Cybercriminelen in de verhoorkamer

Een verkennende studie naar het verhoor van verdachten van hackdelicten

Masterscriptie Opsporingscriminologie

Faculteit der Rechtsgeleerdheid

Vrije Universiteit Amsterdam

Naam: Heleen Goes

Studentnummer: 2707242

Datum: 16 juli 2021

Eerste beoordelaar: MSc Robin Kranendonk

Tweede beoordelaar: dr. Jasper van der Kemp

Voorwoord

Voor u ligt mijn masterscriptie naar het verhoorproces van verdachten van hackdelicten bij de cybercrimeteams in Nederland. Dit onderzoek heb ik in samenwerking met de Politieacademie uitgevoerd ter afronding van de Master Opsporingscriminologie aan de Vrije Universiteit in Amsterdam. Hoewel ik al enige mate van kennis (en een enorme interesse) had opgedaan op het gebied van cybercrime, was het politieverhoor (in Nederland) een tot dan toe nog onbekend onderwerp voor mij. Gedurende mijn onderzoek heb ik me verdiept in het verhoor bij de cybercrimeteams in Nederland. Dit was een uitdagende en leerzame ervaring, waardoor ik me op persoonlijk en professioneel vlak heb ontwikkeld. Ik wil mijn respondenten dan ook enorm bedanken voor de ervaringen en percepties die zij op verhoorgebied met mij hebben gedeeld.

Specifiek wil ik ook mijn begeleiders Robin Kranendonk en Marleen Weulen Kranenbarg vanuit de VU bedanken voor het vertrouwen dat zij mij hebben gegeven om dit onderzoek uit te mogen voeren. Zij waren een belangrijke ondersteuning voor mij gedurende het onderzoeksproces, stonden altijd voor mij klaar en hebben mijn onderzoek naar een hoger niveau weten te tillen. Ik heb onze meetings als erg leuk en leerzaam ervaren, waardoor mijn interesse in cybercrime, het verhoor en nog belangrijker: het doen van onderzoek nog verder is aangewakkerd. Ook wil ik Koen Geijsen, Emma Ratia en Joke Rooyakkers bedanken voor de tijd en moeite die zij in (de voorbereiding van) mijn onderzoek hebben gestoken. Tot slot wil ik mijn familie en vrienden bedanken voor hun steun gedurende het academische jaar. En Rutger, bedankt voor al je feedback en sparringsessies.

Ik wens u veel leesplezier toe.

Heleen Goes

Sleeuwijk, 16 juli 2021

Samenvatting

Hoewel onderzoek naar het algemene politieverhoor in Nederland schaars is, is er tot op heden nog geen onderzoek uitgevoerd naar specifiek het verhoor van hackverdachten. Het doel van deze verkennende studie is daarom om inzicht te krijgen in het verhoor van verdachten van hackdelicten. De onderzoeksvraag luidt daarbij als volgt: *Hoe verloopt het politieverhoor van verdachten van hackdelicten bij cybercrimeteams in Nederland?* Om antwoord te kunnen geven op de onderzoeksvraag zijn 18 semigestructureerde interviews afgenomen met experts die betrokken zijn bij het politieverhoor. In deze studie worden onder experts de respondenten verstaan die werkzaam zijn bij de cybercrimeteams, advocaten en cyberofficieren van justitie.

Hackers blijken een groep mannelijke verdachten te zijn van ongeveer twintig jaar oud en verschillen in opleidingsniveau en technische vaardigheden waarover zij beschikken. Een autismespectrumstoornis blijkt ook relatief vaak voor te komen, al worden deze autistische verdachten niet als kwetsbaar bestempeld door de respondenten uit dit onderzoek. Het verhoor van hackverdachten verloopt verder volgens de algemene richtlijnen. Na het meegeven van de cautie aan de verdachte, komen het persoonsgericht en zaakgericht verhoor aan bod. In het verhoor worden door alle rechercheurs methoden en technieken toegepast, waaronder ook technieken die als risicovol kunnen worden beschouwd. Dat is gevaarlijk, omdat daardoor de kans groter is dat verdachten een valse of een onbetrouwbare verklaring afleggen. Dit risico speelt een nog grotere rol bij kwetsbare verdachten, waar hackverdachten ook onder kunnen worden geschaard (vanwege het feit dat een autismespectrumstoornis relatief vaak voorkomt).

De verhoorteams worden in de meeste gevallen samengesteld door een combinatie van een tactische en een technische rechercheur. Voornamelijk de technische rechercheurs zijn daarbij digitaal onderlegd en de tactische rechercheurs hebben meer verhoorkennis en -ervaring. Gezamenlijk lijken zij over voldoende kennis te beschikken om het verhoor van een verdachte hacker op een professionele wijze uit te kunnen voeren, al lijkt er wel een gebrek aan kennis op het gebied van kwetsbare verdachten en een gebrek aan bewustzijn voor verhoorrisico's te zijn.

Op basis hiervan is de voornaamste aanbeveling van deze studie om binnen de politieorganisatie meer kennis te besteden aan de risico's die verbonden zijn aan het verhoor (met name ook met betrekking tot verhoortechnieken en kwetsbare verdachten). Eventueel vervolgonderzoek zou meer diepgang kunnen aanbrengen wat betreft het verhoorproces van hackverdachten en alle aspecten die daarbij komen kijken, waaronder ook het daadwerkelijke aantal hackverdachten met een psychische gesteldheid. Andere aanbevelingen zijn om audio(visuele) verhoren te analyseren en andere politieteams bij het onderzoek te betrekken.

Inhoudsopgave

1. Introductie van het onderzoek

Het digitale tijdperk brengt naast een hoop kansen, ook allerlei bedreigingen met zich mee in de vorm van cybercrime (Grabosky, 2017). Cybercrime is een groeiend maatschappelijk probleem waar steeds meer burgers mee te maken krijgen (Banach & Van Kampen, 2020). Een veelvoorkomende vorm van cybercrime is hacken (Centraal Bureau voor de Statistiek, 2020). Zo is in maart 2021 een zeventienjarige jongen veroordeeld tot een celstraf van drie jaar, omdat hij de Twitterprofielen van bekende personen als Barack Obama, Bill Gates en Elon Musk had gehackt. Hij probeerde bitcoins te verkrijgen van de volgers van deze profielen (Sullivan, 2021). Ook in Nederland heeft men met hackzaken te maken. Ter illustratie, de Nederlandse Organisatie voor Wetenschappelijk Onderzoek ging in februari 2021 gebukt onder een hack, waarbij allerlei interne documenten zijn gelekt op het dark web (Klein Douwel, 2021).

Vanwege een toename in prevalentie, is cybercrime hoog op de agenda van de politie komen te staan en zijn er verschillende teams opgericht. Zo is in 2007 het Team High Tech Crime (THTC) bij de Landelijke Eenheid opgericht; en bestaan sinds 2015 binnen de regionale politie-eenheden cybercrimeteams (Boekhoorn, 2019; Voskuil, 2019). Deze cybercrimeteams krijgen onder andere veel te maken met de opsporing van hackzaken (Boekhoorn, 2019). Het opsporingsproces bij hackzaken is echter anders dan het reguliere opsporingsproces, omdat de strafbare gedragingen zich in de onlinewereld afspelen (Koops & Oerlemans, 2007). Daardoor speelt technisch bewijs een grote rol bij een hack, terwijl klassieke bewijsmiddelen als camerabeelden en getuigenverklaringen minder vaak voorkomen (Smit-Arnold Bik, 2020).

Hoewel het opsporingsproces is verschoven naar de onlinewereld, speelt het verhoor mogelijkerwijs nog steeds een belangrijke rol bij een hackzaak. Naar verwachting is technisch bewijs niet in iedere zaak toereikend, waardoor de politie afhankelijk kan zijn van medewerking van de verdachte in het verhoor tijdens het opsporingsonderzoek. Zo kan bijvoorbeeld worden gedacht aan een situatie waar de politie pas nader onderzoek kan doen op een inbeslaggenomen computer indien de verdachte van een hackdelict[1] zijn wachtwoord afstaat. Om in dat geval een nauwkeurige en waarheidsgetrouwe verklaring van de verdachte te verkrijgen, is het van belang dat het verhoor op een juiste manier wordt uitgevoerd; en dat toelaatbare verhoormethoden en -technieken worden gebruikt (Gudjonsson & Pearse, 2011). Wanneer risicovolle methoden en technieken worden toegepast, is de kans groter dat een verdachte een valse of onbetrouwbare verklaring aflegt (Kassin, 2017). Sinds mei 2021 bestaat daarom, ter waarborging van de

[1] In dit onderzoek zal er bij de verdachte worden gerefereerd naar ‘hij’ of ‘zijn’. Bovendien zal bij ‘verdachten van hackdelicten’ ook worden gerefereerd naar ‘hackverdachten’ of ‘verdachte hackers’.

veiligheid van verdachten in het verhoor, een nieuwe richtlijn van de Verenigde Naties (VN). Daarin staat beschreven dat ontoelaatbare technieken zoals het stellen van suggestieve vragen of het voorleggen van fictief bewijs niet meer mogen worden toegepast (Association for the Prevention of Torture, Center for Human Rights & Humanitarian Law, & Norwegian Centre for Human Rights, 2021). Het risico op een valse of onbetrouwbare verklaring lijkt een nog grotere rol te spelen bij kwetsbare verdachten (North, Russell, & Gudjonsson, 2008), waar hackers ook onder kunnen vallen. In de literatuur wordt namelijk gesteld dat sommige hackers minderjarig zijn of een autismespectrumstoornis hebben (Ledingham & Mills, 2015; National Crime Agency, 2017; Van der Wagen, Van 't Zand-Kurtovic, Matthijsse, & Fischer, 2019).

1.1 Relevantie van het onderzoek

Hoewel het verhoor vanwege het fair trial beginsel (neergelegd in artikel 6 EVRM) op een juiste manier moet worden uitgevoerd, is onderzoek naar de verhoorpraktijk in Nederland schaars. Nog minder onderzoek is gedaan naar het verhoor van hackverdachten, waar een correcte uitvoering van het verhoor van nog groter belang lijkt te zijn vanwege de potentiële kwetsbaarheid van hackers. Slechts in één studie zijn verhoren van cybercrimeverdachten (waaronder ook een aantal verhoren van hackverdachten) geanalyseerd om inzicht te krijgen in het verhoorgedrag van rechercheurs binnen de politie (Van Kuppevelt, 2020). De genoemde studie heeft echter niet volledig in beeld gebracht hoe het verhoor verloopt en welke methoden of technieken daarbij worden ingezet. Dit onderzoek zal daarom een bijdrage leveren aan de huidige kennisleemte op het gebied van het verhoorproces van hackverdachten.

In deze studie zal met name worden stilgestaan bij het algemene verloop van het verhoor, de verhoormethoden en -technieken die worden toegepast om een hackverdachte te ondervragen en de mogelijke risico's die in het verhoor naar voren komen. Bovendien zal aandacht worden besteed aan de persoonskenmerken van hackverdachten en de mogelijke rol hiervan in het verhoor (bijvoorbeeld met betrekking tot de potentiële kwetsbaarheid van verdachte hackers). Het verhoor van hackverdachten lijkt ook een uniek proces te zijn. Verhoorders hebben namelijk naast algemene verhoorkennis, ook psychologische kennis nodig vanwege de omgang met potentiële kwetsbare verdachten en technische kennis door het cybercrimecomponent. De verwachting is echter dat verhoorders niet op elk van deze gebieden over voldoende kennis beschikken. Zo wordt in de literatuur bijvoorbeeld beschreven dat politieagenten over het algemeen geen speciale opleiding omtrent kwetsbare verdachten volgen (Geijsen, De Ruiter, & Kop, 2018) en dat het kennisniveau op het gebied van cybercrime laag is (Klap, Leukfeldt, & Stol, 2012). Bovendien wordt het verhoor van een cybercrimeverdachte

doorgaans door zowel een tactische als een technische rechercheur uitgevoerd. Technische rechercheurs volgen enkel een korte verhooropleiding en hebben daardoor mogelijk veel kennis op het gebied van cybercrime, maar beschikken over minder verhoorkennis (Van Kuppevelt, 2020). Zodoende behoeven het kennisniveau van de verhoorders op het gebied van het verhoor, kwetsbare verdachten en cybercrime, maar ook de samenstelling van het verhoorteam een nadere analyse in het onderzoek; inclusief de eventuele rol daarvan in het verhoor.

Naast het feit dat een literaire bijdrage omtrent het verhoorproces van hackverdachten waardevol wordt geacht, hebben de onderzoeksresultaten ook maatschappelijke relevantie. Dit onderzoek kan namelijk handvaten bieden voor het optimaliseren van het verhoorproces, zodat verhoorders sneller en op efficiëntere wijze betrouwbare informatie van verdachten kunnen verkrijgen. Hierbij kan worden gedacht aan de keuze voor het toepassen van verhoormethoden en -technieken of de samenstelling van het verhoorteam. Bovendien kan onderzoek naar een mogelijk kennistekort omtrent cybercrime, het verhoor en kwetsbare verdachten leiden tot meer aandacht voor deze onderwerpen binnen de politieorganisatie. Indien rechercheurs op een efficiëntere wijze betrouwbare informatie van een hackverdachte in het verhoor kunnen verkrijgen, heeft dat een positief effect op de bestrijding van cybercrime door de politie. Wanneer meer hackzaken worden opgelost, brengt dat verschillende voordelen met zich mee voor de samenleving zoals minder toekomstige slachtoffers van een hack.

1.2 Onderzoeksvraag, doelstelling en deelvragen

Vanuit de hierboven beschreven context, is het doel van deze studie om een wetenschappelijke bijdrage te leveren wat betreft het verloop van het verhoor van hackverdachten, de methoden en technieken die worden ingezet, de persoonskenmerken (en de potentiële kwetsbaarheid) van hackverdachten en de risico's van het verhoor. Het doel is ook om inzicht te krijgen in diverse aspecten die een rol zouden kunnen spelen in het verhoorproces, zoals het kennisniveau van de verhoorders en de samenstelling van het verhoorteam. Deze studie richt zich specifiek op het verhoor dat wordt uitgevoerd binnen de cybercrimeteams, omdat er in algemene zin beperkt onderzoek naar deze teams is gedaan en zij ook veel te maken krijgen met hackzaken (Boekhoorn, 2019). De centrale onderzoeksvraag luidt daarom als volgt: *Hoe verloopt het politieverhoor van verdachten van hackdelicten bij cybercrimeteams in Nederland?* Ter beantwoording van deze vraag wordt een kwalitatieve onderzoeksmethode gehanteerd. Semigestructureerde interviews met experts werkzaam bij Nederlandse cybercrimeteams, advocaten en cyberofficieren van justitie worden daarbij afgenomen en geanalyseerd.

Om een volledig antwoord te kunnen geven op de centrale onderzoeksvraag, zullen diverse deelvragen worden behandeld die voortkomen uit het hierboven geschetste kader. Bij deze vragen staan de ervaringen en de perceptie van de respondenten met het verhoor centraal:

1. *Op welke manier spelen belangrijke persoonskenmerken van verdachten van hackdelicten een rol in het politieverhoor?*
2. *Op welke manier spelen verhoormethoden en -technieken, die worden gebruikt in het verhoor van verdachten van hackdelicten, een rol in het politieverhoor?*
3. *Op welke manier speelt de samenstelling van het verhoorteam bij verdachten van hackdelicten een rol in het politieverhoor?*
4. *Over welke kennis en vaardigheden beschikken de cybercrimeteams op het gebied van het verhoor van verdachten van hackdelicten en wat voor rol heeft dit in het politieverhoor?*
5. *Welke verschillen bestaan er in het verhoorproces van verdachten van hackdelicten tussen verhoorders met veel en weinig kennis en ervaring op het gebied van het verhoor?*
6. *Hoe kan het verhoorproces bij verdachten van hackdelicten worden geoptimaliseerd?*

1.3 Begrippen en definities

Cybercriminaliteit wordt in het Basisboek cybercriminaliteit door Van der Wagen, Oerlemans, en Weulen Kranenbarg (2020) omschreven als "*alle strafbare gedragingen waarbij ICT-systemen van wezenlijk belang zijn in de uitvoering van het delict*" (p. 15). Daarbij wordt een onderscheid gemaakt tussen cybercriminaliteit in enge zin en cybercriminaliteit in ruime zin (of gedigitaliseerde criminaliteit). In deze studie ligt de focus op cybercriminaliteit in enge zin. Het gaat om nieuwe delicten die in het verleden niet bestonden en waarbij ICT zowel het doelwit als het middel is. Enkele voorbeelden daarvan zijn het verspreiden van een computervirus, hacken of een DDoS-aanval (Van der Wagen et al., 2020, p. 15).

