalo (2015; internationaal)

De resultaten van het grondig uitgevoerde scriptie-onderzoek van Arevalo (2015) bevestigen dat er twee primaire geldezel rekruteringsvormen zijn: face-to-face en online *job scams* (nepbanen waarbij mensen misleid worden). Arevalo (2015) geeft ook aan dat er verschillen tussen landen zijn in het rekruteringproces. Zo zou in Nederland face-to-face rekrutering het meeste voorkomen. Online rekrutering zou in het buitenland vaker voorkomen en ook meer bij malware, terwijl bij phishing vaker face-to-face rekrutering zou worden ingezet. Vanwege deze verschillen richt Arevalo zich op informatie die van belang is voor het begrip van de kenmerken en rekrutering van geldezels in Nederland.

Ter introductie beschrijft Arevalo (2015) dat geldezels gerekruteerd worden via onder andere e-mail, online vacature zoekmachines, face-to-face, school en sociale netwerken. Soms zouden geldezels zich niet bewust zijn van de illegale transacties waar zij bij betrokken raken, totdat ze hierover door de bank of politie/justitie worden geïnformeerd (Stalenberg, 2011; Leukfeldt, 2014). Geldezels worden vaak misleid door recruiters, aangezien zij hun geld beloven (Dunham, 2006; McCombie, Pieprzyk, & Waters, 2009). Geldezel rekrutering zou ook het meest voorkomen onder Nederlanders in de lagere sociaal-economische klassen (Leukfeldt, 2014).

Arevalo (2015) past een flexibel onderzoeksdesign toe en maakt gebruik van drie dataverzamelingsmethoden: secundaire analyse van voorgaand buitenlands onderzoek, semi-gestructureerde interviews met 11 cybercrime experts (bank medewerkers, financiële politierecherchers, een aanklager, cybercrime experts, een onderzoeker en één geldezel) en etnografisch onderzoek (verhalen van drie geldezels via forums en Facebook en een inhoudelijke analyse van een televisieprogramma Meldpunt met daarin 2 geldezel verhalen).

In de resultaten vermeldt Arevalo (2015) dat Dunham (2006) de eerste geldezel zaak (in Australië) beschreef waarbij 61 geldezels gearresteerd werden. Dunham (2006) beschreef dat de meeste van de 61 geldezels adolescenten waren en dat zij zich onbewust waren van het feit dat zij illegaal gedrag vertoonden. In eerdere jaren zouden ook in Nederland adolescenten het voornaamste doelwit voor geldezel rekrutering zijn geweest (NVB, 2011). Die trend zou echter aan het veranderen zijn en rond 2015 zouden volwassenen steeds vaker als geldezels gerekruteerd worden (Mauritz, 2014; Van der Wolf, 2014). Verder rapporteert Arevalo (2015) over een bekende zaak in Nederland (Assen) met 20 geldezels en 4 recruiters. De geldezels kwamen voornamelijk uit Emmen en Coevorden en hun leeftijd varieerde van 15 tot 38 jaar.

De literatuur laat volgens Arevalo (2015) zien dat face-to-face rekrutering plaatsvindt in verschillende sociale omgevingen zoals scholen, parken en sportclubs (Leukfeldt, 2014; Stalenberg, 2011). Het kan zich ook voordoen binnen iemands netwerk zoals binnen de familie en/of vriendenkring. Verder beschrijft Arevalo (2015) ook de hierboven

gerapporteerde bevindingen van Leukfeldt (2014), dat de meeste geldezels in Nederland ook via Nederlandse recruiters geworven worden, en dat Nederlandse money mules zelf ook vrienden aanleveren. Veel recruiters in de Amsterdam zaak (zie Leukfeldt, 2014) met een Surinaamse of Antilliaanse achtergrond zochten ook face-to-face contact binnen hun eigen netwerken, omdat ze die potentiële geldezels beter konden vertrouwen. Wanneer ezels gerekruteerd worden via online methoden, dan bevinden de recruiters zich meestal buiten Nederland (bv. Oost-Europa).

Sommige geldezels die face-to-face gerekruteerd zijn reageren met de zogenaamde *innovatie reactie*. Dit houdt in dat zij wel een idee hadden dat hun handelingen niet helemaal legaal waren, maar dat zij ervoor kozen om dit te ontkennen door alleen op het geld (de beloning) te focussen. Ook ligt het voor de hand dat de geldezels deel uitmaken van sociale netwerken die bekend zijn met de illegale onderwereld en dat delinquentie binnen deze netwerken niet als slecht wordt beoordeeld (zgn. 'normalisatie'; zie tevens Leukfeldt, 2014).

Eén respondent van de studie van Arevalo (2015) vertelde dat recruiters vaak in hun buurt kijken of er mensen zijn die geld nodig hebben; '*jongeren van 14-16 jaar die waarschijnlijk geld wilden om bijvoorbeeld nieuwe sneakers te kopen*'. Recruiters zouden altijd proberen diegenen te identificeren die makkelijk over te halen zouden zijn om als geldezel op te treden. Potentiele geldezels worden ook benaderd met zielige verhalen (geld voor een belangrijke aankoop was overgemaakt door een familielid, maar toen was de bankpas verloren), en een deel van het geld beloofd (vormen van psychologische manipulatie). Ten slotte worden meisjes soms nog geworven door loverboy scams of door zogenaamde vriendjes die deze meisjes dan onder druk zetten om als geldezel op te treden.

Ten aanzien van het cognitieve vermogen/intelligentie/naïviteit van de geldezels gaf een respondent nog het volgende aan: '*Recruiters zijn erg streetwise. Ze rekruteren of vragen 10 kinderen en 1 zal 'ja' zeggen. Het is als schieten met een vuurwapen. Het is proberen, proberen, proberen en dan zal iemand die dom genoeg is ja zeggen (lacht). Dus, ja, zo vind je de zwakkere targets altijd wel*.' Wanneer geldezels gerekruteerd worden via online baansites, dan zijn ze volgens Arevalo (2015) ook vaak naïef en onbewust van de gevolgen/schade van de misdaden waarbij ze betrokken worden.

In de conclusie somt Arevalo (2015) een groot aantal kenmerken van geldezels op. Doelwitten zijn adolescenten die deel van een groep willen uitmaken en niet buitengesloten willen worden. Ook mensen die mentaal beperkt zijn en die niet de consequenties van hun handelen begrijpen zijn een doelwit. Tenslotte zijn mensen met geldproblemen een doelwit. Arevalo (2015) beschrijft dat eerder mensen onder de 18 doelwit waren, maar dat rond 2015 mensen tussen de 18 – 35 vaker benaderd leken te worden. Mogelijk veranderde dit destijds, omdat er beperkingen van banken kwamen, zoals opnamelimieten en bewustzijnsprogramma's (zoals pasopjepas.nl), gericht op adolescenten (Stalenberg, 2011). Het gevonden verschil is echter mogelijk ook veroorzaakt of gekleurd door de toen beschikbare gegevensbronnen (bv. de functie van de geïnterviewden in de onderzoeken of het type data waarop de onderzoeksresultaten gebaseerd waren).

Arevalo (2015) concludeert daarnaast dat geldezels zich vaak onderwerpen aan druk vanuit (vage) kennissen, omdat ze graag bij een groep willen horen. Het zou voornamelijk gaan om mannen in grotere steden. Jonge volwassenen/adolescenten zouden nog sneller verleid kunnen worden door snelle beloningen en zouden minder nadenken over de langere-termijn consequenties. Ook wordt in de conclusie een lager opleidingsniveau/lagere intelligentie genoemd als kenmerk van de geldezels, naast de reeds genoemde financiële problemen en daaraan gerelateerde stress. Personen met financiële problemen zouden

hierdoor, en door hun onwetendheid op dit terrein, makkelijker te beïnvloeden zijn. Geldezels zouden eerst wel signalen hebben gehad dat er iets niet pluis was, maar kozen ervoor om dat te ontkennen of te rationaliseren of hun gedrag goed te praten en zich vervolgens op de korte termijn opbrengsten (snel geld) te richten. Er worden vaak geen negatieve consequenties waargenomen. Personen die zich dus sterk richten op korte termijn doelen zouden makkelijker te rekruteren zijn als geldezels. Face-to-face rekrutering binnen het sociale netwerk met bestaande relaties, vertrouwen, en deviante normen speelt een grote rol bij de rekrutering van de Nederlandse geldezel. Het gaat om jongeren uit de mindere buurten in stedelijke centra die deel zijn van een subcultuur waarin delinquent gedrag anders wordt gezien dan in de mainstream maatschappij. Deze jongeren gaan zich delinquent gedragen omdat ze elkaar daarin versterken. En opleiding en woonplaats spelen dus ook een duidelijke rol. Bij deze nog enkele citaten die deze bevindingen illustreren (Arevalo, 2015): '*Zij zijn geronseld via netwerken – daarom zie je ze over heel Nederland, maar je hebt hotspots in de grotere gemeenten. Ook, omdat leefomstandigheden minder zijn – er is meer, hoe zeg je dat? Mensen zijn armer zou ik zeggen, minder opgeleid, en ook minder mobiel en dat soort dingen*.' '*De meeste geldezels komen uit de grotere steden en voornamelijk uit de sociaal-economisch mindere buurten. Een mogelijke verklaring hiervoor is dat deze buurten bestaan uit mensen met een lagere opleiding, die veel sociale contacten op straat hebben etc.*' '*Vaak zijn het jongeren, uit de grotere steden, hebben een lager opleidingsniveau, en die in contact komen met criminelen.' 'In geval van phishing zijn de geldezels niet hoog opgeleid*'. Arevalo (2015) concludeert ook nog dat het opvallend is dat er zo weinig onderzoek naar geldezels is gedaan, aangezien zij zo'n belangrijke schakel in het hele proces vormen.

Oerlemans, Clusters, Pool, & Cornelisse (2016; nationaal)

Voor dit onderzoek hebben de vier grootste Nederlandse banken transactiegegevens beschikbaar gesteld die betrekking hadden op banking malware en phishing over de periode 2012 tot en met 2015. Dankzij de identificatieplicht bij banken is het mogelijk om zo een goed inzicht te krijgen in de kenmerken van de money mules. De dossiergegevens zijn aangevuld met 20 interviews met experts in cybercrime, witwassen of het gebruik van digitale betalingsmiddelen (uit de opsporingspraktijk, het bankwezen en de digitale betalingsdiensten sector).

Het dossieronderzoek en gepubliceerde uitspraken bevestigen het beeld dat ook uit andere studies naar voren is gekomen, namelijk dat money mules in Nederland worden geronseld. Money mules kunnen echter maar één keer gebruikt worden en voor het witwassen van grote bedragen zijn dus veel money mules nodig. Geldezels worden soms ingezet voor het doorsturen van pakketjes (dan ook wel een katvanger genoemd, omdat een adres wordt gebruikt en geen bankrekening) die met het frauduleus verkregen geld zijn gekocht, maar meestal voor het beschikbaar stellen van een bankrekening en voor het opnemen van geld. Het via een geldezel doorsluizen van geld naar een andere rekening zou veel minder vaak voorkomen. Uit dit onderzoek blijkt dat het in de meeste gevallen gaat om geldezels die op straat geronseld worden en bewust aan het witwassen meewerken in ruil voor een vergoeding (naast onbewuste money mules).

Hiernaast is specifiek gekeken naar de kenmerken van de money mules. Met betrekking tot de gemeenten waarin de geldezels woonachtig zijn is gebleken dat de money mules door heel Nederland wonen, maar dat de meeste geldezels in de grootste gemeenten van Nederland wonen (negen van de tien gemeenten met het hoogste aantal money mules

behoren tot de top vijftien grootste gemeenten van Nederland). De drie grootste gemeenten (Amsterdam, Rotterdam en Den Haag) domineren elk jaar de gegevens. Via de postcodes is nagegaan in wat voor een type wijken de money mules wonen. De money mules blijken zich voornamelijk in achterstandswijken of armere buurten gehuisvest te hebben. Ook het gemiddelde inkomen in de wijken waarin de geldezels wonen, bevestigt dit beeld dat money mules in de armere wijken wonen, en dan vooral van de drie grote steden. Buiten de grote steden wonen de money mules ook in de armere wijken, maar deze zijn minder arm dan in de drie grote steden. Er zijn geen significante veranderingen over tijd gevonden in deze omgevingskenmerken.

