De samenwerking omtrent VIN-fraude

Daan Meijerink
Denis Damoiseaux
Jan Berendsen
Julia Prins
Maureen Kluitman
Michelle de Roo
Roos Kerssenberg
Shanna Grift

Apeldoorn, juni 2022

Informatiepagina

Persoonlijke gegevens

Naam	Klas	Studentnummer	E-mail	Telefoonnummer
Daan Meijerink	DUS2V.E	482811	482811@student.saxion.nl	+31 6 33799626
Denis Damoiseaux	DUS2V.A	476320	476320@student.saxion.nl	+31 6 83057499
Jan Berendsen	DUS2V.A	465868	465868@student.saxion.nl	+31 6 57264834
Julia Prins	DIV3V.B	467463	467463@student.saxion.nl	+31 6 13436276
Maureen Kluitman	DUS2V.E	500970	500970@student.saxion.nl	+31 6 36506964
Michelle de Roo	DIV3V.A	480925	480925@student.saxion.nl	+31 6 25264234
Roos Kerssenberg	DUS2V.A	498530	498530@student.saxion.nl	+31 6 28662907
Shanna Grift	DIV3V.B	482264	482264@student.saxion.nl	+31 6 21377251

Opleiding	Integrale Veiligheidskunde Bestuurskunde
Onderwijsinstelling	Saxion Hogeschool (Deventer)

Gegevens schoolcoach Integrale Veiligheidskunde

Naam	Lisan van Bolhuis
E-mailadres	l.vanbolhuis@saxion.nl
Telefoonnummer	+31 6 30333596

Gegevens schoolcoach Bestuurskunde

Naam	Joost Nijrees
E-mailadres	j.j.nijrees@saxion.nl
Telefoonnummer	+31 880191846

Gegevens praktijkcoach

Naam	Sjoerd Obbink
Functie	Teamchef basisteam Apeldoorn
E-mail	Sjoerd.obbink@politie.nl
Telefoonnummer	+31 6 53770725
Organisatie	Politie Oost-Nederland
Afdeling	Basisteam Apeldoorn

Technische gegevens

Periode van onderzoek	7 februari – 22 juni 2022
Plaats	Apeldoorn

Voorwoord

Voor u ligt een adviesrapport over de verschuiving van fysieke naar digitale criminaliteit – verwachtingen aan de politie. Onder begeleiding van de politie Apeldoorn hebben wij ons, in de periode van 7 februari tot en met 22 juni 2022, beziggehouden met dit onderzoek. In opdracht van de politie Apeldoorn en in het kader van onze studies Integrale Veiligheidskunde en Bestuurskunde is dit adviesrapport geschreven.

Graag willen wij onze opdrachtgever van politie Apeldoorn, Sjoerd Obbink, bedanken voor de totstandkoming van dit adviesrapport. Sjoerd Obbink is de opdrachtgever vanuit de politie Oost-Nederland, gevestigd in het basisteam van Apeldoorn. Ook willen wij onze begeleiders vanuit Saxion, Lisan van Bolhuis en Joost Nijrees, bedanken voor de prettige begeleiding. Verder willen wij de respondenten bedanken die mee hebben gewerkt aan dit onderzoek. Zonder hun medewerking hadden we dit onderzoek niet kunnen voltooien.

Veel leesplezier gewenst.

Daan Meijerink, Denis Damoiseaux, Jan Berendsen, Julia Prins, Maureen Kluitman, Michelle de Roo, Roos Kerssenberg en Shanna Grift
Apeldoorn, juni 2022

Samenvatting

Dit adviesrapport is opgesteld op aanvraag van Sjoerd Obbink, tevens opdrachtgever van dit onderzoek. Cybercriminaliteit blijkt over het algemeen steeds meer greep te krijgen op de maatschappij. Om die reden wilt de politie graag weten wat voor invloed de politieorganisatie hierop heeft en wat een burger van de lokale politieorganisatie mag en kan verwachten met betrekking tot dit veiligheidsvraagstuk. In dit onderzoek wordt er gefocust op het fenomeen VIN-fraude. De hoofdvraag van dit onderzoek luidt: "**In hoeverre werken de ketenpartners van de politie samen op het gebied van VIN-fraude en wie draagt welke verantwoordelijkheid?"**
Om de hoofdvraag te kunnen beantwoorden zijn de volgende deelvragen opgesteld:

Deelvraag 1: Wat is de huidige situatie rondom de verschuiving van fysieke naar digitale criminaliteit?
Ten opzichte van 2019 zag de politie een ruime verdubbeling van het aantal geregistreerde digitale misdrijven (Sabel, 2021). Er is een duidelijke verschuiving van fysieke criminaliteit naar digitale criminaliteit (CBS, 2022). Door alle respondenten wordt aangegeven dat de traditionele criminaliteit al jaren afneemt en de digitale criminaliteit alleen maar toeneemt.

- *Deelvraag 1.1: Op welke manier heeft de coronacrisis hier invloed op gehad?*

De coronacrisis heeft de toename van digitale criminaliteit versterkt. "De criminaliteit bewoog mee met wat er gebeurde: iedereen was thuis, dus criminelen gingen op zoek naar andere methodes" (BNNVARA, 2022). De respondent van de politie (projectleider cybercrimeteam) benoemt dat tijdens de coronacrisis de VIN-fraude steeg. Er ontstond een nieuwe dynamiek.

Deelvraag 2: Welke actoren zijn in het kader van VIN-fraude van belang, hoe zien zij de verschuiving van criminaliteit en welke verantwoordelijkheid dragen zij daarin?
Banken spelen een grote rol in het online betaalverkeer en hebben daarom veel met WhatsApp-fraude, helpdeskfraude, *spoofing* en andere vormen van online fraude en oplichting te maken. Zowel de slachtoffers als de daders regelen hun geldzaken via deze banken. De politie heeft de toename van digitale criminaliteit in de afgelopen jaren waargenomen en investeert tijd, geld en personeel in de aanpak daarvan. Ook adviseert de politie andere actoren hetzelfde te doen (Betaalvereniging Nederland, 2021). WhatsApp heeft 12,5 miljoen gebruikers in Nederland (Oosterveer, 2022). Dit maakt WhatsApp erg aantrekkelijk voor criminelen. Door de pandemie is deze vorm van fraude sterk toegenomen. De gemeente speelt een rol bij het informeren van burgers en probeert online fraude tegen te gaan door middel van informeren via webinars, filmpjes en presentaties. Een andere taak die de gemeente uitvoert, is slachtoffers doorverwijzen naar relevante actoren zoals de bank, politie en de Fraudehelpdesk (Gemeente Lelystad, 2022). Het primaire doel van het Nationaal Cyber Security Centrum (NCSC) is om de digitale infrastructuur te beschermen en te verbeteren. Het NCSC houdt zich dus meer bezig met cybercriminelen die banden hebben met statelijke actoren uit of namens andere landen (Nationaal Cyber Security Centrum, 2021). Het Openbaar Ministerie (OM) is actief bezig met de aanpak van cybercrime. In samenwerking met diverse partijen, waaronder politie, wetenschappers en ethische hackers, worden de daders zoveel mogelijk opgespoord en vervolgd. Deze samenwerking leidt niet alleen tot meer opsporing, maar ook tot betere digitale beveiliging (computers en andere *devices*). Volgens het Ministerie van Justitie en Veiligheid is het aan de overheid om kwetsbare groepen te categoriseren. Online fraude moet bestreden worden door middel van bewustwording, preventie, interventies, barrières en handelingsperspectief voor slachtoffers. Het is belangrijk duidelijkheid te bieden aan slachtoffers over hoe zij schade kunnen verhalen (Tweede Kamer der Staten-Generaal, 2021).

Overig aangemerkte actoren vanuit de geïnterviewden:
Als laatste wordt het Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) door de VNG aangemerkt als belangrijke actor in de samenwerking tegen VIN-fraude. Echter zagen zij zichzelf niet als ketenpartner en is omtrent deze organisatie geen verder interview gehouden of verdere informatie verzameld.

- *Deelvraag 2.1: Wat zijn de verwachtingen van de inwoners van Nederland aan de overheid op het gebied van VIN-fraude?*

Uit een onderzoek blijkt dat de verwachtingen van de inwoners uit Nederland op het gebied van VIN-fraude bij de overheid liggen. De overheid zou meer aan preventie moeten doen. 26 procent van de respondenten die meededen aan een onderzoek dat ging over in welke mate je met online fraude te maken had, geeft aan dat ze meer informatie hadden moeten opzoeken. Twee procent geeft aan dat ze alerter hadden moeten zijn (Junger et al., 2022).

- *Deelvraag 2.2: Hoe verloopt de huidige samenwerking tussen de ketenpartners?*

Vanuit de interviews is duidelijk geworden dat de huidige samenwerking met de ketenpartners van de politie omtrent VIN-fraude gericht is op informatiewisseling. In de praktijk verloopt dit moeizaam, het delen van informatie wordt moeilijk gemaakt door de geldende privacyregels en AVG. Tevens speelt er ook een kennistekort binnen de politieorganisatie maar ook bij de actoren.

<u>Deelvraag 3: Welke vormen van VIN-fraude bestaan er en wat zijn de gevolgen voor de betrokken actoren?</u>
VIN-fraude zou geschaald kunnen worden onder de digitale criminaliteitsvorm '*spoofing*'. Bij *spoofing* nemen internetcriminelen een identiteit over. Als zogenaamde bekende of erkende afzender probeert de cybercrimineel achter je persoonsgegevens of je pincode te komen, *malware* op je computer te plaatsen of je direct geld afhandig te maken (Veilig internetten, z.d.). Een andere vorm dat officieel niet onder VIN-fraude wordt aangeduid maar er wel mee te maken heeft, is het werven van '*money mules*'. Bij het witwassen van crimineel geld wordt binnen de georganiseerde criminaliteit, met name binnen cybercriminaliteit, dikwijls gebruik gemaakt van deze *money mules.* Door het ter beschikking stellen van een bankrekening en/of pinpas aan criminelen, fungeert de *money mule* als dekmantel voor misdadige organisaties (Versprille, 2016).

<u>Deelvraag 4: Welke aanpak bestaat er omtrent VIN-fraude en welke kansen zijn er voor de politie en ketenpartners in de toekomst omtrent deze aanpak?</u>
De geïnterviewden van de politie vertellen over een redelijk nieuwe implementatie in de aanpak, waarbij er direct online aangifte kan worden gedaan nadat het slachtoffer is opgelicht. Van de online aangiftes worden de bankrekeningnummers, berichten en telefoonnummers gecategoriseerd en waar mogelijk aan elkaar gekoppeld, om hiermee dichter bij de dader te komen.

De meerderheid van de geïnterviewden, geven aan dat er een betere informatiewisseling tussen de betrokken partners moet komen. Vanuit de geïnterviewden van de politie is het duidelijk naar voren gekomen dat er een wens ligt voor grensoverschrijdende samenwerkingen. Dit komt door het verschil in slachtoffer- en daderplaats. Hier zit er voor de politie dus (naast de interventiespecialist, gebundelde aangiftes) nog een kans. Over het algemeen gaven de banken aan dat contact tussen bijvoorbeeld Whatsapp en Snapchat kan helpen in de aanpak. De platformen waar VIN-fraude zich dus op afspeelt. Hier zit een kans voor de politie om met de data van social media platforms criminelen makkelijker op te sporen.

Aan de preventiekant liggen er ook kansen. Bijvoorbeeld door aan mogelijke slachtoffers te communiceren hoe zij vormen van digitale criminaliteit eerder kunnen herkennen.

Conclusie

De hoofdvraag: **"In hoeverre werken de ketenpartners van de politie met hen samen op het gebied van VIN-fraude en wie draagt welke verantwoordelijkheid?"** is in de conclusie als volgt beantwoord. Op het gebied van VIN-fraude en andere online fraudevormen is er een samenwerking actief tussen de politie en haar ketenpartners. Om deze fraudevorm toch zo goed mogelijk tegen te gaan hebben vele ketenpartners contact met elkaar en proberen zij elkaar van informatie te voorzien. Het is gebleken dat informatie met elkaar te delen moeizaam gaat door de geldende privacywetgeving zoals de AVG waar deze organisaties aan gebonden zitten. De overdracht van informatie wordt hierdoor vertraagd. De verantwoordelijkheid van de ketenpartners zijn uiteenlopend, passend bij de organisatie en functie.

Aanbevelingen

Voor de aanbeveling is het zaak om te kijken naar de kansen voor de politie (tevens de opdrachtgever) en de samenwerking tussen haar ketenpartners. Een kans om cybercriminaliteit zo goed mogelijk tegen te gaan is door de samenwerkingsstructuur te vernieuwen. Momenteel worstelt de politie met welk veiligheidsgebied welke zaak oppakt. Vanuit de vroegere traditionele criminaliteit is de politie gewend de fysieke zaken op te pakken die in hun eigen gebied plaatsvinden. Doordat cybercriminaliteit grensoverschrijdend is (de daderplaats en slachtofferplaats is vaak verschillend), is het onduidelijk wie de zaak oppakt. Om deze verwarring te voorkomen zou het waardevol zijn als er landelijke teams ingericht worden (Politie, persoonlijke communicatie, 5 april 2022). Daarbij heeft de politie de behoefte om in elke eenheid een interventiespecialist toe te voegen, wiens werk gericht is op deze digitale fraudes. Daarnaast is het raadzaam om meer te investeren aan de voorkant. Het is waardevol om meer samenwerking te zoeken met partners om tot een beter preventiepakket te komen (Politie, persoonlijke communicatie, 11 mei).

Ook de ketenpartners zelf zien verbeterpunten. De ABN Amro wil graag een betere samenwerking met banken onderling en willen dat overheidsinstellingen sneller informatie delen. De ING en Rabobank hebben behoefte aan ingangen bij WhatsApp en Snapchat. Het Openbaar Ministerie kan en wil nog meer uit hun samenwerkingsverband (HUB) halen en dit verder doorvoeren binnen de politie. Voor alle gemeentes en de VNG is het zaak nog meer te investeren in de preventieve kant van cybercrime.

Een samenwerking die nog niet tot stand is gekomen, maar wel gewenst is, is die met social mediabedrijven zoals WhatsApp, Instagram en Snapchat en met telefoonproviders. Zij zouden meer verantwoordelijkheid op zich mogen nemen en daarom is het van belang een actieve samenwerking met deze partijen op te zoeken.

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

In de afgelopen jaren is het type criminaliteit waar Nederlanders mee te maken krijgen steeds vaker veranderd. Van traditionele criminaliteit zoals inbraken, geweld, en vernieling naar digitale criminaliteit zoals online aan- en verkoopfraude, identiteitsfraude en hacken (Centraal Bureau voor de Statistiek, 2022b). Deze trend is relevant voor dit onderzoek omdat er in kaart wordt gebracht wat de huidige situatie is rondom de verschuiving van fysieke naar digitale criminaliteit.

Cybercriminaliteit blijkt steeds meer greep te krijgen op onze maatschappij. Daarom wil de politie graag weten wat voor invloed ze hierop heeft en wat een burger van de lokale politieorganisatie mag en kan verwachten met betrekking tot dit veiligheidsvraagstuk. Dit veiligheidsvraagstuk is complex omdat het te maken heeft met het web dat wereldwijd is. Ondanks dit wereldwijde web, voelen slachtoffers zich even onveilig bij cybercrime als wanneer er ingebroken wordt, zelfs wanneer de oplichter zich mogelijk in een ander land bevindt (Leukfeldt et al., 2019). Daarnaast brengt deze verschuiving een nieuw vraagstuk met zich mee: wie is er verantwoordelijk voor de aanpak van deze vorm van cybercriminaliteit?

Het doel van dit onderzoek is: inzicht krijgen in wie betrokken is bij VIN-fraude, wie welke verantwoordelijk draagt voor de aanpak en hoe de samenwerking is onder de desbetreffende actoren.

Hieruit komt een advies over deze samenwerking, met inbegrip van de inzichtelijkheid bij de VIN-fraude en het verantwoordelijkheidsvraagstuk. Dit advies focust zich op het landelijke aspect van de VIN-fraude.

Dit onderzoek is praktisch relevant omdat op basis van de resultaten die hieruit naar voren komen verbeteringen doorgevoerd kunnen worden. Hiermee kunnen de ketenpartners van de politie op het gebied van VIN-fraude beter samenwerken, waardoor VIN-fraude eerder gesignaleerd en mogelijk voorkomen zou kunnen worden. Ook is het onderzoek wetenschappelijk relevant. Op basis hiervan kunnen conclusies getrokken worden over de validiteit van de resultaten van eerdere onderzoeken over VIN-fraude.

1.1.1 Situatiebeschrijving

De verschuiving van fysieke naar digitale criminaliteit is een trend die zich zowel landelijk als lokaal flink doorzet. Een bekende vorm van digitale criminaliteit is ‘Vriend-In-Noodfraude’ (VIN-fraude). Hierbij wordt identiteitsfraude gepleegd door WhatsApp berichten te versturen naar onbekende mensen (waarbij de bedriegers zich voordoen als een bekende) met de vraag of men een bedrag wil overmaken omdat de ‘vriend’ van de slachtoffers in geldnood zit.

Het kenmerkende is dat er nieuwe technieken van criminaliteit worden gebruikt door de technologische vooruitgang. Bij deze nieuwe digitale vorm van fraude zijn er ook nieuwe vragen, zoals: “wat is de categorie van dader en het slachtoffer en wat is de schade die wordt aangericht?”

Omdat deze nieuwe vorm van criminaliteit zich ook op lokaal niveau bewerkstelligt, is het lastig om erachter te komen wie de meeste verantwoordelijkheid draagt bij de aanpak van het probleem. Dit komt ook door de verschillende actoren die hierbij betrokken zijn. Verder is het moeilijk te vinden wie aansprakelijk is voor digitale criminaliteit, omdat het internet vanuit elke locatie te bereiken is en deze daders, daardoor, ook moeilijk op te sporen zijn. Hierdoor kunnen onder andere daders zich ook vaak in het buitenland schuilhouden.