Nog specifieker staat in dit onderzoek het hackdelict centraal, dat in het Wetboek van Strafecht als computervredebreuk strafbaar is gesteld. Het betreft het *"opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk of in een deel daarvan"* (artikel 138a lid 1 Sr). In het verlengde daarvan worden hackers omschreven als individuen die over kennis en mogelijkheden beschikken om wederrechtelijk in te breken op een geautomatiseerd werk (Boekhoorn, 2019; Nationaal Cyber Security Centrum, 2012).

Tot slot heeft dit onderzoek betrekking op het verdachtenverhoor. Een verdachte wordt in het Wetboek van Strafvordering omschreven als degene *"te wiens aanzien uit feiten of omstandigheden een redelijk vermoeden van schuld aan een strafbaar feit voortvloeit"* (artikel 27 lid 1 Sv). Daarnaast wordt het verhoor door de Hoge Raad (1979) omschreven als "*alle*

vragen aan een door een opsporingsambtenaar als verdachte aangemerkt persoon betreffende diens betrokkenheid bij een geconstateerd strafbaar feit". Verhoeven en Duinhof (2017) spreken daarom bij het verhoor van *"de directe interactie tussen opsporingsambtenaren en de verdachte die is gericht op het verkrijgen van informatie over de toedracht van het delict"* (p. 46). Het doel van het verhoor is zodoende om alle relevante informatie over een gepleegd strafbaar feit te verkrijgen (Gudjonsson & Pearse, 2011).

1.4 Leeswijzer

In het volgende hoofdstuk zal worden stilgestaan bij de beschikbare literatuur op het gebied van cybercrime op de publieke agenda, (verdachte) hackers, het verdachtenverhoor, kwetsbare verdachten en de kennis en vaardigheden van verhoorders binnen de politieorganisatie. In het derde hoofdstuk wordt de methode van het onderzoek toegelicht, waarbij onder andere wordt beschreven op welke manier de dataverzameling en analyse hebben plaatsgevonden. Het daaropvolgende hoofdstuk beschrijft de resultaten van het onderzoek. In het vijfde hoofdstuk zal in de conclusie antwoord worden gegeven op de onderzoeksvraag en deelvragen. Tot slot worden in de discussie in hoofdstuk zes de bevindingen van het onderzoek in het licht van de literatuur beschouwd. Daarbij zullen diverse praktijkaanbevelingen worden gedaan ter verbetering van het verhoor van hackverdachten en aanbevelingen voor vervolgonderzoek, maar komen ook enkele beperkingen van het uitgevoerde onderzoek aan bod.

2. Theoretisch kader

2.1 Cybercrime op de publieke agenda

De politie wordt in Nederland gezien als de hoofdrolspeler in de strijd tegen cybercrime, waardoor het fenomeen hoog op de agenda van de politie is komen te staan (Stol & Jansen, 2014). Enerzijds besteedt men aandacht aan kennisontwikkeling van minder onderzochte fenomenen, zoals het verhoor van cybercrimeverdachten wat sinds 2020 onderdeel uitmaakt van het Onderzoeksprogramma van de Politieacademie (Politieacademie, 2020). Anderzijds zijn er teams opgericht om cybercrime te kunnen bestrijden. Zo is in 2007 het THTC bij de Landelijke Eenheid opgericht en bestaan er sinds 2015 binnen de regionale politie-eenheden cybercrimeteams (Boekhoorn, 2009; Voskuil, 2019). Kenmerkend is het multidisciplinaire karakter van deze cybercrimeteams; waarin intelligence, tactiek en specialisme zijn vertegenwoordigd (Politie, 2020). De specialisten (zoals financieel rechercheurs, digitaal specialisten en analisten) worden vaak vanwege hun kennispositie van buiten de politie aangenomen (Boekhoorn, 2019; Bogaart, 2018; Politie, z.d.; Van Kuppevelt, 2020).

Daarnaast wordt ook op politiek niveau steeds meer aandacht op cybercrime gevestigd. De bestrijding van cybercrime is in de Veiligheidsagenda 2019-2022 van het Ministerie van Justitie en Veiligheid als beleidsdoelstelling opgenomen. Hiervoor is een onderscheid gemaakt tussen verschillende soorten cybercrimezaken die door diverse politieteams moeten worden uitgevoerd. Zo wordt het THTC bijvoorbeeld verantwoordelijk gehouden voor de meest complexe cybercrimezaken, zoals delicten die zijn gericht op vitale sectoren en onderzoeken met een high tech component. Verder worden de reguliere zaken uitgevoerd door de districtsrecherches, de basisteams en de cybercrimeteams. De cybercrimeteams zijn daarbij met name verantwoordelijk voor de complexere zaken die buiten de taakstelling van het THTC vallen, maar ook voor fenomeenonderzoeken; waarbij de bestrijding van cybercriminele fenomenen of dadergroepen centraal staat (Ministerie van Justitie en Veiligheid, 2018).

2.2 Motivatie en persoonskenmerken van hackverdachten

In de praktijk zijn de cybercrimeteams veel bezig met de opsporing van hackzaken, waarbij zij ook verantwoordelijk zijn voor het verhoor van hackverdachten (Boekhoorn, 2019). Vermoedelijk krijgen de rechercheurs in het verhoor met diverse typen hackverdachten te maken, omdat in de literatuur uiteenlopende motivaties worden beschreven die betrokkenheid bij een hack verklaren. Motieven die onder andere een rol spelen, zijn een behoefte aan kennis op het gebied van technische problemen, persoonlijke uitdaging, spanning, nieuwsgierigheid,

macht en verveling (Turgeman-Goldschmidt, 2005; Van der Hulst & Neve, 2008; Van der Wagen et al, 2019). Verder beschrijven diverse auteurs dat een financieel motief in de praktijk maar zelden voorkomt (Turgeman-Goldschmidt, 2005; Weulen Kranenbarg, 2018; Zebel, De Vries, Giebels, Kuttschreuter, & Stol, 2013). Daarentegen blijkt uit het onderzoek van Van der Wagen et al. (2019), die onder andere interviews hebben afgenomen met cyberdaders, dat geld toch een rol kan spelen; bijvoorbeeld in het geval van een fraude-gerelateerde hackzaak.

Hoewel geen algemeen daderprofiel van 'de hacker' kan worden opgesteld (Leukfeldt, Domenie, & Stol, 2012), blijken er toch enkele persoonskenmerken te zijn die afwijken van de gemiddelde traditionele dader die offline delicten pleegt. Doordat er grote verschillen worden gevonden tussen daders die offline en online delicten plegen, wordt er zelfs gesproken van een nieuw type dader bij hackers (Rokven, Weijters, & Van der Laan, 2017). Bij het beschrijven van de persoonskenmerken van hackers zullen voor zover mogelijk de overeenkomsten en verschillen met de traditionele dadergroep worden beschreven. Bestaande onderzoeken naar hackers bevatten echter veelal geen representatieve samples en de steekproeven zijn vaak klein. Ook wordt er geprobeerd om zoveel mogelijk te refereren naar studies die ingaan op hackverdachten, maar het uitgevoerde onderzoek hieromtrent is beperkt[2]. Meer onderzoek naar de persoonskenmerken van (verdachte) hackers is aldus van groot belang (Steinmetz, 2015).

2.2.1 Demografische kenmerken

Op het gebied van demografische kenmerken van hackers, blijkt allereest uit een kwantitatief onderzoek in Maleisië dat jongeren ten aanzien van ouderen eerder geneigd zijn om te gaan hacken (Jafarkarimi, Sim, Saadatdoost, & Hee, 2015). Uit kwalitatief onderzoek blijkt verder dat hackers ongeveer twintig jaar oud zijn (Aiken, Davidson, & Amann, 2016; Van der Wagen et al., 2019; Yar, 2005). Daarom concluderen Leukfeldt et al. (2010) in hun studie op basis van politiegegevens dat hackverdachten ongeveer dezelfde leeftijd lijken te hebben als andere verdachten die offline delicten plegen. Bovendien blijkt de '*age crime curve*' toepasbaar te zijn op hackers; in de tienerjaren is er sprake van een toename in crimineel gedrag, waarna er langzaam een daling optreedt (Farrington, 1986; Ruiter & Bernaards, 2013).

Verder blijkt uit internationaal onderzoek dat het bij hackers veelal om mannelijke daders gaat (Aiken et al., 2016; Chiesa, Ducci, & Ciappi, 2009; Jafarkarimi et al., 2015; Steinmetz, 2015; Van der Wagen et al., 2019). Hier wordt een overeenkomstig beeld gevonden met de traditionele daders die offline delicten plegen, die ook vaak van het mannelijke geslacht

[2] In sommige gevallen wordt daarom gerefereerd naar cyberdaders, waar hackers ook onder vallen.

zijn (Centraal Bureau voor de Statistiek, 2021; Leukfeldt et al., 2010). Bovendien wordt in diverse kwalitatieve studies gesteld dat hackers voornamelijk een autochtone achtergrond hebben (Leukfeldt et al., 2010; Rokven et al., 2017; Steinmetz, 2015; Van der Wagen et al., 2019). Daarentegen beschrijft Weulen Kranenbarg (2018) dat in haar studie slechts een kleine meerderheid van het aantal autochtone daders bij cyberdaders werd gevonden in vergelijking met traditionele daders. Het is zodoende maar de vraag of de etnische achtergrond van hackers daadwerkelijk verschilt met de traditionele dadergroep die offline delicten pleegt.

2.2.2 Opleidingsniveau en computervaardigheden

Naast de demografische kenmerken, wordt er op het gebied van het opleidingsniveau van hackers ook een verschil gevonden ten aanzien van traditionele daders die offline delicten plegen. In de literatuur worden traditionele daders vaak omschreven als jongeren met een laag opleidingsniveau (Straub, Leerdam, Autar, & Sanches, 2020; Van der Laan & Blom, 2006). Jongeren die voortijdig stoppen met school zouden eerder in aanraking komen met de politie (Blom, Oudhof, Bijl, & Bakker, 2008). Daarentegen wordt in enkele kwalitatieve onderzoeken beschreven dat hackers intelligente jongeren zijn met een hoog opleidingsniveau. Zij zouden over ontwikkelde computervaardigheden beschikken en zijn nieuwsgierig naar technologie (Aiken et al., 2016; Stambaugh et al., 2001; Steinmetz, 2015; Van der Hulst & Neve, 2008; Van der Wagen et al., 2019). Marcum, Higgins, Ricketts, en Wolfe (2014) hebben in hun kwantitatieve studie zelfs een verband gevonden tussen schoolprestaties en het plegen van een hack. Jongeren die beter presteren op school, zouden meer geneigd zijn om te gaan hacken.

Naar verwachting bestaan er echter ook minder opgeleide hackers. In enkele studies wordt namelijk een tegenstellend beeld geschetst van hackers die hun opleiding niet afmaken, omdat ze deze te saai of te gemakkelijk vinden (Chiesa et al., 2009; Steinmetz, 2015). Daarnaast zijn er ook hackers met een laag opleidingsniveau die over minder digitale vaardigheden beschikken (Van der Wagen et al., 2019). Dat kan worden verklaard door het feit dat er tegenwoordig op het internet allerlei kant-en-klare tools zijn te vinden die gemotiveerde daders kunnen gebruiken om een hack uit te voeren. Hackers hoeven dus niet zelf meer te beschikken over computervaardigheden, waardoor het instapniveau voor hackdelicten veel lager ligt (Van der Wagen et al., 2019). Bovendien blijkt dat hackers in lijn met de sociale leertheorie ook delinquent gedrag van vrienden kunnen imiteren of kunnen leren van deze vrienden (Holt & Bossler, 2014; Holt, Burruss, & Bossler, 2010; Navarro & Marcum, 2020). In de huidige maatschappij is digitale kennis namelijk makkelijk over te dragen, waardoor ook minder digitaal vaardige jongeren een hack kunnen plegen (Zebel et al., 2013).

2.2.3 Psychische kenmerken

Zoals hierboven ook deels is beschreven, worden hackers in de wetenschappelijke literatuur neergezet als extreem slimme jongeren met een hoog IQ (Chiesa et al., 2009; Van der Wagen et al., 2019). Hackers blijken daarbij over een hoger IQ te beschikken ten opzichte van de meeste Nederlandse en buitenlandse gedetineerden, zo blijkt uit eerder uitgevoerd onderzoek (Aiken et al., 2016; Marcum et al., 2014; Platje, Cornet, & De Kogel, 2017).

Daarnaast wordt in twee studies, op basis van onderzoek onder medewerkers van wetshandhavingsinstanties uit diverse landen, beschreven dat een autismespectrumstoornis in de praktijk relatief vaak voorkomt bij cyberdaders (en daardoor waarschijnlijk ook bij hackers) (Ledingham & Mills, 2015; National Crime Agency, 2017). Het betreft een neurobiologische aandoening die alle gebieden van het sociaal functioneren en communiceren aantast (Ledingham & Mills, 2015). In de studie van Van der Wagen et al. (2019) veronderstellen diverse experts, op basis van hun contact met cyberdaders, dat cyberdaders bepaalde autistische kenmerken hebben. Te denken valt aan kenmerken zoals wegkijken, in de eigen wereld zitten, moeite hebben met communiceren en het niet goed kunnen praten over gevoelens. Het hebben van autistische kenmerken wordt in de kwantitatieve studie van Payne et al. (2019) zelfs in verband gebracht met een verhoogd risico op het plegen van een cybercrimedelict (en daarmee waarschijnlijk ook een hack). Een groot gedeelte van die relatie wordt echter verklaard door digitale vaardigheden. Dat zou erop kunnen wijzen dat mensen met autistische kenmerken goed zijn in het ontwikkelen van digitale vaardigheden en vanwege die vaardigheden een grotere kans lopen op het plegen van een cyberdelict. Tot op heden is er echter nog geen specifiek onderzoek uitgevoerd naar het verband tussen een autismespectrumstoornis en het plegen van een hack; of de prevalentie van het aantal hackverdachten met een dergelijke stoornis.

2.3 Het verdachtenverhoor

In de literatuur worden, zoals hierboven is beschreven, enkele verschillen gevonden tussen daders die offline en online delicten plegen. Ook ziet het opsporingsproces bij een hackzaak er anders uit ten opzichte van het klassieke opsporingsproces. Zoals beschreven in de inleiding speelt vooral technisch bewijs een grote rol bij een hackzaak (Smit-Arnold Bik, 2020), maar is het verhoor waarschijnlijk ook nog steeds een belangrijk onderdeel van het opsporingsproces. Hoewel nog geen onderzoek is uitgevoerd naar het verloop van het verhoor van hackverdachten, bestaat de verwachting dat het verhoor grotendeels overeenkomt met de algemene richtlijnen uit de Handleiding Verhoor. Het Nederlandse politieverhoor is in drie onderdelen opgedeeld, namelijk het eerste contact, het persoonsgericht verhoor en het zaakgericht verhoor. Tijdens het

eerste contact wordt aan de verdachte duidelijk gemaakt hoe het verhoor zal verlopen en worden zijn rechten herhaald. Vervolgens worden in het persoonsgericht verhoor de persoonsgegevens van de verdachte verder aangevuld, wordt de verklaringsbereidheid van de verdachte vastgesteld en proberen de verhoorders een verstandshouding op te bouwen met de verdachte (Van Amelsvoort & Rispens, 2017; Verhoeven & Duinhof, 2017). Tot slot wordt in het zaakgericht verhoor aan waarheidsvinding gedaan en proberen de verhoorders betrouwbare en volledige informatie van de verdachte te verkrijgen om erachter te komen wat er is gebeurd tijdens het strafbare feit (Duker & Stevens, 2009; Van Amelsvoort & Rispens, 2017).