Deze studie toont ook aan dat de meeste geldezels van het mannelijk geslacht zijn (66%). Ten aanzien van de leeftijd van de geldezels constateren Oerlemans en collega's (2016) een sterke piek tussen de 18 en 22 jaar (slechts een kleine fractie is jonger dan 18 jaar). Hierin zijn ook geen veranderingen gevonden in de periode 2012-2015.

Daarnaast zijn enkele aanwijzingen gevonden dat personen met een Oost-Europese achtergrond een grotere kans hebben om geldezel te worden, omdat ze bijvoorbeeld makkelijker te ronselen zijn of de bankrekening doelbewust voor witwasactiviteiten openen. Zo had van de Amsterdamse geldezels tussen de 8 en 13% een Oost-Europese nationaliteit (terwijl slechts 1.4% van alle Amsterdamse inwoners deze nationaliteit had). Er zijn ook enkele aanwijzingen gevonden dat geldezels vaak in dezelfde periode gerekruteerd worden.

Voor ongeveer 600 geldezels die actief waren in 2012 is gezocht naar mogelijke antecedenten (t/m sept 2015). De resultaten tonen aan dat de helft van de geldezels geen antecedent had, 19% had 1 antecedent en 12% was veelpleger (meer dan 10 antecedenten). In 2012 werd in veel gevallen echter geen aangifte gedaan tegen de geldezels en dus was 69% niet of nauwelijks bekend bij de politie. Geldezels die al wel bekend waren bij de politie waren voornamelijk betrokken bij diefstal- en/of geweldsdelicten. Slechts een kleine fractie was betrokken bij oplichting, fraude of heling.

Oerlemans en collega's (2016) benoemen dat het opvallend is dat tot 2008 de leeftijd van de money mules rond de 15 jaar lijkt te liggen en dat dit daarna naar ongeveer 21 jaar lijkt te zijn gesprongen. De bevindingen ten aanzien van leeftijd, in combinatie met de aantallen antecedenten per jaar, wijzen op vier groepen money mules: de grootste groep zonder antecedenten, daarna de mules van gemiddeld 20 jaar oud met 1 of 2 antecedenten. De derde groep komt al op 15-jarige leeftijd in aanraking met de politie en heeft 4 tot 8 antecedenten. Tot slot is er nog de groep van veelplegers (meer dan 10 antecedenten) die over het algemeen ook op 15-jarige leeftijd al in aanraking komt met de politie. Omdat de ontwikkelingen volgens Oerlemans en collega's (2016) volop in beweging zijn geven ze aan dat de resultaten beperkt houdbaar zouden zijn. Banking malware leek destijds alweer af te nemen, terwijl dit bij phishing (tevens vaak de eerste stap in de cybercriminaliteit) niet het geval was. De onderzoekers adviseren dan ook om meer onderzoek te doen naar phishing en de mogelijke aanpak daarvan verder te onderzoeken.

Versprille (2016; nationaal)

Versprille verrichte een studie naar katvangers in de wereld van de hennepteelt. Katvangers zijn personen die zichzelf beschikbaar stellen als eigenaar of registratiehouder van een voertuig, bedrijf, bankrekening of ander goed, waardoor de werkelijke eigenaar of houder zichzelf buiten het zicht van de autoriteiten kan houden (Schoenmakers e.a., 2012, p. 31). In de introductie beschrijft Versprille (2016) dat de geldezel (money mule) 1 van de 5

onderzochte typen katvangers is. Om die reden is dit onderzoek ook meegenomen huidige literatuurverkenning (al gelden de resultaten dus niet specifiek voor geldezels maar voor de bredere categorie van de katvangers). Voor dit onderzoek zijn 18 interviews met actoren in het veld van de aanpak en preventie van de illegale hennepteelt geanalyseerd.

Het theoretische model van de situationele preventie van criminaliteit (SCP-model; Clarke, 2009) wordt beschreven, waaronder de 4 assumpties: 1) criminaliteit is het resultaat van een wisselwerking tussen een gemotiveerde dader en de gelegenheid die een situatie biedt, 2) overtreders maken de keuze om misdaden te plegen, 3) gelegenheid is een belangrijke veroorzaker van criminaliteit, 4) situationele factoren kunnen criminaliteit stimuleren. Het traditionele model van de situationele criminaliteitspreventie past volgens Versprille (2016) niet volledig bij het idee van de georganiseerde misdaad, maar geeft wel aanknopingspunten voor de preventie via zogenaamde *crime facilitators*, waaronder de katvangers.

Er wordt beschreven dat katvangers weet kunnen hebben van de illegale praktijken waarvoor zij ingezet worden, maar dat zij bij het rekruteren ook voor de gek gehouden kunnen worden, waardoor zij niet op de hoogte zijn van de eventuele gevolgen of betrokkenheid bij criminaliteit. Alle geïnterviewde respondenten zijn het er echter over eens dat personen die fungeren als katvanger in de hennepteelt daar bewust voor kiezen. Er zou volgens Versprille echter wel verschil zijn in of er initiatief genomen wordt en of ze weet hebben van de illegale praktijken die verricht worden. Daarvan zou gezegd kunnen worden dat het vermoeden er zou moeten zijn, maar dat de personen naïef zijn.

Over de kenmerken van katvangers schrijft Versprille (2016) dat over het algemeen alle type katvangers uit de lagere sociaal economische klassen komen. In bijna alle gevallen is er sprake van een financieel moeilijke situatie zoals armoede of het hebben van schulden. De volgende kenmerken worden het meest door de respondenten genoemd bij de vraag om wat voor personen het gaat in geval van katvangers: werkloos, naïef, beïnvloedbaar, laag IQ, diverse verslavingen, LVB, geen sociaal netwerk/controle, kwetsbaar, bevinden zich in criminele circuits, echtscheiding, lange termijn gevolgen niet in kunnen schatten, risico's niet goed in kunnen zien. Het zou voornamelijk gaan om mannen, in de leeftijd van 30 tot 50 jaar. Een enkele keer wordt over jongere (20 – 30 jaar) katvangers gesproken. Alhoewel de respondenten aangeven dat etniciteit een rol speelt (Bulgaren, Vietnamezen, Polen, Roemenen, Turken, Albanezen en Marokkanen zouden relatief vaak als katvanger optreden), worden katvangers volgens Versprille (2016) gevonden in alle lagen van de samenleving. Geld was wel volgens alle respondenten het belangrijkste motief. Daarnaast zouden enkele katvangers een 'vriendendienst' verrichten. Bij verschillende vormen van rekrutering (zichzelf aanbieden en mensen die geworven worden) gebeurt dit het vaakst binnen de eigen netwerken.

Versprille geeft hierop aansluitend aan dat preventiemaatregelen zich in eerste instantie zouden moeten richten op de bewustwording van het probleem en het vergroten van kennis met betrekking tot katvangers en de illegale hennepteelt. Er zou meer voorlichting moeten zijn en bewustwording (liefst al op de basisschool) over wat de gevolgen zijn, oftewel, wat het voor potentiele katvangers zou betekenen als zij gepakt zouden worden. Op die manier zou het besef van de risico's versterkt kunnen worden.

Odinot, Verhoeven, Pool & De Poot (2016; internationaal)

In datzelfde jaar publiceren Odinot, Verhoeven, Pool en De Poot een studie waarvoor

11 cybercrime zaken (geselecteerd door experts als de meest informatieve zaken) zijn onderzocht en 12 interviews met rechtsbeklederes (OM; rechercheteams) zijn geanalyseerd. De resultaten hiervan duiden erop dat geld het belangrijkste motief achter de cybermisdaden is. Volgens de experts wordt er vooral gebruik gemaakt van geldezels bij phishing en malware gericht op online bankieren. Onschuldige, vaak kwetsbare mensen zouden onder druk worden gezet om mensen hun accounts te laten gebruiken in ruil voor een klein bedrag.

In de transcripten van interne communicatie binnen de netwerken is meer te lezen over hoe geldezels gerekruteerd worden. De recruiters blijken de geldezels vaak nog niet te kennen, maar zij vinden deze letterlijk op de hoek van de straat. De geldezels zouden zo graag geld willen verdienen dat ze bereid zijn om hun bankrekening beschikbaar te stellen en met de crimineel naar een bankautomaat te gaan om geld op te nemen. In één geval gebruikten de verdachten ook nauwe relaties als geldezel (een zus en vriendin; laatste werd gevraagd een bankrekening voor hun zoon te openen).

De geïnterviewde experts hebben aangegeven dat geldezels een belangrijke rol spelen in de politieonderzoeken van cybercrime zaken. Geldezels ontvangen vaak een bedrag voor hun diensten, maar zijn zich soms niet bewust van de illegale aard. Vaak worden de mensen beschreven als kwetsbaar, woonachtig in moeilijke sociale omstandigheden, en/of kampend met verslavingsproblemen. Preventie door adequate informatie te verstrekken zou waardevol kunnen zijn volgens Odinot en collega's (2016; zie ook Leukfeldt, 2014). Inspanningen hiervoor werden destijds al ondernomen door Nederlandse banken.

Leukfeldt, Kleemans, & Stol (2017; internationaal)

Deze studie bouwt voort op de studie van Soudijn en Zegers (2012) en Leukfeldt (2014) en bestaat uit een analyse van alle phishing en malware zaken in Nederland van 2004 – 2014 (18 cybercriminele netwerken/onderzoeken; via politiedossiers) en aanvullende interviews met OM, rechercheurs en onderzoeksleiders. Hierbij wordt wederom het *social opportunity structure perspective* als uitgangspunt genomen.

De resultaten tonen aan dat recruiters vaak binnen het gebied waarin ze wonen opereren en dat ze hun sociale netwerk gebruiken om nieuwe geldezels te rekruteren. Eén van de geldezels gaf verder aan (citaat Leukfeldt, Kleemans, & Stol, 2017): '*Ik zei al dat iedereen in Nederland dit doet. Vooral jonge mensen. Je kunt makkelijk geld maken en veel willen dat doen. Veel jonge mensen of verslaafden die niets te verliezen hebben*.' Deze geldezel was op straat in Den Haag geworven door iemand die hij vaag kende uit zijn buurt. Hij ontmoette die persoon af en toe en er was hem meerdere keren geld aangeboden om zijn bankpas en pincode uit te lenen. In een ander geval dat wordt beschreven werden geldezels geworven binnen een bepaalde etnische gemeenschap in een mediumgrote stad in Noordwest Nederland. Deze geldezels kregen betaald voor hun diensten, dus het was voor deze recruiters niet moeilijk om nieuwe geldezels te vinden. Nieuwe geldezels bleken recruiters zelfs uit zichzelf te benaderen. 'Op straat' zou iedereen weten dat een bepaalde recruiter betrokken was bij criminele activiteiten, waarmee makkelijk geld verdiend kon worden.

Leukfeldt en collega's (2017) concluderen dat geldezels worden gebruikt in 17 van de 18 onderzochte netwerken. Ze worden voornamelijk gerekruteerd door daarvoor gerekruteerde *enablers*, of door de kernleden zelf/professionele *enablers*. In de meeste gevallen bieden de geldezels hun diensten ook spontaan aan bij de recruiters, bijvoorbeeld

als een recruiter lang genoeg in een bepaald gebied opereert en het na een tijdje algemeen bekend wordt dat via hem makkelijk geld verdiend kan worden.