1.2 Doelstelling

Het doel van dit onderzoek is om inzicht te krijgen in hoe ketenpartners en medewerkers van de politie Apeldoorn de verschuiving van fysieke criminaliteit naar digitale criminaliteit ervaren. Er wordt onderzocht wat de ideale samenwerking is van de betrokken ketenpartners op het gebied van VIN-fraude en welke verantwoordelijkheid zij nemen in de aanpak tegen deze fraudevorm.

1.3 Onderzoeksvragen

1.3.1 Hoofdvraag

In hoeverre werken de ketenpartners van de politie met hen samen op het gebied van VIN-fraude en wie draagt welke verantwoordelijkheid?

1.3.2 Deelvragen

1. Wat is de huidige situatie rondom de verschuiving van fysieke naar digitale criminaliteit?
    - Op welke manier heeft de coronacrisis hier invloed op gehad?
2. Welke actoren zijn in het kader van VIN-fraude van belang, hoe zien zij de verschuiving van criminaliteit en welke verantwoordelijkheid dragen zij daarin?
    - Wat zijn de verwachtingen van de inwoners van Nederland aan de overheid op het gebied van VIN-fraude?
    - Hoe verloopt de huidige samenwerking tussen de ketenpartners?
3. Welke vormen van VIN-fraude bestaan er en wat zijn de gevolgen voor de betrokken actoren?
4. Welke aanpak bestaat er omtrent VIN-fraude en welke kansen zijn er voor de politie en ketenpartners in de toekomst omtrent deze aanpak?

1.4 Leeswijzer

In hoofdstuk 2 wordt de organisatie beschreven en in hoofdstuk 3 het theoretisch kader. Hierna gaat hoofdstuk 4 in op de methodologie van het onderzoek. In hoofdstuk 5 worden de resultaten beschreven. Vervolgens wordt in hoofdstuk 6 de conclusie van het onderzoek benoemd. Gevolgd met hoofdstuk 7 die de aanbevelingen weergeeft. In hoofdstuk 8 is de discussie opgenomen. In hoofdstuk 9 wordt de literatuurlijst weergegeven. Ten slotte staan in hoofdstuk 10 de bijlagen.

2 Organisatieomschrijving

De politie in Nederland (Nationale Politie) is een politiedienst, belast met het handhaven van de wetten van Nederland, het bewaren van de openbare orde en het verlenen van hulp. De politiewet omschrijft de taak van de politie als volgt: “De politie heeft tot taak in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.”

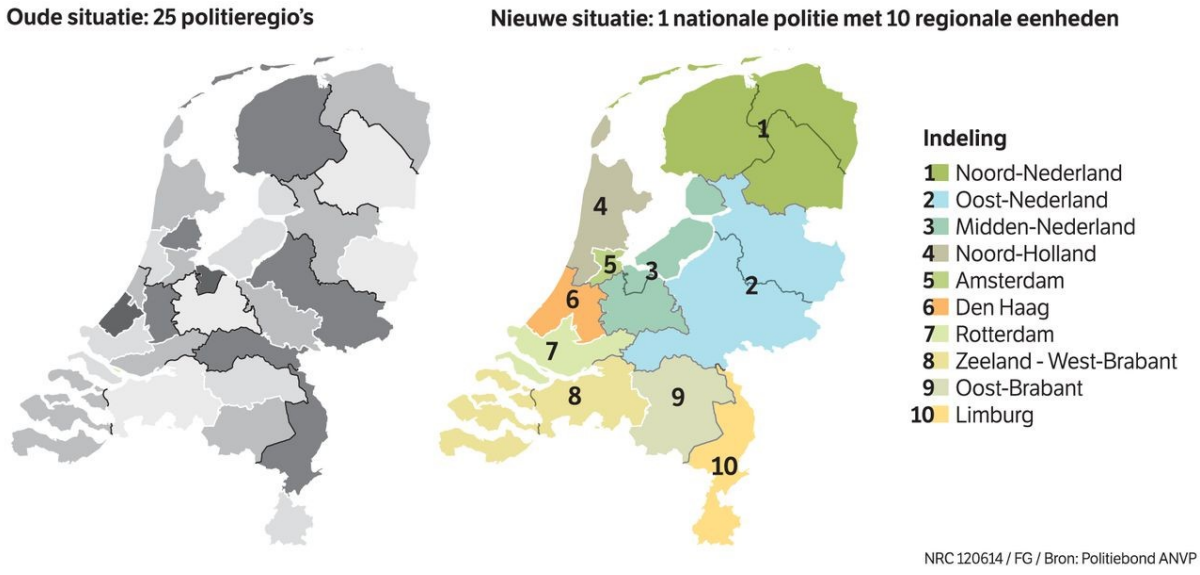
De politie zorgt dat burgers de wetgeving naleven door op te treden tegen overtredingen en misdrijven. Daarnaast beschermt ze iedereen die in Nederland woont of verblijft en verleent ze hulp aan mensen die deze nodig hebben. Kortom, de politie ordent de samenleving door ontsporingen te bestrijden (Infopolitie, 2022).

De Nationale Politie is het landelijke politiekorps. De organisatie bestaat uit:

- De Landelijke Eenheid;
- Het Politiedienstencentrum;
- De regionale eenheden (Rijksoverheid, z.d.).

Op 1 januari 2013 gingen de 26 huidige politiekorpsen op in één landelijk politiekorps dat bestaat uit tien regionale eenheden, een landelijke eenheid en een Politiedienstencentrum. Het hoofdkantoor van de Nationale Politie wordt gevestigd in Den Haag (Infopolitie, 2022).

Dit onderzoek wordt uitgevoerd voor de eenheid Oost-Nederland, basisteam Apeldoorn. Een basisteam werkt voor een hele gemeente, een deel van een (grote) gemeente of voor meerdere (kleinere) gemeenten. Het team voert de kerntaken van de politie uit: de basispolitiezorg. Wijkagenten vervullen daarin een hoofdrol. Zij weten immers goed wat er in hun wijk speelt en welke kwesties aandacht van de politie vragen. Elk basisteam telt ten minste één opsporingsmedewerker die ondersteunt bij de aanpak van veelvoorkomende criminaliteit. Waar nodig werkt het basisteam samen met andere teams binnen het district, met de districtsrecherche en met externe partners op lokaal niveau, zoals gemeentes, reclassering en jeugdzorg (Infopolitie, 2022).



3 Theoretisch kader

Dit theoretisch kader bevat informatie die betrekking heeft op VIN-fraude in de tegenwoordige verschuiving van fysieke- naar digitale criminaliteit. De informatie is verdeeld en wordt nader toegelicht op de volgende drie gebieden: beleidsmatig, juridisch en bestuurlijk.

Ook is het van belang om begrippen af te bakenen, om extra context te geven. De belangrijkste begrippen voor dit onderzoek die regelmatig gebruikt worden, zijn in hoofdstuk 3.4 weergegeven.

3.1 Beleidsmatig

Volgens een bericht van het CBS blijkt dat steeds minder Nederlanders aangeven dat ze slachtoffer zijn geweest van traditionele vormen van criminaliteit zoals geweld, inbraak, diefstal en vernieling. De politie registreerde als gevolg dan ook minder van deze misdrijven. Daarentegen zijn meer burgers slachtoffer geworden van cybercrime (Centraal Bureau voor de Statistiek, 2020).

In dit onderzoek zal nader worden ingegaan op VIN-fraude ofwel, Vriend-In-Noodfraude. Bij VIN-fraude wordt via WhatsApp een zogenaamd dringend verzoek van een vriend(in), familielid of bekende om zo snel mogelijk om wat voor reden dan ook geld over te maken. In werkelijkheid wordt dit WhatsApp bericht door een cybercrimineel verstuurd, die zich in de hoop, door zich voor te doen als een bekende, op deze manier geld wil aftroggelen (Cybercrimeinfo, z.d.). Deze fraude komt het meest voor op WhatsApp, maar vindt ook zijn weg via e-mail, SMS, Snapchat en Telegram.

Tot op heden is er nog geen concrete aanpak voor VIN-fraude vanuit de politie en de daarbij horende ketenpartners. De missie van de politie is: “onveranderd is de politie, waakzaam en dienstbaar aan de waarden van de rechtsstaat”. Dit wordt voornamelijk vervuld door de politie door, afhankelijk van de situatie, gevraagd of ongevraagd eenieder te beschermen, te begrenzen of te bekrachtigen. Digitalisering heeft tevens geleid tot de huidige netwerksamenleving van nu. Hierdoor wordt de overheid en de politie verplicht om zich steeds aan de huidige netwerksamenleving aan te passen. De politie staat midden in de tegenwoordig snel veranderde samenleving. De ontwikkelingen in de samenleving vraagt om aanpassingen binnen de politieorganisatie (Ministerie van Justitie en Veiligheid, 2018). Een interessant vraagstuk als het VIN-fraude betreft.

3.2 Juridisch

Bij de opdrachtgever Sjoerd Obbink is nagevraagd welke wetgeving de politie gebruikt voor het handhaven van digitale criminaliteit. VIN-fraude wordt berecht via het strafrecht. Artikel 326 SR (Strafrecht) wat staat onder het kopje bedrog, volgens Sjoerd Obbink. Zo geeft Sjoerd Obbink aan dat strafvordering vaak wordt aangepast, of wel wordt veranderd. Het strafrecht daarentegen niet: “Fraude blijft hetzelfde, fysiek maar ook online”, volgens Sjoerd Obbink. “Wel is er jurisprudentie over digitale fraude beschikbaar van de Hoge Raad”, aldus Sjoerd Obbink (persoonlijke communicatie, 28 maart 2022).

3.3 Bestuurlijk

De algemene bevoegdheid ter handhaving van de openbare orde is vastgelegd in artikel 172 van de Gemeentewet. Daarin staat dat de burgermeester belast, ofwel verantwoordelijk is voor de handhaving van de openbare orde (Het Nederlands Genootschap van Burgemeesters, z.d.-a). In de Gemeentewet is opgenomen dat de politie optreedt onder het gezag van de burgemeester bij de hulpverlening en ter handhaving van de openbare orde. In artikel 11 van de Politiewet staat beschreven dat wanneer de politie optreedt ter handhaving van de openbare orde en ter uitvoering van de hulpverleningstaak, het onder gezag van de burgermeester staat. De burgemeester kan de politie de nodige aanwijzingen geven voor de vervulling van deze taken.

Het gezag van de burgemeester strekt zich uit tot alle politiefunctionarissen als ze in de gemeente optreden ter handhaving van de openbare orde (Het Nederlands Genootschap van Burgemeesters, z.d.-b).

Het handhaven van de openbare orde bestaat uit twee elementen:

- De daadwerkelijke voorkoming en beëindiging van zich concreet voordoende of dreigende verstoringen van de openbare orde, en;
- De algemene bestuurlijke voorkoming van strafbare feiten, die vorm krijgt in de participatie van de politie in het preventieve veiligheidsbeleid (Het Nederlands Genootschap van Burgemeesters, z.d.-b).

Tijdens het gesprek met Sjoerd Obbink Kwam naar voren dat de burgemeester ook in zekere zin verantwoordelijk is voor wat er met data gebeurt binnen de gemeente. Als er bijvoorbeeld een datalek ontstaat kan de burgemeester daar wel op aangesproken worden. De burgemeester is dus verantwoordelijk voor de openbare veiligheid, voornamelijk in het fysieke aspect, maar kan ook deels gezien worden als verantwoordelijke voor het digitale aspect (persoonlijke communicatie, 28 maart 2022). Hoever deze grens wijkt, is een interessant aspect wat meegenomen kan worden in het interview met de gemeente.

3.4 Begripsafbakening

Onderstaand staan relevante begrippen die regelmatig terug zullen komen in dit onderzoek of vrij specifiek zijn en extra uitleg vereisen. Er is bijvoorbeeld besloten om inwoners toe te voegen in de begripsafbakening zodat daarmee aangegeven kan worden dat het om inwoners van Nederland gaat en niet specifiek een gemeente of provincie.

3.4.1 Gemeente Apeldoorn

De gemeente Apeldoorn is een gemeente in de provincie Gelderland. De gemeente Apeldoorn heeft afgerond een totale oppervlakte van 34.115 hectare. Er wonen 74.301 huishoudens en de gemeente telt twaalf woonplaatsen, zestien wijken en 95 buurten. Het aantal inwoners in de gemeente Apeldoorn is in 2021 gemeten op 164.781 (AlleCijfers, 2022*)*.

3.4.2 Doelgroep

Het begrip doelgroep wordt gedefinieerd als een afgebakende groep personen waar een onderzoek zich op richt. Doelgroepen kunnen worden onderscheiden doordat de groepsleden bepaalde kenmerken delen (Online Marketing Agency, 2021).

3.4.3 Ketenpartners

Ketensamenwerking vraagt om fundamentele veranderingen in de manier van denken en doen van alle betrokken organisaties en mensen. Een ketenpartner is een persoon of organisatie, buiten de eigen organisatie, die een bijdrage levert aan de totstandkoming en/of levering van het product of professioneel betrokken is bij het product of klant (Consultancy, 2017).

3.4.4 Politie

De politie is een organisatie met als taak in ondergeschiktheid met het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp en hen die deze behoeven (Politie, z.d.).

3.4.5 Gemeente

De gemeente is de bestuurslaag die het dichtste bij de burger staat. De andere twee bestuurslagen zijn de provincie en het Rijk. Gemeenten hebben een democratisch gekozen bestuur en zijn verantwoordelijk voor verschillende taken. Dit zijn taken op bijvoorbeeld het gebied van huisvesting,

verkeer, openbare orde, cultuur en onderwijs. Naast deze taken voert de gemeente ook rijkstaken uit, bijvoorbeeld ten aanzien van ruimtelijke ordening, werk en inkomen, jeugdzorg en zorg aan langdurig zieken en ouderen (Parlement, 2022).

3.4.6 NCSC

Het nationaal cybersecuritycentrum (NCSC) is een organisatie van het Ministerie van Justitie en Veiligheid. De organisatie werkt, als expert aan een digitaal veilig Nederland. Zo identificeert de NCSC digitale risico's en trends, verbind de NCSC kennis, informatie en partijen. Door hun werk voorkomen ze maatschappelijke schade en beperken ze dreigingen (Nationaal Cyber Security Centrum, 2022).

3.4.7 Openbaar Ministerie

Het Openbaar Ministerie (OM) heeft als voornaamste taak verdachten voor de strafrechter te brengen (OM, z.d. a). Hier speelt cybercrime dus ook een rol, gezien het OM de enige organisatie in Nederland is die vervolgingsmacht heeft. Dat het OM bezig is met cybercrime, blijkt wel aan de hoeveelheid aandacht die eraan wordt besteed online (Openbaar Ministerie, z.d. b).

3.4.8 Ministerie van Justitie en Veiligheid

De taak van het Ministerie van Justitie en Veiligheid is het voorbereiden en het uitvoeren van regeringsbeleid. In dit geval beleid rondom cybercriminaliteit. Het belang van het ministerie van J&V is het handhaven van de rechtsorde en het veiliger en rechtvaardiger maken van de samenleving. Hier is het ministerie immers verantwoordelijk voor (Rijksoverheid z.d.).

3.4.9 Preventie en repressie

Preventie is het nemen van maatregelen om onveiligheid die zich kan voordoen te voorkomen of vroegtijdig te stoppen, en daarmee ongewenste gevolgen te beperken. Repressie is het optreden om de onveilige situatie te beëindigen, hulp te verlenen en de schade te beperken (Stol, 2016).

3.4.10 Fysieke en digitale criminaliteit

Door de opkomst van het digitale domein vindt er een verschuiving van fysieke criminaliteit naar digitale criminaliteit plaats. Dit wordt bevestigd door het onderzoek van het WODC, waarbij wordt aangegeven dat bij gedigitaliseerde criminaliteit ICT wordt gebruikt om traditionele vormen van fysieke criminaliteit te plegen, zoals fraude en oplichting (Smits et al., 2019).

In dit onderzoek wordt bij het begrip fysieke criminaliteit, criminaliteit zoals fysieke fraude en oplichting bedoeld. Met digitale criminaliteit (cybercriminaliteit) wordt in dit onderzoek het uitvoeren van criminaliteit met behulp van ICT bedoeld, zoals online oplichting en fraude.

3.4.11 Cybercrime

Onder cybercrime wordt criminaliteit verstaan dat is gepleegd met behulp van een computer of netwerk. Een nader onderscheid daarbij wordt vaak aangebracht in 'cybercrime in brede zin' (computer-assisted crimes) en 'cybercrime in enge zin' (computer-focused crimes) (Van Erp et al., 2013).

3.4.12 VIN-fraude

Bij vriend-in-noodfraude wordt er via WhatsApp een zogenaamd dringend verzoek van een vriend(in), familielid of bekende om zo snel mogelijk om wat voor reden dan ook geld over te maken. In werkelijkheid wordt dit WhatsApp bericht door een cybercrimineel verstuurd, die zich in de hoop, door het zich voordoen van een bekende, op deze manier geld wil aftroggelen. Deze fraude komt het meest voor op WhatsApp, maar vindt ook zijn weg via e-mail, SMS, Snapchat en Telegram (Cybercrimeinfo, z.d.).

Werkwijze van VIN-fraude
Een vriend, familielid of een andere bekende verstuurt een bericht dat hij of zij dringend financiële hulp nodig heeft. Voorbeeld van een reden kan zijn dat hij of zij zogenaamd in het buitenland vast zit, en zijn geld, telefoon en papieren kwijt is. De 'bekende' vraagt of er zo snel mogelijk geld overgemaakt kan worden. Als je hierin meegaat, volgt er vaak een tweede verzoek (Cybercrimeinfo.nl, z.d.).

VIN-fraude houdt in dit onderzoek in dat wanneer er per WhatsApp, SMS, Snapchat en/of Telegram, een bericht wordt gestuurd naar een onschuldige ontvanger door een zogenaamde vriend, familielid, en/of bekende, met het verzoek om geld over te maken.