In het persoonsgericht verhoor kunnen verhoorders ook een vermoeden krijgen van de potentiële kwetsbaarheid van de verdachte (Van Amelsvoort & Rispens, 2017). Dat is van belang, omdat kwetsbare verdachten een groter risico lopen op het afleggen van een valse of onbetrouwbare verklaring (North et al., 2008). Het herkennen van een kwetsbare verdachte kan plaatsvinden aan de hand van enkele vragen die staan genoteerd in de ‘Vragenlijst indicatie kwetsbaarheid’ uit de Handleiding Verhoor (de zogenaamde ‘VIK-vragen’). De vragen hebben onder andere betrekking op onderwerpen als het krijgen van hulpverlening, de psychische gesteldheid, mogelijk medicijngebruik, het opleidingsniveau en de woon- en werksituatie van de verdachte. In de Handleiding Verhoor staat omschreven dat verhoorders geen diagnose moeten opstellen, maar dat ze enkel een vermoeden moeten krijgen van de potentiële kwetsbaarheid van de verdachte in kwestie. Zodra dit vermoeden bestaat, krijgt de verdachte ter bescherming verplicht een advocaat in het verhoor toegewezen. Bovendien kan het verhoor worden aangepast aan de problematiek van de verdachte in kwestie of wordt een gespecialiseerde verhoorder ingezet (Van Amelsvoort & Rispens, 2017). Deze verhoorders hebben de opleiding ‘Verhoren van Kwetsbare Verdachten’ afgerond en zijn gespecialiseerd in het goed kunnen uitvoeren van het verhoor van kwetsbare verdachten (Politieacademie, z.d.-a).

In de praktijk wordt echter gesteld dat binnen de gehele politieorganisatie onvoldoende kennis, herkenning en bewustzijn is voor kwetsbare verdachten (Geijsen, 2018). Uit het onderzoek van Geijsen, De Ruiter et al. (2018) blijkt dat weinig politieagenten een opleiding hebben gevolgd op het gebied van kwetsbare verdachten. Hierdoor bestaat de verwachting dat ook binnen de cybercrimeteams weinig rechercheurs een dergelijke opleiding hebben gevolgd, wat gezien de aanwezigheid van bijvoorbeeld een autismespectrumstoornis bij hackverdachten risicovol kan zijn. Het is maar de vraag of in het verhoor van kwetsbare hackverdachten een verhoorder wordt ingezet die de opleiding ‘Verhoren van Kwetsbare Verdachten’ heeft gevolgd en of rechercheurs weten hoe zij moeten omgaan met dergelijke verdachten. Zie verder voor het verhoor van kwetsbare verdachten en de betrouwbaarheid van de verklaring paragraaf 2.4.

2.3.1 Verhoormethoden

Tijdens het persoonsgericht verhoor wordt, zoals hierboven beschreven, informatie verkregen over de verklaringsbereidheid van de verdachte. De bereidwilligheid om te verklaren zal per hackverdachte variëren, omdat er in Nederland op basis van artikel 29 van het Wetboek van Strafvordering geen verplichting is tot het afgeven van een verklaring. Een hackverdachte kan bijvoorbeeld op advies van zijn advocaat gebruikmaken van zijn zwijgrecht. Wanneer een verdachte niet wil verklaren, kan dat een probleem zijn voor de cybercrimeteams. Dat is bijvoorbeeld het geval wanneer de verdachte informatie bij zich draagt over de locatie van het bewijsmateriaal van het gepleegde strafbare feit. Dan kunnen de cybercrimeteams vastlopen met het opsporingsonderzoek of tijd verspillen aan het onderzoeken van een bepaalde richting op basis van foutieve informatie, waardoor een mogelijk schuldige verdachte niet strafrechtelijk kan worden vervolgd. Om toch een verklaring van de verdachte proberen te verkrijgen, kunnen de cybercrimeteams gebruikmaken van verhoormethoden. Een verhoormethode is een bepaalde strategie om de verdachte zover te krijgen een verklaring af te leggen (Kranendonk, 2017; Verhoeven & Duinhof, 2017). In de Handleiding Verhoor worden vier verschillende methoden voorgeschreven, waarbij de keuze voor een verhoormethode wordt afgestemd op de verklaringsbereidheid van de verdachte in kwestie (Van Amelsvoort & Rispens, 2017).

De eerste methoden zijn toepasbaar op verdachten met een hoge verklaringsbereidheid, maar worden ook gebruikt wanneer verhoorders onder tijdsdruk staan om het verhoor op een juiste manier uit te voeren. Allereerst de Vrije Verklaringsmethode (VVM), die ook kan worden toegepast wanneer er redenen zijn om geen bewijsmateriaal aan de verdachte voor te leggen. Bij deze methode krijgt een hackverdachte de gelegenheid om zijn eigen verhaal te doen. Voor het verkrijgen van een spontaan verhaal kunnen verhoorders, zonder druk uit te oefenen, gebruikmaken van allerlei startvragen. Zo kan de verdachte worden gevraagd wat hij heeft te zeggen over het strafbare feit of wat hij op een bepaalde datum heeft gedaan. Indien er voldoende bewijs voorhanden is, kan daarnaast ook de Directe Stapelmethode (DSM) worden ingezet. Bij deze methode wordt de verdachte in één keer geconfronteerd met bijna alle tactische en technische aanwijzingen, waarna hij de gelegenheid krijgt om te reageren. De verdachte kan bijvoorbeeld worden verteld dat op zijn computer strafbare feiten zijn aangetroffen en dat zijn IP-adres is aangetroffen bij een hack. In de Handleiding Verhoor wordt echter als nadeel beschreven dat een verdachte een vals verhaal kan construeren op basis van de eerder verkregen tactische en technische aanwijzingen. In dat geval moeten verhoorders overgaan op de bewijsvraagmethode (Van Amelsvoort & Rispens, 2017).

De laatste twee methoden kunnen worden toegepast wanneer een verdachte een lage verklaringsbereidheid heeft. De Bewijsvraagmethode (BVM) wordt gebruikt om te voorkomen dat de verdachte later op zitting zegt: "*Als ik dat geweten had, had ik er wel wat over willen zeggen"* (Van Amelsvoort & Rispens, 2017, p. 483). De verdachte wordt dan geconfronteerd met wat de verhoorders zien als het meest waardevolle bewijsmateriaal, waarna de verdachte de gelegenheid krijgt om een verklaring af te leggen (Geijsen, 2018). Het verschil met de DSM is dat bij de BVM enkel de belangrijkste tactische en/of technische aanwijzingen worden voorgelegd aan de verdachte (Van Amelsvoort & Rispens, 2017). Als laatste kunnen verhoorders ook de Scenario's Onderzoekende Methode (SOM) toepassen (voorheen de standaardverhoorstrategie). Deze methode wordt veel gebruikt in de algemene Nederlandse verhoorpraktijk (Geijsen, 2018; Stevens & Verhoeven, 2011) en vermoedelijk ook in het verhoor van hackverdachten. Doorgaans begint het verhoor met het confronteren van de verdachte met tactische aanwijzingen waar hij gemakkelijk een verklaring over kan afleggen en worden er omsingelingsvragen gesteld. Dan krijgt de verdachte de gelegenheid om een potentieel alternatief scenario te schetsen. Enkele voorbeeldvragen zijn: "*Wat heb je vrijdagavond gedaan?"* of "*Wat doe je zoal in de week?"* (Van Amelsvoort & Rispens, 2017, p. 469). Vervolgens wordt de druk langzaam opgebouwd doordat verhoorders steeds meer gaan vragen naar onderwerpen waar de verdachte minder makkelijk over kan verklaren, zoals het aantreffen van het IP-adres van de verdachte bij een hack. Bij het toepassen van de SOM proberen de verhoorders de weerstand van de verdachte te minimaliseren, zodat hij geneigd is om de waarheid te vertellen (Van Amelsvoort & Rispens, 2017). Enkele voorbeelden daarvan zijn actief luisteren naar de verdachte, vragen hoe het met de verdachte gaat en tegemoetkomen aan de behoeften van de verdachte. Zo kan bijvoorbeeld aan de verdachte worden verteld: "*Nou, wil je wat eten, drinken, roken, toilet? Dan geef je dat maar aan*." (Verhoeven & Duinhof, 2017, p. 209). De verhoorders mogen echter geen ontoelaatbare druk uitoefenen, omdat dan de kans op een onbetrouwbare of valse verklaring groter is. Onder andere is er sprake van ontoelaatbare druk wanneer verhoorders de verdachte uitschelden, beloften doen, liegen of suggestieve vragen stellen (Van Amelsvoort & Rispens, 2017). Ondanks de populariteit is de SOM niet empirisch getoetst en wordt er zelfs gesproken over het mogelijke gevaar van tunnelvisie bij verhoorders (Geijsen, 2018). Het toepassen van toelaatbare druk kan namelijk, net als bij het toepassen van ontoelaatbare druk, tot stress leiden bij verdachten. Mogelijk wordt hierdoor het proces van herinneren verstoord en is de kans op een valse of onbetrouwbare verklaring groter (Boon, Odinot, Horselenberg, & Geijsen, 2016; Geijsen & De Ruiter, 2017). Dit kan ook een risico vormen voor hackverdachten indien de SOM vaak wordt toegepast.

Vanwege het mogelijke gevaar van drukopbouw tijdens het verhoor beschrijven diverse auteurs dat de Nederlandse verhoorpraktijk moet worden hervormd. De politie zou over moeten gaan op het neutralere ‘investigative interviewing’; oftewel het ‘forensische interview’ met het daarbij horende PEACE-interviewmodel (Boon et al., 2016; Geijsen, 2018; Geijsen & De Ruiter, 2017). Het model komt oorspronkelijk uit het Verenigd Koninkrijk, waar tijdens de implementatie van het model een positief effect is gevonden op de verhoorpraktijk (Clarke, Milne, & Bull, 2011). In de literatuur staat beschreven dat het model bijdraagt aan het verminderen van valse bekentenissen en dat het de kans op het verkrijgen van een betrouwbare verklaring in het verhoor verhoogt. Dat komt doordat de focus ligt op informatievergaring en niet op het verkrijgen van een bekentenis (Clarke et al., 2011; Howes, 2020; Meissner et al., 2014). Inmiddels wordt het model ook in andere landen toegepast zoals Australië, Nieuw-Zeeland, Canada en Noorwegen (Boon et al., 2016; Geijsen, 2018).

Het PEACE-model bestaat uit de fasen ‘Planning & Preparation’, ‘Engage & Explain’, ‘Account’, ‘Closure’ en ‘Evaluation’ (Boon et al., 2016). Na het voorbereiden van het verhoor en het vergaren van informatie over de verdachte in de eerste fase, wordt aan de verdachte verteld hoe het verhoor zal verlopen en bouwen de verhoorders een band op met de verdachte (Clarke et al., 2011; Howes, 2020; Snook, Eastwoord, & Barron, 2014; Walsh & Bull, 2012). Deze tweede fase lijkt daarmee sterk op het eerste contact en het persoonsgericht verhoor uit de Nederlandse verhoorpraktijk. Vervolgens wordt in de derde fase geprobeerd om informatie over het strafbare feit te verkrijgen, waar de verdachte net als bij de VVM de gelegenheid krijgt om zelf met een verklaring te komen. Daarbij kunnen ook open vragen worden gesteld en wordt de verdachte op een empathische en niet-oordelende manier geconfronteerd met eventuele inconsistenties in zijn verhaal (Boon et al., 2016; Snook et al., 2014). In de vierde fase vatten de verhoorders de belangrijkste bevindingen van het verhoor samen en krijgt de verdachte de gelegenheid om informatie aan te passen of toe te voegen. De laatste fase heeft tot slot betrekking op een evaluatie van het verhoorproces (Howes, 2020; Snook et al., 2014).

2.3.2 Verhoortechnieken

In de uitvoering van een verhoormethode, kunnen de cybercrimeteams gebruikmaken van verhoortechnieken om de verklaringsbereidheid van verdachten te beïnvloeden (Verhoeven, 2014). Een verhoortechniek wordt omschreven als een concrete vraag of opmerking van een opsporingsambtenaar (Verhoeven & Duinhof, 2017). Het zijn aldus gesprekstechnieken die kunnen worden gebruikt om een verdachte aan te moedigen te gaan praten in het verhoor. In Nederland worden verschillende verhoortechnieken gebruikt, waarvan diverse technieken als

ontoelaatbaar kunnen worden beschouwd. Hieronder zullen eerst enkele toelaatbare technieken aan bod komen, waarna verschillende ontoelaatbare technieken zullen worden beschreven.

2.3.2.1 Toelaatbare verhoortechnieken

Bij alle verhoormethoden worden toelaatbare technieken toegepast, zoals het confronteren van de verdachte met tactische en technische aanwijzingen (Van Amelsvoort & Rispens, 2017). Een ander voorbeeld is het opbouwen van vertrouwen en een verstandshouding met de verdachte (Stevens & Verhoeven, 2011; Verhoeven & Duinhof, 2017). In tabel 1 zijn ter illustratie enkele andere toelaatbare technieken weergeven die uit één van de weinige Nederlandse studies op het gebied van verhoortechnieken komen. Naar verwachting komen deze technieken ook voor in het verhoor van hackverdachten bij de cybercrimeteams in Nederland.

Tabel 1.

Toelaatbare verhoortechnieken uit het onderzoek van Verhoeven en Duinhof (2017).

Verhoortechniek	Voorbeeld
De verdachte confronteren met uitspraken van anderen	*"Kijk er zijn mensen. Die hebben wij ook gehoord. Die hebben dingen over jou verteld." (p. 194)*
Benadrukken van oprechtheid of vertrouwen	*"Wij zitten hier niet om jou te oordelen of veroordelen" (p. 208)*
Identificeren van en tegemoetkomen aan de behoeften van de verdachte	*"Als je wat wilt drinken. Naar toilet wil. Alles is bespreekbaar. Geef het aan." (p. 209)*
Bezorgdheid tonen over de verdachte en zijn situatie	*"Nou, ja, dat is toch al wat, toch? Die aanhouding?" (p. 211)*
Vragen of de verdachte nog iets wil toevoegen aan de verklaring	*"Oké, wil je nog iets kwijt aan ons? Wil je nog iets zeggen?" (p. 212)*

2.3.2.2 Ontoelaatbare verhoortechnieken

Naast bovenstaande toelaatbare verhoortechnieken, worden in het verhoor ook ontoelaatbare technieken toegepast. Een voorbeeld daarvan is het voorleggen van fictief bewijs aan de verdachte (Kassin, 2008; Kassin, Drizin et al., 2010). Ook komt het voor dat er ongepaste vragen aan de verdachte worden gesteld, zoals suggestieve of gesloten vragen (Geijsen, 2018; Geijsen, Vanbelle, Kop, & De Ruiter, 2018; Stevens & Verhoeven, 2011). Een suggestieve vraag is bijvoorbeeld: *"Hoe kan het dan dat wij jouw IP-adres hebben gevonden?"* (Verhoeven

& Duinhof, 2017, p. 202). In tabel 2 worden enkele andere risicovolle technieken weergeven, die eveneens voortkomen uit het onderzoek van Verhoeven en Duinhof (2017). Ook deze verhoortechnieken worden mogelijkerwijs toegepast in het verhoor van hackverdachten.

Tabel 2.

Ontoelaatbare verhoortechnieken uit het onderzoek van Verhoeven en Duinhof (2017).