Kruisbergen, Leukfeldt, Kleemans, & Roks (2018; nationaal)

In deze rapportage wordt enige aandacht besteed aan geldezels, op basis van de vijfde ronde van de Monitor Georganiseerde Criminaliteit. In twee van de bestudeerde casussen bestaat de onderste laag van de netwerken uit katvangers die hun rekening ter beschikking stelden aan kernleden. De gegevens tonen aan dat de katvangers veelal binnen de sociale netwerken van de kernleden en *facilitators* worden geworven. Daarbij worden zowel offline sociale contacten (zoals mensen uit de buurt, bij het uitgaan) als online sociale contacten (oproepen op sociale media of online games) gebruikt. Eén van de recruiters uit een casus rekruteerde bijvoorbeeld nieuwe money mules onder kennissen. Als iemand meewerkte, werden ook de vrienden van die persoon benaderd. Uit de communicatie tussen de kernleden blijkt verder dat ronselaars bewust op zoek zijn naar personen die gemakkelijk te beïnvloeden zijn, bijvoorbeeld personen met hoge schulden of psychische problemen of drugsverslaafden. In de dossiers waren inderdaad voorbeelden te vinden van een katvanger met schulden, een dakloze en iemand in een begeleid-wonen traject.

Leukfeldt & Kleemans (2019; internationaal)

Deze studie is erg relevant voor huidige literatuurverkenning. In de introductie geven Leukfeldt en Kleemans (2019) aan dat verschillende onderzoekers de belangrijke rol van money mules al wel hadden erkend, maar zich toch meer op de kernleden van criminele netwerken hadden geconcentreerd (evenals politie overigens). De cruciale functie van money mules bij phishing en malware netwerken zorgt er echter voor dat deze specifieke groep extreem relevant is voor de situationele preventie van criminaliteit, bijvoorbeeld door het lastiger te maken om money mules te rekruteren, door het minder aantrekkelijk te maken om een geldezel te zijn of door excuses weg te nemen (Cornish & Clarke, 2003). De situationele criminaliteitspreventie zou zich kunnen richten op het wegnemen van excuses en op neutralisatie technieken (voorbeelden van excuses/neutralisaties: hij stemde alleen in na verschillende keren geweigerd te hebben; hij had serieuze problemen en had extra geld nodig; er was geen geld op zijn bankrekening dat gestolen kon worden). Meer inzicht in de aard van deze excuses zou ook kunnen helpen bij het ontwikkelen van effectieve interventie strategieën. Situationele criminaliteitspreventie strategieën omvatten overigens een breed scala aan maatregelen die de gelegenheid beperken met als doel om misdaad te verhinderen of te voorkomen. Leukfeldt en Kleemans (2019) beschrijven vijf strategieën voor situationele criminaliteitspreventie: 1) maak het lastiger om de misdaad te plegen, 2) versterk het risico van de misdaad, 3) verminder de beloningen van de misdaad, 4) verminder provocaties die uitnodigen tot crimineel gedrag, 5) verminder de excuses voor crimineel gedrag.

Leukfeldt en Kleemans (2019) onderzochten 14 Nederlandse misdaadzaken (2004 – 2014) en vonden dat vaak honderden geldezels zijn gebruikt door de netwerken achter de misdaden. Het aantal ondervraagde geldezels was echter veel lager, omdat onderzoeken zich niet op de geldezels richten, maar op de kernleden of belangrijke helpers. Daarnaast is het opsporen en bevragen van alle geldezels te tijdsintensief. Om die redenen varieerde het aantal ondervraagde geldezels per onderzoek. Uiteindelijk bevatten de 14 onderzoeken ondervragingen van 211 geldezels. Daarvan waren er 112 geschikt voor analyse (de rest

werkte niet mee en 30 claimden onschuldig te zijn). Deze 112 geldezels gaven toe te hebben geholpen. Het ging overigens alleen om afgeronde online bankzaken (phishing en malware aanvallen). Contacten werden gevraagd zaken aan te leveren. Daarnaast werd een online database met gerechtelijke documenten geraadpleegd en er werd een media analyse gedaan om nieuws te vinden over relevante casussen.

De bevindingen van Leukfeldt en Kleemans (2019) tonen aan dat de meerderheid van de 112 geldezels beperkte financiële middelen heeft. Tenminste 40 geldezels zaten nog op de middelbare school of universiteit en hadden alleen deeltijd baantjes, vijf andere waren gestopt met school en hadden een parttime baan, 35 geldezels hadden geen werk en hadden een uitkering en 58 gaven aan dat ze schulden hadden. Recruiters lijken gebruik te maken van deze kwetsbaarheid. Zij beloven geld voor weinig moeite. Een illustratief citaat van een geldezel: '*Ik werd meerdere keren per dag gevraagd door een jongen of ik mijn bankpas en pincode wou geven. Ik zou er iets voor terug krijgen. Op dat moment had ik serieuze problemen*.'

De bevindingen tonen ook aan dat in bijna alle gevallen (in 13 van de 14 onderzoeken) de geldezels worden geronseld via bestaande sociale contacten. Kernleden of recruiters zoeken contact met mensen die ze kennen van hun eigen buurt, school of sportclub. Zij stellen vragen over de financiële situatie van potentiele geldezels, of ze vragen gewoon of ze makkelijk geld willen verdienen. Geldezels worden ook via (spam)mails geworven.

Ten aanzien van motieven en neutralisatie technieken beschrijven Leukfeldt en Kleemans (2019) dat niet alle verdachten toegeven dat ze met opzet hebben gehandeld. Er is variatie in de motieven en neutralisaties. Eén groep geldezels gaf toe dat ze bewust hadden meegewerkt en dat ze het gewoon niet konden weerstaan om makkelijk geld te verdienen. Veel van deze geldezels zijn deel van een subcultuur waarin het normaal is om mee te werken aan dit soort frauduleuze activiteiten en zij zeggen vaak dat ze zich onder druk gezet voelen door recruiters. Er waren ook verschillende geldezels die toegaven dat ze meegewerkt hadden, maar zij gebruikten als excuus dat ze zich er niet bewust van waren dat de activiteiten frauduleus waren (bv. omdat ze dachten dat de geldtransacties legaal waren of dat virtueel geld niet echte slachtoffers zou hebben). Een derde groep legde de schuld bij de slachtoffers (die zich bv. beter hadden moeten beschermen).

Bijna een kwart van de geldezels (26 geldezels) gaf aan dat ze deel waren van een subcultuur waarin frauduleuze activiteiten normaal zijn (hiervoor ook al aangegeven). Het is dus relatief normaal dat ze benaderd worden door mensen die hen vragen om hun bankpas uit te lenen. Iets meer dan een kwart (31 geldezels) stelde dat ze gewoon simpel geld wilden verdienen. '*Hij vroeg of ik een manier wist om meer geld te verdienen. Zijn studiefinanciering was te laag. Hij wou meer geld voor schoenen, petten enzovoorts. Ik vertelde hem toen dat hij 800 of 900 euro kon verdienen door zijn bankpas aan te bieden*.' Een kleiner deel van de geldezels (15 geldezels) gaf tijdens de ondervragingen aan dat ze opkeken tegen de manier van leven van de kernleden of recruiters. Deze leden hebben een hoog aanzien onder lokale jongeren, en jongeren die als recruiters beginnen, hebben opeens veel geld te besteden. Ze rijden luxe auto's, dragen mooie kleding en spenderen veel geld in het nachtleven. Jongeren willen zelf ook graag makkelijk geld verdienen. Ze worden vaak benaderd op straat, op hangplekken, in het nachtleven of op school. Andere personen worden actief benaderd via sms'jes. Jongeren krijgen dan berichten van vrienden of vage kennissen waarin gevraagd wordt naar bankpassen. Binnen de subcultuur waarin kernleden en recruiters hun dure levensstijl tonen kwam het ook voor dat geldezels zichzelf aanboden (n = 7). Sommige

geldezels voelen zich echter onder druk gezet door de recruiters, ze zeggen eerst 'nee', maar na een tijdje geven ze toch toe.

Iets meer dan een kwart (30 geldezels) gaf aan dat ze dachten dat de geldtransacties legitiem waren (bv. dat het geld van familie was en dat de eigen bankpas verloren was). Andere excuses zijn dat ze denken dat de activiteiten geen slachtoffers zouden maken (bv. van banken die geld rondpompen voor belasting). Een kleiner aantal geldezels (*n* = 13) beschuldigden de slachtoffers (alleen geldezels die via spam gerekruteerd werden; bedrijven waren slecht beveiligd).

Als mogelijke situationele criminaliteitspreventie strategieën adviseren Leukfeldt en Kleemans: 1) verminder de provocaties die crimineel gedrag uitlokken (vooral peer pressure verminderen en peer imitatie) en 2) haal excuses voor crimineel gedrag onderuit (voornamelijk potentiële money mules bewust maken van het criminele gedrag). Een bewustzijnscampagne zou zich kunnen richten op het bewust maken van potentiële money mules dat ze samenwerken met criminelen die geld stelen van onschuldige mensen en op het duidelijk communiceren dat geldezels misbruikt worden door criminelen om politie en justitie bij hen weg te houden (en juist te leiden naar de geldezels). Volgens Leukfeldt en Kleemans (2019) zouden geldezels in bepaald opzicht ook slachtoffers zijn.

Jansen, Westers, Twickler, & Slot (2019; nationaal)

Om de crimescripts en aanvalsstrategieën van aankoopfraude in kaart te brengen hebben Jansen, Westers, Twickler en Slot (2019) 150 meldingen van het Landelijk Meldpunt Internetoplichting (LMIO) geanalyseerd, 20 semi-gestructureerde interviews met slachtoffers geanalyseerd en 16 interviews met experts en een brainstormsessie met de klankbordgroep gehouden. Het juridische kader is ten slotte nog in kaart gebracht via deskresearch.

Op basis van de resultaten zijn verstoringsmogelijkheden van aankoopfraude beschreven (vanuit de situationele criminaliteitspreventie benadering). De techniek van het neutraliseren van groepsdruk (*peer pressure*) wordt in verband gebracht met geldezels. De experts die geïnterviewd zijn benoemden de geldezels vaak (dit kwam overigens niet naar voren in de analyses van de crimescripts). Potentiele geldezels zouden beter voorgelicht moeten worden. Een expert beschreef het EMMA-project in 2016 (waarbij 81 geldezels gearresteerd werden) en de campagne 'Word geen money mule'. Dit soort initiatieven zouden effect hebben, omdat potentiële geldezels zo zouden beseffen dat banken en de politie ze in het vizier heeft. Via voorlichting over de gevolgen van medeplichtigheid aan fraude zou een extra drempel kunnen worden opgeworpen. *Knock and talk* acties (stopgesprekken; bv. een wijkagent die een jonge geldezel thuis bezoekt en een waarschuwend, maar indringend gesprek heeft met de geldezel en ouders) worden beschreven als een andere verstoringsmogelijkheid. Ten slotte zou het volgens Jansen en collega's (2019) met betrekking tot geldezels van belang zijn om de pakkans te verhogen. Hier zou vooral een rol liggen voor private partijen met een preventief karakter (bv. banken die geldezels zouden kunnen aanspreken of waarschuwen), mogelijk ondersteund door politie en/of de overheid.

Havenaar (2019; nationaal)

Havenaar verrichtte een relevante studie naar katvangers, oftewel 'personen die de werkelijke zeggenschap, eigendomsverhouding of gerechtigheid tot een object of vermogen

verhullen' (Soudijn, 2016, p. 15), ook wel geldezels, stromannen of money mules genoemd. Havenaar beschrijft dat binnen de financiële sector de katvanger iemand is die de eigen bankrekening misbruikt of laat misbruiken, voor het uitvoeren van transacties namens een derde partij. Voor deze studie is een literatuuronderzoek verricht, een kwantitatieve analyse van gegevens van gedetecteerde katvangers (in 2018) gedaan (*N* = 1308 zaken van particuliere rekeningen met één rekeninghouder) en 5 semigestructureerde interviews met personen die de katvangersproblematiek in hun dagelijkse werkzaamheden tegenkwamen (bv. van de afdeling Veiligheidszaken) geanalyseerd.