3.4.13 Money mule – Geldezel
Bij het witwassen van criminele gelden wordt binnen de georganiseerde criminaliteit, met name binnen cybercriminaliteit, dikwijls gebruik gemaakt van de money mule (Verspille, 2016). De money mule, ook wel geldezel of katvanger genoemd, kan zodoende gekwalificeerd worden als een cruciale actor in het witwasproces (Oerlemans, Custers, Pool, & Cornelisse, 2016). "Money mules zijn individuen die zichzelf beschikbaar stellen als eigenaar van een voertuig, bedrijf, bankrekening of enig ander goed, waardoor de werkelijke eigenaar zichzelf buiten het zicht van de autoriteiten kan houden" (Schoenmaker et al., 2012). Door het ter beschikking stellen van een bankrekening en/of pinpas aan criminelen, fungeert de money mule als dekmantel voor misdadige organisaties (Versprille, 2016).

3.4.14 Spoofing
Banken refereren regelmatig naar *spoofing. Spoofing* betekent dat een oplichter zich voordoet als een medewerker van de bank, een helpdesk of een webwinkel. Door zich voor te doen als een legitieme medewerker probeert de oplichter geld van iemand afhandig te maken. Banken noemen bankhelpdeskfraude een vorm van *spoofing* waarbij vaak in een korte tijd veel geld van iemand afhandig wordt gemaakt (slachtofferhulp Nederland, 2022).

3.4.15 Veiligheidsbeleving
Veiligheidsbeleving is de manier waarop mensen veiligheid ervaren (Van Noordenburg, 2022). Subjectiviteit voert bij dit begrip de boventoon. Hoewel objectief er minder criminaliteit kan zijn in bijvoorbeeld een wijk, kan de veiligheidsbeleving die objectiviteit aantasten door een subjectieve invulling. Het CBS doet onderzoek naar deze veiligheidsbeleving, alsmede hoe dit zich uit in gedrag (Centraal Bureau voor de Statistiek, 2019).

4 Methode van onderzoek

In dit onderzoek wordt de combinatie van de methoden kwantitatief en kwalitatief gebruikt. Deze combinatie heet ‘’mixed methodes’’. Deze methode geeft een beter en vollediger beeld dan alleen kwantitatief of kwalitatief onderzoek, omdat de voordelen van beide methoden worden gecombineerd (George, 2021). Dit geeft een zo betrouwbaar mogelijk beeld van de omvang, aard en aanpak van de verschuiving van fysieke naar digitale criminaliteit (Verhoeven, 2018). Bij kwantitatief onderzoek wordt er voornamelijk data geanalyseerd en verzameld, dit kan zich vormgeven door enquêtes, experimenten, observatie en secundair onderzoek (Bhandari, 2021). Bij kwalitatief onderzoek wordt niet-numerieke data (zoals teksten, video’s of audio’s) verzameld en geanalyseerd, dit om meningen of ervaringen beter te kunnen begrijpen. Dit type onderzoek wordt vaak gebruikt om meer inzicht te krijgen in een al vastgesteld probleem, of om ideeën op te doen voor een nieuw onderzoek (Bhandari, 2022).

De verschillende onderzoekmethoden die gepaard gaan met dit ‘mixed methodes’ onderzoek zijn in onderstaande paragrafen nader toegelicht.

4.1 Deskresearch

In het eerste deel van dit project zal deskresearch plaatsvinden. Bij deskresearch wordt er zelf geen nieuwe data verzameld. In bestaande literatuur worden antwoorden op de onderzoeksvragen gezocht (Krul, 2021).

4.1.1 Archiefonderzoek (kwalitatief onderzoek)

Door het raadplegen van bijvoorbeeld manuscripten, documenten of archieven van bibliotheken of databases kunnen historische gebeurtenissen onderzocht worden (Bhandari, 2022).
Archiefonderzoek kan onder meer worden gebruikt bij de geschiedenis van de verschuivingen van fysieke criminaliteit naar digitale criminaliteit. Hoe het is ontstaan en welke manieren er zijn. Het is van belang om een volledig overzicht te kunnen creëren. Er wordt met archiefonderzoek dus relevante publicaties geraadpleegd die in zullen gaan op de aard en omvang van digitale criminaliteit, te denken valt aan: rapporten van de politie en gemeenten.

4.1.2 Secundaire dataverzameling (zowel kwalitatief als kwantitatief onderzoek)

Secundaire dataverzameling komt tot stand door data te analyseren van gegevens die niet toegankelijk zijn. Uiteindelijk wordt dit verwezenlijkt door informatie te zoeken in bestaande datasets, bijvoorbeeld in overheidsdatabases of eerdere onderzoeken (Bhandari, 2022). Secundaire dataverzameling kan onder meer gebruikt worden bij de vragen wat VIN-fraude kenmerkt en hoe deze aanpak in de praktijk momenteel verloopt. Deze informatie komt goed tot zijn recht om kennis over dit onderwerp te vergaren.

4.2 Fieldresearch

Het tweede deel van dit project zal bestaan uit fieldresearch. Fieldresearch houdt in dat er nieuwe informatie (primaire data) wordt verzameld, geanalyseerd en geïnterpreteerd (Benders, 2021).

4.2.1 Interviews (kwalitatief onderzoek)

Inhoudende dat er vragen worden gesteld aan respondenten tijdens individuele gesprekken (Bhandari, 2022). Dit zal in dit onderzoek bestaan uit het interviewen van relevante ketenpartners van de politie en medewerkers van de politie met betrekking tot VIN-fraude.

Een interview is een gesprek waarin beleving van de geïnterviewde vooropstaat. In dit onderzoek is gekozen voor het houden van een half gestructureerd interview. Hierbij worden vragen gesteld aan de hand van vooraf vastgestelde onderwerpen, wat deze vastgestelde onderwerpen zullen zijn hangt samen met de informatie die relevant is voor het beantwoorden van de onderzoeksvragen. Er wordt echter ook geanticipeerd op antwoorden van de geïnterviewde, waarna bijvoorbeeld doorgevraagd kan worden. Voor deze methode is gekozen, omdat dit een richtlijn geeft voor de interviewer en ook omdat er de mogelijkheid is om door te vragen. Door de interviews op deze wijze af te nemen ontstaan diepte-interviews.

Deelvragen beantwoorden
De deelvragen uit dit onderzoek zullen allen beantwoord worden door de ketenpartners of door medewerkers van de politie die worden geïnterviewd. Dit onderzoek richt zich voornamelijk op organisaties en bedrijven die te maken hebben met VIN-fraude en hier invloed op kunnen hebben.

4.3 Betrouwbaarheid en validiteit

Het onderzoek moet betrouwbaar en valide zijn. Betrouwbaarheid is de mate waarin het onderzoek vrij is van (toevallige) fouten. Het onderzoek is betrouwbaar als het onderzoek herhaalbaar met dezelfde uitkomst is, de onderzoeker het eens is met de resultaten en wanneer de onderzoeker onafhankelijk is. Daarnaast moet het onderzoek weerlegbaar en openbaar zijn. Validiteit geeft aan of er gemeten is wat de onderzoeker wilde weten en of dat ook op de juiste manier is gedaan. Hierbij moet de steekproef generaliseerbaar zijn naar de populatie van het onderzoek. De steekproef moet willekeurig zijn en voldoende groot zijn (Verhoeven, 2018).

4.4 Tabel interviews

Respondent	Organisatie	Functie	Locatie
1	Politie	Cybercrime Team	Oost-Nederland
2	Politie	Senior Digitale Criminaliteit	Basisteam Apeldoorn
3	Politie	Digitale Wijkagent	Basisteam Apeldoorn
4	Politie	Projectleider Cybercrime Team	Oost-Nederland
5	OM	Parketsecretaris OM (gespecialiseerd digitale opsporing en cybercrime)	Oost-Nederland
6	Gemeente	Adviseur Orde en Veiligheid	Gemeente Apeldoorn
7	VNG	Teamleider Digitale veiligheid incl. cybercrime	Landelijk georganiseerd
8	ABN AMRO	Coöperate Information Security Officer & Security Culture and Transformation	Landelijk georganiseerd
9	Rabobank	Adviseur Fraude / Fraude Analist	Landelijk georganiseerd
10	ING	Expert Lid Fraude Onderzoek	Landelijk georganiseerd

5 Resultaat

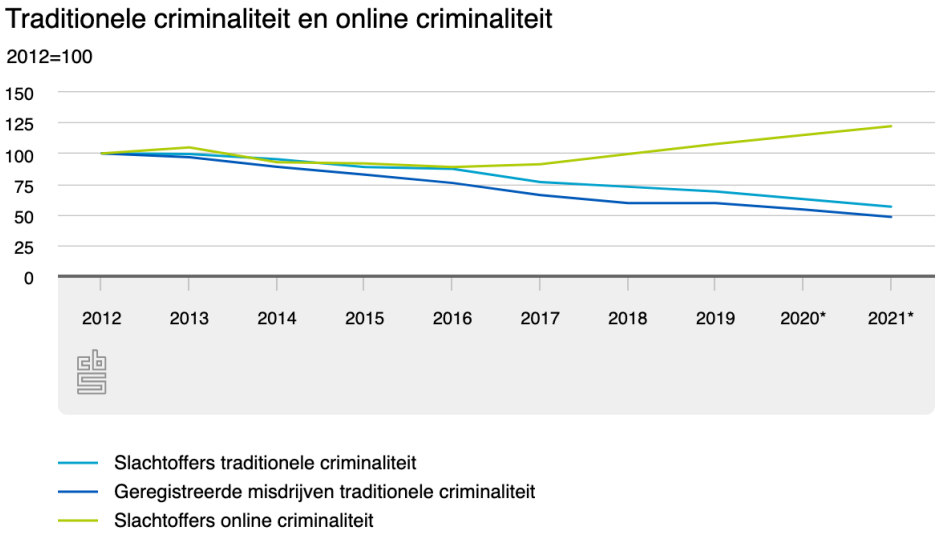
5.1 Deelvraag 1

Wat is de huidige situatie rondom de verschuiving van fysieke naar digitale criminaliteit?

'Cybercrime groeit, wordt complexer en veroorzaakt steeds meer maatschappelijke schade', waarschuwen recherche chef Arjan de Zwart en officier van justitie Marieke Vreugdenhil. Ze zijn samen voorzitter van het Landelijk Operationeel Cybercrime Overleg (LOCO). Maandelijks komen hierin de cybercrimeteams, *Team High Tech Crime* en cyberofficieren van justitie bijeen. Het doel is de gezamenlijke bestrijding van cybercrime (Sabel, 2021).

Ten opzichte van 2019 zag de politie een ruime verdubbeling van het aantal geregistreerde digitale misdrijven (Sabel, 2021). Er is een duidelijke verschuiving van fysieke criminaliteit naar digitale criminaliteit (CBS, 2022). Zo ook te zien in onderstaande Figuur 1.

Figuur 1



Opmerking. Overgenomen uit Minder traditionele criminaliteit, meer online criminaliteit door CBS, 2022 (https://www.cbs.nl/nl-nl/nieuws/2022/09/minder-traditionele-criminaliteit-meer-online-criminaliteit).

De gelegenheid neemt toe, de criminaliteit wordt complexer en het levert meer schade op (Deiters, 2022). De politie constateert meer gevallen van fraude via WhatsApp, met name het fenomeen VIN-fraude. Daarbij doet iemand zich bijvoorbeeld voor als een dochter die haar moeder vraagt om het storten van een geldbedrag vanwege plotseling te betalen collegegeld. Door een hack, is aan het telefoonnummer of de profielfoto niet te zien dat het om een oplichter gaat. Ook ziet de politie meer fraude met onlinehandel, waarbij wel voor iets wordt betaald, maar het bestelde nooit wordt ontvangen (Sabel, 2021).

Aan de andere kant nemen *high impact crimes* als overvallen en inbraken af (Deiters, 2022). Zo worden er minder auto's gestolen en straatovervallen gepleegd en kwam ook zakkenrollerij minder voor (CBS, 2022). Arjan de Zwart ziet dat reguliere of jonge criminelen die eerder bij de politie in de systemen voorkwamen voor bijvoorbeeld straatroof, nu vaker kiezen voor allerlei vormen van cybercrime (Deiters, 2022).

Bij de aanhouding van cybercrimeverdachten is de vondst van wapens geen uitzondering meer. In die zin zijn *high impact crimes* en cybercrime communicerende vaten. Het is dus zeker niet zo dat er minder misdaad is; het zijn meer schuivende panelen (Deiters, 2022). Criminelen die zich met traditionele zaken als drugshandel en inbraken bezighielden, verleggen hun werkterrein naar het internet. Wouter Stol, bijzonder hoogleraar cyberveiligheid, herkent de uitkomsten. “Je kunt bijna niet meer bankieren zonder internet, we doen onze boodschappen digitaal; logisch dat criminelen van een oud model naar een nieuw model overgaan” (Sabel, 2021). Met al die ontwikkelingen worden de dilemma’s voor de politie weer groter, omdat je nog meer moet kiezen waar je je kwaliteit en capaciteit op richt (Deiters, 2022). De politie moet in toenemende mate ook een ICT-deskundige zijn om digitaal misdrijven op te sporen, er is meer kennis nodig (Sabel, 2021).

De online veiligheidsbeleving is in 2021 verslechterd ten opzichte van 2020. Maar liefst drie op de vijf Nederlanders maken zich zorgen om de online veiligheid in hun thuissituatie. Dit deel is in één jaar tijd gestegen met 14 procent. Een gedeelte van deze zorgen zijn toegenomen sinds de coronacrisis. Ouderen en lager opgeleiden maken zich meer zorgen om hun online veiligheid, dan jongeren en hoger opgeleiden. Ze geven aan vaak niet te weten hoe ze zich online kunnen beschermen (Cybersecurity onderzoek Veilig Online 2021, 2022). Negen op de tien Nederlanders geven aan de betekenis van vriend-in-nood (WhatsApp)-fraude te kennen. Negen procent van de Nederlands heeft zelf al een keer te maken gehad met VIN-fraude (Cybersecurity onderzoek Veilig Online 2021, 2022).

<u>Resultaten over verschuiving volgens ketenpartners</u>
Door alle respondenten wordt aangegeven dat de traditionele criminaliteit al jaren afneemt en de digitale criminaliteit alleen maar toeneemt. Alleen de geïnterviewde van de VNG benoemt dat de fysieke criminaliteit gelijk blijft en de digitale criminaliteit er extra bij komt. Er is veel ouderwetse criminaliteit te zien met een digitaal karakter benoemd de geïnterviewde van Politie Apeldoorn (Senior digitale criminaliteit). Digitale criminaliteit is heel makkelijk om te plegen. De moeite is minimaal en de buit is maximaal. De respondenten vanuit de politie (respondenten 1, 2, 3 en 4) benoemen dat de verschuiving bij de politie heel duidelijk zichtbaar is. Digitale criminaliteit is meer grens-/gebied overschrijdend dan fysieke criminaliteit. Hier dient de politie en het Openbaar Ministerie op te acteren aangezien er een andere aanpak nodig is voor de oplossing hiervan.

Verschillende vormen van cybercrime zijn nu gewoon online te koop (Deiters, 2022). De respondent van Politie Apeldoorn (Senior digitale criminaliteit) benoemt: “met de komst van de computers is het heel gemakkelijk om anoniem op afstand door allerlei hele simpele trucjes, bijvoorbeeld Marktplaats oplichting, allerlei mensen op te lichten. Bedrijven en overheidsinstellingen moeten zich bewuster worden van de gevaren op internet en beter controleren of wat ze daar doen wel beveiligd is”. De geïnterviewde van de ING benoemt dat veel banken hun kantoren sluiten en online gaan werken. Hierdoor wordt de kans om slachtoffer te worden van digitale criminaliteit groter. De bevolking is gewend geraakt aan aankopen in een paar klikken, en dat een bank virtueel terugpraat alsof het een bekende is. Hierdoor is een vergissing snel gemaakt (Sabel, 2021).

De respondent van politie Apeldoorn (Senior digitale criminaliteit) benoemt dat bij de verschuiving van fysieke naar digitale criminaliteit, een vorm van anonimiteit komt kijken. Dat wil zeggen dat de crimineel redelijk anoniem achter een *firewall* of VPN zijn of haar activiteiten kan ondernemen en daar geld mee kan genereren, waardoor er een nieuwe verschuiving ontstaat. Dat betekent dat de opsporingshandelingen complexer worden. Door de digitale component en complexiteit hiervan haken veel politiecollega’s af.

5.1.1 Deelvraag 1.1
Op welke manier heeft de coronacrisis hier invloed op gehad?

In maart van 2020 kondigde de overheid een lockdown aan om besmettingen van het coronavirus zo goed mogelijk tegen te gaan. Dit deed de overheid onder andere door scholen en horeca te sluiten en een thuiswerk advies op te leggen (Klaassen, 2020). Door deze maatregelen waren mensen genoodzaakt thuis te blijven. Doordat mensen hele dagen thuisbleven, daalde de fysieke criminaliteit zoals inbraken (Politie, 2021). Hierdoor moesten deze criminelen een andere manier vinden om aan hun geld te komen. Dit deden ze dan ook vaak via digitale criminaliteit (Sabel, 2021). Een voordeel van digitale criminaliteit voor de daders is dat ze sneller en veel anoniemer zijn via het internet dan de fysieke/klassieke criminaliteit (PVO, z.d.).

De coronacrisis versterkt de toename van cybercriminaliteit. “De criminaliteit bewoog mee met wat er gebeurde: iedereen was thuis, dus criminelen gingen op zoek naar andere methodes” (BNNVARA, 2022). De gemeente Apeldoorn bevestigt de sterkere toename van digitale criminaliteit tijdens de coronacrisis ook te hebben gezien.