Verhoortechniek	Voorbeeld
Benadrukken van de consequenties van het blijven ontkennen	*"En je bent er niet bij gebaat door je mond te houden en niet met ons te praten." (p. 177)*
Beroep doen op het geweten van de verdachte	*"En diep in je hart weet je ook dat je gewoon het goede ding moet doen." (p. 178)*
Dreigen met psychologische pijn	*"En ik hoop dat het heel zwaar weegt. Echt waar. Dat hoop ik van ganser harte." (p. 183)*
Dreigen met lichamelijke pijn (fysieke intimidatie van de verdachte)	*"Dat je er elke dag hoofdpijn van heb. Echt waar. Ik hoop het echt." (p. 184)*
De verdachte beledigen	*"Wees toch eens een vent, man!" (p. 186)*
Het geven van een compliment aan de verdachte[3]	*"Nee, nou, vind wel echt goed van je dat je dit verteld hebt." (p. 211)*
Een beloning aanbieden aan de verdachte	*"Als je dat tegen mij vertelt, dan zijn we klaar. Ik beloof het je." (p. 215)*
Autoriteit en ervaring ten opzichte van de verdachte benadrukken	*"Wij werken met internet, hè? Dus we weten dat wel. Ik doe heel veel internet. Mijn hobby, dus ik weet hoe het werkt, hè?" (p. 193)*

Nog specifieker heeft Van Kuppevelt (2020) in haar onderzoek naar het verhoor van cyberdaders (waaronder ook een aantal hackers) gevonden dat ook cybercrimeteams risicovolle technieken toepassen. Zo uiten de verhoorders bijvoorbeeld twijfels over de onschuld van een verdachte of geven zij hun mening over het delict. In mindere mate komt het ook voor dat verhoorders aan het drammen zijn om informatie bij de verdachte los te krijgen: "*Ik zie aan je dat je het misschien wel kan vertellen. We gaan je nog een paar vragen stellen en misschien dat je tot de conclusie komt dat je het beter wel kan vertellen*." (Van Kuppevelt, 2020, p. 30).

[3] Hierbij moet worden benadrukt dat het geven van complimenten in sommige gevallen ook toelaatbaar kan zijn. Het is in ieder geval risicovol wanneer de verdachte wordt aangemoedigd verder te gaan met zijn verhaal.

Het toepassen van ontoelaatbare technieken, zeker in combinatie met een langdurend verhoor, brengt diverse gevaren met zich mee (Drizin & Leo, 2004; Redlich, Kulish, & Steadman, 2011; Verhoeven & Duinhof, 2017). Allereerst is het mogelijk dat een hackverdachte dichtslaat of weerstand biedt vanwege de technieken die worden toegepast in het verhoor (Beijer, 2012). Indien geen ander bewijsmateriaal voorhanden is in de zaak, kan het cybercrimeteam daardoor met lege handen komen te staan en gaat een mogelijk schuldige hackverdachte vrijuit. Verder kan een verdachte ook onbetrouwbare informatie delen wanneer in het verhoor gebruik wordt gemaakt van druk (Geijsen & De Ruiter, 2017). Het team verliest mogelijk kostbare tijd als zij verder gaat rechercheren op basis van onjuiste informatie. Tot slot bestaat de mogelijkheid dat een onschuldige verdachte onder druk van verhoortechnieken een valse bekentenis aflegt (Kassin, 1997; Van Amelsvoort & Rispens, 2017). Die kans is bijvoorbeeld erg groot wanneer verhoorders fictief bewijs voorleggen aan de verdachte (Kassin, 2008; Kassin, Drizin et al., 2010). Zodra dat gebeurt, is er geen sprake meer van een waarheidsgetrouwe en nauwkeurige bekentenis; terwijl dat juist van belang is (Gudjonsson & Pearse, 2011). Een onbetrouwbare of valse verklaring heeft een grote negatieve consequentie voor een onschuldige verdachte; hij kan immers op basis van de verklaring ten onrechte worden veroordeeld, wat tevens ondermijnend is voor het rechtssysteem (Verhoeven, 2014). Vanwege de risico's die verbonden zijn aan het verhoor is het van belang dat de verhoorders binnen de cybercrimeteams kennis hebben van en rekening houden met de mogelijke beïnvloeding van het menselijke gedrag. Ook moeten toelaatbare technieken worden gebruikt in het verhoor van hackverdachten (Van Amelsvoort & Rispens, 2017).

2.4 Kwetsbare verdachten in het verhoor

Bij kwetsbare verdachten is het van nog groter belang dat verhoorders rekening houden met de mogelijke beïnvloeding van het menselijke gedrag. In de Nederlandse politiepraktijk wordt een verdachte onder andere aangemerkt als kwetsbaar wanneer hij onder de zestien jaar oud is (Van Amelsvoort & Rispens, 2017). Jongeren zijn over het algemeen kwetsbaar in het verhoor, omdat zij doorgaans nog geen goede afwegingen kunnen maken (Kassin, Drizin et al., 2010; Kassin & Gudjonsson, 2004). Daardoor nemen zij veel korte termijn beslissingen en zijn ze erg gevoelig voor onmiddellijke beloningen en straffen (Kassin, 2008). Naast jongeren worden ook verdachten met een verstandelijke beperking, een cognitieve functiestoornis of een psychiatrische stoornis binnen de politieorganisatie gezien als een kwetsbaar persoon (Van Amelsvoort & Rispens, 2017). Zodoende worden ook verdachten met bijvoorbeeld ADHD of een autismespectrumstoornis als kwetsbaar geacht (Politieacademie, z.d.-a). Aangezien

sommige hackers minderjarig zijn of een autismespectrumstoornis hebben (Aiken et al., 2016; Ledingham & Mills, 2015; National Crime Agency, 2017; Van der Wagen et al., 2019), kunnen zij ook worden aangemerkt als kwetsbare verdachten in het politieverhoor.

Kwetsbare verdachten zijn gevoeliger voor het afleggen van een valse bekentenis of een onbetrouwbare verklaring (Kassin, 2008, 2017; Kassin, Appleby, & Torkildson Perillo, 2010; Kassin, Drizin et al., 2010; Kassin & Gudjonsson, 2004; North et al., 2008). Bovendien bestaat de kans dat zij dichtslaan in het verhoor (Beijer, 2012). Deze gevaren spelen met name een rol wanneer kwetsbare verdachten worden onderworpen aan een normaal verhoor waarin allerlei technieken worden toegepast (Kassin, 2008, 2017). Dat heeft te maken met het feit dat kwetsbare verdachten gevoeliger zijn voor druk, meer geneigd zijn tot compliant gedrag en vatbaarder zijn voor suggestieve vragen (Kranendonk, 2017; Van Amelsvoort & Rispens, 2017). Bovendien kunnen zij doorgaans geen goede inschatting maken van de gevolgen van eigen verklaringen vanwege het beperkte inzicht in oorzaak-gevolgrelaties (Kranendonk, 2017; Uzieblo, 2014). In de literatuur worden drie redenen beschreven waarom verdachten een valse bekentenis afleggen. Zo zijn er de vrijwillige valse bekentenissen (‘*voluntary false confessions*’), waarbij verdachten zonder druk van de politie een verklaring afleggen. Dat kan een verdachte bijvoorbeeld doen om een familielid te beschermen (Kassin, 1997; Kassin & Wrightsman, 1985). Een kwetsbare verdachte kan dat specifiek ook doen om stoer te zijn of omdat hij ergens bij wil horen (Kranendonk, 2017). De overige valse bekentenissen zullen bij de neiging tot compliant gedrag en de vatbaarheid voor suggestibiliteit aan bod komen.

Kwetsbare verdachten zijn aldus gevoelig voor suggestibiliteit (Garrett, 2010; Kassin, 2017; Kassin & Gudjonsson, 2004; Kranendonk, 2017). Opmerkelijk genoeg worden in de Nederlandse verhoorpraktijk veel suggestieve vragen gesteld aan kwetsbare verdachten (Geijsen, Vanbelle et al., 2018). Dat is gevaarlijk, omdat kwetsbare verdachten doorgaans een verminderd geheugen hebben, veel angst vertonen in het verhoor en een laag zelfbeeld hebben. Wanneer verhoorders suggestieve vragen stellen, negatieve feedback geven of fictief bewijs voorleggen, kunnen de herinneringen van kwetsbare verdachten worden vervormd. Dan is de kans groot dat zij met onbetrouwbare en misleidende informatie komen (Kassin, 2008; Kassin, Drizin et al., 2010; Kassin & Kiechel, 1996). Vaak gaat het om ingebeelde, geïnternaliseerde valse bekentenissen (‘*coerced-internalized false confessions’*) waarbij de verdachten erin gaan geloven dat zij het misdrijf hebben gepleegd (Kassin & Wrightsman, 1985).

Verder komt de neiging tot compliant gedrag bij kwetsbare verdachten voort uit het willen ‘pleasen’ van anderen en het willen vermijden van confrontaties in sociale situaties (zoals het verhoor) (Kassin, 2008). Bovendien zijn kwetsbare verdachten geneigd om met alle

vragen van de verhoorders in te stemmen, ongeacht de inhoud van de vraag; wat ook wel acquiescence wordt genoemd. Overigens komt het ook voor dat niet-kwetsbare verdachten volgzaam zijn, omdat ze de verhoordruk willen verminderen. Verdachten kunnen denken dat ze door het vertonen van compliant gedrag eerder naar huis mogen (Kranendonk, 2017). Zodra een verdachte een verklaring aflegt om te kunnen ontsnappen aan de druk van het verhoor, kan er worden gesproken van een gedwongen valse bekentenis door de politie (‘*coerced-compliant false confessions’*) (Kassin, 1997; Kassin & Wrightsman, 1985). Wanneer kwetsbare verdachten valse bekentenissen afleggen, is de kans groot dat de verklaring onder deze groep bekentenissen valt. Zij zijn immers erg gevoelig voor compliant gedrag (Kranendonk, 2017).

Specifiek spelen bij autistische kwetsbare verdachten, waar hackers ook onder kunnen vallen, de volgende risico’s een rol. Autistische verdachten blijken met name geneigd te zijn om confrontaties te voorkomen in het verhoor (North et al., 2008). Zij denken de vervelende situatie van het verhoor te kunnen ontwijken door met valse informatie te komen (Beijer, 2012). Een ander risico kan zijn dat zij een bekentenis afleggen terwijl dat niet in het eigen belang is. Autistische verdachten kunnen in het verhoor namelijk de neiging hebben om de regie tijdens een gesprek over te nemen en veel te gaan praten (Beijer, 2012). Dat kan onder andere betekenen dat kwetsbare verdachten hun rechten niet begrijpen of dat ze hun rechten wel begrijpen maar tegen hun zin in het verhaal gaan vertellen, omdat ze niet kunnen zwijgen.

Vanwege bovenstaande gevaren is het van groot belang dat verhoorders door het stellen van de eerder genoemde VIK-vragen een vermoeden krijgen van de kwetsbaarheid van de verdachte in kwestie. In dat geval krijgt de verdachte ter bescherming een advocaat toegewezen in het verhoor. Tevens is het van belang dat verhoorders kennis hebben van de omgang met kwetsbare verdachten, zodat zij rekening kunnen houden met de problematiek van de verdachte in kwestie (zoals bij het toepassen van methoden en technieken). Zij kunnen in dat geval er ook voor kiezen om een gespecialiseerde verhoorder in te zetten die een verhooropleiding heeft gevolgd op het gebied van kwetsbare verdachten (Van Amelsvoort & Rispens, 2017).

2.5 Kennis en vaardigheden van de verhoorders

Naast de kennis op het gebied van kwetsbare verdachten, wordt in de Handleiding Verhoor ook benadrukt dat rechercheurs in algemene zin verhoorkennis moeten hebben om het verhoor op een professionele manier uit te voeren (Van Amelsvoort & Rispens, 2017). Voor het verkrijgen van competenties om het verhoor goed uit te kunnen voeren en het worden van een verhoorspecialist, bestaan de module ‘Verdieping op Verhoor’ en de opleiding ‘Professioneel Verhoor Verkort’ (Odinot, Boon, & Wolters, 2015; Politieacademie, z.d.-b, z.d.-c). Enkele

competenties zijn bijvoorbeeld het kunnen toepassen van verhoormethoden, het op de hoogte zijn van relevante wet- of regelgeving en het beschikken over communicatieve vaardigheden (Van Amelsvoort & Rispens, 2017). Tot op heden is het niet bekend in welke mate rechercheurs binnen de cybercrimeteams een verhooropleiding hebben gevolgd en over wat voor verhoorkennis zij beschikken. De verwachting is echter dat de technische rechercheurs in vergelijking met de tactische rechercheurs minder opgeleid zijn, omdat zij van buiten de politie worden aangenomen. Daardoor zouden zij mogelijk minder of zelfs onvoldoende competenties hebben om het verhoor op een professionele manier uit te kunnen voeren.

Bovendien is het van belang dat rechercheurs bekend zijn met de inhoudelijke materie van het delict in kwestie (Van Amelsvoort & Rispens, 2017). Dat betekent dat de verhoorders over relevante computerkennis en -vaardigheden moeten beschikken, zodat zij het verhaal van de verdachte kunnen begrijpen en kunnen doorvragen naar technologische onderwerpen die een rol spelen bij de hack. Uit de studie van Harkin, Whelan, en Chang (2018) naar cybercrimeteams in Australië blijkt echter dat de huidige trainingen binnen de politie op het gebied van cybercrime en computervaardigheden inadequaat zijn. Ook in Nederland wordt gesproken over een tekort aan kennis op deze deelgebieden (Klap et al., 2012; Stol, 2010). Zo is er binnen de Politieacademie bijvoorbeeld ook geen gerichte opleiding omtrent cybercrime. Hoewel het inhuren van ICT-experts van buiten de politieorganisatie bij zal dragen aan het verbeteren van het kennisniveau binnen de cybercrimeteams, is het tot op heden niet bekend in hoeverre de tactische rechercheurs over de benodigde digitale kennis beschikken. Wanneer zij niet over voldoende kennis beschikken, bestaat de verwachting dat zij het verhoor minder succesvol kunnen uitvoeren. Dan is het risico dat er niet voldoende kan worden doorgevraagd op de materie in kwestie en is een verdachte wellicht ook minder geneigd een verklaring af te leggen, omdat hij bijvoorbeeld van mening is dat de verhoorder hem toch niet begrijpt.

Mogelijk wordt vanwege de verschillende kennisniveaus het verhoor van hackverdachten uitgevoerd door zowel een tactische als een technische verhoorder (Van Kuppevelt, 2020). Gezamenlijk lijken zij over voldoende kennis te beschikken om het verhoor van een hackverdachte op een juiste manier uit te kunnen voeren. Het is tot op heden echter niet bekend of de samenstelling van het verhoorteam en de kennisniveaus van de verhoorders daadwerkelijk een rol spelen in het verhoor van verdachten van hackdelicten.

3. Data en methode

3.1 Onderzoeksmethode en dataverzameling

Voortkomend uit het feit dat het verhoor van hackverdachten een weinig onderzocht fenomeen is, betreft deze studie een verkennend en beschrijvend onderzoek. Op basis van kwalitatief onderzoek wordt een poging gedaan om eerste diepgaande inzichten te verkrijgen in het verhoorproces van verdachten van hackdelicten bij de cybercrimeteams (Bijleveld, 2013). Het voordeel van een kwalitatieve onderzoeksmethode is dat er een diepgaand gevarieerd beeld van het verhoorproces kan ontstaan, waarbij de perspectieven van verschillende respondenten kunnen worden beschreven (Hennink, Hutter, & Bailey, 2011). Daarvoor is in dit onderzoek gebruikgemaakt van een deductieve onderzoeksmethode. Met behulp van een onderzoeksvraag en meerdere deelvragen wordt het verhoor van hackverdachten beschreven in het licht van verschillende belangrijke empirische gegevens en concepten uit de literatuur op het gebied van het algemene verhoorproces. Verder heeft de dataverzameling plaatsgevonden middels semigestructureerde interviews met experts die betrokken zijn bij het verhoor van verdachte hackers (Baarda & Van der Hulst, 2017). In deze studie worden onder experts de respondenten verstaan die werkzaam zijn bij de cybercrimeteams, advocaten en cyberofficieren van justitie.

Een nadeel van kwalitatief onderzoek is de beperkte generaliseerbaarheid of externe validiteit. De bevindingen die in de onderzochte groep gelden, hoeven niet noodzakelijkerwijs te gelden buiten die groep (Bijleveld, 2013). In deze studie kunnen door de focus op cybercrimeteams geen conclusies worden getrokken over het verhoor bij andere teams, zoals de districtsrecherche, de basisteams of het THTC. Toch wordt de beperkte generaliseerbaarheid niet als een beperking gezien, omdat het doel van dit verkennend onderzoek was om een eerste inzicht te krijgen in het verhoor en niet om algemene uitspraken te doen.