Over de kenmerken van de populatie door de bank gedetecteerde katvangers beschrijft Havenaar dat de katvangers bestonden uit drie keer zoveel mannen dan vrouwen en dat de gemiddelde leeftijd 27.9 jaar was. Meer dan een derde van de katvangers viel in de leeftijdscategorie 18 tot en met 25 jaar. De meeste katvangers woonden in Amsterdam, (Zuidoost), Rotterdam en Den Haag. Iets meer dan een derde deel van de katvangers was betrokken bij online handelsplaatsfraude, ongeveer een kwart bij phishing en ongeveer één tiende deel bij oplichting via WhatsApp (de rest bij overige vormen van fraude). Het gemiddelde fraudebedrag dat via de rekening van de katvangers werd weggesluisd was 17.051,34 euro. Bij ongeveer de helft van de katvangers lag het bedrag echter onder de 4.000,- euro. De gemiddelde duur van de klantrelatie was 8,11 jaar. Echter, bij bijna een kwart van de onderzoekspopulatie werden al risico's gezien in het eerste jaar. Van deze groep gebeurde dit voor meer dan de helft zelfs in de eerste vier maanden van de klantrelatie. Zowel uit de kwantitatieve, als de kwalitatieve data is gebleken dat de klantrelatie doorgaans van korte aard is. De gemiddelde 'systematische voeding' (d.w.z. de gemiddelde maandelijkse inkomsten op de rekening over de afgelopen zes maanden) bleek 611,11 euro te zijn, meer dan de helft van de katvangers had zelfs een gemiddelde systematische voeding van onder de 500 euro en voor bijna een vijfde deel was dit 0 euro. Daarnaast bleek het gemiddelde vermogen 836,97 euro, terwijl meer dan de helft van de katvangers een gemiddeld vermogen van onder de 100 euro had; voor meer dan een derde deel was dit zelfs 0 euro. Ook uit de kwalitatieve data is gebleken dat katvangers vaak weinig financiële middelen hebben. Er is vaak sprake van een laag saldo en er wordt geen salaris op de rekening ontvangen. Uit de kwalitatieve data is daarnaast gebleken dat het verhogen van de opnamelimiet, het koppelen van een nieuw mobiel apparaat aan de rekening en meerdere pinpogingen indicatoren zijn voor een katvangersrekening.

Tot op zeker hoogte kan onderscheid worden gemaakt in het typische katvangerprofiel en de typische katvangersrekening. De typische *katvanger* kan gekenmerkt worden als jong, naïef en in veel gevallen niet bewust van de betrokkenheid bij het criminele netwerk. Tevens is uit de studie van Havenaar (2019) gebleken dat er een verschuiving is naar jongeren door het gebruik van sociale media door katvanger recruiters. In de afgelopen jaren is er tevens een verschuiving geweest van katvangers onder de 18 jaar, naar katvangers boven de 18 jaar. Dit is volgens Havenaar (2019) toe te schrijven aan de verlaging van de opnamelimiet voor jongeren onder de 18. Bij de typische katvanger wordt de persoonlijke rekening gebruikt voor het doorsluizen van de geld, waardoor er minder snel indicatoren in het rekeninggebruik naar voren komen. Omdat demografische factoren om ethische redenen niet gebruikt kunnen worden in de fraudedetectie, is het lastig om dergelijke gevallen tijdig in beeld te krijgen.

Over de typische *katvangersrekening* is gebleken dat de rekening vaak puur wordt geopend om de fraude te plegen. Daarbij komen bepaalde rekeningindicatoren vaker naar voren: een net geopende rekening, lage gemiddelde systematische voeding en een laag

gemiddeld vermogen. De kwalitatieve data toonden aan dat er op de typische katvangersrekening doorgaans weinig tot geen transactieverkeer plaatsvindt.

Er zijn geen verschillen gevonden in de leeftijd, de duur van de klantrelatie en het gemiddeld vermogen tussen de katvangers bij phishing, online handelsplaatsfraude of oplichting via WhatsApp. Er is wel een verschil gevonden in de gemiddelde systematische voeding: bij online handelsplaatsfraude was dit significant hoger dan voor de overige groepen. Voor deze fraudevorm worden doorgaans ook jongere katvangers gerekruteerd in de offline omgeving, die zich veelal niet bewust zijn van het feit dat zij als katvanger worden gebruikt.

Havenaar concludeert dat personen die voldoen aan het typische katvangersprofiel vaak van het mannelijke geslacht en jong zijn, de Nederlandse nationaliteit hebben en in grote steden wonen. Het zouden vaak naïeve personen met geldproblemen zijn, die niet nadenken over de lange termijn gevolgen van hun daden. Bewustmakende acties zouden zich moeten richten op deze groep. Hierbij zou nauw moeten worden samengewerkt met sociale media platformen. Zo zou relevante informatie gedeeld kunnen worden en groepsgerichte bewustmakende acties ontwikkeld kunnen worden.

Daarnaast is gebleken dat typische katvangersrekeningen te herkennen zijn aan een korte klantrelatie, een lage systematische voeding, een laag vermogen en weinig transacties op de rekening. Dergelijke rekeningindicatoren zouden moeten worden meegenomen in toekomstige katvangersdetectie. Ook het verbinden van een nieuw mobiel apparaat aan de rekening zou daarbij als indicator kunnen worden meegenomen. Tevens zou de opnamelimiet vaak verhoogd worden. Havenaar (2019) geeft aan dat het van belang is om hier restricties aan te verbinden.

Ten aanzien van eventuele verschillen tussen katvangersprofielen per fraudedelict is zoals gezegd alleen gevonden dat katvangers bij online handelsplaatsfraude maandelijks significant meer gemiddelde systematische voeding ontvingen op hun rekening dan de katvangers bij phishing of bij oplichting via WhatsApp. Dit is echter het enige gevonden verschil en uit de resultaten van de kwalitatieve analyse kwamen geen verschillen naar voren.

Ten slotte is uit de onderzoeksresultaten gebleken dat als gevolg van het veelvuldig gebruik van sociale media, vooral jongeren gedetecteerd worden. Om deze reden zou het van belang zijn dat er voor deze groep wordt ingezet op *awareness*. En aangezien kortstondige awareness acties niet het gewenste effect hebben gehad volgens Havenaar wordt aanbevolen om langdurige en herhalende awareness acties te ontwikkelen waarbij een nauwe samenwerking gezocht wordt met partijen zoals als Telegram en Instagram.

Kruisbergen, Leukfeldt, Kleemans, & Roks (2019; nationaal)

Voor deze exploratieve studie zijn de gegevens van 30 grootschalige criminele onderzoeken geanalyseerd (deel van de vijfde ronde van de Monitor Georganiseerde Criminaliteit). De onderzoekers wilden inzicht krijgen in hoe georganiseerde misdaadplegers IT inzetten om geld wit te wassen. Ze richten zich niet alleen op cybercrimes, maar ook op de traditionele vormen van georganiseerde misdaad zoals offline drugssmokkel. Eén van de opvallendste overeenkomsten tussen cybercrime en traditionele misdaden die zijn gevonden is dat de plegers een voorkeur voor cash hebben: zowel malware en phishing plegers, als online drugshandelaren wisselen hun digitale valuta's graag in voor geld.

Over geldezels toonde de communicatie tussen de plegers in een malware zaak aan dat criminelen zoeken naar geldezels onder personen die makkelijk te beïnvloeden zijn, zoals

jonge mensen met schulden, psychologische problemen, of drugsverslaving. De gegevens tonen verder aan dat geldezels niet altijd de beloofde compensatie ontvangen (phishing zaak). Kruisbergen en collega's (2019) concluderen dat in geval van het cashen vanuit banking malware of phishing aanvallen, plegers vaak geldezels gebruiken. Deze geldezels worden vaak gerekruteerd in de lokale nabijheid (zie ook Leukfeldt, Kleemans, & Stol, 2017a; Custers, Pool, & Cornelisse, 2019).

Roks & Monshouwer (2020; nationaal)

De studie van Roks en Monshouwer (2020) is een interessant, zogenaamd netnografisch onderzoek (d.w.z. etnografische technieken zijn ingezet voor de studie van culturen en gemeenschappen die ontstaan zijn via elektronische netwerken) naar fraude en oplichting op het platform Telegram Messenger. Op dit platform staan *encrypted messaging* en privacy centraal. Ook is een zoekfunctie aanwezig die het mogelijk maakt om verschillende groepen te vinden waar je lid van kunt worden en berichten en bestanden kunt delen met de gehele groep. Het versturen van privéberichten is ook mogelijk. De onderzoekers hebben eerst relevante groepen gezocht op Telegram (o.a. via de zoektermen *swipen* en bonken) en deze regelmatig bezocht zonder lid te worden. Vervolgens hebben de onderzoekers gedurende vier maanden om de twee dagen de berichten in vijf groepen (variërend van 134 tot 3239 leden) gelezen en meer dan 1650 screenshots gemaakt van de berichten die te maken hadden met phishing (en fraude meer in het algemeen). Deze zijn op kwalitatieve wijze geanalyseerd.

In de introductie beschrijven Roks en Monshouwer (2020) overigens eerst nog voorgaande studies van onder andere Soudijn en Zegers (2012), Leukfeldt (2014) en Roks en Van den Broek (2017). Deze laatste studie, een analyse van het gebruik van sociale media door een problematische jeugdgroep uit de Rotterdamse wijk Spangen, illustreerde al hoe jongeren platforms als Twitter gebruiken om naar specifieke bankpassen te vragen en waar ze poseren met verschillende betaalpassen (Roks & Van den Broek, 2017, p. 40).

De resultaten van de studie van Roks en Monshouwer (2020) tonen aan dat bij de vraag op Telegram naar betaalpassen de voorkeur uitgaat naar zogenaamde '18+' – of zakelijke kaarten, omdat deze een limiet kennen tot 10.000 euro in tegenstelling tot 'kinderkaarten' die 'slechts' een limiet van 5.000 hebben. Een gebruiker schreef dat hij niet op zoek was naar afhakers, grappenmakers, kleine kinderen en *bledders* (mensen die enkel praatjes hebben).

Op basis van de resultaten van deze studie concluderen Roks en Monshouwer (2020) dat Telegram beschouwd kan worden als een *digital offender convergence setting*. Het veelvuldige gebruik van straattaal in de berichten doet daarbij vermoeden dat het gaat om personen die zijn ingebed in de staatcultuur en hun werkterrein hebben verplaatst van de fysieke naar de digitale straat (Lane, 2019).

Leukfeldt & Roks (2020; internationaal)

Deze studie baseert zich op dezelfde data als de eerder beschreven studie van Leukfeldt en Kleemans (2019; 14 onderzoeken uit de periode 2004 – 2014, aangevuld met interviews). De resultaten van deze studie duiden erop dat sommige rekrutering processen gedigitaliseerd zijn, maar dat zowel offline als online potentiële ezels worden gevonden. Offline interacties blijven echter van belang volgens leukfeldt en Roks (2020). Met andere woorden: zowel de fysieke als de digitale *streets* zijn van belang zijn voor de rekrutering van geldezels.

Leukfeldt en Roks (2020) richten zich met deze studie op de straatcultuur (slang) en beschrijven dat, terwijl de casussen geen gedetailleerde informatie over de persoonlijke achtergronden van de plegers gaven, ze wel verschillende voorbeelden zagen van kwetsbare mensen, vooral jongeren uit achtergestelde buurten, die overgehaald waren door de verleiding van makkelijk geld via recruiters op de fysieke en digitale straat. Een zoektocht naar geld is één van de belangrijkste kenmerken van de straatcultuur. Verder werden er aanwijzingen gevonden voor het 'normaliteit-idee', waarbij jongeren opkijken tegen recruiters die geld laten zien (zie tevens voorgaande studies). Daarop aansluitend lieten de meeste netwerken ook offline criminaliteit zien, oftewel, ze waren niet gespecialiseerd in één type online misdaad en geldezels werden dus zowel offline als online benaderd in Nederland. De offline wereld blijft dus van belang. En daarbij maken de kernleden, recruiters en geldezels onderdeel van een Nederlandse straatcultuur. De misdaden kan je dan ook zien als digitale vormen van traditionele (economische straat) misdaden. Oftewel, straatplegers hebben zich aangepast aan de technologische ontwikkelingen.