De respondent van de politie (projectleider cybercrimeteam) benoemt dat toen in de coronacrisis de VIN-fraude steeg, er een nieuwe dynamiek ontstond. De urgentie groeide met de aangiftes. Het aantal aangiftes van digitale criminaliteit zijn ook fors gestegen sinds de lockdown, vooral onder oudere mensen is deze stijging aanzienlijk. Zo is het aantal aangiften van digitale criminaliteit driemaal zo hoog (De Waal et. al., 2020). Uit de Veiligheidsmonitor van 2021 bleek dat in 2021 slechts negentien procent aangifte had gedaan van digitale criminaliteit (Centraal Bureau voor de Statistiek, 2022). Doordat niet iedereen aangifte doet van criminaliteit liggen de daadwerkelijke cijfers veel hoger, hierdoor kan er een beeld ontstaan wat niet klopt (RTL Nieuws, 2018).

5.2 Deelvraag 2

Welke actoren zijn in het kader van VIN-fraude van belang, hoe zien zij de verschuiving van criminaliteit en welke verantwoordelijkheid dragen zij daarin?

De verschuiving van fysieke naar digitale criminaliteit was al voor de coronacrisis in opkomst, maar is tijdens de coronacrisis in een stroomversnelling gekomen. Er worden meer delicten online gepleegd terwijl de fysieke delicten afnemen. In bijlage 1 staan de relevante betrokken actoren van VIN-fraude benoemd in tabellen. De informatie gaat in op hun taak en positie, belang, dominante perceptie van het probleem, ter beschikking staande machtsbronnen, dominante afhankelijkheidspatronen, dominante perceptie van relevante aanpakken, gevolgen en te verwachten strategische interactiepatronen.

Banken

Banken spelen een grote rol in het online betaalverkeer en hebben daarom veel met WhatsApp-fraude, helpdeskfraude, *spoofing* en andere vormen van online fraude en oplichting te maken. Zowel de slachtoffers als de daders regelen hun geldzaken via deze banken. Daarom is het essentieel om hun visie te horen. Klanten die slachtoffer worden, verliezen hun geld en vertrouwen. Daarbij leiden banken schade, wantrouwen en financiële kosten.

De ABN AMRO bank geeft aan dat het hen tegenwoordig goed lukt om de daders buiten te houden. Echter, blijven de klanten wel slachtoffers worden. De grootbanken hebben *security operation centers* die elkaar informeren. Banken kunnen geautomatiseerd detecteren of een transactie frauduleus is. Deze informatie kan gedeeld worden met de politie. Hoe sneller de informatiedeling is tussen de actoren, hoe eerder deze criminelen aangepakt kunnen worden. De respondent van de Rabobank geeft aan dat ze dagelijks inspelen op VIN-fraude en dat ze het idee hebben dat het hen vaak sneller lukt de fraude in kaart te brengen dan dat de politie hier grip op krijgt. Dit is deels ook logisch omdat de politie in een andere fase van het proces zit.

In het Jaarrapport van 2021 geeft de Rabobank aan dat ze een verwijzing van De Nederlandse Centrale Bank heeft gekregen waarin staat dat ze niet aan de Wwft (Wet ter voorkoming van witwassen en financiering van terrorisme) voldoen en dat moet verbeteren vóór 15 December 2023 (Rabobank, 2021). De ABN AMRO voldoet ook niet aan de Wwft en is daarvoor beboet (Ministerie van Justitie en Veiligheid, 2021). De Consumentenbond vindt dat Bunq meer tegen online-oplichting moet doen en krijgt relatief veel klachten over de onlinebank (RTL Nieuws, 2021). Oplichting is makkelijker via Bunq omdat je tot voor kort geen IBAN-naam controle nodig had om een rekening aan te maken en de klant bij Bunq 25 IBAN-rekeningen tot zijn beschikking heeft met één account.

Het sentiment dat banken meer tegen WhatsApp-fraude, helpdeskfraude en *spoofing* moeten doen wordt ook gedeeld door de klanten van de banken (Data&Privacyweb, 2022). Banken worden door de klanten verantwoordelijk gehouden en willen een stukje gemak inleveren voor veiligheid. Klanten geven aan dat het overboeken van grote bedragen lastiger gemaakt zou moeten worden (consumentenbond, z.d.).

Een voorbeeld van een effectieve maatregel die Triodos, Volksbank en ING al hebben genomen is het invoeren van een wachttijd voor het verhogen van de overboeklimiet en een noodnummer. Mocht er een andere partij controle over je bankrekening krijgen dan kunnen er minder snel hoge bedragen van je bankrekening worden afgehaald.

In de toekomst zullen banken online fraude meer proberen tegen te gaan met *artificial intelligence* (AI), *big data analytics* en *behaviour analytics* (Betaalvereniging Nederland, 2021).

Politie

De politie heeft de toename van digitale criminaliteit in de afgelopen jaren waargenomen en investeert tijd, geld en personeel in de aanpak daarvan. Ook adviseert de politie andere actoren hetzelfde te doen (Betaalvereniging Nederland, 2021). In 2021 pleitte de politie daarom voor extra geld om digitale criminaliteit beter te kunnen aanpakken. Ook moet er driehonderd miljoen euro extra geïnvesteerd worden voor data-infrastructuur, innovatie, extra personeel en om digitale kennis bij te brengen (Politie, 2021).

Slachtoffers van digitale criminaliteit doen echter weinig aangifte. Van online oplichting heeft slechts 25 procent van de slachtoffers in 2021 aangifte gedaan (Centraal Bureau voor de Statistiek, 2022). Ten opzichte van 2020 is dat een stijging van 13 procent (Junger et al., 2022). De politie is zich hiervan bewust en probeert het sentiment van slachtoffers actief te veranderen met een proef waarmee slachtoffers direct hun geld terug kunnen vorderen (Binnenlandredactie, 2022). De pakkans voor digitale criminaliteit zal na investeringen en kennis toenemen (Politie, 2021). Maar er ligt ook een taak voor de overheid in het voorkomen van online fraude door middel van voorlichting. Hier ligt ook een kans voor samenwerking met het bedrijfsleven en organisaties omdat banken, de Consumentenbond en andere actoren ook verantwoordelijkheid delen.

De politie heeft al een samenwerking opgezet met verschillende bedrijven en organisaties die ze als belangrijk beschouwen over informatie. Winkels, hotels, vakantieparken en casino's zijn voorbeelden van bedrijven waar de politie ook haar informatie vandaan haalt. Deze bedrijven komen soms oog in oog te staan met criminelen die hun geld witwassen door de transacties in deze winkels, hotels en casino's. Dit zijn grote informatiebronnen voor de politie. De politie en gemeente werken ook samen met jongerenwerk. Hier komen jongeren die slachtoffer worden van criminele groepen (*money mules*) of de daadwerkelijke daders.

WhatsApp

WhatsApp heeft 12,5 miljoen gebruikers in Nederland, waardoor WhatsApp het grootste sociale media platform van Nederland is (Oosterveer, 2022). Dat betekent dat 71,7 procent van de Nederlandse bevolking gebruik maakt van deze app. Dit maakt WhatsApp daarom erg aantrekkelijk voor criminelen. Door de pandemie is deze vorm van fraude sterk toegenomen. In 2020 was er al een verviervoudiging van het aantal meldingen bij de Fraudehelpdesk (Voskuil, 2020).

Gezien er geen interview heeft plaatsgevonden met Whatsapp hebben zij hun kijk op de verschuiving en hun verantwoordelijkheid daarin niet kunnen toelichten.

Gemeente

De gemeente speelt een rol bij het informeren van burgers en probeert online fraude tegen te gaan door middel van informeren via webinars, filmpjes en presentaties. Een andere taak die de gemeente uitvoert, is slachtoffers verwijzen naar relevante actoren zoals de bank, politie en de Fraudehelpdesk (Gemeente Lelystad, 2022). De gemeenten voeren dit beleid gezamenlijk uit en alle gemeenten verwijzen door naar dezelfde actoren.

Bij het tegengaan van online fraude en andere criminaliteit wordt de driehoek ingezet. De driehoek bestaat uit de burgemeester, de officier van justitie en de politiechef (regioburgemeesters, z.d.). De gemeente kan preventief invloed uitoefenen.

De burgemeester is uiteindelijk verantwoordelijk voor de openbare orde en wil zijn burgers een bepaalde veiligheid bieden. Naast alle losse gemeenten is ook de beleidsafdeling van de Vereniging van Nederlandse Gemeenten (VNG) verantwoordelijk.

NCSC

Het primaire doel van het Nationaal Cyber Security Centrum (NCSC) is om de digitale infrastructuur te beschermen en te verbeteren. Het NCSC houdt zich dus meer bezig met cybercriminelen die banden hebben met statelijke actoren uit of namens andere landen (Nationaal Cyber Security Centrum, 2021). Deze statelijke actoren houden zich bezig met spionage, sabotage, datalekken, ICT-storingen en *ransomware* aanvallen op infrastructuur (Data&Privacyweb, 2021). Het NCSC is door overige geïnterviewden aangemerkt als ketenpartner, echter beschouwden ze zichzelf niet als schakel in het tegengaan van VIN-fraude.

OM

Het Openbaar Ministerie (OM) is actief bezig met de aanpak van cybercrime. Het is ingewikkelde materie, waarbij de daders niet zichtbaar zijn en niet alleen vanuit Nederland werken. In samenwerking met diverse partijen, waaronder politie, bedrijven, wetenschappers en ethische hackers, worden de daders zoveel mogelijk opgespoord en vervolgd. Deze samenwerking leidt niet alleen tot meer opsporing, maar ook tot betere digitale beveiliging (computers en andere *devices*). Aangezien de daders niet alleen binnen de Nederlandse landsgrenzen werken is het van belang goed contact te onderhouden met andere landen en duidelijke afspraken met ze te maken (Openbaar Ministerie, z.d.). Ook doet het OM aan het preventief informeren van de burgers over cybercrime en welke straf het OM kan eisen. Zo heeft het OM een brochure gemaakt met verschillende soorten van digitale misdrijven om daarmee te laten zien welke straf de daders voor deze digitale misdrijven hebben gekregen (Openbaar Ministerie, 2022). Hiermee wordt ook gepromoot dat mensen aangifte blijven doen van digitale criminaliteit.

J&V

Volgens het Ministerie van Justitie en Veiligheid raakt online oplichting zowel burgers als het bedrijfsleven. Ook ondermijnt het de veiligheid op het internet en het vertrouwen in het betaalverkeer. Volgens het ministerie is het aan de overheid om kwetsbare groepen te categoriseren. Online fraude moet worden bestreden door middel van bewustwording, preventie, interventies, barrières en handelingsperspectief voor slachtoffers. Het is belangrijk duidelijkheid te bieden aan slachtoffers over hoe zij schade kunnen verhalen (Tweede Kamer der Staten-Generaal, 2021). Het ministerie wil dit realiseren door samen te werken met publieke en private partijen. Zij streven naar een integrale aanpak. Telecom- en internetproviders, social media platforms, banken en betaalinstellingen worden hierin genoemd. Er moet meer op Europees verband samengewerkt worden omdat daders vaak anoniem in het buitenland opereren. Hier ligt een rol voor uitwisseling van informatie tussen lidstaten en Europol (Tweede Kamer der Staten-Generaal, 2021).

Overig aangemerkte actoren vanuit de geïnterviewden

Als laatste wordt het Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) door de VNG aangemerkt als belangrijke actor in de samenwerking tegen VIN-fraude. Echter, zagen zij zichzelf niet als ketenpartner en is omtrent deze organisatie geen verder interview gehouden of verdere informatie verzameld.

5.2.1 Deelvraag 2.1
Wat zijn de verwachtingen van de inwoners aan de overheid op het gebied van VIN-fraude?

De overheid zou meer aan preventie moeten doen. 26 procent van de respondenten die meededen aan een onderzoek wat ging over in welke mate je met online fraude te maken had, geeft aan dat ze meer informatie hadden moeten opzoeken en twee procent geeft aan dat ze alerter hadden moeten zijn (Junger et al., 2022). De informatie is online vindbaar bij de verschillende actoren. Dat neemt niet weg dat slachtoffers van online fraude wettelijk niet goed beschermd zijn en daders kunnen moeilijk worden opgepakt. Dit komt omdat de politie de wettelijke bevoegdheden niet heeft. Sinds 2021 kunnen slachtoffers gebruik maken van de Procedure Naw-gegevens Begunstigde bij niet-bancaire Fraude (PNBF), waarbij slachtoffers een brief kunnen sturen of een deurwaarder kunnen inschakelen (Zuurmond, 2022).

Nog een optie wat inwoners minder kwetsbaar maakt tegen online fraude is het verminderen van het nemen van snelle beslissingen door consumenten. Kennis over hoe fraudeurs te werk gaan, is cruciaal en hier kan de overheid een rol in spelen door met voorlichting uit te leggen hoe deze criminelen te werk gaan (Junger et al., 2022).

De respondent gemeente Apeldoorn geeft aan dat de organisatie zelf op het gebied van preventie moet doorgaan of nog verder uitbreiden. Het voeren van campagnes, duidelijke voorlichtingen en sessies voor jongeren. Indirect gebeurt dit al op vele plekken, maar het is niet zo dat zij al een grote campagne hebben uitgezet. De gemeente vermoedt dat daar nog wel een verwachting van de burger ligt. De gemeente Apeldoorn hoopt dat er vanuit het RAAK-project doeltreffende interventies ontstaan. De ‘formule’ voor de beste interventie is momenteel nog niet bekend bij hen.

5.2.2 Deelvraag 2.2
Hoe verloopt de huidige samenwerking tussen de ketenpartners?

De actoren werken al zorgvuldig met elkaar samen, maar er zijn ook verbeteringen nodig. De gemeentes verwijzen je snel door naar de bank, politie, Fraudehelpdesk of www.veiliginternetten.nl (Gemeente Lelystad, 2022). Banken hebben samen met de Vereniging van Banken, Fraudehelpdesk, Rijksoverheid, Consumentenbond, Microsoft en nog meerdere partijen de website www.veiligbankieren.nl opgezet. Daarin lichten ze klanten voor over fraude. Ook adviseren zij als je slachtoffer bent geworden van fraude om een noodnummer van de bank te bellen of je wordt doorverwezen naar de politie (Veilig bankieren, 2021).

Het NCSC en partners hebben samen een security meldpunt gelanceerd waarin de overheid samenwerkt met het bedrijfsleven (Van der Klugt, 2022). Het NCSC doet internationaal onderzoek wat ertoe heeft geleid dat de politie een *ransomware* bende kon arresteren (Data&Privacyweb, 2022). De politie werkt samen met veel verschillende actoren.

De politie heeft recent een succesvolle proef uitgevoerd in samenwerking met Landelijke Associatie van Gerechtsdeurwaarders (LAVG) en de Service Organisatie Directe Aansprakelijkstelling (SODA) waarin slachtoffers hun geld konden terugvorderen (Binnenlandredactie, 2022). De politie werkt samen met hogescholen en universiteiten om meer kennis te vergaren over online fraude en de financiële/psychologische impact op de slachtoffers (Junger et al., 2022).

Vanuit de interviews is duidelijk geworden dat de huidige samenwerking met de ketenpartners van de politie omtrent VIN-fraude gericht is op informatiewisseling. In de praktijk verloopt dit moeizaam, het delen van informatie wordt moeilijk gemaakt door de geldende privacyregels en AVG.

Tevens speelt er ook een kennistekort binnen de politieorganisatie evenals bij andere de actoren. Toch lijkt er vanuit de politievisie wel hoop te zijn. Zo werd er gezegd dat de onderlinge afspraken beter afgestemd kunnen worden en dat goede samenwerkingen naar boven komen na goed overleg.

Het Openbaar Ministerie geeft aan samen te werken vanuit de opsporing en vervolging met onder andere de politie en landelijk met het ECTF (Electronic Crime Task Force). Het Openbaar Ministerie laat zich door eigen zeggen niet tegenhouden door de grenzen binnen Nederland en daarbuiten. In de praktijk wordt vaak zichtbaar dat wanneer het Openbaar Ministerie meer inzicht krijgt, zij ook meer uitdragen en bespreken met de partners. Dit moet wel altijd snel, volgens de geïnterviewde. “VIN-fraude is één van de lagere stapjes en men ontwikkeld zich snel verder, dus je moet snel kunnen aanpassen”. Het vergt een goede afstemming en dit probeert het Openbaar Ministerie dan ook landelijk op te pakken.

De medewerker van de Vereniging van Nederlandse Gemeenten (VNG) geeft aan dat zij drie taken hebben met betrekking tot VIN-fraude. De VNG is een belangenbehartiger; zij praten met Europa, de Rijksoverheid en departementen over welk wettelijk kader of welk beleid wenselijk is. De tweede taak is dat zij de gemeenten ondersteunen en de derde taak is dat zij een kennisplatform hebben. De VNG draagt kennis over cybercrime over naar de gemeente. Dit doen zij door middel van verschillende bijeenkomsten, nieuwsbrieven en appgroepen. Het hangt af van de gevoeligheid van de informatie, want hoe gevoeliger deze informatie is, hoe minder snel zij iets zouden delen. Wel geven zij aan dat ze voortdurend overleg hebben met alle ketenpartners: burgemeesters, politie, het Openbaar Ministerie, het Ministerie van Justitie en Veiligheid, het NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid), NCSC (Nationaal Cyber Security Centrum) en hun eigen beleidsafdelingen.

Gemeente Apeldoorn leunt volgens eigen zeggen op de politie als het gaat om de samenwerking rondom VIN-fraude. De gemeente geeft dit aan omdat de verantwoordelijkheid voor het pakken van een dader volgens hen dan ook bij de politie ligt, omdat de politieorganisatie de aangifte binnenkrijgt. Vanuit de gemeente wordt er ook samengewerkt met het Openbaar Ministerie, de banken en het jongerenloket. Ze proberen een actieve samenwerking te zoeken, maar zitten momenteel nog in de beginfase. Tevens voorziet de gemeente in preventieavonden die voor ouderen zijn bedoeld, dit doet de gemeente samen met de banken en boa’s.
Voorheen had de gemeente Apeldoorn een samenwerking met de Rabobank, daar hadden zij een contactpersoon die heel actief bezig was met digitale criminaliteit. Dit contactpersoon had een andere baan aangenomen, waarna de samenwerking is verwaterd. Banken opereren op nationaal niveau. Lokaal trekken zij zich steeds meer terug, dit is ook zichtbaar doordat er steeds meer lokale bankkantoren sluiten. Doordat zij op landelijk niveau opereren wordt er opgemerkt dat een bank lang niet altijd geïnteresseerd is om met een van de zoveel gemeenten om de tafel te gaan zitten. Daarnaast hebben banken hun eigen campagnes lopen.