3.2 Respondenten en werving

Voor het werven van de respondenten zijn verschillende strategieën toegepast, die een groep van 18 respondenten hebben opgeleverd. Het merendeel van de respondenten was man, de gemiddelde leeftijd lag rond de 45 jaar (variërend van 30 tot en met 58 jaar) en de gemiddelde werkervaring was ongeveer 16 jaar (variërend van 2 tot en met 36 jaar). In tabel 3 zijn de persoonskenmerken in willekeurige volgorde inzichtelijk gemaakt. Omwille van de anonimiteit en eventuele herleidbaarheid van de respondenten zijn in deze tabel geen respondentnummers opgenomen. In de volgende drie paragrafen worden per respondentengroep afzonderlijk de wervingsstrategie en persoonskenmerken beschreven.

Tabel 3.

Persoonskenmerken van de respondenten.

Geslacht	Leeftijd	Werkervaring
Man	58 jaar	21 jaar
Man	49 jaar	13 jaar
Man	39 jaar	14 jaar
Man	47 jaar	26 jaar
Vrouw	34 jaar	2 jaar
Man	45 jaar	21 jaar
Man	37 jaar	9 jaar
Vrouw	57 jaar	36 jaar
Man	50 jaar	6 jaar
Man	54 jaar	29 jaar
Man	39 jaar	8 jaar
Man	42 jaar	16 jaar
Man	40 jaar	16 jaar
Man	47 jaar	21 jaar
Man	30 jaar	10 jaar
Man	33 jaar	6 jaar
Man	46 jaar	14 jaar
Vrouw	49 jaar	26 jaar

3.2.1 Cybercrimeteams

Binnen de politie is ervoor gekozen om interviews af te nemen bij de cybercrimeteams, onder andere omdat deze teams veel te maken krijgen met hackzaken (Boekhoorn, 2019). Na het verkrijgen van schriftelijke toestemming vanuit de onderzoekscoördinatie van de politie, verliep het contact met het eerste team via het netwerk van de scriptiebegeleiders. Vanuit het Landelijk Operationeel Cyber Overleg (LOCO) werd een mail verstuurd naar de teamleider met de vraag om deel te nemen aan het onderzoek en is er gevraagd naar potentiële respondenten met verhoorervaring. Met deze respondenten is telefonisch of via de mail de deelname aan het interview verder besproken. Bovendien is aan de geïnterviewden gevaagd om andere mogelijk geïnteresseerde respondenten binnen het eigen of een ander team aan te dragen. Op die manier is ook contact gelegd met respondenten werkzaam bij drie andere cybercrimeteams in het land.

Zodoende is in dit onderzoek naast het contact via LOCO de sneeuwbalmethode als wervingsstrategie gebruikt. Hiervoor is gekozen omdat rechercheurs binnen de teams kunnen worden gezien als een lastige doelgroep, omdat ze niet makkelijk vindbaar zijn (Bijleveld, 2013). Doorgaans is een risico van de sneeuwbalmethode het verkrijgen van een homogene respondentenpopulatie (Bijleveld, 2013). In deze studie is dat echter geen beperking, omdat de methode juist landelijke spreiding heeft opgeleverd (Hennink et al., 2011). Bovendien is er bewust geprobeerd om een heterogene groep respondenten te verkrijgen. Zo is tijdens de werving bijvoorbeeld aan de respondenten gevraagd om collega's met een andere achtergrond aan te dragen, zoals technische rechercheurs of collega's met een bepaalde verhooropleiding.

De respondenten zouden dat bespreken met hun collega's, waardoor de response rate niet bekend is bij deze groep respondenten. Het is wel bekend dat zeven teams zijn benaderd, waarvan uiteindelijk in vier verschillende teams interviews zijn afgenomen. De teams zijn gevarieerd wat betreft de soorten zaken waarmee zij te maken krijgen en hoelang ze al bestaan. Twee teams bestaan daarbij al enige tijd en twee andere teams zijn meer recentelijk opgericht[4]. In het eerste team zijn 6 interviews afgenomen, in het tweede team 3 interviews, in het derde team 1 interview en in het vierde team 2 interviews. Zodoende hebben de wervingsstrategieën in totaal een groep van 12 respondenten opgeleverd (aangegeven met R1 tot en met R12[5]).

Daarvan zijn 7 interviews afgenomen met tactische rechercheurs en 3 interviews met technische rechercheurs die binnen de cybercrimeteams het verhoor uitvoeren. In deze studie is ervoor gekozen om technische rechercheurs te interviewen, omdat op basis van het theoretisch kader de verwachting bestond dat zij minder verhoorkennis zouden hebben. Het doel was daarom om te kijken of zij andere inzichten zouden hebben op het gebied van het verhoor in vergelijking met tactische collega's. Bovendien zijn er 2 teamleiders geïnterviewd om een overzichtelijk beeld te krijgen van de cybercrimeteams, waaronder de samenstelling van de verhoorteams. De respondenten waren gemiddeld 46 jaar oud en de gemiddelde werkervaring was ongeveer 18 jaar. Enkel de tactische rechercheurs hadden binnen de politie al ervaring opgedaan met het verhoor van andere verdachten die offline delicten plegen. Verder liep de ervaring wat betreft het verhoor van hackverdachten sterk uiteen, variërend tussen de 1 en 100 uitgevoerde verhoren door de rechercheurs. Tot slot hadden 4 tactische rechercheurs een verhooropleiding gevolgd en gaf de meerderheid van de respondenten aan over voldoende inhoudelijke kennis op het gebied van cybercrime te beschikken.

[4] Deze laatste twee cybercrimeteams zijn in de afgelopen 4 jaar opgericht.
[5] Deze respondentnummers zijn omwille van de anonimiteit en eventuele herleidbaarheid van de respondenten willekeurig toegekend.

3.2.2 Advocaten

Verder zijn in dit onderzoek ook interviews afgenomen met advocaten, omdat de verwachting bestond dat zij het verhoor vanuit een andere invalshoek zouden kunnen beschrijven. Daardoor zou een gevarieerder beeld van het verhoor kunnen ontstaan. Voor de werving is online gezocht naar strafrechtadvocaten die zich onder andere bezighouden met cybercrime of zich daarin hebben gespecialiseerd. Met hen is via de mail contact opgenomen en is voor zover mogelijk geprobeerd om telefonisch de deelname aan het interview verder te bespreken.

Tijdens de wervingsprocedure zijn 13 verschillende advocaten benaderd, waarvan 4 advocaten mee wilden werken aan het onderzoek (aangegeven met RA1 tot en met RA4). De gemiddelde leeftijd van de respondenten was rond de 37 jaar en de gemiddelde werkervaring was ongeveer 11 jaar. Verder gaven de advocaten aan dat zij geen opleiding hadden gevolgd op het gebied van cybercrime, maar dat ze wel over redelijk veel kennis beschikten op dat gebied. Ook hadden zij al ervaring opgedaan met het verhoor van hackverdachten. Drie advocaten gaven aan dat zij vooral in aanraking kwamen met de districtsrecherche of het THTC, waardoor zij niet altijd volledig antwoord konden geven op de onderzoeksvraag die betrekking heeft op het verhoorproces bij de cybercrimeteams. Dat heeft invloed op de interne validiteit van de studie, waarbij de vraag centraal staat of er gemeten is wat er beoogd werd te meten en of de onderzoeksresultaten een juiste afspiegeling zijn van het verhoorproces bij de cybercrimeteams (Boeije 2014). Desalniettemin bespraken de advocaten in sommige gevallen toch relevante inzichten met betrekking tot het verhoor bij de overige teams. Vanwege de verkennende aard van deze studie, zullen deze resultaten worden beschreven indien ze ook betrekking zouden kunnen hebben op het verhoorproces bij de cybercrimeteams.

3.2.3 Officieren van justitie

Tot slot zijn voor het verkrijgen van een nog gevarieerder beeld van het verhoor cyberofficieren van justitie geïnterviewd die te maken krijgen met cybercrimezaken. Zij geven leiding aan de cybercrimeteams tijdens het opsporingsonderzoek en moeten ervoor zorgen dat dit zorgvuldig en volgens de regels gebeurt (Openbaar Ministerie, 2018). Daardoor hebben zij zicht op het verhoorproces van hackverdachten. De cyberofficieren zijn in dit onderzoek geworven via de contacten van een scriptiebegeleider binnen het Openbaar Ministerie (OM). Doordat de contactpersonen binnen het OM contact hebben opgenomen met hun collega's, is de response rate bij deze groep niet bekend. Uiteindelijk is met twee geïnteresseerde respondenten (aangegeven met RO1 en RO2) via de mail contact opgenomen om de deelname aan het onderzoek te bespreken. De gemiddelde leeftijd van deze respondentengroep lag rond de 45

jaar en daarnaast waren de respondenten al zo'n 18 jaar in dienst bij het OM. Beide officieren gaven aan over voldoende kennis te beschikken op het gebied van cybercrime.

3.3 Onderzoeksprocedure

Voorafgaand aan de interviews is aan de respondenten toestemming gevraagd voor het auditief opnemen van het interview met een audiorecorder (Baarda & Van der Hulst, 2017). Dat is bevorderlijk voor de betrouwbaarheid van de studie, omdat de waarnemingen van de interviews dan zo min mogelijk worden beïnvloed door toevallige fouten (Boeije, 2014). Ook is aan de respondenten gevraagd om via de mail toestemming te geven op het informed consentformulier (opgenomen in bijlage 2), zodat men geïnformeerd is over het doel van het onderzoek en de manier waarop de data zal worden gebruikt (Decorte & Zaitch, 2016). Eén respondent, met wie het interview fysiek is afgenomen, heeft dit formulier schriftelijk ondertekend.

De interviews duurden allemaal ongeveer een uur. In deze studie is gekozen voor een semigestructureerde interviewmethode, omdat door de flexibiliteit van de methode diepgaande verhoorinzichten kunnen worden verkregen. Vooraf is een vragenlijst opgesteld met open vragen, waardoor tijdens de interviews grotendeels dezelfde vragen aan bod kwamen. De interviews kunnen op deze manier beter met elkaar worden vergeleken, wat bevorderlijk is voor de interne validiteit van het onderzoek (Boeije, 2014). De volgorde van het stellen van vragen werd bepaald door het verloop van het interview en het was ook mogelijk om tijdens de interviews zelf op bepaalde onderwerpen dieper in te gaan (Baarda & Van der Hulst, 2017).

De interviews zijn vanwege de coronamaatregelen grotendeels online via Microsoft Teams afgenomen. Desalniettemin zijn 6 interviews telefonisch en 1 interview via Whatsapp videobellen afgenomen, omdat Teams niet werkte of de voorkeur van de respondent hiernaar uitging. Bovendien heeft 1 interview op verzoek van een advocaat fysiek plaatsgevonden. Hoewel het bij online en telefonisch interviewen vanzelfsprekend lastiger is om de lichaamstaal van de respondenten te observeren (Janghorban, Latifnejad Roudsari, & Taghipour, 2014; Nind, Meckin, & Coverdale, 2021), worden deze interviewmethoden in de literatuur omschreven als een goed alternatief voor het fysieke interview (Cachia & Millward, 2011; Johnson, Scheitle, & Ecklund, 2019; Lobe, Morgan, & Hoffman, 2020; Lo Iacono, Symonds, & Brown, 2016; Nind et al., 2021). In de praktijk gaven de respondenten in de meeste gevallen uitgebreide antwoorden en kon bij het online interview toch een groot deel van de lichaamstaal van de respondenten worden geobserveerd (Lo Iacono et al., 2016).

Uiteindelijk zijn de interviews getranscribeerd via het programma Express Scribe. Tijdens de interviews is actief geluisterd naar de respondenten, maar de stopwoorden van de

interviewer (zoals ‘ja’ of ‘nee’) zijn niet uitgewerkt. Ook is ervoor gekozen om versprekingen niet te transcriberen, omdat het geen toegevoegde waarde zou hebben voor het onderzoek. Verder is tijdens het uitwerken van de interviewtranscripten de anonimiteit van de respondenten gewaarborgd en is op een vertrouwelijke manier omgegaan met zaakspecifieke informatie, omdat persoonlijke en herleidbare zaken zijn weggelaten. De audio-opnames en geanonimiseerde interviewtranscripten zijn op een beveiligde USB-stick opgeslagen.

3.4 Operationalisering

Zoals eerder beschreven is in dit onderzoek gebruikgemaakt van een vragenlijst bestaande uit open vragen waarin de centrale onderzoeksvraag en deelvragen zijn geoperationaliseerd. Bij deze vragen staan de ervaring en perceptie van de respondenten met het verhoor centraal. De vragenlijst is gezamenlijk met de scriptiebegeleiders opgesteld, wat bevorderlijk is voor de betrouwbaarheid van de studie (Boeije, 2014). Bij het opstellen van de vragenlijst is rekening gehouden met relevante verhoorconcepten uit de literatuur, waaronder uit de Handleiding Verhoor van Van Amelsvoort en Rispens (2017). In de vragenlijst wordt ingegaan op (1) de achtergrond van de respondent en (2) het cybercrimeteam waar de respondent werkzaam is. In het geval van een interview met een advocaat of een cyberofficier van justitie is gevraagd naar de eigen werkachtergrond en diens ervaring met de cybercrimeteams. Daaropvolgend kwamen (3) hacken en de persoonskenmerken van hackers, (4) het verhoorproces van hackverdachten (inclusief de verhoormethoden en -technieken die worden toegepast), (5) de samenstelling van de verhoorteams en (6) het kennisniveau van de verhoorders aan bod. De afsluitende vragen gingen over (7) de knelpunten en optimalisaties van het verhoor van hackverdachten.

In bijlage 2 is de vragenlijst inzichtelijk gemaakt, waarbij de gekleurde vragen worden gezien als de meest belangrijke vragen om de onderzoeksvraag en deelvragen te kunnen beantwoorden. De overige vragen werden in tijdnood overgeslagen, omdat deze vragen enkel meer diepgang zouden aanbrengen op het gebied van de belangrijkste verhoorconcepten. Zodoende kwamen in alle interviews de belangrijkste vragen aan bod en werd in sommige interviews iets meer diepgang aangebracht met de overige vragen. Bovendien zijn tijdens de dataverzameling, op basis van de gegeven antwoorden door de respondenten, enkele vragen qua bewoording aangepast of toegevoegd. Een voorbeeld heeft betrekking op de etnische achtergrond van hackverdachten. Halverwege de dataverzameling werd namelijk tijdens een interview een verschil gevonden ten opzichte van de literatuur, waarna in de daaropvolgende interviews voor het eerst actief naar etniciteit is gevraagd. Een nadeel daarvan is uiteraard dat

op dit onderwerp minder harde conclusies kunnen worden getrokken, omdat tijdens de eerdere interviews niet op de etnische achtergrond van hackverdachten in is gegaan.

3.5 Analysemethoden

Met behulp van een kwalitatieve data-analyse zijn de interviewtranscripten geanalyseerd middels het programma ATLAS.ti. Om de dataset overzichtelijk te maken, zijn verschillende analysetechnieken toegepast (Evers, 2015). Zo is een deductieve analysetechniek gebruikt met enkele vooraf bedachte thematische codes, gebaseerd op de onderwerpen van de vragenlijst (bijvoorbeeld VH_techniek_verstandshouding[6] en Hacken_leeftijd). Daarnaast is ook gebruikgemaakt van een inductieve analysetechniek met open codes die uit de data zelf voortkomen (bijvoorbeeld VH_methode_verdachteafhankelijk of Hacken_slimmejongens). Vervolgens is er middels axiaal coderen nogmaals gekeken naar de codes en is er gezocht naar patronen in de data (Van Gorp, 2007). Overeenkomende codes zijn daarbij samengevoegd en ondergebracht door middel van een hoofdcode. Zo zijn ter illustratie de codes Hacken_ADHD en Hacken_psychkenmerken samengevoegd, omdat ADHD minder citaten bevatte en de code omtrent psychische kenmerken van verdachten algemener en meer overkoepelend was.