Bekkers, Schiks, & Leukfeldt (2020)

In oktober verscheen er nog een rapport van Bekker, Schiks en Leukfeldt (2020) gebaseerd op een bestudering van de literatuur en tien aanvullende expertinterviews. Het doel was om meer inzicht te krijgen in effectieve interventies die de gemeente Haarlem in zou kunnen zetten ter preventie van het *money mulen*.

In het kader van het literatuuronderzoek beschrijven Bekker, Schiks en Leukfeldt (2020) de jaarlijkse inventarisatie van Europol (de *European Money Mule Actions*) waarbij in 2019 3.833 geldezels geïdentificeerd zijn bij 7.520 gevallen van fraude (228 geldezels zijn ook gearresteerd). Volgens deze inventarisatie worden vaak mensen van jonger dan 35 jaar gerekruteerd, maar is er een stijging te zien in het ronselen van jongere generaties (12-21 jaar). Verder zouden mensen met een migratie-achtergrond, werklozen, studenten en mensen met weinig financiële middelen geldezel risicogroepen vormen.

De steekproef van geïnterviewden was een zogenaamd *convenience sample* (geworven via het netwerk van de onderzoekers en de gemeente Haarlem) en de respondenten waren allemaal werkzaam in de regio Haarlem. Het ging om drie medewerkers van de politie, twee jeugdwerkers, één HALT medewerker, OM medewerker, LVB-jeugdspecialist, reclasseringsmedewerker en een bankmedewerker. De resultaten op basis van de tien interviews geven vooral aan dat de groep geldezels als 'divers' te kenmerken is. De meeste geïnterviewden waren het er wel over eens dat de meerderheid van de geldezels jongeren of jongvolwassenen zijn. Bij deze bevinding (en de overige) moet echter wel rekening worden gehouden met het feit dat veel van de respondenten van deze studie met jeugdigen werkten en dit heeft deze resultaten mogelijk gekleurd. Aangezien huidige literatuurverkenning echter ook gericht is op jonge geldezels zijn ze zeker van belang. De meeste geldezels zijn volgens de geïnterviewden jongens, maar er zijn ook meisjes die als geldezel optreden. Verder zijn er geldezels op alle opleidingsniveaus te vinden, maar vooral de lager opgeleiden lijken een risicogroep te vormen, omdat zij eenvoudiger te misleiden zouden zijn en vanwege beperkter toezicht door de ouders bij deze groep. Dit laatste aspect (gebrekkig ouderlijk toezicht) zou ook kunnen verklaren waarom jongeren met een lagere sociaal-economische status volgens een meerderheid van de geïnterviewden oververtegenwoordigd zijn binnen de groep geldezels, al geldt hierbij wederom dat geldezels in alle lagen voorkomen. Datzelfde geldt voor de delictgeschiedenis, ook hier zien de

geïnterviewden veel variatie, maar veel geldezels zouden mogelijk wel *first-offenders* zijn. Naast de achtergrondkenmerken die naar voren kwamen uit de interviews is er door Bekkers en collega's (2020) nog gekeken naar geldezel risicofactoren. De 10 geïnterviewden gaven aan dat jongeren die er graag bij willen horen en gevoelig zijn voor 'snel geld' een risicogroep vormen. Ook vormen jongeren in de rapcultuur, waarin jongeren zich optrekken aan het imago van rappers, een risicogroep. Verder zijn volgens de respondenten jongeren met een LVB kwetsbaar, vanwege hun beïnvloedbaarheid, gebrek aan perspectief en beperkte sociale netwerk (waarin weer andere mensen met LVB). Deze groep zou met name ingezet worden voor de grotere transacties. De meerderheid van de respondenten gaf ook aan dat jongeren uit arme gezinnen en/of wijken een risicogroep vormen, vanwege hun gevoeligheid voor 'snel geld'. Verslaafden, daklozen en mensen met schulden zouden met name in de volwassen geldezel groep voorkomen. Ten aanzien van de jongeren kwam verder nog een instabiele thuissituatie naar voren tijdens de interviews. Het zou dan gaan om jongeren met weinig toezicht van de ouders of om gezinnen met multiproblematiek. Ook hierbij wordt echter opgemerkt dat het beeld heel divers is, en dat er ook geldezels zijn met heel gunstige achtergronden. Ten slotte duidden nog drie van de tien geïnterviewden erop dat jongeren die net in Nederland zijn komen wonen (de zgn. 'nieuwe Nederlanders') eveneens een risicogroep vormen, omdat zij de Nederlandse taal nog minder goed beheersen, financieel beperkt zijn, minder kennis van het Nederlandse rechtssysteem hebben en omdat zij door hun heftige ervaringen extra kwetsbaar zijn.

Bevindingen vanuit buitenlandse (wetenschappelijke) studies

Mikhaylov & Frank (2016)

Voor deze studie zijn twee Russische openbaar toegankelijke online carding en hacking forums gedownload en onderzocht aan de hand van sleutelwoorden die te maken hebben met online witwassen. De resultaten van deze studie laten zien dat fraudeplegers voor hun witwas praktijken kwetsbare sociale groepen uitbuiten, zoals de armen en de drugsverslaafden. Een citaat: '*Vind een kind of een student op straat, beloof hem 100 – 200 roebels voor het ontvangen van een transactie van jou. Stuur een sms met de naam van het kind, hij krijgt de overboeking en geeft het aan jou*.' Het vooruitzicht van *easy money* is volgens Mikhaylov en Frank (2016) een machtig lokmiddel voor onwetende potentiële geldezels. Twee andere forum gebruikers stelden voor om daklozen en drugsverslaafden te huren als geldezels. Juist onwetende geldezels zouden gerekruteerd worden vanwege hun gebrek aan kennis van het financiële systeem of gebrek aan zorgen over de herkomst van het geld. Gebaseerd op de kenmerken die geïdentificeerd werden door de forum gebruikers zouden schoolkinderen, arme studenten, drugsverslaafden, daklozen en ouderen de ideale doelwitten vormen voor geldezel rekrutering.

Chang, Lai, Chou, & Chen (2017)

Deze onderzoekers hebben een model ontwikkeld waarmee de onderliggende structuur van fraudegroepen en de rollen van de leden kunnen worden blootgelegd. De verbindingen tussen de verdachten worden gelegd op basis van vluchtinformatie, en co-offending gegevens. Sociale netwerk analysetechnieken zijn toegepast om de groepsstructuren en de

invloeden van alle leden te analyseren. Het model is ook toegepast op een telecom fraude dataset met 113 leden (gearresteerd in Taiwan) uit vier landen en zeventien steden (voornamelijk in Zuidoost Azië). De eerste resultaten tonen aan dat het model goed toegepast kan worden, en dat geldezels meestal tieners zijn. Vanwege hun lage posities in de groepen kon er verder weinig informatie verkregen worden van de money mules.

Hülsse (2017)

Hulsse (2017) schreef ten slotte nog een artikel over de *discourse* rondom geldezels in nationale en internationale documenten van anti-witwas autoriteiten zoals *Financial Intelligence Units* (FIU's), Europol, en de *Financial Action Task Force* (FATF) en de implicaties hiervan. Hij beschrijft dat de typische geldezel via case study verhalen, visualisaties en metaforen geportretteerd wordt als een jong mannelijke persoon in een Westers/Noordelijk land, die graag extra inkomen wil. Het zou vaak een student/leerling zijn, die er door criminelen is ingeluisd en daarom niet bewust is dat hij een misdaad heeft gepleegd. Geldezels worden veelal omschreven als onschuldige slachtoffers van georganiseerde criminele netwerken uit West-Afrika en Oost-Europa (gesteund door overboekingsbedrijven zoals de Western Union) in plaats van als criminelen.

Verder zouden jonge mensen eerder als geldezel gebruikt worden dan oudere personen. Europol (2015) claimde dat de typische ezel 18 tot 34 jaar oud was, en de oververtegenwoordiging van jonge mensen zou ook benadrukt worden in de meeste visuele gegevens die door Hülsse (2017) geanalyseerd zijn. Er zijn echter ook bronnen gevonden die aangeven dat de slachtoffers niet zo onschuldig zijn als ze lijken. Moneyval stelde bijvoorbeeld dat dit een naïef beeld is, en ook in twijfel wordt getrokken door de politie en door banken omdat gevonden is dat ezels vaak volledig bewust zijn van de illegale aard van hun daden. Een Zwitsers politierapport zou ook hebben aangegeven dat het een uitdaging is geworden voor criminelen om mensen te vinden die naïef genoeg zijn om als geldezel gerekruteerd te worden.

Conclusie

Beperkingen

Voordat we conclusies trekken over wat de besproken studies zeggen over de kenmerken van de jonge geldezels willen we wijzen op een aantal beperkingen waar rekening mee gehouden moet worden bij de interpretatie van de bevindingen. Wat in de eerste plaats is opgevallen bij de bestudering van de bronnen is dat veel bronnen zich baseren op deels overlappende gegevens (bv. dezelfde Nederlandse opsporingsgegevens). Daarbij wordt vaak gewerkt met interviews met experts en ook deze bevindingen kunnen eerdere resultaten doen weerklinken. Nieuwe onderzoeksresultaten waarbij andere informatiebronnen gebruikt worden zijn dan ook zeer gewenst.

Daarnaast is er ook sprake van bias bij verschillende onderzoeken, doordat de gegevens over de geldezels (en de netwerken waar zij deel van uitmaken) slechts een selectie zijn van het gehele spectrum. Hierbij kan gedacht worden aan onderzoeken die zich alleen richten op door banken gedetecteerde geldezels, of aan onderzoeken die zich baseren op de

grotere afgeronde cyberzaken. Ook Soudijn (2016) waarschuwt voor vertekening in de resultaten op dit onderzoeksterrein door aan te geven dat het beeld dat op grond van analyses van de dossiers van georganiseerde misdaadzaken is ontstaan een grotere structurele vertekening kent dan de onderzoekers zich bewust van lijken te zijn, doordat de behaalde opsporingsresultaten niet totaalbeelden vormen van de criminele organisaties. Zeker bij sociale netwerkanalyses, die sterk leunen op de kwantificering van persoonscontacten, moet volgens Soudijn (2016) rekening worden gehouden met vertekeningen.

En ten slotte is het een beperking dat alle ontwikkelingen op dit gebied in beweging zijn (zie ook Oerlemans e.a., 2016). Bekkers en collega's (2020) geven aan dat er volgens de Europol cijfers van 2019 met betrekking tot geldezels een stijging is te zien in het ronselen van jongere generaties van 12 tot 21 jaar. Ook de recentere nieuwsberichten lijken de indruk te geven dat de laatste tijd vooral weer jongeren misbruikt worden als geldezels (zie bv. NOS nieuws, 2018; RTL nieuws, 2020; RTV Oost, 2018; Security.nl, 2020). De krantenartikelen en hernieuwde aandacht voor de jongere geldezels van de afgelopen maanden zijn ten dele een gevolg van de resultaten van de laatste jaarrapportage van de politie waarin wordt aangegeven dat vooral bij fraude via internet het aantal verdachten onder de 18 jaar flink is toegenomen (Jaarverantwoording, 2019; van 12% in 2018 naar 29% in 2019). Korpschef Erik Akerboom geeft aan dat hij de cijfers eerst bijna niet geloofde. Het beschikbaar stellen van de bankrekening zou eenvoudiger zijn en meer opbrengen dan bijvoorbeeld een inbraak plegen. Akerboom wenst dat de politie meer preventief op zou kunnen treden (in plaats van repressief). Dit zou echter onder druk staan door de krapte (Algemeen Dagblad, 2020). Ook in andere landen, bijvoorbeeld in Schotland, is meer recent door de autoriteiten gewaarschuwd dat georganiseerde criminele bendes tieners op scholen rekruteren om als geldezel op te treden, vaak via sociale media (Ovaska-Few, 2019). In Nederlandse krantenartikelen en online media zijn eveneens aanwijzingen te vinden dat de werving steeds meer online gebeurt (Eemskrant, 2020; NOS nieuws, 2018), en dat door Corona internetoplichting ook nog verder is geëxplodeerd (RTL nieuws, 2020). Het mag duidelijk zijn: er zijn ontwikkelingen richting de jonge geldezel en er is dan ook een dringende behoefte aan betere preventieprogramma's gericht op deze jonge geldezel die offline, maar ook steeds vaker online geronseld wordt.