Voor dit onderzoek meerdere banken geïnterviewd. De ABN AMRO geeft aan dat zij samenwerken met andere grote banken in Nederland, dit doen zij door middel van *security operation centers* die elkaar informeren. De ING geeft aan dat zij de aangiftes bij elkaar verzamelen, wat voor hen best ingewikkeld kan zijn. Wat de ING doet, ligt aan de behoefte van de politie, daar ondersteunen zij het opsporingsonderzoek waar mogelijk. De ING geeft aan veel meer informatie in te kunnen zien dan de klant zelf. Waaronder bijvoorbeeld het IP-adres van de fraudeur. De Rabobank geeft aan dat zij meerdere overlegvormen hebben met andere banken, met de NVB (Nederlandse Vereniging Banken) en daarnaast ook met de politie en het OM. Bij deze overlegvormen delen zij ervaringen en maatregelen, om het zo samen te bestrijden. Tevens geeft de Rabobank aan dat zij proberen samen te werken, maar dat het toch wel eilanden-werk blijft. Iedereen neemt zijn eigen maatregelen en heeft zijn eigen ideeën.

5.3 Deelvraag 3
Welke vormen van VIN-fraude bestaan er en wat zijn de gevolgen voor de betrokken actoren?

Vormen van VIN-fraude

Er zijn tegenwoordig veel verschillende vormen van cybercrime bekend. VIN-fraude is een redelijk nieuwe vorm van cybercrime. VIN-fraude kan geschaald worden onder de digitale criminaliteitsvorm '*spoofing'*. Bij *spoofing* nemen internetcriminelen een identiteit over. Als zogenaamde bekende of erkende afzender probeert de cybercrimineel achter je persoonsgegevens of je pincode te komen, *malware* op je computer te plaatsen of je direct geld afhandig te maken (Veilig internetten, z.d.).

Een andere vorm, die officieel niet onder VIN-fraude wordt aangeduid maar er wel mee te maken heeft, is het werven van '*money mules*'. Bij het witwassen van crimineel geld wordt binnen de georganiseerde criminaliteit, met name binnen cybercriminaliteit, dikwijls gebruik gemaakt van deze *money mules.* Door het ter beschikking stellen van een bankrekening en/of pinpas aan criminelen, fungeert de *money mule* als dekmantel voor misdadige organisaties (Versprille, 2016). De *money mule*, ook wel geldezel of katvanger genoemd, kan zodoende gekwalificeerd worden als een cruciale actor in het witwasproces (Oerlemans, Custers, Pool, & Cornelisse, 2016).

Gevolgen voor de betrokken actoren

Slachtoffers

De eerst betrokken actor bij deze criminele praktijken zijn de slachtoffers. De meeste gevolgen die slachtoffers van online delicten ervaren, komen overeen met de gevolgen van traditionele offline delicten. De meeste slachtoffers ervaren financiële gevolgen, zowel bij reguliere delicten in het fraudecluster als bij interpersoonlijke delicten, zedenzaken en cybercrimes. Naast financiële gevolgen, is de kans op psychologische en emotionele gevolgen van digitale criminaliteit ook groot. Te denken valt hierbij aan: verlies van vertrouwen, schuldgevoel en schaamte (Leukfeldt, Malsch, & Notté, 2018).

Een belangrijke constatering is dat online delicten een grote impact kunnen hebben op de slachtoffers. Bij een mishandeling of straatroof mijdt het slachtoffer bepaalde straten op bepaalde momenten. Bij slachtoffers van digitale delicten zullen zij wellicht het gehele internet mijden (Leukfeldt, Malsch, & Notté, 2018).

Banken

Naast de opgelichte burgers, zijn banken ook een actor in dit proces. Wanneer je slachtoffer bent geworden van bankspoofing of WhatsApp-fraude, hoeven banken volgens de wet de schade niet te vergoeden (Consumentenbond, z.d.).

Eind 2020 besloten vier grootbanken om particuliere klanten die slachtoffer zijn geworden van bankhelpdeskfraude, ook wel *spoofing* genoemd, uit coulance te vergoeden. Aanleiding voor die beslissing was het feit dat er bij deze vorm van fraude misbruik wordt gemaakt van het vertrouwen dat klanten hebben in hun bank en hun telefoonnummer en naam wordt gebruikt (Nederlandse Vereniging van Banken, z.d.). Wie geld overmaakt aan een oplichter na een betaalverzoek via WhatsApp (VIN-fraude), kan niet de bank aansprakelijk stellen voor de schade. Uit een niet-bindende uitspraak van de Geschillencommissie Financiële Diensteverlening is gebleken dat banken zulke betalingen niet hoeven te blokkeren (Vermeer, 2021).

De geïnterviewde bankmedewerkers van de ABN-Amro, Rabo en ING-banken geven aan dat bovenstaande informatie klopt. Zij vergoeden de klant alleen het afgenomen bedrag wanneer er vanuit hun naam is opgelicht. Bij VIN-fraude wordt de schade niet vergoed, omdat de oplichter zich heeft voorgedaan als kennis of familielid.

Politie/justitie
In februari en maart 2020 steeg het aantal aangiften van VIN-fraude van 130 naar driehonderd per week. Om deze fraudevorm beter aan te pakken zijn er landelijke internet-aangiftes gebundeld en wordt er geautomatiseerd onderzocht op naam en telefoonnummer of bankrekeningnummer zodat geanalyseerd kan worden hoe de criminele netwerken in elkaar zitten (Politie, 2020).

Door het opkomen van (verschillende vormen van) digitale criminaliteit heeft dit veel gevolgen voor het werk van politie en justitie. Uit onderzoek is gebleken dat het gemiddelde kennisniveau voor digitale aspecten van het politiewerk omhoog moet. Dit betekent dat de politie dient te investeren in de kennis en kunde van haar medewerkers omtrent digitale criminaliteit. Cybercrime, gedigitaliseerde criminaliteit en criminaliteit met een digitale component komen nu zo veel voor dat het niet alleen aan specialisten kan worden overgelaten (Politie, 2021).

Om ook strafrechtelijk op deze vormen van criminaliteit te kunnen berechten is er per 1 maart 2019 de wet Computercriminaliteit III in werking getreden. Door deze wet krijgen politie en justitie nieuwe bevoegdheden om computercriminaliteit beter te bestrijden. Deze wet geeft opsporingsambtenaren de mogelijkheid om van een afstand de computer van de dader binnen te treden en onderzoek handelingen te verrichten (Ministerie van Justitie en Veiligheid, 2019).

Gemeente Apeldoorn
Om optimaal met de huidige trends mee te bewegen en om aan te sluiten bij de verwachtingen van inwoners, is optimalisering voor gemeenten van groot belang. Het is een ontwikkeling die veel van doen heeft met de informatiesamenleving. Burgers, ondernemers en maatschappelijke organisaties zijn constant online om producten en diensten af te nemen. Een context waar de overheid zich bij aan dient te sluiten. Daarbij kan digitalisering bijdragen aan een vlotte dienstverlening, flexibiliteit en bereikbaarheid via diverse kanalen. Zo kunnen gegevens en diensten veel beter in het openbaar worden gedeeld. Dit maakt processen transparant en toegankelijk voor ondernemers en inwoners (te Voert, 2018).

Ondanks de voordelen, deinzen nog veel gemeenten terug om zich volledig te laten digitaliseren. Er bestaan discussies over de risico's die digitalisering met zich meebrengt. Vooraf moet goed nagedacht worden over de informatiebeveiliging. Gemeenten beschikken over persoonsgegevens van de burgers. Wanneer deze op straat komen te liggen zorgt dat voor grote privacy schade. In het interview met de gemeente Apeldoorn gaven zij zelf aan risico's te lopen met digitaliseren. Er zijn al meerdere keren bestanden op straat komen te liggen. De rol van de gemeente is om de veiligheid van haar burgers te garanderen.

Digitalisering kan als gevolg hebben dat de gemeente een doelgroep gaat verliezen die angstig is geworden voor de online wereld, omdat zij hier eerder slachtoffer van zijn geworden.

Als gevolg van de komst van VIN-fraude zet de gemeente vooral in op preventie, om zo potentiële slachtoffers te voorkomen. Er wordt door de gemeente Apeldoorn ingezet op voorlichting op basisscholen. Dit doen zij om ervoor te zorgen dat de toekomstige generatie weerbaar is tegen deze vormen van criminaliteit. Naast jongeren wordt er in samenwerking met banken ook ingezet op de preventie bij ouderen. De gemeente merkt dat preventie voor cybercrime een lastige opgave is. Dit heeft volgens de gemeente met de risicoperceptie van mensen te maken, die erg laag blijkt te zijn.
Daarnaast is volgens de gemeente Apeldoorn cybercrime niet tastbaar en hierdoor is het lastiger om een goede interventie te plegen. Uit cijfers van een bewonerspanel van de gemeente Apeldoorn blijkt de suggestie dat slachtoffers van cybercrime zelfs voor een tweede keer opnieuw in de fout gaan. Een perfecte interventie is dus ook nog niet gevonden.

Winkels
Wanneer de daders hun slachtoffers hebben opgelicht, moeten ze de geldbuit nog in hun bezit krijgen. Hiervoor gebruiken zij niet hun eigen bankrekening omdat dat herleidbaar is.

Het witwasproces wordt in de criminologische theorie uitgelegd als het driefasenmodel:

1. *Placing* (storten, wisselen)
2. *Layering* (versluiering)
3. *Integration* (opgaan in de legale economie) (van Koningsveld, 2008).

Voor de eerste fase, *placing*, worden *money mules* (geldezels) ingezet om het 'verdiende' geld naar toe te sluizen. Deze geldezels stellen hun bankrekening beschikbaar aan de crimineel in ruil voor bijvoorbeeld een kleine beloning. Doordat meerdere rekeningen, en dus geldezels, gebruikt worden voor het doorsluizen van het geld, is de dader moeilijker op te sporen. Om het geld van een bankpas af te halen is het casino een vaak gebruikte locatie. Hier staan geldkasten waar contant geld gepind kan worden en in het casino gebruikt kan worden. Uit constatering van de politie is gebleken dat deze machines niet altijd voorzien zijn van cameratoezicht. Zo heeft de crimineel vrij spel het opgelichte geld veilig in eigen zak te steken.

In de tweede fase, *layering*, wordt het misdaadgeld in het wettige betalingsverkeer gebracht en kan het voor uiteenlopende doelen worden gebruikt. Het belangrijkste doel is de herkomst en eigendom van het oorspronkelijke misdaadgeld verder te verhullen door hetzelfde geld verscheidene keren te verplaatsen, desnoods over de gehele wereld. Deze transacties versluieren het controlespoor. Men spreekt in dit verband ook wel over het giraal kriskrassen. Daarbij wordt de oorspronkelijke geldsom gesplitst in kleinere sommen of 'plakjes': 'layering' (laagjes). Deze fase wordt wel de meest complexe fase genoemd (van Koningsveld, z.d.)

In de derde fase, *integration*, gaat het geld op in de legale economische geldstromen. Het is gericht op het integreren van het geld in de bovenwereldeconomie (Van Koningsveld, z.d.). Dit gebeurt vaak via winkels. Het contante geld dat gepind is via de geldezel, wordt in grote getalen uitgegeven in luxe kleding- of elektronicawinkels. Deze aankopen worden allen contant afgerekend. Om deze illegale geldstromen tegen te gaan, is de politie Apeldoorn samen gaan werken met veel van deze winkels.

De politie ziet het als haar taak de winkelier op de hoogte te stellen van de illegale geldstromen en deze tegen te gaan door bijvoorbeeld een maximaal bedrag contant geld te accepteren of opvallende signalen aan de politie door te geven. Ook is goed cameratoezicht van belang. De politie benadrukt hierbij het belang van de winkelier bij het tegengaan van witwassen. Wanneer de winkelier deze illegale geldstromen accepteert zonder alert te zijn of melding te doen kan dit ook juridische gevolgen hebben voor hen. Een winkelier dient te staan voor de veiligheid van al zijn klanten, en crimineel gedrag niet te tolereren.

5.4 Deelvraag 4

Welke aanpak bestaat er omtrent VIN-fraude en welke kansen zijn er voor de politie en ketenpartners in de toekomst omtrent deze aanpak?

Aanpak

De geïnterviewden van de politie vertellen over een redelijk nieuwe implementatie in de aanpak, waarbij er direct online aangifte kan worden gedaan nadat het slachtoffer is opgelicht. Van de online aangiftes worden de bankrekeningnummers, berichten en telefoonnummers gecategoriseerd en waar mogelijk aan elkaar gekoppeld, om hiermee dichter bij de dader te komen. Het cybercrime team heeft een project op VIN-fraude gedraaid, waarbij zij bij banken bulkaanvragen kunnen doen op rekeningnummers.

Daarnaast is de politie bezig met enkele preventieaanpakken om potentiële slachtoffers van cybercrime hierop te attenderen. Enkele voorbeelden van dit soort aanpakken zijn:

- Mobiele Media Lab: een truck waar mensen er op een speelse manier achter kunnen komen hoeveel zij weten van digitale veiligheid. Ook kennis over digitale criminaliteit wordt getest met een quiz, de wijkagent gaat met de deelnemers in gesprek hoe zij zichzelf en anderen het best kunnen beschermen online.
- *Talkshow* 'De ondernemer Draait Door': een *talkshow* waar het MKB-bedrijf centraal staat. Hoe kun je je MKB-bedrijf beschermen tegen cybercriminelen; welke beveiligingsmaatregelen kun je nemen en hoe kan de politie daarmee helpen.
- Cyberaangifte avonden: avonden die zijn ingericht om *cybercrime* aangiften te doen. Een voorbeeld is de Politie in Vleuten-De Meern, die op 9 en 23 maart 2021 een zogenaamde 'cyberavond' presenteerde (Politie, 2021).

Banken werken samen doormiddel van een interbancair overleg. In dit overleg bespreken zij trends die zich voordoen op het gebied van cybercrime. Banken hebben naast dit overleg een detectiesysteem waarmee ze verdachte transacties opsporen. Als ze een verdachte transactie op het spoor zijn dan kan ervoor gekozen worden om de rekening te blokkeren. Op dat moment proberen de banken het geld terug te vorderen, dit lukt ze helaas niet altijd. Wat de ING doet, ligt aan de behoefte van de politie, daar ondersteunen zij het opsporingsonderzoek waar mogelijk. De ING geeft aan veel meer informatie in te kunnen zien dan de klant zelf. Waaronder bijvoorbeeld het IP-adres van de fraudeur. De Rabobank geeft aan dat zij meerdere overlegvormen hebben met andere banken, met de NVB (Nederlandse Vereniging Banken) en daarnaast ook met de politie en het OM. Banken vergoeden alleen de schade van slachtoffers als de dader zich voordoet als de bank. De schade van VIN-fraude wordt dus niet vergoed.

De geïnterviewde van de gemeente Apeldoorn geeft aan, dat zij, net als alle gemeenten, een integraal veiligheidsplan hebben, waarvoor ze in 2023 een nieuw plan gaan opstellen. Waar in de huidige versie digitale criminaliteit een speerpunt is, zal dit hopelijk ook voor 2023 het geval zijn. Daarnaast worden er preventiecampagnes gevoerd. Deze campagnes worden gericht op MKB-ondernemers, jongeren en ouderen. Tevens geeft de geïnterviewde gemeente aan dat er een gezamenlijk overleg plaatsvindt tussen het jongerenloket, jongerenwerkers en de Rabobank in het kader van *money mules*. De gemeente hoopt hier bewustzijn te creëren onder jongeren over dit fenomeen. Waardoor er in de toekomst (hopelijk) minder *money mules* zijn die dus meehelpen met VIN-fraude.

Het kabinet wil de komende jaren 26 miljoen euro beschikbaar stellen ter bestrijding van cybercrime. Naast het werven van extra personeel bij de politie voor inzet tegen cybercriminaliteit zowel landelijk als regionaal, wil het kabinet ook dat de politie zich meer bezig gaat houden met digitale forensische opsporing (sporenonderzoek).

Voor het opsporen van oplichting, fraude en criminaliteit op het internet worden hoogopgeleide specialisten aangenomen. Ter bestrijding van cybercrime hebben politie en justitie meer bevoegdheden, waaronder helers van digitale gegevens arresteren, gegevens ontoegankelijk maken, denk hierbij aan bijvoorbeeld e-mails met informatie over misdrijven. Dit alles is vastgelegd in de Wet Computercriminaliteit III.

Ook zijn er hoge straffen vastgelegd voor cybercriminaliteit. Denk hierbij aan het vernielen van computergegevens, daarbij kunnen gevangenisstraffen van maximaal twee jaar worden gegeven.
Daarnaast zal in de toekomst door bepaalde organisaties (in vitale sectoren) melding worden gemaakt van digitale veiligheidsincidenten (ICT-inbreuken). Dit zijn onder andere de sectoren: elektriciteit, gas, drinkwater, telecom e.d. (Rijksoverheid, z.d.).

De huidige aanpak van het Openbaar Ministerie is voornamelijk gericht op opsporing en vervolging. Zoals al eerder gesteld; is deze samenwerking met de vier groot banken van Nederland en de politie. Uit het interview werd duidelijk dat voor deze nieuwe (veranderende) vorm van fraude er gekeken zal moeten worden waar de verantwoordelijkheid ligt voor de betrokken actoren.

<u>Kansen</u>
De meerderheid van de geïnterviewden, geven aan dat er een betere informatiewisseling tussen de betrokken partners moet komen. In het geval van de politie, stellen de geïnterviewden dat er nog genoeg kansen zijn op de aanpak van VIN-fraude. Waarbij een geïnterviewde van de politie opmerkt dat er voor elke eenheid een interventiespecialist zou moeten komen, specifiek op dit thema. Deze geïnterviewde laat ook weten het prettig te vinden als banken gebundeld aangiftes zouden doen, in plaats van dit aan de individuele klant over te laten. Aanvullend benoemd een andere geïnterviewde van de politie dat in de samenwerking met de banken nog veel winst is te behalen.