Hierop volgend is tijdens de fase van selectief coderen gezocht naar verbanden en tegenstellingen in de interviewtranscripten (Boeije, 2014). Daarbij is aan de hand van de analysetechnieken geprobeerd om tot een antwoord te komen op de centrale onderzoeksvraag en deelvragen; en om de onderzoeksresultaten te beschouwen in het licht van het theoretisch kader (Evers, 2015). In de resultatenparagraaf zijn verschillende citaten uit de interviewtranscripten gebruikt om de onderzoeksresultaten toe te lichten. Tot slot zijn gedurende het gehele analyseproces memo's bijgehouden, omdat dat volgens Hennink et al. (2011) zou leiden tot een beter begrip van de data en een kritischere blik daarop. Binnen deze memo's is onder andere gereflecteerd op de eigen werkwijze en zijn gemaakte keuzes tijdens de analyse toegelicht. Ook zijn tussentijdse gedachten en reflecties bijgehouden, zodat deze niet verloren zouden gaan. Hiervoor is gekozen, omdat het documenteren van het proces volgens Evers (2015) bevorderlijk is voor de externe betrouwbaarheid van het onderzoek.

[6] VH is een afkorting die in ATLAS.ti is gebruikt om het verhoor aan te duiden.

4. Resultaten

In dit hoofdstuk worden de belangrijkste onderzoeksbevindingen beschreven. Het doel van deze studie is om inzicht te krijgen in het verhoorproces van verdachten van hackdelicten bij de cybercrimeteams in Nederland. Daarvoor zijn 18 interviews afgenomen met respondenten werkzaam bij diverse cybercrimeteams (N = 12), advocaten (N = 4) en cyberofficieren van justitie (N = 2). Hieronder zal eerst worden ingegaan op de persoonskenmerken van verdachte hackers, waarna het verhoorproces aan bod komt. Daarbij worden de fasen, de verschillen ten opzichte van het verhoor van verdachten die offline delicten plegen, methoden en -technieken, en de risico's van het verhoor beschreven. Tot slot komen de samenstelling van het verhoorteam, het kennisniveau van de rechercheurs en de optimalisatie van het verhoor aan bod. Indien relevant zal een onderscheid worden gemaakt tussen rechercheurs met en zonder opleiding. Wanneer een resultaat samenhangt met het volgen van een specifieke opleiding dan zal dat worden aangegeven. In totaal hebben vier tactische rechercheurs een opleiding gevolgd[7].

4.1 Persoonskenmerken van hackverdachten

4.1.1 Leeftijd, geslacht en psychische kenmerken

De respondenten geven aan dat zij geen standaard profiel kunnen opstellen van 'de verdachte hacker'. Wel benoemen alle respondenten dat zij enkel mannelijke verdachten in het verhoor hebben getroffen en dat de verdachten rond de twintig jaar oud zijn. Het komt volgens enkele respondenten ook weleens voor dat hackverdachten minderjarig of tussen de dertig en vijftig jaar oud zijn. Elf respondenten vermoeden bovendien dat ze weleens te maken hebben gehad met een verdachte met een autismespectrumstoornis. Kenmerken waarover de verdachten beschikken zijn onder andere het hebben van weinig sociale contacten, het in zichzelf gekeerd zijn, het hebben van één focus en het voelen van de noodzaak dat alles geordend moet zijn. Andere psychische kenmerken die in mindere mate door enkele respondenten worden teruggevonden zijn ADHD, een licht verstandelijke beperking en een hoog intelligentieniveau.

Afgezien van deze gedetecteerde psychische kenmerken, worden hackverdachten zonder duidelijke redenen door de meerderheid van de respondenten niet gezien als kwetsbare verdachten. Drie advocaten en één rechercheur (die de training Communiceren met Kwetsbare Personen had gevolgd) zijn daarentegen wél van mening dat autistische hackverdachten als kwetsbaar kunnen worden aangemerkt. Bovendien geven twee niet-opgeleide rechercheurs aan dat minderjarige hackverdachten als kwetsbaar kunnen worden aangemerkt. Ondanks het feit

[7] In deze studie wordt hier een verhooropleiding of een opleiding omtrent kwetsbare verdachten onder verstaan.

dat hackverdachten over het algemeen niet als kwetsbaar worden bestempeld, stellen enkele rechercheurs dat zij wel in enige mate rekening houden met psychische kenmerken van verdachten. Het onderstaande citaat biedt een illustratie:

> *(…) Ja en je gaat even peilen van hoe, hoe groot is zijn kennis hè. Dus als hij moeilijke woorden zegt en hij heeft elke keer zoiets van nou geen idee wat je bedoelt, ja dan zul je toch je woorden moeten aanpassen met een, met een verhoor. (…)* (R10)

4.1.2 Opleidingsniveau, technische vaardigheden en motivatie

Verder worden grote verschillen gevonden op het gebied van opleidingsniveau, technische vaardigheden en de motivatie om te gaan hacken. Op basis van deze persoonskenmerken lijken er zelfs twee typen hackverdachten te zijn. Enerzijds bespreekt een deel van de respondenten dat zij te maken krijgen met hoogopgeleide hackverdachten die een IT-opleiding hebben gevolgd en dusdanig technisch zijn dat ze allerlei tools in elkaar kunnen zetten. Zij zouden met name uit enthousiasme, interesse en uitdaging betrokken raken bij een hack. In mindere mate kunnen een financieel motief en het verkrijgen van macht ook een rol spelen bij dit type hackverdachte. Bovendien blijkt uit de antwoorden van de respondenten dat deze technische jongeren over het algemeen nog nooit eerder in aanraking zijn geweest met politie en justitie en dat bij dit type verdachte een autismespectrumstoornis het meest voorkomt. Anderzijds schetsen de overige respondenten een tweede type hackverdachte, die veelal een allochtone afkomst blijken te hebben[8]. De belangrijkste motieven die bij deze verdachten een rol blijken te spelen, zijn een financieel motief en het verkrijgen van macht. De respondenten geven aan dat dergelijke jongens veelal niet geschoold zijn, maar een hack kunnen plegen doordat zij relevante tools op het internet kopen. Op die manier zou cybercrime in vergelijking met vroeger veel toegankelijker zijn geworden en hebben hackers minder technische vaardigheden nodig. Die ontwikkeling wordt door de respondenten aangeduid als ‘cybercrime as a service’:

> *(…) Waar je eigenlijk de kennis die je nodig hebt, kun je online kopen hè. Dus als jij een phishingsite nodig hebt, die koop je gewoon, die je hoef je niet zelf meer te gaan bouwen. Daar wordt nog zelfs een instructievideo bij geleverd, hoe je die moet gaan gebruiken. Dus je hebt heel weinig technische kennis nodig. In principe zou iedereen met een handleiding daarmee aan de slag kunnen (…).* (R4)

[8] De etnische achtergrond van de technische hackers is onbekend, omdat dat niet met alle respondent is besproken.

Doordat cybercrime steeds toegankelijker is geworden, spreekt een deel van de respondenten bij de tweede groep hackverdachten over een verschuiving van straatcriminaliteit naar de onlinewereld. De straatjongens die vroeger klassieke delicten pleegden zoals woninginbraken of oplichting, zouden volgens de respondenten nu meer betrokken zijn geraakt bij cybercrime.

4.2 Het verhoor van verdachten van hackdelicten

4.2.1 Verhoorfasen

Hoewel er twee typen hackverdachten lijken te zijn, kan uit de antwoorden van de respondenten worden opgemaakt dat de verhoorfasen identiek aan elkaar zijn. Ook geeft men aan dat het verhoorproces overeenkomt met het verhoor van andere verdachten die offline delicten plegen. Het verhoor begint volgens de respondenten met het meegeven van de cautie aan de verdachte; wat volgens een respondent inhoudt dat de verdachte niet tot antwoorden verplicht is. Daarna vindt het persoonsgericht verhoor plaats, dat door veel respondenten wordt aangeduid met het 'sociaal verhoor'. Meerdere tactische rechercheurs geven aan dat ze deze fase erg belangrijk vinden, omdat ze dan erachter kunnen komen wie ze voor zich hebben zitten en ze de verdachte ook op zijn gemak kunnen stellen. R10 zegt daar het volgende over: "*(…) Ik vind dat een sociaal verhoor juist, juist is om contact te leggen met de verdachte om te kijken hoe staat hij erin en wat is zijn verklaringsbereidheid erin*." De minderheid van de respondenten benoemt ook dat er dan vragen worden gesteld over de woonsituatie, de financiële situatie, het opleidingsniveau, de werksituatie, mogelijke psychische aandoeningen en het medicijngebruik van de verdachte.

Toch zegt R8 het volgende over het persoonsgericht verhoor: *"(…) Met name (…) het persoonsgericht verhoor waar volgens mij toch heel snel, zeker door mensen die al veel langer dan ik bij de politie werken, snel overheen wordt gestapt*." Twee opgeleide rechercheurs benoemen inderdaad dat zij steeds minder algemene vragen aan de verdachte (laten[9]) stellen. R6 zegt: "*(…) Dan krijg je echt het antwoord van wat ben je nou voor sukkel? Jij werkt bij de politie dat hoor jij te weten, weet je dat, dat slaat nergens op. Het moet zin hebben die vragen. (…)"* Daarom is de rechercheur van mening dat de vragen een link met de zaak moeten hebben: *"(…) En persoonsgericht verhoor ga je een aantal onderwerpen ga je aankaarten, vier, vijf die wel te maken hebben met de zaak. (…*)" Ook vijf andere respondenten geven aan dat in deze fase al gegevens worden binnengehaald die mogelijk later in het onderzoek van belang zijn. Dat wordt door de respondenten omsingeling genoemd, waar R4 de volgende definitie van geeft: *"(…) Hoe je soms vragen eromheen kan stellen om de verdachte bij een punt te krijgen*

[9] In het geval van een verhoorcoach.

waarop hij eigenlijk al iets heeft verklaard waar hij later misschien ontkent (…).” Een voorbeeld is het stellen van vragen omtrent het alleengebruik van de computer van de verdachte:

> *(…) De verdachte verklaart in het sociaal verhoor van nou weet je, ja ik vind het lekker om te, om te gamen, ja dat doe ik op die laptop. Ja het is echt mijn laptop en ik ben de enige die erop zit en ik heb als enige het wachtwoord. Ja dan, als je dan vervolgens allerlei criminele dingen vindt op die laptop, dan kan je, dan kan hij niet meer zeggen ja nee dat heeft iemand anders gedaan. (…)* (R3)

Doordat veel vragen in het persoonsgericht verhoor al gericht blijken te zijn op de zaak, zijn twee advocaten en enkele rechercheurs van mening dat daardoor geen duidelijk onderscheid meer bestaat met de laatste fase van het verhoor, het zaakgericht verhoor. Het onderstaande citaat biedt een illustratie van een mening van een advocaat daaromtrent:

> *Formeel gezien gaat het er alleen over wie de verdachte is en niet over de zaak, niet over de verdenking. (…) Maar in feite valt dat altijd in elkaar over. Hè want sommige vragen bijvoorbeeld wat, wat vind je leuk, wat zijn je hobby’s? Ja hacken. Ja dan zit je al in het zakelijke dus dat loopt een beetje in elkaar over. Kijk die scheiding is wat, wat kunstmatig moet ik zeggen.* (RA2)

Tot slot wordt in de laatste fase van het verhoor daadwerkelijk ingegaan op de zaak. Na de afronding van het verhoor krijgt de cyberofficier van justitie mondeling of schriftelijk informatie over het verhoor van het cybercrimeteam, waarna deze zich gaat voorbereiden op de inhoudelijke zitting. Daar zegt RO1 het volgende over: *“(…) Dan krijg ik vaak een mondelinge terugkoppeling of kort op de mail. En af en toe zit het verhoor er ook achter als bijlage.*”

4.2.2 Verschillen met het verhoor van andere verdachten

Hoewel de verhoorfasen overeenkomen, bespreken de respondenten enkele verschillen wat betreft het verhoor van hackverdachten ten opzichte van het verhoor van andere verdachten die offline delicten plegen. Deze verschillen zullen hieronder worden beschreven. Een eerste verschil dat door zeven respondenten wordt besproken, heeft betrekking op het bewijs dat bij een hackzaak meer sluitend en overtuigend zou zijn ten aanzien van een reguliere zaak:

> *Het mooie is af en toe wel van ons werk dat ons bewijs heel zwart wit is. Dat anderen dat zien op jouw computer en we zien daar ook de foto's, de screenshots, al je verzonden mailtjes, je verschillende accounts, je IP-adressen, dat soort dingen (…).* (R6)

Aansluitend bij het bewijsmateriaal in een hackzaak, bespreekt een andere respondent het volgende over de duur van het verhoor van een hackverdachte:

> *(…) Ik vind hem veel interessanter, want je kan er veel meer uithalen. (…) Je bent tot in detail ben je al, heb je al, ik noem maar wat twintig pagina's aan vragen voor iemand weet je wel. In een normaal verhoor heb je dat natuurlijk niet. Jawel, maar niet zoveel. Dus het verhoor is al langer, maar het, maar het is een wereld van verschil.* (R5)

Het verhoor kan volgens vier rechercheurs[10] vier tot zeven uur lang duren. Een enkeling geeft aan dat het verhoor soms zelfs de hele dag duurt. Desalniettemin is een andere opgeleide rechercheur, die ook de cursus Communiceren met Kwetsbare Personen heeft gevolgd, van mening dat het verhoor zeker niet tien uur lang mag duren. De respondent is net als andere rechercheurs van mening dat het verhoor over meerdere dagen moet worden verspreid.

Wat betreft het bewijsmateriaal zijn diverse respondenten, en met name advocaten, echter van mening dat in sommige gevallen ook een andere uitleg van het bewijs mogelijk is en dat het bewijs helemaal niet zo sluitend hoeft te zijn bij een hackzaak. R8 stelt: "*(…) Dus hè IP-verkeer is heel arbitrair plus dat je ook nog alleen nog maar hebt dat er blijkbaar IP-verkeer is geweest, maar de stap die je nog moet maken naar een persoon die wordt dan heel lastig (…).*" Toch bespreekt de meerderheid van de rechercheurs dat ze doorgaans pas overgaan op het verhoor zodra ze over voldoende bewijsmiddelen beschikken en de zaak in principe rond is. In dat geval wordt de verklaring van de verdachte niet meer als noodzakelijk gezien. Het verhoor is dan volgens de rechercheurs vooral een mogelijkheid voor de verdachte om zijn kant van het verhaal te doen, maar is hij niet verplicht om daadwerkelijk een verklaring af te leggen.

Aansluitend beschrijven de respondenten die met de meer technische hackers te maken krijgen dat hackverdachten meer verklaringsbereid zijn, omdat ze trots zouden zijn op de gepleegde hack en ook zouden inzien dat ze vanwege al het bewijsmateriaal niet onder het strafbare feit uit kunnen komen (zie ook paragraaf 4.3 hieromtrent). De respondenten die met

[10] Dit onderwerp is niet aan elke respondent voorgelegd; deze rechercheurs gaven dit punt zelf aan of het kwam toevallig tijdens de interviews aan bod.

de minder technische verdachten te maken krijgen, schatten de verklaringsbereidheid lager in. Op het gebied van de verklaringsbereidheid, blijkt dat advocaten ook een belangrijke rol spelen:

> *(…) En sommige advocaten gaan erin mee hè, die hebben zoiets van joh, die zeggen van vertel maar. Die weten een beetje waar de zaak overgaat of die hebben de stukken al ingelezen. (…) En die zeggen ze hebben zoveel, verklaar nou maar, want dat is ten gunste van jou. Andere advocaten zeggen joh beroep je maar op je zwijgrecht en we zien het wel bij de rechtbank. Dat is totaal verschillend bij een advocaat. (…)* (R10)

De advocaten bespreken zelf dat het advies dat zij geven afhankelijk is van de cliënt en diens wens om wel of niet een verklaring af te leggen in het verhoor. Toch blijkt uit de interviews dat advocaten zeker ook kijken naar de hoeveelheid aan bewijs dat de politie voorhanden heeft:

> *Als er heel veel is ben ik een groot voorstander van openheid. Dan probeer ik ook echt mijn cliënten te bewegen om, om te zeggen ja, leg alles op tafel want het is niet in je belang om dan te zwijgen of om te ontkennen. Maar als er wel een plausibel verhaal is dat je het niet bent geweest, dat het anders zit dan volg ik de keuze van de cliënt. Maar juist in die zaken waar heel veel bewijs is en iemand toch wil blijven ontkennen, dan ben ik wel actief in het afraden van ja je geeft jezelf een jarenlange gevangenisstraf als je geen verantwoordelijkheid neemt.* (RA1)

Een laatste verschil ten opzichte van het verhoor van verdachten die offline delicten plegen, heeft betrekking op het technische aspect van het verhoor en de samenstelling van het verhoorteam. Bij een hackzaak kan volgens enkele respondenten een technisch verhoor plaatsvinden waarin de technische aspecten van de zaak worden behandeld, zoals de software die de verdachte heeft gebruikt bij het plegen van een hack. Dan wordt vaak een technische rechercheur meegenomen in het verhoor (zie verder voor de samenstelling paragraaf 4.3).