Kenmerken van de jonge geldezels

Ondanks de hiervoor besproken beperkingen bieden de beschreven resultaten, wanneer ze worden samengevoegd, een aantal duidelijke kenmerken van geldezels. De onderzoeksresultaten laten zien dat het vaak gaat om jonge mannen woonachtig in de mindere buurten van grotere steden. Over de precieze leeftijdscategorie van de geldezels zijn de bevindingen wisselend: de meeste bronnen duiden erop dat de geldezels vooral worden gevonden in de 18+ leeftijdscategorie (tot 35 jaar), terwijl de leeftijd eerder lager lag (adolescenten). Meer recente berichten wijzen weer nadrukkelijker op de jongere categorie geldezel (zie: Beperkingen). Bij low-tech zaken zouden ook weer de wat jongere geldezels betrokken zijn. Wat wel duidelijk is, is dat de potentiële geldezels zich zowel op online platforms als op straat, op school of in de sportclub laten verleiden door de belofte van 'makkelijk geld'. Kwetsbare groepen jonge mensen zoals jongeren uit multiprobleem gezinnen, met beperkt ouderlijk toezicht, en jongeren met psychische problemen, verslaving,

die dakloos zijn en financiële problemen hebben, zouden nog makkelijker te verleiden zijn door de recruiters.

Over in hoeverre de geldezels zich nu bewust of onbewust zijn van de illegale aard van hun praktijken en als dader of als slachtoffer bezien moeten worden zijn de meningen ook verdeeld. Het is wellicht beter om te spreken van een continuüm met aan het ene uiterste de onbewuste, naïeve geldezels. Een aantal bronnen benadrukt dat geldezels zich veelal onbewust zouden zijn van het feit dat ze criminele netwerken ondersteunen met hun acties. Deze jongeren zouden zich hier pas van bewust worden wanneer zij hierover geïnformeerd worden door de bank en/of politie. Het zou gaan om jongeren die naïef en beïnvloedbaar zijn, of die opkijken tegen recruiters en heel graag bij een groep willen horen. Deze naïviteit kan deels verklaard worden door het onvolgroeide 'puberbrein' (Crone, 2008), waardoor adolescenten en jong volwassenen impulsiever zijn, gericht op directe bevrediging van behoeften en minder nadenken over de lange termijn gevolgen.

Jongeren met een verstandelijke beperking zijn in dit verband ook genoemd als potentieel *easy targets* van recruiters, en dit past wanneer we kijken naar de kenmerken van deze groep zoals naïviteit, beïnvloedbaarheid, en een gerichtheid op korte termijn doelen (in plaats van op de lange termijn gevolgen) (Wissink, Creemers, Moonen, & Stams, 2019).

Wood (2020) gaat zelfs zo ver dat ze stelt dat het rekruteren van jongeren (onder de 18 jaar) om bankrekeningen te gebruiken voor het witwassen van geld een vorm van moderne kinderslavernij of mensenhandel (*trafficking*) is. *Trafficking* vindt dan plaats in de context van gang activiteiten, geweld en illegale drugshandel. Zogenaamde *traffickers* (in dit geval: recruiters) zijn in staat om kwetsbare kinderen (of jongeren) direct of online te observeren en passen *grooming* technieken toe om vertrouwen te verkrijgen. Die tactieken zijn gericht op de vaak onvervulde behoeften van kwetsbare jongeren: ze geven complimenten, waardering, romantiek, liefde, avontuur en een goede toekomst, materiële goederen en cadeaus die status kunnen verlenen en ze een gevoel kunnen geven dat ze zijn verkozen/geselecteerd (hand-picked) en dat ze geaccepteerd worden door een peer groep waar ze graag bij willen horen. Tactieken kunnen er ook op gericht zijn om de jongeren te isoleren van hun bestaande verzorgers, vrienden, steunnetwerken, en om politie en andere mogelijk behulpzame autoriteiten op afstand te houden. Jongeren vanuit liefdevolle 'goede' gezinnen kunnen ook geëxploiteerd worden, maar dan wordt er gebruik gemaakt van de kwetsbaarheid van jongeren als gevolg van hun onvolgroeid brein. In elk geval ziet Wood (2020) de geronselde kinderen (of jongeren) geheel als slachtoffers.

Er zijn in de besproken onderzoeksbevindingen echter ook geldezels beschreven die wel een gevoel hebben dat er iets niet helemaal pluis is, maar die dit vervolgens ontkennen of rationaliseren. Zij gebruiken ook excuses voor het gedrag (zoals de schuld neerleggen bij de benadeelde partij), of instructies voor als ze gepakt worden (door te zeggen dat ze hun pas verloren zijn). Deze geldezels bevinden zich ergens tussen de twee uitersten van het continuüm.

Aan de andere geheel ' bewuste' kant van het continuüm bevinden zich dan nog de geldezels die zich volledig bewust zijn van de illegale praktijken waarmee ze zich bezighouden en zij geven, nadat ze gepakt zijn, ook gewoon toe dat ze het doen voor het geld. Deze geldezels maken vaak deel uit van een straatcultuur waarin offline en online gekoketteerd wordt met geld en een luxe levensstijl en waarin delinquent gedrag genormaliseerd en geïmiteerd wordt. Jonge geldezels worden dan misleid om daarin mee te gaan, soms echter wel onder enige druk vanuit groepsleden tegen wie wordt opgekeken.

Preventie

Idealiter zou je bij een preventieprogramma alle potentiële geldezels (variërend van geheel onbewust tot volledig bewust) willen bereiken. De realiteit is echter dat het zeer lastig zal zijn om te achterhalen op welk punt van het continuüm elke jongere zich precies zal bevinden en hier vervolgens het programma op af te stemmen. Wat bijna alle geldezels echter met elkaar gemeen hebben is dat zij totaal geen weet hebben van de *gevolgen* van het gepakt worden als geldezel: namelijk dat je een strafblad hebt, geen Verklaring Omtrent Gedrag meer kan krijgen, dat banken een register hanteren voor personen die frauduleuze handelingen hebben verricht en dat dat er toe kan leiden dat je bijvoorbeeld geen lening of hypotheek meer kan afsluiten. Preventieprogramma's zouden deze consequenties nog veel meer onder de aandacht moeten brengen, mogelijk met behulp van ervaringsdeskundigen die hun verhaal doen om zo nog beter door te dringen bij de jongere doelgroep. Daarbij zal ook nog eens benadrukt moeten worden dat geldezels echt misbruikt worden door criminele netwerken, en dat er een uitermate hoge pakkans is. Alhoewel eerdere campagnes misschien een kortdurend effect hebben gehad, zijn er nu aanwijzingen dat er weer hernieuwde aandacht voor het onderwerp nodig is (zie tevens: Beperkingen).

Met een dergelijk awareness-programma, gericht op het informeren van jongeren over 1) het feit dat geldezels misbruikt en zeer waarschijnlijk gepakt worden en 2) de lange termijn gevolgen daarvan, kunnen wellicht ook nog enkele meer 'bewust' overtredende geldezels bereikt worden. Houd daarbij ook zoveel mogelijk rekening met de straatcultuur waar jongeren door beïnvloed worden en betrek, voor zover mogelijk, invloedrijke personen op sociale media vanwege hun status en zeggingskracht. In België worden tevens influencers en graffiti kunstenaars ingezet om de jongeren hiervan te doordringen (zie de Febelfin campagne, 2019). Simpel gezegd: verander het geldezel imago van 'stoer' naar 'dom'. Een samenwerking met sociale media platforms wordt daarbij in elk geval aangeraden. Een ander idee voor een onderdeel van een dergelijk bewustwordingsprogramma is het werken met een soort risicotaxatie 'quizje' waarmee aan de hand van enkele simpele vragen elke participant een indruk krijgt van zijn/haar 'geldezelrisicoscore'. De programma's kunnen zich daarnaast richten op het onderuit halen van excuses en neutralisaties, de normalisatie gedachte ('iedereen doet het'; 'het is normaal'), op het leren 'nee' zeggen (omgaan met groepsdruk) en op het benadrukken dat als iets te mooi lijkt om waar te zijn, dat het dan ook vaak niet waar is.

Er zou ook moeten worden nagedacht via welke wegen preventieprogramma's de doelgroep het beste zouden kunnen bereiken. Om een zo groot mogelijke doelgroep te bereiken, en gezien de bevindingen over de leeftijd (adolescenten – jong volwassenen) en het opleidingsniveau (lager) van de geldezels in Nederland, ligt het voor de hand om bijvoorbeeld preventieprogramma's aan te bieden aan jongeren via het middelbaar beroepsonderwijs (MBO). Het is uiteraard aan te bevelen om dergelijke initiatieven zo breed mogelijk (landelijk dekkend) aan te bieden, maar MBO-scholen met veel leerlingen uit de lagere sociaal-economische klassen en de achtergestelde wijken in de grotere steden zullen naar verwachting de meeste potentiële geldezels in huis hebben. Het zal een uitdaging zijn om deze jongeren, die dikwijls deel uitmaken van een gemeenschap waarin de straatcultuur een prominente plek inneemt, op zo'n manier aan te spreken dat het ze weerhoudt van de belofte van 'het snelle geld'.

Ouders zouden hierover echter ook meer geïnformeerd moeten worden en in het algemeen over de risico's waar hun kinderen (online) mee te maken kunnen krijgen, zodat zij hun kinderen beter kunnen waarschuwen en begeleiden (Wissink, 2021). Ouders moeten er met hun kinderen over praten wat eventuele risico's zijn ('*If it's too good to be true*…'). Wanneer de jongeren deelnemen aan een preventieprogramma dan zouden de ouders hier dus ook duidelijk over geïnformeerd, en liefst ook bij betrokken moeten worden. In krantenartikelen doen ouders van gepakte geldezels al oproepen aan andere ouders: '*Praat hier alstublieft over met je kinderen*' (Febelfin, 2019). De teamleider van de *Electronic Crimes Task Force* (ECTF) van de Landelijke Eenheid van de politie gaf ook al aan dat preventie belangrijk is en deed in dat kader een oproep aan de ouders: '*Praat er met uw kinderen over: Krijgen ze een aanbod om snel geld te verdienen? Dat is foute boel, altijd*.' (Eemskrant, 2020; Security.nl, 2020).

Banken zouden welllicht ook bij het bereiken van een bepaalde leeftijd (bv. 12 jaar) kinderen of jongeren kunnen informeren over de risico's (zie ook Galdo, Tait, & Feldman, 2018). Jongeren die op die manier geïnformeerd zijn, kunnen op een later moment minder goed volhouden dat ze van niets wisten. Dit zou samen kunnen gaan met bijvoorbeeld een sticker bij geldautomaten of waarschuwing bij het pinnen.

Ten slotte zou er nog voor gekozen kunnen worden om daarnaast nog een specifiek voorlichtingsprogramma op te zetten voor de meest kwetsbare 'onwetende' groepen (bv. jongeren met een LVB), om hen nog beter te informeren over hoe criminele netwerken functioneren en wat het betekent als je daarin als geldezel bijdraagt. In de 'Richtlijn Effectieve Interventies LVB' geven De Wit, Moonen en Douma (2011) een beschrijving van de kenmerken van jongeren met LVB en zetten ze uiteen hoe op die kenmerken aangesloten kan worden voor het ontwikkelen, aanpassen en uitvoeren van gedragsveranderende interventies voor deze groep. Door de informatie in die richtlijn te verbinden aan wat we nu weten over de kenmerken van geldezels kan een belangrijke aanvullende stap gezet worden naar meer effectieve interventies voor deze doelgroep.

Referenties

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

Aston, M., McCombie, S., Reardon, B., & Watters, P. (2009). A preliminary profiling of internet money mules: An Australian perspective. In: *Ubiquitous, Autonomic and Trusted Computing, 2009. UIC-ATC'09. Symposia and Workshops on* (p. 482-487). IEEE.