Vanuit de geïnterviewden van de politie is het duidelijk naar voren gekomen dat er een wens ligt voor grensoverschrijdende samenwerkingen. Dit komt door het verschil in slachtoffer- en daderplaats. Hier zit er voor de politie dus (naast de interventiespecialist, gebundelde aangiftes) nog een kans.

Over het algemeen gaven de banken aan dat contact tussen bijvoorbeeld Whatsapp en Snapchat kan helpen in de aanpak. De platformen waar VIN-fraude zich dus op afspeelt. Hier zit een kans voor de politie om met de data van social media platforms criminelen makkelijker op te sporen. Daarnaast werd breed onder de geïnterviewden gesteld dat de telecomproviders vitale data beheren voor de aanpak. Het feit dat social media platforms en telecomproviders geen verantwoordelijkheid nemen voor de aanpak van dit vraagstuk, maakt het niet bevorderlijk voor de aanpak van VIN-fraude.

Aan de preventiekant liggen er ook kansen. Bijvoorbeeld door aan mogelijke slachtoffers te communiceren hoe zij vormen van digitale criminaliteit eerder kunnen herkennen. In 2018 waren ruim 1,2 miljoen mensen slachtoffer van digitale criminaliteit. Dat blijkt uit een grootschalig onderzoek naar digitale veiligheid en criminaliteit van het Centraal Bureau voor de Statistiek (Politie, 2019). Hedendaags wordt één op de tien Nederlanders en één op de vijf MKB-bedrijven slachtoffers van digitale criminaliteit (Politie, 2021). Hier ligt dus een grote kans voor de aanpak van VIN-fraude.

Het OM werkt mee aan een strategische ontwikkeling genaamd ‘HUB’, deze ontwikkeling zorgt er met digitale kennis voor dat cybercrime beter kan worden aangepakt. Specifiek zorgt deze techniek voor inzicht welke zaken wel of niet opgepakt dienen te worden. De HUB kan worden gezien als een rad in verschillende raderen, stelt de geïnterviewde van het OM. Hierin ziet het OM een goede kans om cybercrime beter aan te pakken.

6 Conclusie

Nu de deelvragen volledig zijn beantwoord door de verschillende methodes van desk- en fieldresearch, kan de hoofdvraag worden beantwoord in dit hoofdstuk; conclusie.
De hoofdvraag in dit onderzoek luidt als volgt: **"In hoeverre werken de ketenpartners van de politie met hen samen op het gebied van VIN-fraude en wie draagt welke verantwoordelijkheid?"**

Samenwerking
Op het gebied van VIN-fraude en andere online fraudevormen is er een samenwerking actief tussen de politie en haar ketenpartners. Echter, is het moeilijk informatie met elkaar te delen door de geldende privacywetgeving zoals de AVG waar deze organisaties aan gebonden zitten. De overdracht van informatie wordt hierdoor vertraagd. Wanneer er gekeken wordt naar het tegengaan van fysieke criminaliteit wordt er opsporing verricht in de buurt van het delict of het slachtoffer. Bij digitale criminaliteit is dit geen oplossing omdat deze criminaliteitsvorm grensoverschrijdend is. De slachtoffers en daders zijn niet aan dezelfde locatie te koppelen. Om deze fraudevorm toch zo goed mogelijk tegen te gaan hebben vele ketenpartners contact met elkaar en proberen zij elkaar van informatie te voorzien. De Vereniging van Nederlandse Gemeenten geeft aan voortdurend in overleg te zijn met het Openbaar Ministerie, Nationaal Cyber Security Centrum, burgemeester, politie, Ministerie van Justitie en Veiligheid en Nationaal Coördinator Terrorismebestrijding en Veiligheid. Gemeente Apeldoorn geeft in dit onderzoek aan vooral te leunen op de politie. De Nederlandse banken hebben een interbancair overleg waar deze zaken in besproken worden. De banken kunnen meer informatie inzien over klanten dan dat de klanten over zichzelf kunnen inzien. De banken kunnen deze informatie voor opsporingsdoeleinden overhandigen aan de politie.

Verantwoordelijkheid
De verantwoordelijkheid van de ketenpartners zijn uiteenlopend, passend bij de organisatie en functie. De overheid, gemeente en burgemeester richten zich op de preventiekant van dit probleem. De burgemeester staat voor de orde en veiligheid in zijn of haar gemeente en probeert de burgers veilig te houden door hen vooraf te informeren en voor te lichten. De politie neemt ook haar verantwoordelijkheid in het preventiestuk, maar heeft als belangrijkste taak de daders op te sporen en te laten vervolgen. Dit wordt gecontroleerd door het Ministerie van Justitie en Veiligheid, zij schrijven het beleid en voeren de controle uit. Wanneer er een verdachte is gevonden neemt het OM de taak op zich deze persoon te vervolgen. Ook hebben zij contact met andere landen en informeren zij burgers. Betreffende VIN-fraude worden de geldtransacties via de banken gedaan. De banken sporen frauduleuze transacties op en delen deze informatie met de politie en het OM.

Vanuit organisaties als Whatsapp, Facebook, Microsoft en telefoonproviders wordt nog niet de gewenste verantwoordelijkheid getoond. Deze organisaties zijn een belangrijke schakel in het VIN-fraude proces en daarom belangrijk mee samen te werken.

Kansen
De banken geven aan geen contact en/of samenwerking met verschillende *social media* bedrijven te kunnen krijgen als Snapchat en Whatsapp, terwijl dit belangrijke samenwerkingsverbanden kunnen opleveren. Deze bedrijven zouden hun regels betreffende veiligheid voor hun klanten hoger op hun prioriteitenlijst kunnen zetten en de samenwerking aangaan om dit te realiseren.

Verder zou verbetering gevonden kunnen worden in de samenwerking met ketenpartners en al hun onderlinge kansen. Zo ziet de ABN Amro graag een betere samenwerking met banken onderling en zou het prettig zijn als overheidsinstellingen sneller informatie delen. De ING en Rabobank hebben behoefte aan ingangen bij WhatsApp en Snapchat.

Het Openbaar Ministerie kan en wil nog meer uit hun samenwerkingsverband (HUB) halen en dit verder doorvoeren binnen de politie. Voor alle gemeentes en de VNG is het zaak nog meer te investeren in de preventieve kant van cybercrime.

Naast deze missende organisaties dient er tussen de samenwerkende partijen nieuwe protocollen, procedures en afspraken te worden gemaakt volgens de VNG. Er dient grensoverschrijdend met elkaar te worden samengewerkt (landelijke samenwerking). Hierdoor wordt de informatiedeling hopelijk makkelijker. Daarnaast is het voor iedere betrokken partij belangrijk te kijken welke verantwoordelijkheid zij dienen te nemen. De politie ziet het tegengaan van online fraude positief in wanneer er in elke eenheid een interventiespecialist wordt aangenomen en wanneer er meer landelijke teams worden ingericht. Dit wordt nog duidelijker in de aanbeveling. Het Openbaar Ministerie ziet kansen in de HUB. Dit samenwerkingsverband bundelt namelijk alle aangiftes direct bij binnenkomst en bekijkt welke opgepakt moeten worden. Hierdoor wordt er veel sneller geacteerd op aangiftes van online fraude.

7 Aanbevelingen

In de conclusie is duidelijk geworden dat er een actieve samenwerking is tussen de ketenpartners van de politie, alleen bemoeilijkt wetgeving de informatiewisseling. De mate van verantwoordelijkheid voor de aanpak van cybercrime is uiteenlopend onder diezelfde ketenpartners. De verantwoordelijkheden zijn specifiek gericht op functie en organisatie. Voor de aanbeveling is het zaak om te kijken naar de kansen voor de politie en in de samenwerking tussen haar ketenpartners.

Een kans om cybercrime zo veel mogelijk tegen te gaan is door de samenwerkingsstructuur te vernieuwen. Momenteel worstelt de politie met welk veiligheidsgebied welke zaak oppakt. Vanuit de vroegere traditionele criminaliteit is de politie gewend de fysieke zaken op te pakken die in hun eigen gebied plaatsvinden. Doordat digitale criminaliteit grensoverschrijdend is (de daderplaats en slachtofferplaats is vaak verschillend), is het onduidelijk wie de zaak oppakt.

Om deze verwarring te voorkomen zou het waardevol zijn als er landelijke teams ingericht worden (Politie, persoonlijke communicatie, 5 april 2022). Daarbij heeft de politie de behoefte om in elke eenheid een interventiespecialist toe te voegen, wiens werk gericht is op deze digitale fraudes. Daarnaast is het raadzaam om meer te investeren aan de voorkant. Het is waardevol om meer samenwerking te zoeken met partners, zoals overheden, banken en telecomproviders, om tot een beter preventiepakket te komen (Politie, persoonlijke communicatie, 11 mei).

Tot slot is het waardevol om te werken aan een beter preventiepakket voor betere informatiedeling. Daarnaast ligt er een grote verbetering om de samenwerking uit te breiden met actoren zoals Whatsapp, Instagram en Snapchat en met telefoonproviders. Deze actoren kan meer verantwoordelijkheid worden opgelegd en daarom is het van belang om als politieorganisatie een actieve samenwerking met deze partijen te zoeken.

8 Discussie

Betrouwbaarheid, Validiteit en bruikbaarheid

In het theoretisch kader is eerder al beschreven dat dit onderzoek betrouwbaar en valide moet zijn. Betrouwbaarheid is de mate waarin het onderzoek vrij is van (toevallige) fouten. Het onderzoek is betrouwbaar als het onderzoek herhaalbaar met dezelfde uitkomst is, de onderzoeker het eens is met de resultaten en wanneer de onderzoeker onafhankelijk is. Daarnaast moet het onderzoek weerlegbaar en openbaar zijn (Verhoeven, 2018). Het herhalen van dit onderzoek is mogelijk, doordat er bij een herhaling van de deskresearch dezelfde uitkomsten bereikt zullen worden. Echter, is de herhaalbaarheid van de informatie verkregen uit interviews discussieerbaar. Mogelijk zal een interview met een andere respondent van dezelfde instantie tot een andere uitkomst kunnen leiden. In de vragen werd namelijk ingegaan op persoonlijke ervaringen en adviezen. Deze kunnen per persoon verschillen, ongeacht hun functie, en kunnen dus leiden tot een andere uitkomst.

Dit onderzoek bevat ook triangulatie, wat betekent dat we gebruik hebben gemaakt van verschillende methodes. Er is gebruik gemaakt van diepte-interviews en deskresearch met verschillende literatuurcreaties (Verhoeven, 2018b). Er is gebruik gemaakt van primaire literatuur, secundaire literatuur en grijze literatuur. Primaire literatuur verwijst naar een wetenschappelijk artikel waar het voor het eerst wordt behandeld, secundaire literatuur naar auteurs die rapporteren over een al behandeld onderwerp waarin nieuwe inzichten worden aangegeven en grijze literatuur naar onder andere beleidsstukken van ministeries en jaarverslagen.

Validiteit geeft aan of er gemeten is wat de onderzoeker wilde weten en of dat ook op de juiste manier is gedaan, zonder systematische fouten. Hierbij moet de steekproef generaliseerbaar zijn naar de populatie van het onderzoek. De steekproef moet volgens willekeurig en voldoende groot zijn (Verhoeven, 2018).

Dit onderzoek is valide, omdat er in totaal tien personen geïnterviewd zijn. Hiervan waren vier personen afkomstig uit de politieorganisatie, drie personen vanuit de bankenwereld, één persoon vanuit het Openbaar Ministerie, één persoon vanuit de gemeente Apeldoorn en één persoon vanuit de VNG. De hoeveelheid en verscheidenheid aan geïnterviewde personen, maakt de steekproef voldoende groot. Daarbij voldoet het onderzoek ook aan de interne validiteit, doordat er bij de interviews gebruik is gemaakt van dezelfde instrumentatie.

Bij elk interview is gebruik gemaakt van het zogenoemde ongestructureerd interview/diepte-interview. Dat houdt in dat een lijst met onderwerpen, ook wel een topiclijst of gesprekspuntenlijst, is aangehouden. Door de lijst met open vragen aan te houden blijft de rode draad hetzelfde, maar is er ruimte voor eigen inbreng van de respondent (Verhoeven, 2018a). Er is gekozen voor het gebruik van diepte-interviews omdat het voor dit onderzoek van belang was dezelfde rode draad aan te houden en omdat de respondenten uit verschillende sectoren afkomstig waren waardoor de inbreng van de respondent verschilt. Door gebruik te maken van diepte-interviews kon er gereageerd worden op het verhaal van de respondent door het in context te plaatsen en op zijn of haar antwoorden te reageren. Het alternatief, enquêtes biedt geen gelegenheid om door te vragen op specifieke onderwerpen die verschillen per respondent. Met als gevolg dat bruikbare informatie gemist zou worden.

Beperkingen onderzoek

Tijdens dit onderzoek is contact gezocht met allerlei verschillende actoren, met een verzoek voor een interview of vragenlijst. Hierop hebben tien personen ingestemd, maar zijn er ook zes afwijzingen binnengekomen. De NCTV, het Ministerie van Justitie en Veiligheid, WhatsApp, Fox-IT, de Bunq bank en de SNS konden allemaal om verschillende redenen niet meewerken aan dit onderzoek. Het NCSC gaf aan dat zij zich niet met dit onderwerp bezighielden. De exacte verslagleggingen van deze afwijzingen zijn te vinden in bijlage 2.11.

Het gebrek aan contact met deze actoren, heeft geleid tot beperkingen in dit onderzoek. Door deze afwijzingen, ontstond er een informatietekort betreft deze actoren en zijn er mogelijk bepaalde invalshoeken niet belicht. In dit onderzoek is er diep ingegaan op de informatie verkregen uit de interviews met de respondenten, maar is er minder diep ingegaan op de actoren die niet zijn geïnterviewd.

Suggesties vervolgonderzoek

We raden sterk aan om in het vervolgonderzoek rekening te houden met het benodigde tijdspad voor interviews. Het is niet dat daar te weinig tijd voor is gepland of geen rekening is gehouden met actoren die niet of moeilijk te bereiken waren, maar het heeft in enkele gevallen flinke moeite gekost om contact te krijgen met relevante actoren. Een aantal actoren wilden niet meewerken om verschillende redenen. Het is van belang op tijd te weten welke actoren je wilt spreken en een andere actor als back-up te hebben.

De ontwikkeling van online fraude methoden gaat ontzettend snel. Dit kan als gevolg hebben dat bepaalde delen van ons onderzoek al snel minder of niet meer relevant zijn, gezien dit specifiek op VIN-fraude is gericht. Het kan bijvoorbeeld zijn dat iedereen binnen een jaar of twee niet meer in VIN-fraude trapt en dat oplichting door deep fakes de nieuwste fraudemethode is. Inspelen of in kaart brengen van toekomstige fraudemethoden kan relevant zijn.

Het aantal actoren die met VIN-fraude en online fraude te maken hebben is groot en zal waarschijnlijk in de toekomst groter worden. Dit heeft als gevolg dat we aanraden om een apart onderzoek te doen naar de burger/inwoner als actor. Daar is in dit onderzoek maar beperkt aandacht aan besteden.