4.2.3 Verhoormethoden

In het verhoor kunnen diverse verhoormethoden worden ingezet. De meerderheid van de rechercheurs kan echter niet omschrijven welke methoden zij gebruiken, omdat zij niet weten wat er wordt bedoeld met verhoormethoden. Drie opgeleide rechercheurs benoemen specifiek twee methoden bij naam; namelijk de DSM en de SOM. Zij bespreken daarbij ook dat de keuze

voor een bepaalde methode afhankelijk is van de verdachte in kwestie en diens bereidheid om te verklaren; en dat tijdens het verhoor ook kan worden gekozen voor een andere methode.

De overige niet-opgeleide rechercheurs beschrijven dat zij geleidelijk druk opbouwen tijdens de confrontaties met verdachten. R12 stelt: "*(…) In principe beginnen we altijd met of ja een makkelijke vraag of gewoon meer bevestigingsvragen van klopt het dat dit of bladiebla. En uiteindelijk wordt het steeds complexer, dus hoeveel slachtoffers heb je gemaakt of denk je? (…)*" Daarnaast geven enkele verhoorders ook aan dat ze vaak eerst de gelegenheid geven aan de verdachte om met een eigen verhaal te komen. R3 stelt: *"(…) Dus je begint heel algemeen gewoon van joh je wordt daar, daar en daarvan verdacht, wat kan je er zelf over vertellen? Voor hetzelfde geld komt hij met het hele verhaal, nou prima, hartstikke mooi. (…)"*

4.2.4 Verhoortechnieken

Net als bij de methoden weet niet iedere respondent (waaronder ook een opgeleide rechercheur) wat verhoortechnieken zijn. Uiteindelijk kwamen tijdens de interviews verschillende technieken aan bod. De respondenten geven aan dat deze technieken niet specifiek zijn gericht op verdachte hackers, maar ook in het verhoor van andere verdachten worden toegepast. Deze technieken worden zowel door opgeleide als niet-opgeleide rechercheurs toegepast.

Een eerste veelvoorkomende verhoortechniek die wordt gebruikt, is het opbouwen van een verstandshouding met de verdachte en het investeren in een vertrouwensband. Daarbij geven de rechercheurs aan dat ze verdachten op hun gemak willen stellen en hen ook het idee willen geven dat ze serieus worden genomen. Op die manier zou een betere en ontspannenere sfeer in de verhoorkamer ontstaan, wat een voordeel met zich meebrengt in het verhoor:

> *(…) Stel dat de verdachte een verhoor houdt bij twee verschillende verhoorkoppels. En het ene koppel is ontzettend sympathiek en het andere koppel (…) zijn echt de, de stoere agenten. Nou ik weet honderd procent zeker dat die eerder een verklaring zal afleggen bij de sympathieke agenten dan bij de stoere agenten. (…)* (R3)

Bovendien benoemen de respondenten dat er complimenten aan de hackverdachten worden gegeven, hoewel een opgeleide rechercheur dit niet echt als een techniek ziet. R3 stelt: "*Ja als het een techniek moet worden dan, dan komt het volgens mij ook niet meer oprecht over*." Het geven van complimenten wordt volgens een deel van de respondenten gedaan wanneer de verdachte zijn verhaal bijstelt in het zaakgericht verhoor om hem op die manier te motiveren om verder te vertellen, maar dit komt ook voor op technisch vlak:

> *(…) We gingen hem een beetje ja complimentjes geven over zijn werk. En dat werkte, want hij vond het inderdaad helemaal tof wat hij deed. (…) Omdat hij zo'n techneut is die meestal trots is op wat hij maakt, hebben we dat een beetje dus gebruikt ja. (…) Ik weet dat techneuten dat leuk vinden om te horen. (…)* (R12)

Een andere veelvoorkomende techniek die al eerder aan bod kwam, is het omsingelen van de verdachte. De verdachte kan ook worden geconfronteerd met een eerdere verklaring die hij voortkomend uit de omsingelingstechniek heeft afgelegd. Verder geven de respondenten aan dat verdachten ook regelmatig worden geconfronteerd met het bewijsmateriaal. De verhoorders stapelen dan al het gevonden bewijsmateriaal op en vragen vervolgens aan de verdachte om een verklaring. Volgens enkele respondenten is dit een effectieve techniek, omdat de verdachte vanwege deze opstapeling niet meer onder het strafbare feit kan uitkomen en daarom een verklaring zal gaan afleggen. Het onderstaande citaat van een rechercheur biedt een voorbeeld van hoe deze confrontatietechniek wordt toegepast in het verhoor van hackverdachten:

> *(…) Van hoe kan het dan dat we die gegevens hebben gevonden, hoe kan het dan dat we jouw foto hebben gevonden, hoe kan het dan dat jouw IP-adres naar voren is gekomen of hoe kan het dat je 06-nummer naar voren is gekomen, maar ook je toestel hebben gevonden bij jou op je slaapkamer die jij alleen hebt gebruikt, wat je al eerder hebt aangegeven in het sociaal verhoor? (…)* (R7)

Een laatste verhoortechniek die vaak wordt toegepast wanneer een hackverdachte niet mee wil werken in het verhoor, is het benoemen van de consequentie daarvan. Enkele respondenten bespreken dat dan aan de verdachte wordt meegegeven dat er zoveel bewijs tegen hem is gevonden, dat hij beter een verklaring kan geven. Een rechter zou volgens de respondenten de maximum opgelegde straf kunnen opleggen wanneer een verdachte niet meewerkt. Onderstaand citaat is een illustratie van hoe een opgeleide rechercheur deze techniek toepast:

> *(…) Ik had laatst een verdachte die, die draaide er elke keer om heen en toen hebben we gezegd van joh er staat zoveel op papier, deze bewijzen hebben we allemaal tegen jou, als jij nu je verhaal zo vertelt, dat leest de rechter ook en die gaat er wat van vinden. (…) Dus misschien is het handig met deze bewijzen om toch eens je, je verhaal bij te stellen zodat het verhaal kloppend is met wat wij hebben. (…)* (R10)

Daarnaast geven enkele respondenten aan dat er weleens aan de verdachte wordt verteld dat hij langer in voorarrest wordt gehouden indien hij zich blijft beroepen op zijn zwijgrecht. In dat geval wordt soms ook aan de verdachte beloofd dat hij naar huis mag gaan indien hij een verklaring aflegt, omdat de rechercheurs dan niets meer hoeven uit te zoeken. Een advocaat geeft echter aan dat hij het benoemen van de consequentie een kwalijke zaak vindt:

> *(…) Het is niet zo dat je maar één kans hebt, maar dat wordt wel zo gebracht om de druk wat op te voeren. (…) Van je moet het nu doen, want straks heb je het dossier gelezen en dan is het niet meer geloofwaardig. (…) Maar goed ja, je kunt altijd tot inkeer komen,kan ook later nog.* (RA1)

Naast deze veelvoorkomende verhoortechnieken, bespreken de respondenten ook enkele technieken die minder vaak worden toegepast. Zo geven de verhoorders weleens een mening over de hack of tonen zij autoriteit aan. Ook bespreekt een andere niet-opgeleide rechercheur dat hij een keer fictief bewijs had voorgelegd aan de verdachte:

> *(…) Nou dat vind ik wel mooi dat hij daar ja op zegt terwijl ik helemaal geen aanleiding had dat ik dat… ik had geen bewijs daarvoor. Maar ik had wel het idee van nou dat zou best weleens kunnen weet je. Het zou me niks verbazen als hij dat ook doet. En hij zegt gewoon ja. Nou prima, het is zijn verklaring. Hij had ook niks kunnen zeggen of gewoon nee. (…)* (R2)

Hoewel de desbetreffende respondent aangeeft dat hij weleens iets heeft gevraagd zonder daar bewijs voor te hebben, gaf een klein aantal respondenten aan dat er juist niet mag worden gebluft en rechercheurs ook niet met misleidende informatie mogen komen in het verhoor.

Tot slot bespreken de respondenten dat naast de technieken ook verschillende soorten vragen in het verhoor worden gesteld. Daarbij geven de rechercheurs aan dat zij gesloten vragen zoveel mogelijk proberen te vermijden en ook niet meerdere vragen achter elkaar stellen. In plaats daarvan wordt er geprobeerd om zoveel mogelijk open vragen te stellen. Toch komen in het verhoor volgens de respondenten weleens suggestieve vragen voor, hoewel de rechercheurs dat zoveel mogelijk proberen te vermijden. Zij mogen immers geen woorden in de mond van de verdachte leggen, zo bespreken enkele rechercheurs.

4.2.5 Risico's in het verhoor

De rechercheurs proberen suggestieve vraagstellingen zoveel mogelijk te vermijden, omdat daar allerlei risico's aan verbonden zouden zijn. Zo bespreekt R3 bijvoorbeeld: *"(...) In de voorbereiding mag het niet, maar het zal echt wel een keer in the heat of the moment gebeuren. Maar als je het alleen maar doet, dan haal je jezelf onderuit. (...) Dan ben je niet geloofwaardig meer."* Wanneer wordt gevraagd naar andere risico's die mogelijk een rol spelen in het verhoor van hackverdachten, weet de meerderheid van de rechercheurs daar geen antwoord op te geven. Enkele respondenten benoemen het risico van het prijsgeven van informatie aan de verdachte, omdat dan een medeverdachte kan worden ingelicht en een verdachte in het vervolg ook beter zijn best kan doen om niet opnieuw te worden gepakt. De mogelijkheid dat een hackverdachte een onbetrouwbare verklaring aflegt in het verhoor, lijken de respondenten verder niet als een risico te beschouwen. Zo wordt bijvoorbeeld besproken dat het afleggen van een onbetrouwbare verklaring vooral een risico is voor de verdachte hacker zelf en niet voor de cybercrimeteams:

> *(...) Onbetrouwbare verklaring vind ik ook prima, kunnen we dat weer weerleggen. Heb ik net zo lief. (...) Ik heb echt graag een lulverhaal, want dan kunnen we dat helemaal afschieten. En dan is iemand natuurlijk ook af en ben je gediskwalificeerd eigenlijk, want denken ze ja je hebt iets verklaard en dan kun je later ook niet meer zeggen nee het is niet zo of je kan niet met een ander verhaal komen. Ja dan denkt de rechter ook van wat is dit. (...) Je kan niet eerst A zeggen en dan B. (...)* (R9)

Daarentegen stellen de advocaten dat er per definitie altijd risico's verbonden zijn aan het verhoor. Zo zegt RA3 bijvoorbeeld: *"Een verhoor is altijd levensgevaarlijk. (...) Mensen kunnen zich terecht of onterecht ophangen aan één verkeerde opmerking, één verkeerd antwoord. (...)"* Wat de advocaten verder ook als een risico beschouwen, is dat de verhoorders soms overtuigd zijn van het bewijs en daardoor niet meer openstaan voor een alternatieve interpretatie van het bewijsmateriaal (zie hieromtrent ook paragraaf 4.2.2).

4.3 Samenstelling van het verhoorteam binnen de cybercrimeteams

De samenstelling van het verhoorteam wordt, zoals eerder beschreven, ook gezien als een verschil ten opzichte van het verhoor van andere verdachtengroepen die offline delicten plegen. In de onderzochte cybercrimeteams bestaat de samenstelling voornamelijk uit een combinatie van een tactische en een technische rechercheur en in sommige gevallen uit twee tactische verhoorders. Uit de antwoorden van enkele respondenten blijkt dat de tactische rechercheurs

doorgaans algemene vragen stellen en dat de technische rechercheurs ingaan op de technische aspecten van het verhoor. Ook typen de technische rechercheurs gedurende het verhoor in de meeste gevallen mee. RA1 zegt het volgende over de samenstelling: "(…) *En die technische persoon die is dan vaak veel beter toegerust om alle technische dingen te snappen en die vragen te stellen. En de tactische rechercheur die overziet meer het geheel en stuurt ja op tactisch niveau*." In enkele teams komen ook vaste verhoorkoppels voor die bestaan uit een tactische en een technische rechercheur[11]. Deze koppels hebben een klik met elkaar en de communicatie tussen de twee verloopt ook goed, aldus enkele respondenten. Over de communicatie tussen tactische en technische rechercheurs in een vast verhoorkoppel stelt een respondent:

> *(…) Dus dat ik alleen mijn vinger opsteek, dat alles even stilligt. Dat ik gewoon even door kan tikken (…). Ik merk wel (…) met deze collega was ik niet zo moe als met een andere collega die maar doorratelde en ratelde en ratelde. En daar krijg ik de opmerking joh het lijkt wel een telegramstijl. Ja maar (…) die ratelt maar door, die let niet op mij en die let niet op hoe ver ik ben.* (R2)

Bij de bepaling van de samenstelling spelen volgens de respondenten verschillende overwegingen een rol. Zo wordt bijvoorbeeld gekeken naar de beschikbaarheid van een rechercheur en diens betrokkenheid bij het onderzoek, maar wordt ook rekening gehouden met de technische vaardigheden van een verdachte. Wanneer een hackverdachte over weinig IT-kennis lijkt te beschikken, volstaat het volgens de rechercheurs om daar twee tactische verhoorders tegenover te zetten. Indien dat niet het geval is, zal juist een technische rechercheur worden meegenomen in het verhoor. Een technisch rechercheur kan volgens de respondenten namelijk dieper ingaan op de technische aspecten van het delict, waardoor een verdachte technisch kan blijven en zich ook meer op zijn gemak voelt. Daardoor zou de verdachte meer geneigd zijn om een verklaring af te leggen. Het onderstaande citaat biedt een illustratie van de voordelen van het meenemen van een technische rechercheur in het verhoor:

> *(…) Maar je merkt wel dat gelijkwaardigheid een belangrijke component is om te zorgen dat je een goede gesprekspartner bent om ook voor zo iemand naja, dat kan, dat is eigenlijk tweedelig. Punt 1 zie je vaak dat er een soort klik ontstaat, omdat je weet hé wij kennen, wij spreken dezelfde taal. En de andere kant is ook van ah shit ik kom hier*

[11] Het is niet bekend of er in ieder team vaste verhoorkoppels zijn en of elke rechercheur een vast verhoorkoppel heeft, omdat daar niet actief naar is gevraagd.

> *niet weg met een soort, met een soort slecht verhaal en ze geloven me toch wel, want ze zijn te dom. Dat voorkom je daarmee ook. Dus het mes snijdt wel aan twee kanten.* (R8)

Ook een officier van justitie is erg positief over de gemixte verhoorkoppels.