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

Chang, Y., Lai, K., Chou, S., & Chen, M. (2017). *Mining the networks of telecommunication fraud groups using Social Network Analysis*. Conference proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Sydney, Australia.

Clarke, R.V. (1997). *Situational crime prevention: Successful case studies* (2nd edition). New York: Harrow and Heston.

Clarke, R.V. (2009). Situational crime prevention: Theoretical background and current practice. In: *Handbook on crime and deviance* (p. 259-276). New York: Springer.

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

Dunham, K. (2006). Money mules: An investigative view. *Information Security Journal: A Gloval Perspective, 15*, 6-10.

Felson, M. (2003). The process of co-offending. In: M.J. Smith & D.B. Cornish (Eds.), *Theory for practice in situational crime prevention, vol. 16* (p. 149-168). Devon: Willan Publishing.

Galdo, M.C., Tait, M.E., & Feldman, L.E. (2018). Money mules: Stopping older adults and others from participating in international crime schemes. *United States Attorneys Bulletin, 66*, 95.

Havenaar, P. (2019). *Kat in 't bakkie: Een gemengd methodeonderzoek naar het profiel van de gedetecteerde katvangers binnen een Nederlandse grootbank* (MA thesis). Amsterdam: Vrije Universiteit.

Holt, J.T., & Lampke, E. (2009). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies, 23*, 33-50.

Hülsse, R. (2017). The money mule: Its discursive construction and the implications. *Vanderbilt Journal of Transnational Law, 50*, 1007-1032.

Jansen, J., Westers, S., Twickler, S., & Slot, W. (2019). *Aankoopfraude vanuit het buitenland: Alternatieven voor opsporing*. Den Haag: Sdu Uitgevers.

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

Kruisbergen, E.W., Leukfeldt, E.R., Kleemans, E.R., & Roks, R.R. (2018). *Georganiseerde criminaliteit en ICT: Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit.* Den Haag: WODC.

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*, 569-581.

Lane, J. (2019). *The digital street.* New York: Oxford University Press.

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

Leukfeldt, E.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*, 173-184.

Leukfeldt, E.R., & Kleemans, E.R. (2019). Cybercrime, money mules and situational crime prevention: Recruitment, motives and involvement mechanisms. In: *Criminal networks and law enforcement* (p. 75-89). Milton Park: Routledge.

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

Leukfeldt, E.R., & Roks, R.A. (2020). Cybercrimes on the streets of the Netherlands? An exploration of the intersection of cybercrimes and street crimes. Deviant Behavior, DOI: 10.1080/01639625.2020.1755587

Mauritz, H.J. (2014). *De aard en omvang van money muling: Fraude met internetbankieren en witwassen.* Onderzoeksrapport.

McCombie, S., Pieprzyk, J., & Watters, P. (2009). *Cybercrime attribution: An eastern European case study*. DOI: https://doi.org/10.4225/75/57b2880840ccf

Meijering, T.J. (2013). *Carding: Crime prevention analysis*. Enschede: Universiteit Twente.

Mikhaylov, A., & Frank, R. (2016). Cards, money and two hacking forums: An analysis of online money laundering schemes. *European Intelligence and Security Informatics Conference* (EISIC), 80-83.

Nederlandse Vereniging van Banken (NVB; 2011). *Factsheet Incidentenwaarschuwings-systeem Financiële Instellingen*.

Odinot, G., Verhoeven, M., Pool, R., & De Poot, C. (2016). *Cyber-OC-Scope and manifestations in selected EU member states*. Den Haag: WODC.

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

Peretti, K. K. (2008). Data breaches: What the underground world of “carding” reveals. *Santa Clara High Technology Law Journal, 25*, 345-414.

Roks, R., & Monshouwer, N. (2020). F-gamers die ‘mapsen’, ‘swipen’ en ‘bonken’: Een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger. *Justitiële Verkenningen, 46*, 44 - 58.

Roks, R.A., & Van den Broek, J.B.A. (2017). #HOUHETSTRAAT: Straatcultuur op social media? *Tijdschrift over Cultuur en Criminaliteit, 7*, 31-50.

Schoenmakers, Y., Bremmers, B., & Van Wijk, A. (2012). *Oosterse teelt: Vietnamezen in de hennepteelt*. Arnhem: Bureau Beke.

Soudijn, M. (2016). *Witwassen: Criminaliteitsbeeldanalyse*. Driebergen: Dienst Landelijke Informatieorganisatie.

Soudijn, M.R.J., & Zegers, B.C.H.T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime, 15*, 111-129.

Stalenberg, F. (2011). *Find out how you can start making 6487 a month at home! Een analyze op katvangers*. Amsterdam: Vrije Universiteit.

Van der Wolf, B. (2014). Onderzoek naar verklaring van money mules: Betrokken bij het witwassen van geld afkomstig van fraude met internetbankieren. Politierapport.

Versprille, I.M. (2016). *De katvanger in beeld: Een onderzoek naar het type katvanger in de wereld van de hennepteelt* (MA thesis). Amsterdam: Vrije Universiteit.

Wissink, I.B. (2021). Jongeren en cybercrime. In: G.J.J.M., Stams, J. Hendriks, & J.J. Asscher (Eds.), *Handboek forensische orthopedagogiek*. Rotterdam: Lemniscaat.

Wissink, I.B., Creemers, H.E., Moonen, X.M.H., & Stams, G.J.J.M. (2019). Sectorstudie Geweld in de residentiele LVB-jeugdsector. In: *Sector- en themastudies: Commissie Onderzoek naar Geweld in de Jeugdzorg* (p. 125-158). Den Haag: Commissie Onderzoek naar Geweld in de Jeugdzorg.

Wood, L.C.N. (2020). Child modern slavery, trafficking and health: A practical review of factors contributing to children's vulnerability and the potential impacts of severe exploitation on health. *BMJ Paediatrics Open* 2020;4:e000327. doi:10.1136/bmjpo-2018-000327

Overige (nieuws)bronnen:

Algemeen Dagblad, 2020: https://www.ad.nl/binnenland/politie-bezorgd-om-criminaliteit-onder-jongeren-voorkomen-dat-nieuwe-taghi-s-opgroeien~a6de1dc3/

Eemskrant, 2020: https://www.eemskrant.nl/politie-en-banken-waarschuwen-jongeren-wordt-geen-geld-ezel/

Febelfin campagne, 2019: https://www.febelfin.be/nl/press-room/1-jongere-op-10-bereid-om-bankrekening-en-bankkaart-uit-te-lenen-ruil-voor-geld

Jaarverantwoording, 2019: https://www.politie.nl/binaries/content/assets/politie/nieuws/2020/00-km/jaarverantwoording-politie-2019-incl-accountantsverklaring.pdf

NOS nieuws, 2018: https://nos.nl/artikel/2248735-politie-waarschuwt-voor-ronselaars-op-instagram-en-telegram.html

RTL nieuws, 2020: https://www.rtlnieuws.nl/tech/artikel/5159956/cybercrime-fraude-corona-misdaad-inbraak-zakkenrollen-politie en https://www.rtlnieuws.nl/nieuws/nederland/artikel/4986241/fraude-online-handel-cybercrime-misdaadcijfers-politie

RTV Oost, 2018: https://www.rtvoost.nl/nieuws/290883/Jeugdige-criminelen-ronselen-jongeren-op-scholen-voor-illegale-handel-in-hennep

Security.nl, 2020: https://www.security.nl/posting/680334/Politie%3A+probleem+met+katvangers+blijft+zorgelijk

Overzichtstabel 1.

Jr.	Auteurs (NL/BL)	Titel	Tijdschrift/ bron	Gegevens	Bevindingen kenmerken	Bevindingen preventie
Nederlandse studies						
'12	Soudijn & Zegers	Cybercrime and virtual offender convergence settings	*Trends in Organized Crime*, 15, 111-129.	Kwalitatieve tekstuele analyse van forum berichten (2003 – 2008; *N* = 153.936 posts en *N* = 60.437 priveberichten => ideaal crime script	-Geldezels zijn misleid bij de werving (via emails) met aantrekkelijk baanaanbod	-Alert maken van potentiele geldezels -Undercover geldezels inzetten
'13	Meijering	Carding; Crime prevention analysis	Universiteit Twente (bachelor thesis); Politie	Kwalitatieve en kwantitatieve analyse van wetenschappelijke literatuur, NHTCU rapporten, online nieuwsartikelen over carding processen (over phishing *n* = 13; of skimming *n* = 25; 2004-2011); diepteinterview met NHTCU expert (*N* = 1)	-Geldezels zijn zich onbewust van de illegale aard van het 'snelle' geld dat ze kunnen verdienen (aangeboden via advertenties)	-Bewust maken van potentiele geldezels - Moeilijker maken van optreden als geldezel - Risico's van het optreden als geldezel vergroten - Excuses voor het optreden als geldezel onderuit halen
'14	Leukfeldt	Cybercrime and social ties: Phishing in Amsterdam	*Trends in Organized Crime*, 17, 231-249.	Casestudy van Amsterdamse phishing zaak (2012-2013); verhoren, transcripten van telefoontaps, internetverkeer, en surveillance rapporten); Interviews met de openbaar aanklager, de leider van het politieteam en een financiële expert van het onderzoeksteam (*N* = 3).	-Jonge mensen -Snel geld -Misleid, maar ook geïnstrueerd -Uit sociale netwerken/ omgeving van recruiters/ andere geldezels -Deel bewust -Verzoeken zijn 'normaal'	-Mogelijk bewustzijns-campagne onwetende geldezels (meer info over motieven nodig) -Mogelijk berechting van geldezels -Sociale banden in netwerken -Technologische maatregelen gericht op forums

'15	Leukfeldt & Jansen	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, 173-184.	Kwantitatieve analyse van gegevens van een fraude registratie database van een Nederlandse bank (*N* = 600 fraude incidenten; 2011-2013).	-Geldezels in NL vooral bij low-tech zaken (waarmee meer geld werd verdiend door de geldezels) -Mannelijk geslacht -Low-tech: 56% < 25 jr (bij high-tech 29%) -Uit bestaande sociale netwerken (scholen/ sportclubs)	
'15	Arevalo	Money mules: Facilitators of financial crime	Universiteit Utrecht (master thesis)	Secundaire analyse van voorgaand onderzoek, semi-gestructureerde interviews met cybercrime experts (uit het bankwezen, financiele politie rechercheurs, aanklager, onderzoeker *N* = 11; 6 geldezel casussen (*N* = 6; 1 geldezel interview en 5 geldezel verhalen via 2 Nederlandse forums en in tv programma via etnografisch onderzoek).	-In NL worden geldezels het meeste face-to-face binnen eigen netwerk/ omgeving gerekruteerd (bij phishing vs malware) -Soms onbewust van de illegale aard -Vaak misleid met belofte van geld -Lagere SES -In NL eerder adolescenten maar rond 2015 steeds vaker 18-35jr -Ontkenning/ rationaliseren/ goedpraten van illegaliteit -Uit netwerken die delinquentie niet veroordeelden -Makkelijk over te halen met snel geld of 'zielige' verhalen -Loverboys achtige praktijken (meisjes) -Dom/zwak -Naïef en onbewust (bij online werving) -Adolescenten die deel van groep willen uitmaken -Mentaal beperkt/ lagere opleiding/ lagere intelligentie -Mensen met geldproblemen -Mannen uit de mindere buurten in de grotere steden -Gericht op korte termijn doelen	