9 Literatuurlijst

AlleCijfers (2022). *Héél véél informatie over Apeldoorn.* Geraadpleegd op 18 maart 2022, van https://allecijfers.nl/gemeente/apeldoorn/

Benders, L. (2021*). Veldonderzoek (fieldresearch) doen voor je scriptie*. Geraadpleegd op 18 maart 2022, van https://www.scribbr.nl/onderzoeksmethoden/fieldresearch-veldonderzoek/

Betaalvereniging Nederland. (2021, 1 juli*). Ken uw klant in het kort*. Geraadpleegd op 14 april 2022, van https://www.betaalvereniging.nl/actueel/achtergrondinformatie/in-het-kort/ken-uw-klant-in-het-kort/

Bhandari, P. (2021). *Een introductie tot kwantitatief onderzoek*. Geraadpleegd op 18 maart 2022, van https://www.scribbr.nl/onderzoeksmethoden/kwantitatief-onderzoek/

Bhandari, P. (2022*). Een introductie tot kwalitatief onderzoek*. Geraadpleegd op 18 maart 2022, van https://www.scribbr.nl/onderzoeksmethoden/kwalitatief-onderzoek/

Binnenlandredactie. (2022, 2 april). *Politie: proef om na online fraude zelf geld terug te vorderen is een succes*. Geraadpleegd op 15 april 2022, van https://www.ad.nl/binnenland/politie-proef-om-na-online-fraude-zelf-geld-terug-te-vorderen-is-een-succes~a43fc496/

BNNVARA. (2022, 17 januari). *Winkeldiefstallen namen af, cybercrime nam toe in 2021*. Geraadpleegd op 8 maart 2022, van https://www.BNNVARA.nl/kassa/artikelen/winkeldiefstallen-namen-af-cybercrime-nam-toe-in-2021

Boekhoorn, P. (2019). *De aanpak van cybercrime door regionale eenheden van de politie*. Geraadpleegd op 17 maart 2022, van https://open.overheid.nl/repository/ronl-ab43a1df-1d25-4cbe-8d26-3c332dcee2e9/1/pdf/tk-bijlage-de-aanpak-van-cybercrime-door-regionale-eenheden-van-de-politie.pdf

Centraal Bureau voor de Statistiek. (2019, 2 maart). *Veiligheidsbeleving - Veiligheidsmonitor 2019*. Geraadpleegd op 18 maart 2022, van https://longreads.cbs.nl/veiligheidsmonitor-2019/veiligheidsbeleving/

Centraal Bureau voor de Statistiek. (2020, 2 maart). *Minder traditionele criminaliteit, meer cybercrime.* Geraadpleegd op 17 maart 2022, van https://www.cbs.nl/nl-nl/nieuws/2020/10/minder-traditionele-criminaliteit-meer-cybercrime

Centraal Bureau voor de Statistiek. (2022, 1 maart). *2,5 miljoen Nederlanders in 2021 slachtoffer van online criminaliteit.* Geraadpleegd op 15 april 2022, van https://www.cbs.nl/nl-nl/nieuws/2022/09/2-5-miljoen-nederlanders-in-2021-slachtoffer-van-online-criminaliteit

Centraal Bureau Voor Statistiek. (2022, 1 maart). *Veiligheidsmonitor 2021*. Geraadpleegd op 14 april 2022, van https://www.cbs.nl/nl-nl/publicatie/2022/09/veiligheidsmonitor-2021

Consultancy.nl. (2017). *Ketensamenwerking vraagt om fundamentele verandering in mindset.* Geraadpleegd op 18 maart 2022, van https://www.consultancy.nl/nieuws/13370/ketensamenwerking-vraagt-om-fundamentele-verandering-in-mindset

Consumentenbond (z.d.). *Vergoed bankoplichting*. Geraadpleegd op 26 maart 2022, van https://www.consumentenbond.nl/acties/vergoed-bank-oplichting

Cybercrimeinfo (z.d.*). Vriend-in-nood-fraude (VIN fraude)*. Geraadpleegd op 22 maart 2022, van https://www.cybercrimeinfo.nl/cybercrime/vriend-in-nood-fraude-vin-fraude

Data&Privacyweb. (2021, 29 oktober*). Grote rol NCSC in onderzoek opgerolde ransomware bende*. Geraadpleegd op 17 april 2022, van https://privacy-web.nl/nieuws/grote-rol-ncsc-in-onderzoek-opgerolde-ransomware-bende/

Data&Privacyweb. (2022, 7 januari). *Klanten eisen meer actie van banken tegen fraude*. Geraadpleegd op 14 april 2022, van https://privacy-web.nl/nieuws/klanten-eisen-meer-actie-van-banken-tegen-fraude/

De Nederlandse Bank. (z.d.) *Cybercrime*. Geraadpleegd op 14 april 2022, van https://www.dnb.nl/innovatie-in-betalen-en-bankieren/cybercrime/

De Waal, B., Tukker, S. (2020). *Opvallende stijging aangiftes van online fraude tijdens coronacrisis: 'Vooral kwetsbaren en ouderen zijn slachtoffer'*. Geraadpleegd op 11, april 2022, van https://eenvandaag.avrotros.nl/item/opvallende-stijging-aangiftes-van-online-fraude-tijdens-coronacrisis-vooral-kwetsbaren-en-ouderen/

Deiters, E. (2022). *Cybercrime is het nieuwe verdienmodel voor criminelen*. Blauw, 1, 31-36.

Gemeente Lelystad. (2022, 15 april). *Hulpvraagfraude (via WhatsApp*. Geraadpleegd op 16 april 2022, van https://www.lelystad.nl/4/seniorenenveiligheid/hulpvraagfraude.html

George, T. (2021). *Een introductie tot mixed methods onderzoek*. Geraadpleegd op 18 maart 2022, van https://www.scribbr.nl/onderzoeksmethoden/mixed-methods/
Geraadpleegd op 5 juni 2022, van https://www.mijnzakengids.nl/digitalisering-gemeenten-onvermijdelijk/

Het Nederlands Genootschap van Burgemeesters. (z.d.). *Algemene bevoegdheid ter handhaving openbare orde.* Geraadpleegd op 28 maart 2022, van https://www.burgemeesters.nl/themas/bevoegdheden/algemene-bevoegdheid-ter-handhaving-openbare-orde/

Het Nederlands Genootschap van Burgemeesters. (z.d.). *Politiewet 2012.* Geraadpleegd op 28 maart 2022, van https://www.burgemeesters.nl/themas/bevoegdheden/politiewet-2012/
https://www.dnb.nl/innovatie-in-betalen-en-bankieren/cybercrime/

Infopolitie. (2022). *De politie vanaf 2013*. Geraadpleegd op 18 maart 2022, van https://www.infopolitie.nl/index.php/algemene-categorie/jeugd/58-jeugdhoek/spreekbeurt/2709-de-politie-vanaf-2013

Junger, M., Veldkamp, B., & Koning, L. (2022, maart). *Fraudevictimisatie in Nederland (Nr. 1).* Geraadpleegd op 7 april 2022, van https://www.utwente.nl/nl/bms/fraudvic/fraudevictimisatie-in-nederland.pdf

Kamerstukken II, kv-tk-2020Z29911, (2021, 18 juni). Geraadpleegd op 16 april 2022, van https://zoek.officielebekendmakingen.nl/kst-29911-314.html

Klaassen, N. (2020). *Bestrijding virus gaat nieuwe fase in: Nederlanders moeten thuiswerken, evenementen geschrap*t. Geraadpleegd op 7 april 2022, van https://www.ad.nl/binnenland/bestrijding-virus-gaat-nieuwe-fase-in-nederlanders-moeten-thuiswerken-evenementen-geschrapt~a68a48c9/

Krul, A. (2021) *Hoe voer je deskresearch uit*? Geraadpleegd op 18 maart 2022, van https://www.scribbr.nl/onderzoeksmethoden/deskresearch/

Leukfeldt, R., Malsch, M., & Notté, R. (2019). *Slachtofferschap van online criminaliteit kan ingrijpend zijn.* Geraadpleegd op 18 maart 2022, van https://ccv-secondant.nl/platform/article/slachtofferschap-van-online-criminaliteit-kan-ingrijpend-zijn%20delen

Ministerie van Justitie en Veiligheid. (2018, 27 juni). *Ontwikkelingen in de taakuitvoering van de politie.* Geraadpleegd op 18 maart 2022, van https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2021/12/17/ek-bijlage-10-ontwikkelingen-in-de-taakuitvoering-van-de-politie/ek-bijlage-10-ontwikkelingen-in-de-taakuitvoering-van-de-politie.pdf

Ministerie van Justitie en Veiligheid. (2019, 28 februari). *Nieuwe wet versterkt bestrijding computercriminaliteit*. Geraadpleegd op 28 maart 2022, van https://www.rijksoverheid.nl/actueel/nieuws/2019/02/28/nieuwe-wet-versterkt-bestrijding-computercriminaliteit

Ministerie van Justitie en Veiligheid. (2021, 19 april). *ABN AMRO betaalt 480 miljoen euro vanwege ernstige tekortkomingen bij het bestrijden van witwassen*. Geraadpleegd op 14 april 2022, van https://www.om.nl/actueel/nieuws/2021/04/19/abn-amro-betaalt-480-miljoen-euro-vanwege-ernstige-tekortkomingen-bij-het-bestrijden-van-witwassen

Ministerie van Justitie en Veiligheid. (2006). Witwassen. Justitiële verkenningen, 44. http://doi.org/10.5553/JV/016758502021047004005

Ministerie van Justitie en Veiligheid. (z.d.). *Nationaal Cyber Security Centrum*. Geraadpleegd op 30 maart 2022, van https://www.nctv.nl/onderwerpen/nationaal-cyber-security-centrum

Nationaal Cyber Security Centrum. (2021, 16 november). *Cybersecuritybeeld Nederland*. Geraadpleegd op 17 april 2022, van https://www.ncsc.nl/onderwerpen/cyber-security-beeld-nederland

Nationaal Cyber Security Centrum. (2022). *Nederland digitaal veilig*. Geraadpleegd op 10 maart 2022, van https://www.ncsc.nl/

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2020). *Cybersecuritybeeld Nederland*. Geraadpleegd op 17 maart 2022, van https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2020/juni/29/csbn-2020/CSBN+2020.pdf

Nederlandse Verenging van Banken. (2021, 4 juni). *Toetsingscriteria voor coulance bij bankhelpdesk fraude*. Geraadpleegd op 18 april 2022, van https://www.nvb.nl/nieuws/toetsingscriteria-voor-coulance-bij-bankhelpdesk-fraude-spoofing/

Nederlandse Vereniging van Banken (z.d.) *Toetsingscriteria voor coulance bij bankhelpdesk fraude (spoofing*). Geraadpleegd op 26 mei 2022, van https://www.nvb.nl/nieuws/toetsingscriteria-voor-coulance-bij-bankhelpdesk-fraude-spoofing/

Nederlandse Vereniging van Banken. (z.d.). *De bank en uw gegevens*. Geraadpleegd op 13 maart 2022, van https://www.nvb.nl/bank-en-data/de-bank-en-uw-gegevens/#:%7E:text=Bijvoorbeeld%3A%20uw%20bank%20moet%20met,producten%20en%20diensten%20te%20wijzen.

Obbink, S. (2022, 28 maart) Persoonlijke communicatie.

Oerlemans, J., Custers, B., Pool, R., & Cornelisse, R. (2016). Cybercrime en witwassen. Uitgeverij Boom

Online Markering Agency (2021*). Wat is een Doelgroep?* Geraadpleegd op 18 maart 2022, van https://onlinemarketingagency.nl/marketingtermen/doelgroep/

Oosterveer, D. (2022, 29 januari). *Social media in Nederland 2022: WhatsApp minder intensief gebruikt, opmars TikTok zet door.* Geraadpleegd op 13 juni 2022, van https://www.marketingfacts.nl/berichten/social-media-in-nederland-2022/

Openbaar Ministerie. (2022). *Wat is cybercrime en digitale criminaliteit*? Geraadpleegd op 28 april 2022, van https://www.om.nl/onderwerpen/cybercrime

Openbaar Ministerie. (z.d.). *Aanpak cybercrime*. Geraadpleegd op 28 maart 2022, van https://www.om.nl/onderwerpen/cybercrime/aanpak-cybercrime

Openbaar Ministerie. (z.d.). *Cybercrime*. Geraadpleegd op 21 maart 2022, van https://www.om.nl/onderwerpen/cybercrime

Openbaar Ministerie. (z.d.). *Het werk van het OM*. Geraadpleegd op 21 maart 2022, van https://www.om.nl/onderwerpen/cybercrime

Openbaar Ministerie. (z.d.). *Rol Openbaar Ministerie in het Nederlands strafrecht*. Geraadpleegd op 16 juni 2022, van https://www.om.nl/onderwerpen/mh17-vliegramp/rol-om-in-nederlands-strafrecht

Parlement. (2022). *Gemeente*. Geraadpleegd op 18 maart 2022, van https://www.parlement.com/id/vic0lcq0aryx/gemeente

Parlement. (2022). Ministerie. Geraadpleegd op 16 juni 2022, van https://www.parlement.com/id/vh8lnhronvwm/ministerie#:~:text=De%20voorbereiding%20van%20beleid%2C%20wetten,rechtspersonen%20met%20een%20wettelijke%20taakParlement

Politie. (2019). *Beroepscode politie*. Geraadpleegd op 17 maart 2022, van https://kombijde.politie.nl/binaries/content/assets/academie/algemeen/beroepscode-politie-8-jan-2017.pdf

Politie. (2020, 1 december). *Politie investeert in digitale fitheid*. Geraadpleegd op 28 maart 2022, van https://www.politie.nl/nieuws/2020/december/1/politie-investeert-in-digitale-fitheid.html

Politie. (2020, 15 oktober). Landelijke aanpak WhatsApp-fraude. Geraadpleegd op 28 maart 2022, van https://www.politie.nl/nieuws/2020/oktober/15/00-landelijke-aanpak-whatsapp-fraude.html

Politie. (2021, 15 april). *'Investeer in aanpak cybercrime'*. Geraadpleegd op 15 april 2022, van https://www.politie.nl/nieuws/2021/april/15/investeer-in-aanpak-cybercrime.html

Politie. (2021, 15 januari). *Criminaliteit 2020: minder inbraak, meer cybercrime*. Geraadpleegd op 28 maart 2022, van https://www.politie.nl/nieuws/2021/januari/15/00-criminaliteit-2020-minder-inbraak-meer-cybercrime.html

Politie. (2021, 8 maart). *Politie Vleuten–De Meern organiseert digitale veiligheidsmaand*. Geraadpleegd op 11 april 2022, van https://www.politie.nl/nieuws/2021/februari/25/03-weet-jij-alles-over-digitale-veiligheid-politie-vleuten-de-meern-organiseert-digitale-veiligheidsmaand.html

Politie. (2021). *Jaarverantwoording 2020 in teken van corona.* Geraadpleegd op 11 april 2022, van https://www.politie.nl/nieuws/2021/mei/19/jaarverantwoording-2020-in-teken-van-corona.html

Politie. (z.d.). *Kerntaken politie*. Geraadpleegd op 14 maart 2022, van https://www.politie.nl/informatie/kerntaken-politie.html

Politie. (z.d.). *Wat kan ik zelf doen om geen slachtoffer te worden van cybercrime*? Geraadpleegd op 17 maart 2022, van https://www.vraaghetdepolitie.nl/misdaad-en-geweld/oplichting/wat-kan-ik-zelf-doen-om-geen-slachtoffer-te-worden-van-cybercrime.html

PVO. (z.d.) *Hoe digitaliseert criminaliteit?* Geraadpleegd op 11 april 2022, van https://www.pvo-oostnederland.nl/cybercrime-alert/hoe-digitaliseert-criminaliteit/

Rabobank. (2021, maart). *Annual Report 2020 Rabobank. Rabobank Communications & Corporate Affairs.* Geraadpleegd op 18 maart 2022, van https://statics.rabobank.com/binaries-processed/annual-report-2020_931168957.pdf

Rabobank. (z.d.). De dynamiek van ethiek. Rabobank.Com. Geraadpleegd op 14 april 2022, van https://www.rabobank.com/nl/about-rabobank/in-society/ethics/index.html

Rabobank. (z.d.). *De toekomst van het bankwezen: de visie van de Rabobank.* Geraadpleegd op 14 april 2022, van https://www.rabobank.com/nl/about-rabobank/in-society/principles/The_future_of_the_banking_industry.html

Regioburgemeesters (z.d.) *Burgemeesters*. Geraadpleegd op 30 mei 2022, van https://regioburgemeesters.nl/thema/politiebestel/lokale-verankering-en-gezag/burgemeesters/#:%7E:text=De%20driehoek%20bestaat%20uit%20de,de%20voorzitter%20van%20het%20driehoeksoverleg.

Rijksoverheid. (z.d.). *Ministerie van Justitie en Veiligheid*. Geraadpleegd op 21 maart 2022, van https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid

Rijksoverheid. (z.d.). *Waar kan ik terecht met vragen over fraude als ik twijfel over een product of dienst?,* Rijksoverheid.nl. Geraadpleegd op 14 april 2022, van https://www.rijksoverheid.nl/onderwerpen/identiteitsfraude/vraag-en-antwoord/waar-kan-ik-terecht-met-vragen-over-fraude-als-ik-twijfel-over-een-product-of-dienst

RTL Nieuws. (2018). 'Crim*inaliteitscijfers eigenlijk veel hoger, bijna niemand doet aangifte'*.. Geraadpleegd op 11 april 2022, van https://www.rtlnieuws.nl/nederland/artikel/3886451/criminaliteitscijfers-eigenlijk-veel-hoger-bijna-niemand-doet-aangifte

RTL nieuws. (2021, 21 januari). "*Internetbank Bunq doet niet genoeg tegen oplichting*. Geraadpleegd op 14 april 2022, van https://www.rtlnieuws.nl/tech/artikel/5209930/online-bank-bunq-fraude-oplichting-phishing-naam-bankrekening

RTL nieuws. (2021, 15 april). *Enorme toename cybercrime in Nederland.* Geraadpleegd op 15 april 2022, van https://www.rtlnieuws.nl/tech/artikel/5225519/politie-cybercrime-oplichting-whatsapp-aangifte

Sabel, P. (2021). *Criminelen verleggen werkterrein naar internet: digitale criminaliteit in jaar tijd verdubbeld*. Geraadpleegd op 11 april 2022, van https://www.volkskrant.nl/nieuws-achtergrond/criminelen-verleggen-werkterrein-naar-internet-digitale-criminaliteit-in-jaar-tijd-verdubbeld~bc46a195/?referrer=https%3A%2F%2Fwww.google.com%2F

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

Slachtofferhulp Nederland. (2022, 19 mei). *Spoofing*. Geraadpleegd op 16 juni 2022, van https://www.slachtofferhulp.nl/gebeurtenissen/fraude/spoofing/#:%7E:text=Spoofing%20is%20een%20truc%20waarbij,tijd%20veel%20geld%20kan%20kwijtraken.

Smits, I., van der Laan, M., Ehrismann, M., & van der Burg, D. (2019). Onderzoek naar toegenomen mobiliteit en veranderingen in criminaliteit. Geraadpleegd op 16 juni 2022, van https://repository.wodc.nl/bitstream/handle/20.500.12832/2442/2997_volledige_tekst_tcm28-427558.pdf?sequence=2&isAllowed=y

Sparen.nl (z.d.). *Hoe werkt een bank*. Geraadpleegd op 16 juni 2022, van https://kennisbank.sparen.nl/hoe-werkt-een-bank

Stol, W. (2016). Basisboek integrale veiligheid (3de editie). Boomcriminologie.

Te Voert, I.T. (2018, 17 mei). *Digitalisering bij gemeenten onvermijdelijk*. Geraadpleegd op 16 juni 2022, van https://www.mijnzakengids.nl/digitalisering-gemeenten-onvermijdelijk/

Van der Klugt, G. (2022, 21 februari). *NCSC en partners lanceren Nederlands Security Meldpunt.* Techzine.nl. Geraadpleegd op 18 april 2022, van https://www.techzine.nl/nieuws/security/478063/ncsc-en-partners-lanceren-nederlands-security-meldpunt/

Van Erp, J., Stol, W., & Van Wilsem, J. (2013). Criminaliteit en criminologie in een gedigitaliseerde wereld. Tijdschrift voor Criminologie.