‘16	Oerlemans	Cybercrime en witwassen: Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware.	Boom Criminologie; WODC	Deskresearch (literatuur en mediaberichten over cybercrime, witwassen en digitale betalingsmiddelen); interviews bij experts (*N* = 20); dossieronderzoek van cybercrime en witwaszaken van het High Tech Crime Team van de Nationale Politie (*N* = 4); experiment met bitcoins; kwantitatieve analyse van banking malware en phishing transactiegegevens van Nederlandse banken.	-Meestal op straat geronseld en bewust -Deel ook onbewust -Door heel NL, meesten in armere buurten in grootste gemeenten -66% mannelijk geslacht -Sterke piek 18-22 jr -Oost-Europese achtergrond -Meeste geldezels hebben geen antecedenten -4 groepen: 1) grootste groep 21jr zonder antecendenten; 2) 20jr groep met 1/ 2 antecedenten; 3) groep met 4-8 antecedenten vanaf 15jr; 4) veelpleger groep vanaf 15jr	
‘16	Versprille	De katvanger in beeld: Een onderzoek naar het type katvanger in de wereld van de hennepteelt.	Vrije Universiteit Amsterdam (Master thesis)	Interviews met betrokken actoren in het veld en de aanpak en preventie van illegale hennepteelt (*N* = 18; gemeentelijke coördinator bestuurlijke aanpak hennepteelt, gemeentelijke juridisch beleidsmedewerker, politie, woonconsulenten woningcorporatie, financiers van betaalrekeningen en/of hypotheken, netbeheerders).	-Katvangers bij hennepteelt zijn bewust volgens geïnterviewden -Ook naïviteit (wegkijken?) -Lagere SES -Financiële problemen -Werkloosheid -Beïnvloedbaar -Laag IQ/LVB -Verslaving -Geen sociaal netwerk/controle -Criminele circuits -Echtscheiding -Mannen -30-50jr -Etniciteit -Geldmotief -Binnen eigen netwerken gerekruteerd	-Bewustwording en kennisvergroting over diverse rollen en gevolgen (en risico’s); liefst al op de basisschool

‘16	Odinot, Verhoeven, Pool, & De Poot	Cyber-OC: Scope and manifestations in selected EU member states.	WODC (i.s.m. Bundeskriminalamt & Swedish National Council for Crime Prevention; European Commission)	Analyse van 11 afgeronde cybercrime politiezaken (*N* = 11; volgens methode van de National Organised Crime Monitor; 2009-2014; in totaal 107 verdachten) met gegevens over de feiten, verdachten, politieonderzoek en gebruikte methoden, verhoren, getuigenissen, communicatietaps en observaties; 12 semi-gestructureerde interviews met aanklager, rechercheurs, vertegenwoordigers van Electronic Crimes Task Force en Europol (*N* = 12).	-Geldmotief -Geldezels waren soms totaal onbekenden (maar werden op straat gevonden), maar soms ook nauw gerelateerd aan recruiters -Soms onbewust van illegaliteit -Kwetsbaar -Moeilijke sociale omstandigheden -Verslaving	-Adequate informatie-verstrekking (bv. via Nederlandse banken)
‘17	Leukfeldt, Kleemans, & Stol	A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists.	*Crime, Law and Social Change*, 67, 21-37.	Analyse van 18 afgeronde Nederlandse politieonderzoeken naar phishing en banking malware netwerken (2004 – 2014; telefoon- en internetverkeer, observaties, undercover politiewerk en huiszoekingen; *N* = 18); Interviews met de aanklager, teamleider van de politie, senior rechercheurs (financiële of digitale experts).	-Binnen woongebied -Binnen sociale netwerk -Jonge mensen -Snel geld -Verslaafden -‘Iedereen doet het’ (normalisering) -Binnen etnische gemeenschap -Geldezels bieden zichzelf aan	

‘18	Kruisbergen, Leukfeldt, Kleemans, & Roks	Georganiseerde criminaliteit en ICT: Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit.	WODC (i.s.m. Erasmus Universiteit, Vrije Universiteit, NSCR).	Analyse van 30 afgeronde opsporingsonderzoeken op het terrein van de georganiseerde criminaliteit (*N* = 30 volledige opsporingsdossiers); Interviews met zaaksofficieren en/of teamleiders (vijf zaken overlap met Odinot en collega’s).	-Binnen sociale netwerken van de kernleden/ facilitators -Zowel offline als online contacten -Sneeuwbal- Methode -Beïnvloedbaar: schulden, psychische problemen, drugsverslaving	
‘19	Leukfeldt & Kleemans	Cybercrime, money mules and situational crime prevention.	Hoofdstuk in *Criminal networks and law enforcement: Global perspectives on illegal enterprise* (p. 75-89), Hufnagel & Moiseienko (2019). London: Routledge.	Analyse van 14 criminele onderzoeken naar cybercriminele netwerken (2004-2014), waaronder verhoren van 112 geldezels (*N* = 112).	-Beperkte financiële middelen -Snel geld -Meerdere keren benaderd -Rekrutering via bestaande sociale contacten en mails -Deel bewust (makkelijk geld en subcultuur van het etaleren van luxe levensstijl en acceptatie van delinquentie en toegeven aan druk) -Deel met excuus (onbewust/ geen echte slachtoffers / schuld bij slachtoffer) -Jongeren en verslaafden -Geldezels zijn in zekere zin ook slachtoffers	-Peer pressure en imitatie verminderen -Bewustmaking van potentiele geldezels: haal excuses onderuit, benadruk dat wordt samengewerkt met criminelen die geld stelen van onschuldige mensen, en dat de geldezels misbruikt worden

‘19	Jansen, Westers, Twickler, & Stol	Aankoopfraude vanuit het buitenland: Alternatieven voor opsporing.	Sdu Uitgevers (i.s.m. Politie & Wetenschap; NHL Stenden Hogeschool / Politieacademie).	Analyse van 150 meldingen van het Landelijk Meldpunt Internetoplichting (LMIO) (*N* = 150); 20 semigestructureerde interviews met slachtoffers (*N* = 20); interviews met experts (*N* = 16); klankbordgroep brainstormsessie; deskresearch juridische kader.		-Neutraliseren van groepsdruk (peer pressure) -Betere voorlichting van potentiele geldezels (over gevolgen van medeplichtig-heid) -Geldezels moeten het idee krijgen dat banken en politie ze in de gaten heeft -Knock&talk acties -Pakkans verhogen (banken/ politie/ overheid)
‘19	Havenaar	Kat in ’t bakkie: Een gemengd methodeonderzoek naar het profiel van de gedetecteerde katvangers binnen een Nederlandse grootbank.	Vrije Universiteit van Amsterdam (master thesis).	Literatuuronderzoek; Kwantitatieve analyse van gegevensbestand over door de bank gedetecteerde katvangers (N = 1308; 2018); semigestructureerde interviews met 2 medewerkers veiligheidszaken, een medewerker van de informatiebeveiligingsafdeling, de teamleider van het cybercrime team van de politie Amsterdam en de teamleider Electronic Crimes Task Force (ECTF).	-Mannen (en vrouwen) -Jong (27.9jr); meer dan 1/3 18-25jr -Verschuiving naar jongeren door gebruik van sociale media door recruiters -Grote steden -NL nationaliteit -Meeste bij online handelsplaats-fraude -Korte klantrelatie -Weinig financiële draagkracht -Naïef -Vaak onbewust van participatie in criminele netwerk -Niet nadenken over de lange termijn gevolgen	-Langdurige en herhalende bewustmakende acties gericht op de jongeren doelgroep en in samenwerking met sociale media platformen (Telegram, Instagram en Snapchat)

'19	Kruisbergen, Leukfeldt, Kleemans, & Roks	Money talks money laundering choices of organized crime offenders in a digital age	*Journal of Crime and Justice*, 42, 569-581.	Analyse van 30 afgeronde opsporingsonderzoeken op het terrein van de georganiseerde criminaliteit (*N* = 30 volledige opsporingsdossiers; vijfde ronde van de Dutch Organized Crime Monitor; DOCM); (vijf zaken overlap met Odinot en collega's).	-Beïnvloedbaar: jonge mensen met schulden, psychologische problemen of drugsverslaving -Gerekruteerd in lokale nabijheid	
'20	Roks & Monshouwer	F-gamers die 'mapsen', 'swipen' en 'bonken': Een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger	*Justitiële Verkenningen*, 46, 44-58.	Kwalitatieve analyse van Telegram berichten in vijf groepen (variërend in ledenaantal van 134 tot 3239 leden; meer dan 1650 screenshots) over phishing (april t/m juli 2019).	-Voorkeur voor 18+ of zakelijke kaarten (vanwege opnamelimiet) -Rekrutering verplaatst zich naar digitale omgeving (Telegram) -Inbedding in straatcultuur	
'20	Leukfeldt & Roks	Cybercrime on the streets of the Netherlands? An exploration of the intersection of cybercrimes and street crimes.	*Deviant Behavior*, DOI: 10.1080/01639625.2020.1755587	Analyse van 14 afgeronde Nederlandse politieonderzoeken naar criminele netwerken die cybercrimes pleegden (2004 – 2014; telefoon- en internetverkeer, observaties, undercover politiewerk en huiszoekingen; *N* = 14); Interviews met de aanklager, teamleider van de politie, senior rechercheurs (financiële of digitale experts) (overlap met Leukfeldt, Kleemans, & Stol, 2017 en Leukfeldt & Kleemans, 2019).	-Zowel offline als online rekrutering -Kwetsbaar -Jongeren -Achtergestelde buurten -Overgehaald met makkelijk geld belofte -Jongeren die opkijken tegen recruiters met geld -Normaliteit -Inbedding in straatcultuur	

‘20	Bekkers, Schiks, & Leukfeldt	Naar een interventie tegen geldezels: Een pilot inde gemeente Haarlem	Saxion Hogeschool (i.s.m. Centre of Expertise Cybersecurity; Gemeente Haarlem)	Literatuuronderzoek; 10 expertinterviews (3 politiemedewerkers, 2 jeugdwerkers, 1 HALT-, OM-, reclassering-, bankmedewerker en LVB-jeugdspecialist)	-Diversiteit -Jongeren/jong-volwassenen -Jongens -Vooral lager opgeleiden (makkelijker te misleiden en beperkt ouderlijk toezicht) -Lage SES (minder toezicht) -Deels 1st offenders -Graag erbij willen horen -Gevoelig voor ‘snel geld’ -Rapcultuur/ imago -LVB (beïnvloedbaar, weinig perspectief, netwerk) -Arme gezinnen/ wijken -Instabiele thuissituatie -Nieuwe Nederlanders	-Interventie op therapeutische basis is effectiever dan toezicht en sancties - Verminderen van provocaties voor crimineel gedrag - Verminderen van excuses (geldezels bewust maken van strafbaarheid)

Buitenlandse studies						
'16	Mikhaylov & Frank	Cards, money and two hacking forums: An analysis of online money laundering schemes.	European Intelligence and Security Informatics Conference.	Analyse van gegevens van 2 Russisch-gesproken online carding en hacking forums (met 1.530.404 en 468.827 posts). Convenience sample van 420 posts van beide forums (*N* = 840).	-Kwetsbare sociale groepen (armen, daklozen en drugsverslaafden) -Makkelijk geld als lokmiddel -Onwetendheid -Gebrek aan kennis van het financiële systeem -Gebrek aan zorgen over herkomst van geld	
'17	Chang, Lai, Chou, & Chen	Mining the networks of telecommunication fraud groups using social network analysis.	International Conference on Advances in Social Networks Analysis and Mining.	Analyse van een telecom fraude dataset met 113 leden (gearresteerd in Taiwan) uit 4 landen en 17 steden (voornamelijk in Zuidoost Azië) op basis van politie rapportages.	-Meestal tieners	
'17	Hülsse	The money mule: Its discursive construction and the implications.	*Vanderbilt Journal of Transnational Law*, 50, 1007-1032.	Analyse van de discourse van de geldezel in documenten van nationale en internationale anti-witwas autoriteiten (gericht op de narratieven, visualisaties, metaforen; 2005 – 2017; Westerse landen zoals Zwitserland en Duitsland en Westerse internationale organisaties zoals Europol of de Financial Action Task Force).	Geportretteerd als: -Jong -Mannelijk -Westerse achtergrond -Graag extra inkomen -Student/ leerling -Misleiding -Onbewust -18-34jr (Europol) -Aanwijzingen dat geldezels niet meer zo naïef zijn	

Opm. Jr. = publicatiejaar.