Van Koningsveld, T.J. (z.d.) *Witwassen: de fasen van het witwasproces getoetst*. Geraadpleegd op 5 juni 2022, van https://okcnl.nl/artikelen/Artikel%20Koningsveld%20OF%202008-4.pdf

Van Noordenburg, C. (2022). *Wat is veiligheidsbeleving?* Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Geraadpleegd op 18 maart 2022, van https://hetccv.nl/onderwerpen/veiligheidsbeleving/wat-is-veiligheidsbeleving/

Veilig bankieren. (2021, 22 december). *Meld fraude*. Veiligbankieren.nl. Geraadpleegd op 18 april 2022, van https://www.veiligbankieren.nl/meld-fraude/

Veilig internetten. (z.d.). *Welke soorten cybercrime zijn er?* Geraadpleegd op 10 april, van https://veiliginternetten.nl/thema/basisbeveiliging/cybercrime/welke-vormen-van-cybercrime-zijn-er/#:~:text=Bij%20spoofing%20nemen%20internetcriminelen%20een,veel%20voorkomende%20manier%20van%20spoofing.

Veilig Online. (2022). Ministerie van Economische Zaken en Klimaat. Geraadpleegd op 14 april 2022, van https://veiliginternetten.nl/media/documents/Alert_Online_2021_hoofdrapport_DEF.pdf

Verhoeven, N. (2018). Wat is onderzoek? Boom uitgevers Amsterdam.

Verhoeven, N. (2018a). hoofdstuk 9 kwalitatieve methoden van dataverzameling. In Wat is Onderzoek? (1ste editie, p. 147) Boom Lemma.

Verhoeven, N. (2018b). Hoofdstuk 9 Onderzoekskwaliteit. In Wat is onderzoek? (1ste editie, p. 169). Boom Lemma.

Vermeer, L. (2021, 22 februari). *Moet een bank de schade van WhatsApp-fraude vergoeden?*. Geraadpleegd op 26 maart, van https://bg.legal/moet-een-bank-de-schade-van-whatsapp-fraude-vergoeden

Versprille, I. M. (2016). De katvanger in beeld. Utrecht: Vrije Universiteit Amsterdam.

Voskuil, K. (2020, 12 oktober). *Misbruik geraffineerd: fraude met WhatsApp bijna verviervoudigd*, ad.nl. geraadpleegd op 12 mei 2022, van https://www.ad.nl/tech/misbruik-geraffineerd-fraude-met-whatsapp-bijna-verviervoudigd~af5f2d95/

Zuurmond, I. (2022, 11 januari). *Opvragen gegevens oplichter bij je bank*. consumentenbond.nl. Geraadpleegd op 18 april 2022, van https://www.consumentenbond.nl/betaalrekening/opvragen-gegevens-oplichter

10 Bijlagen

Bijlage 1 Actorenanalyse

	Bijlage 1.1 Politie
Taak en positie	De politie doet aan opsporen, voorkomen en verstoren van cybercrime. Dit doen ze samen met (internationale) partners. De positie van de politie is nog niet optimaal, aangezien zij vaak nog achter de feiten aanlopen en de technologische kennis hun veelal te snel gaat (Boekhoorn, 2019).
Belang	De politie staat voor een veilig Nederland, handhaaft de wet en beschermt de democratie (Politie, 2019).
Dominante perceptie van het probleem	Er vindt een verbreding van het criminele takenpakket plaats binnen bestaande dadergroepen. De politie heeft momenteel een achterstand in de aanpak van cybercrime (Boekhoorn, 2019).
Ter beschikking staande machtsbronnen	De politie bezit verschillende machtsbronnen: afgedwongen macht (ze kunnen dreigen met een straf), legitieme macht (ze hebben wettelijk gezag) en expertise macht (ze bezitten kennis).
Dominante afhankelijkheidspatronen	Allerlei actoren zijn afhankelijk van de politie omtrent cybercrime. De politie moet namelijk de criminaliteit opsporen, maar het ook zoveel mogelijk zien te voorkomen. Zo is de gemeente bijvoorbeeld een partij die erg afhankelijk is van de politie. De gemeente Apeldoorn geeft aan dat de politie op dit moment het beste beeld heeft van wat er speelt qua criminaliteit. De gemeente is nog zoekende in deze digitale criminaliteit en is dus afhankelijk van de kennis van de politie (Gemeente Apeldoorn, persoonlijke communicatie, 26 april 2022). Andersom is de politie ook afhankelijk van de gemeente, vooral op het gebied van preventie (Politie, persoonlijke communicatie, 11 mei 2022). Daarnaast is de politie ook afhankelijk van banken en telecombedrijven op het gebied van informatievoorziening (Politie, persoonlijke communicatie, 5 april 2022). De politie kan namelijk een vordering doen, waarbij banken zo snel mogelijk de informatie over verdachte transacties moeten delen.

Dominante perceptie van relevante aanpakken	Een aanpak om cybercrime zo veel mogelijk tegen te gaan is door de samenwerkingsstructuur te vernieuwen. Momenteel worstelt de politie ermee welk veiligheidsgebied welke zaak oppakt. Vanuit de vroegere traditionele criminaliteit is de politie gewend de fysieke zaken op te pakken die in hun eigen gebied plaatsvinden. Maar doordat cybercrime grensoverschrijdend is (de daderplaats en slachtofferplaats is vaak verschillend), is het vaak onduidelijk wie de zaak oppakt. Om deze verwarring te voorkomen moeten er landelijke teams ingericht worden (Politie, persoonlijke communicatie, 5 april 2022). Daarnaast stelt de politie voor om in elke eenheid een interventiespecialist toe te voegen, wiens werk gericht is op deze digitale fraudes (Politie, persoonlijke communicatie, 5 april 2022). Tot slot zou er meer geïnvesteerd moeten worden aan de voorkant. Er moet meer samenwerking gezocht worden met partners om tot een beter preventiepakket te komen (Politie, persoonlijke communicatie, 11 mei 2022).
Gevolgen en te verwachten strategische interactiepatronen	De politie werkt met veel partijen samen rondom cybercrime. Zo heeft de politie samengewerkt in een proef met Landelijke Associatie van Gerechtsdeurwaarders (LAVG) en de Service Organisatie Directe Aansprakelijkstelling (SODA) waarin slachtoffers hun geld konden terugvorderen (Binnenlandredactie, 2022). De politie werkt ook samen met hogescholen en universiteiten om meer kennis te vergaren over online fraude en de financiële/psychologische impact op de slachtoffers (Junger et al., 2022). Daarnaast werken ze samen met hun ketenpartners zoals gemeentes, banken en het Openbaar Ministerie. In de toekomst wenst de politie overkoepelend samen te gaan werken op landelijk niveau (Politie, persoonlijke communicatie, 5 april 2022).

	Bijlage 1.2 Banken (ABN AMRO, Rabobank, ING)
Taak en positie	Een bank heeft veel verschillende taken en posities maar hier wordt alleen benoemd wat relevant is voor dit onderzoek. Zorgen dat klanten hun geld kunnen opnemen, het verstrekken van leningen en veilig betalingsverkeer beheren. Het tegengaan van witwassen en fraude (https://kennisbank.sparen.nl/hoe-werkt-een-bank).
Belang	Banken willen cybercrime tegengaan om klanten te beschermen en het imago van de banken (persoonlijk communicatie, 30 mei 2022).
Dominante perceptie van het probleem	Cybercrime is een probleem. Cybercriminelen verzinnen steeds weer in nieuwe manier om cybercrime te plegen. Ook is het een vorm van criminaliteit die in een rap tempo stijgt (persoonlijke communicatie, 12 mei 2022).
Ter beschikking staande machtsbronnen	Specifieke professionele kennis en vaardigheden van personeelsleden (hangt af van de grote van de bank maar het gaat al gauw om 1000 personeelsleden of meer), daarnaast is de software om dubieuze transacties op te sporen een machtsbron van de banken. Ook de bevoegdheden van de banken om rekeningen te blokkeren is een vorm van macht. Daarnaast bezit de bank over veel informatie en financiën. Machtsbronnen zijn: Informatie, bevoegdheden, systemen, financiën, kennis (persoonlijke communicatie, 30 mei 2022).
Dominante afhankelijkheidspatronen	Banken zijn afhankelijk van de overheid voor een stukje preventie. Banken hebben onderling ook een afhankelijkheid ven elkaar. Zij vormen namelijk gezamenlijk het imago van de bankensector. Als de ING bij wijzen van spreken gehackt wordt, dan heeft de gehele sector daar last van (persoonlijke communicatie, 12 mei 2022). Daarnaast zijn andere actoren zoals het OM afhankelijk van de informatieverstrekking van de bank (persoonlijk communicatie, 30 mei 2022).
Dominante perceptie van relevante aanpakken	Banken zetten in op detectie van verdachte geldstromen. Daarnaast delen zij trends en communiceren zij dat met klanten en andere instanties, zoals

	politie. De communicatie naar klanten kan gezien worden als een vorm van preventie (persoonlijke communicatie, 30 mei 2022).
Gevolgen en te verwachten strategische interactiepatronen	Banken werken samen in een interbancair overleg. In dit overleg bespreken zij trends omtrent cybercrime. De ABN-AMRO geeft aan dat zij samenwerken met andere grote banken in Nederland, dit doen zij doormiddel van *security operation centers* die elkaar informeren. De ING geeft aan dat zij de aangiftes bij elkaar verzamelen, wat voor hen best ingewikkeld kan zijn. Wat de ING doet, ligt aan de behoefte van de politie, daar ondersteunen zij het opsporingsonderzoek waar mogelijk. De Rabobank geeft aan dat zij meerdere overlegvormen hebben met andere banken, met de NVB (Nederlandse Vereniging Banken) en daarnaast ook met de politie en het OM (persoonlijk communicatie, 30 mei 2022).

	Bijlage 1.3 Burgers
Taak en positie	Burgers zijn steeds minder vaak slachtoffer van traditionele criminaliteit, maar worden daarentegen juist vaker slachtoffer van *cybercrime* (CBS, 2020).
Belang	Burgers willen zich zowel online als offline veilig voelen en geen slachtoffer worden van (digitale) criminaliteit.
Dominante perceptie van het probleem	Digitale dreiging en cyberincidenten kunnen leiden tot maatschappij-ontwrichtende schade met grote gevolgen bij burgers (NCTV, 2020).
Ter beschikking staande machtsbronnen	Burgers hebben weinig machtsbronnen tegen *cybercrime*. Wel kunnen ze zichzelf beschermen door een aantal tips te hanteren, zoals: de computer te beveiligen, sterke wachtwoorden te kiezen, persoonlijke gegevens goed afschermen, het checken van het webadres tijdens internetbankieren (Politie, z.d.).
Dominante afhankelijkheidspatronen	Burgers zijn afhankelijk van de politie als het gaat om opsporen en het helpen voorkomen van *cybercrime*. Omgekeerd is de politie ook afhankelijk van burgers.

	Bijlage 1.4 Openbaar Ministerie
Taak en positie	Deelt mede met politie de aanpak van cybercriminaliteit (1) Het doel van het OM is om mensen op te sporen die zich schuldig maken aan cybercrime, alsmede het moeilijker maken voor criminele organisaties om cybercrime te plegen.
Belang	Belang om politie te ondersteunen bij de aanpak doormiddel van strafvordering.
Dominante perceptie van het probleem	Cybercrime vraagt om een nieuwe aanpak en aanpassingen van het OM. Dit is voor het OM zoeken naar bevoegdheden die passen bij de middelen die je wil inzetten Openbaar Ministerie, persoonlijke communicatie, 30 mei 2022).
Ter beschikking staande machtsbronnen	Het Openbaar Ministerie heeft als enige instantie in Nederland de macht om mensen te vervolgen (OM, z.d.).
Dominante afhankelijkheidspatronen	Het OM is afhankelijk van de informatie van banken. Het slachtoffer van online fraude kan ook veel informatie aanleveren, maar de banken ook zeker. Het OM doet een vordering en de banken zijn verplicht dit te leveren. Deze informatie moet zo snel mogelijk geleverd worden, dus in die zin is het OM afhankelijk van de informatievoorziening van banken (Openbaar Ministerie, persoonlijke communicatie, 30 mei 2022).
Dominante perceptie van relevante aanpakken	Het OM ziet de samenwerkingen binnen de HUB als een goede aanpak om cybercrime tegen te gaan. Binnen de HUB werkt het OM samen met de politie aan landelijke cybercrimezaken. Hierbij worden alle aangiftes direct wanneer ze binnenkomen bij elkaar gelegd en gebundeld, zodat gekeken kan worden welke zaken opgepakt moeten worden (Openbaar Ministerie, persoonlijke communicatie, 30 mei 2022).
Gevolgen en de te verwachten strategische interactiepatronen	Het Openbaar Ministerie geeft aan samen te werken vanuit de opsporing en vervolging met onder andere de politie en landelijk met het ECTF (*Electronic Crime Task Force*)

	Bijlage 1.5 Ministerie J&V
Taak en positie	De taak van het ministerie van J en V is het voorbereiden en het uitvoeren van regeringsbeleid. In dit geval beleid rondom cybercriminaliteit (Parlement, z.d.).
Belang	Het belang van het ministerie van J en V is het handhaven van onze rechtsorde en het veiliger en rechtvaardiger maken van onze samenleving. Hier is het ministerie immers verantwoordelijk voor (Rijksoverheid, z.d.).
Dominante perceptie van het probleem	Onbeantwoord
Ter beschikking staande machtsbronnen	Beloningsmacht, expertisemacht, netwerk, legitieme macht, Afgedwongen macht
Dominante afhankelijkheidspatronen	Afhankelijk van de uitvoerende partijen.
Dominante perceptie van relevante aanpakken	Het kabinet wil de komende jaren 26 miljoen euro beschikbaar stellen ter bestrijding van cybercrime. Naast het werven van extra personeel bij de politie voor inzet tegen cybercriminaliteit zowel landelijk als regionaal, wil het kabinet ook dat de politie zich meer bezig gaat houden met digitale forensische opsporing (sporenonderzoek). Voor het opsporen van oplichting, fraude en criminaliteit op het internet worden hoogopgeleide specialisten aangenomen (Rijksoverheid, z.d.).
Gevolgen en de te verwachten strategische interactiepatronen	Samenwerking met uitvoerende partijen.

	Bijlage 1.6 Gemeente
Taak en positie	De taak van de gemeente is helpen bij de preventie en ondersteuning van burgers met kennis en eventueel financiële middelen **(positie is nog onduidelijk, moet eigenlijk ook in interview duidelijk worden)**
Belang	De gemeenten willen dat hun inwoners veilig kunnen wonen in hun gemeenten en zich ook veilig voelen.
Dominante perceptie van het probleem	De taak van de gemeente is om haar inwoners veilig te laten voelen. De inwoners van de gemeente kunnen onwillig blootgesteld worden aan verschillende vormen van criminaliteit, waaronder ook digitale criminaliteit valt. Hierdoor kunnen de inwoners zich niet meer veilig voelen in hun eigen huis.
Ter beschikking staande machtsbronnen	De gemeente kan met haar communicatiemacht uitoefenen richting burgers. Door middel van campagnes en voorlichtingen kunnen ze kennis overdragen aan burgers en hiermee mogelijke slachtoffers voorkomen.
Dominante afhankelijkheidspatronen	De politie is afhankelijk van de gemeente, vooral op het gebied van preventie (Politie, persoonlijke communicatie, 11 mei 2022). Andersom geeft de gemeente Apeldoorn aan afhankelijk te zijn van de politie. De politie heeft nu het beste beeld van wat er speelt qua criminaliteit. De gemeente is nog zoekende in deze digitale criminaliteit en is daarin dus afhankelijk van de politie (Gemeente Apeldoorn, persoonlijke communicatie, 26 april 2022).
Dominante perceptie van relevante aanpakken	De gemeente vindt het belangrijk te focussen op preventie. Inwoners verwachten dit ook van haar gemeente. De gemeente zet in op campagnes, duidelijke voorlichtingen en sessies voor jongeren. Ook werken ze aan de bewustwording van digitale criminaliteit specifiek bij ondernemers (Gemeente Apeldoorn, persoonlijke communicatie, 26 april 2022).
Gevolgen en de te verwachten strategische interactiepatronen	Binnen de gemeente wordt samengewerkt om cybercrime aan te pakken. Dit doen verschillende afdelingen in de gemeente samen met bijvoorbeeld jongerenwerkers en het jongerenloket. Ook is er een samenwerking met de politie en het OM. Gemeente Apeldoorn leunt volgens eigen zeggen op de

	politie als het gaat om de samenwerking rondom VIN-fraude. (Gemeente Apeldoorn, persoonlijke communicatie, 26 april 2022).

	Bijlage 1.7 VNG
Taak en positie	De Vereniging van Nederlandse Gemeenten is een vereniging die alle gemeenten vertegenwoordigd. De vereniging heeft vooral een agendasettende taak bij overheden.
Belang	Het belang van deze organisatie is om de belangen van alle Nederlandse gemeenten te vertegenwoordigen.
Dominante perceptie van het probleem	De nieuwe vorm van criminaliteit staat hoog op de agenda (VNG, persoonlijke communicatie, 11 april 2022). De VNG ziet cybercrime als een dreiging waarop gemeenten voorbereid moeten zijn.
Ter beschikking staande machtsbronnen	Beïnvloeding van organisaties/overheden door middel van netwerk. Groot bereik en erg bekende organisatie. Tevens geeft het VNG duidelijkheid over het ingewikkelde web van wetgeving (VNG, persoonlijke communicatie, 11 april 2022).
Dominante afhankelijkspatronen	Afhankelijk van input Nederlandse gemeenten. Het VNG treedt namelijk gezamenlijk op, waardoor zij een sterke afhankelijkheid hebben van de gemeenten die lid zijn.
Dominante perceptie van relevante aanpakken	Aanpak richt zich vooral op de preventiekant. Vooral communicatieve aanpakken worden geïmplementeerd in gemeentebeleid.
Gevolgen en de te verwachten strategische interactiepatronen	Momenteel heeft de VNG voortdurend overleg met allerlei ketenpartners: burgemeesters, politie, het Openbaar Ministerie, het Ministerie van Justitie en Veiligheid, het NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid), NCSC (Nationaal Cyber Security Centrum) en hun eigen beleidsafdelingen.