> *(…) En ik denk dat die combi echt wel goed is. (…) Op het moment dat ja toch een goeie cybercrimineel om het zo maar te noemen met een verhaal komt. Ja dan moet je daar wel op kunnen reageren en dan zul je ook wel even moeten checken of dat nou klopt of niet klopt, dat technische verhaal wat wordt opgehangen. (…)* (RO2)

Het enkel meenemen van tactische rechercheurs in het verhoor van een technische verdachte kan volgens de respondenten zelfs verschillende risico's met zich meebrengen, waardoor daar doorgaans ook niet voor wordt gekozen. Zo kan een mogelijk risico zijn dat tactische verhoorders belangrijke dingen over de zaak missen en het verhoor erg oppervlakkig blijft, omdat zij niet altijd over voldoende technische kennis beschikken. Daarnaast zou het ook een negatieve invloed kunnen hebben op de bereidheid van de verdachte om te verklaren:

> *Dat als een verdachte inderdaad helemaal over de technische dingen wil gaan vertellen dat hij geïrriteerd raakt, omdat hij het uit moet gaan leggen. Ja want het is toch logisch? (…) Kom op jongens, jullie zijn van cybercrime weet je wel. Waarom snappen jullie het niet? Moet ik dit echt uit gaan leggen? Oh mijn god (…).* (R6)

4.4 Kennisniveau van de verhoorders binnen de cybercrimeteams

De respondenten bespreken, zoals hierboven al kort is beschreven, dat niet alle rechercheurs voldoende technische kennis hebben. Hoewel de tactische rechercheurs over steeds meer digitale kennis gaan beschikken, onder andere door het volgen van een cybercursus bij een extern bedrijf, zullen ze volgens verschillende respondenten nooit echt een IT'er worden. R9 heeft daar een mooie anekdote voor: *"(…) De timmerman is beter, handiger met hout. Dat is, dat is bij ons ook zo*." Het kennisverschil tussen de tactische en technische rechercheurs wordt niet als een nadeel beschouwd. R3 zegt daar namelijk het volgende over: *"(…) Ik bedoel ja, als ik iets echt niet, ja niet begrijp of ergens niet uitkom, dan, dan klop ik inderdaad aan bij digitale rechercheurs. Ja die staan er altijd klaar voor."* De respondenten vinden het wel een nadeel dat in sommige teams de tactische rechercheurs op tijdelijke basis bij de cybercrimeteams werken. Deze gaan na een paar jaar terug naar de basisteams of de districtsrecherche. De

respondenten bespreken dat het achterliggende idee is om rechercheurs cyberkennis over te laten dragen naar andere teams binnen de politieorganisatie. Nadelen zijn echter dat de cybercrimeteams veel technische kennis verliezen en dat het veel tijd kost om nieuwe tactische rechercheurs op te leiden, zo bespreken enkele respondenten. R10 zegt daar het volgende over: "*(...) Dus wat je krijgt is dat er een wisseling komt in tactisch rechercheurs. Die zijn niet zo, als je net begint ben je niet zo bekend met alle ins en outs zeg maar van het cybercrimeteam*." De teamleiders die te maken krijgen met tactische uitgeleende rechercheurs geven daarom aan ervoor te willen zorgen dat deze rechercheurs vast worden aangenomen.

Verder blijkt op het gebied van verhoorkennis dat enkel vier tactische rechercheurs een verhooropleiding hebben gevolgd. Dat niet alle rechercheurs een dergelijke opleiding hebben gevolgd, wordt door de respondenten niet als een nadeel gezien. Het verhoor is volgens de respondenten tijdens de rechercheopleiding aan bod gekomen en de meeste tactische verhoorders zouden ook al ervaring hebben opgedaan met het verhoor van andere verdachten die offline delicten hebben gepleegd. R8 stelt: *"(...) Ik denk niet dat iedereen de VVH*[12]*[Verdieping Verhoor] gedaan moet hebben, omdat je een heel eind komt met goede aanwijzingen, een beetje ervaring en meeliften op iemand die dat al vaker gedaan heeft (...)".* Op deze manier zouden de technische rechercheurs, die geen verhoorervaring hebben, volgens de respondenten door het uitvoeren van het verhoor met een tactische rechercheur ervaring opdoen en steeds beter worden in de uitvoering van het verhoor van hackdelicten.

Hoewel enkele verhoorders een verhooropleiding hebben gevolgd, is er geen enkele respondent die een opleiding heeft gevolgd op het gebied van het verhoor van kwetsbare verdachten. Slechts één rechercheur had de training Communiceren met Kwetsbare Personen afgerond. Tijdens deze training werd bijvoorbeeld geleerd hoe de kwetsbaarheid van een persoon kan worden getoetst en hoe daar beter mee om kan worden gegaan. De respondent vindt de training van groot belang, omdat hackverdachten ook kunnen worden aangemerkt als kwetsbaar en is van mening dat meer rechercheurs de training moeten gaan volgen.

4.5 Knelpunten en optimalisatie

De meerderheid van de respondenten is van mening dat het verhoor van hackverdachten goed verloopt. Het meenemen van een technische rechercheur in het verhoor en het opbouwen van een verstandshouding met de verdachte worden daarbij met name als positief beoordeeld. De

[12] De VVH staat voor de oudere opleiding Verdieping Verhoor die nu is vervangen door de Verdieping op Verhoor (VV). Zie daarvoor paragraaf 2.5.

respondenten komen daarom met weinig knelpunten of optimalisaties op het gebied van het verhoor. Door enkele rechercheurs wordt het belang van verhoorkennis benadrukt. R6 zegt: *"Weet je het is niet alleen opleiding volgen, maar ook tussendoor gewoon het bijschaven. En je moet het eigenlijk gewoon blijven doen om het op een niveau te houden (…)"* Verder stellen andere respondenten voor dat tactische rechercheurs niet meer moeten worden uitgeleend. R1 is zelfs van mening dat er vaste verhoorkoppels dienen te komen, waarbij de rol van een technische rechercheur ook anders moet worden ingedeeld: *"Dus eigenlijk technische collega gestuurd door de tactische collega (…) en eigenlijk moet je dat niet hebben. Je moet juist hebben dat die technische collega volledig ook onderdeel uitmaakt (…) van het verhoor (…)"*

De advocaten kwamen met andere optimalisaties, onder andere wat betreft de lengte van het verhoor. Zij geven aan dat ze steeds op een rechercheur moeten wachten die tijdens het verhoor aan het meetikken is. Een optimalisatie zou daarom kunnen zijn:

> *(…) Gewoon opnemen en dan uit laten typen door iemand die ook minder, minder per uur kost. En ook niet waar vier mensen naar zitten te wachten. En als je dat, dat niet kan regelen dan met een tweede scherm zodat we live kunnen meekijken en niet achteraf gaan steggelen over ja maar ik denk dat hij dit zei, maar ik heb dit gehoord. (…)* (RA2)

Daarnaast bespreekt een advocaat, die voornamelijk te maken krijgt met de districtsrecherche, dat hij het niet goed vindt dat advocaten zich moeten schikken wanneer verhoren over meerdere dagen worden opgesplitst. Dan kan hij vanwege andere afspraken niet bij ieder verhoor aanwezig zijn. Daar heeft de advocaat de volgende aanbeveling voor:

> *(…) Zo'n sociaal verhoor gaan ze dan doen, terwijl ik dan denk doe dat dan de dag erna, hoef ik er niet bij te zijn bij zo'n sociaal verhoor, want dan kunnen ze niet zoveel fout doen. Dus ik zou beginnen met het inhoudelijke verhoor als een advocaat erbij is, want die hoeven dan niet bij het sociale verhoor te zitten. (…)* (RA4)

Uit de antwoorden van de rechercheurs bij de cybercrimeteams, komt ook naar voren dat de verhoren vaak over meerdere dagen worden opgesplitst. Hoewel de overige advocaten hierover niet zijn geïnterviewd en er geen harde uitspraken kunnen worden gedaan, is het goed mogelijk dat de advocaten bij de cybercrimeteams ook keuzes moeten maken wat betreft de verhoren waarbij ze aanwezig zijn. Daardoor slaan zij wellicht ook het sociaal verhoor over.

5. Conclusie

Het doel van dit verkennende onderzoek was om op basis van de onderzoeksvraag en deelvragen inzicht te krijgen in het verhoorproces van hackverdachten. Daarvoor zijn 18 semigestructureerde interviews afgenomen met respondenten werkzaam bij cybercrimeteams uit vier verschillende politie-eenheden, advocaten en cyberofficieren van justitie. De centrale onderzoeksvraag luidt als volgt: *Hoe verloopt het politieverhoor van verdachten van hackdelicten bij cybercrimeteams in Nederland?* De deelvragen zijn daarnaast gericht op de rol van (1) persoonskenmerken van hackverdachten, (2) verhoormethoden en -technieken, (3) de samenstelling van het verhoorteam, (4) het kennisniveau en de vaardigheden van verhoorders op het gebied van het verhoor van hackverdachten en (5) de verschillen tussen rechercheurs met en zonder verhooropleiding in het verhoor van verdachten van hackdelicten. De afsluitende vraag heeft betrekking op (6) de optimalisatie van het verhoor van hackverdachten.

Hackverdachten zijn over het algemeen van het mannelijke geslacht en rond de twintig jaar oud. Hoewel relatief veel rechercheurs in het verhoor vermoedelijk een verdachte met een autismespectrumstoornis (of een andere psychische aandoening) hebben getroffen, speelt dat voor verhoorders waarschijnlijk geen rol in het verhoor. Zij houden namelijk in beperkte mate rekening met psychische kenmerken van verdachten en bestempelen dergelijke verdachten ook niet als kwetsbaar. Verder worden op het gebied van technische vaardigheden, opleiding en motivatie twee typen verdachten gevonden. Enerzijds zijn er technische hackers die een IT-opleiding hebben gevolgd en uit enthousiasme, interesse en uitdaging betrokken raken bij een hack. Anderzijds zijn er ook minder technische hackers die niet geschoold zijn, maar vanuit een financieel motief en het willen verkrijgen van macht een hack plegen met de tools die zij online hebben gekocht. Bij deze groep wordt ook relatief vaak gesproken over een allochtone afkomst.

Het verhoor van beide typen hackverdachten verloopt zoals verwacht volgens de algemene verhoorfasen. Allereerst wordt de cautie aan de verdachte meegegeven, waarna het persoonsgericht en zaakgericht verhoor plaatsvinden. Het onderscheid tussen de laatste twee fasen wordt echter wel minder duidelijk, omdat in het persoonsgericht verhoor steeds meer vragen worden gesteld die zijn gericht op de zaak. Verder zijn er enkele verschillen gevonden in vergelijking met het verhoor van andere verdachten die offline delicten plegen; zoals dat het bewijsmateriaal bij een hack meer sluitend en overtuigend zou zijn. Tegen de verwachting in is daardoor vaak geen verklaring van de verdachte vereist. Een ander verschil hangt samen met de rol van persoonskenmerken in het verhoorproces; en nog specifieker met het treffen van een technische hacker in het verhoor. In dat geval wordt het verhoorteam veelal samengesteld door

een (vast) verhoorkoppel bestaande uit een tactische en een technische rechercheur. Het betrekken van een technische rechercheur bij het verhoor lijkt een positieve impact te hebben op het verkrijgen van een verklaring van de (technische) verdachte. Aldus lijkt de samenstelling een belangrijke rol te spelen in het verhoor, waarbij de verhoorders gezamenlijk over voldoende kennis en ervaring op het gebied van het verhoor van hackverdachten beschikken. De technische rechercheurs zijn met name digitaal onderlegd en de tactische rechercheurs hebben meer kennis op het gebied van het verhoor. Desalniettemin is er wel een gebrek aan kennis voor kwetsbare verdachten, omdat slechts één rechercheur daaromtrent een training had gevolgd.

Verder lijken verhoormethoden en -technieken ook een grote rol te spelen. Wat betreft de verhoormethoden is een duidelijk verschil gevonden tussen opgeleide en niet-opgeleide rechercheurs. Zo wisten slechts drie opgeleide rechercheurs verhoormethoden bij naam te noemen die zij in het verhoor toepassen; namelijk de Scenario's Onderzoekende Methode en de Directe Stapelmethode. Op het gebied van verhoortechnieken zijn geen verschillen gevonden tussen verhoorders met en zonder verhoorkennis; beide typen rechercheurs passen grotendeels dezelfde technieken toe. Enkele toelaatbare technieken die worden gebruikt zijn het opbouwen van een verstandshouding met de verdachte, de omsingelingstechniek en het confronteren van de verdachte met het bewijsmateriaal. Risicovolle technieken die in het verhoor worden toegepast zijn het geven van complimenten aan de verdachte, het benoemen van de consequentie wanneer de verdachte niet meewerkt in het verhoor, het doen van een belofte, het aantonen van autoriteit en het stellen van suggestieve vragen. Ook had een niet-opgeleide rechercheur fictief bewijs voorgelegd aan de verdachte en was hij daar trots op, terwijl dit een enorm risicovolle verhoortechniek is. Waarschijnlijk zijn de rechercheurs niet op de hoogte van het feit dat zij ontoelaatbare technieken toepassen, omdat zij stellen dat er geen risico's aan het verhoor verbonden zijn zoals het verkrijgen van een valse of onbetrouwbare verklaring.

Afsluitend zijn de rechercheurs van mening dat het verhoor van hackverdachten over het algemeen goed verloopt. Toch benoemen zij enkele optimalisaties ter verbetering van het verhoor. Zo moeten rechercheurs blijven werken aan het kennisniveau op het gebied van het verhoor en zouden technische rechercheurs een prominentere rol moeten krijgen in het verhoorteam. Ook is het een aanbeveling om tactische rechercheurs vast in de cybercrimeteams te laten werken, zodat minder technische kennis verloren gaat binnen de cybercrimeteams. De advocaten hebben daarentegen geen inhoudelijke verbeterpunten en komen enkel met wensen over de structuur en de algemene uitvoering van het verhoor van verdachten van hackdelicten.

6. Discussie

6.1 Bijdrage aan de wetenschappelijke literatuur

In deze studie zijn eerste stappen gezet wat betreft het inzichtelijk maken van het verhoorproces van hackverdachten bij cybercrimeteams. Daarvoor zijn 18 interviews afgenomen met respondenten die betrokken zijn bij het verhoor[13]. Hieronder worden de belangrijkste resultaten beschreven die bijdragen aan de wetenschappelijke literatuur op het gebied van het verhoor.

Tegengesteld aan de literatuur (Rokven et al., 2017; Van der Wagen et al., 2019) toont dit onderzoek aan dat (niet technische) hackers een allochtone achtergrond kunnen hebben. De overige persoonskenmerken komen wel overeen met de bestaande literatuur, waaronder dat relatief veel respondenten in het verhoor een hackverdachte met een autismespectrumstoornis blijken te treffen (Ledingham & Mills, 2015; National Crime Agency, 2017). Hierbij moet een kanttekening worden geplaatst, omdat het aantal autistische verdachten ook kan worden overschat. Hackers kunnen onterecht worden bestempeld als autistisch, omdat er mogelijk een algemeen beeld heerst dat cyberdaders autistisch zijn. Tegelijkertijd lijken de verhoorders uit deze studie, in overeenstemming met eerder uitgevoerd onderzoek (Geijsen, 2018), zich niet bewust te zijn van het feit dat autistische verdachten tot een kwetsbare groep behoren. Rechercheurs kunnen een bepaald beeld hebben van autistische hackers, waarin de focus ligt op overduidelijk autistische kenmerken zoals het hebben van weinig sociale contacten (Van der Wagen et al., 2019). Wanneer subtiele kenmerken over het hoofd worden gezien, kan dat zorgen voor het niet herkennen (en juist een onderschatting) van de populatie kwetsbare verdachten.

Zowel onder- als overschatting kunnen worden tegengegaan door een vermoeden van kwetsbaarheid vast te stellen, waarna een verdachte ter bescherming in het verhoor een advocaat krijgt toegewezen. Daarvoor moeten verhoorders in het persoonsgericht verhoor VIK-vragen stellen en voldoende doorvragen (Van Amelsvoort & Rispens, 2017). De resultaten van deze studie laten echter zien dat te snel over VIK-vragen heen wordt gestapt of dat deze in sommige gevallen volledig worden overgeslagen (zelfs door opgeleide rechercheurs). Mogelijk is men zich niet bewust van het doel van het stellen van VIK-vragen, omdat in overeenstemming met eerder uitgevoerd onderzoek (Geijsen, De Ruiter et al., 2018) binnen de cybercrimeteams er een gebrek aan kennis (en verhooropleidingen) lijkt te zijn voor kwetsbare verdachten.

Het feit dat sommige verhoorders alleen onderwerpen willen bespreken die te maken hebben met de zaak, kan mogelijk worden verklaard door de potentiële tijdsdruk waaronder zij staan. Een gevaar is echter dat bij een gebrek aan herkenning kwetsbare personen worden

[13] Bij de discussie moet rekening worden gehouden met een beperkte representativiteit.

blootgesteld aan een regulier verhoor. Uit de antwoorden van de respondenten kan worden opgemaakt dat in een regulier verhoor diverse methoden uit de Handleiding Verhoor van Van Amelsvoort en Rispens (2017) worden toegepast. Opgeleide rechercheurs lijken daar meer kennis over te hebben. Op basis van de onderzoeksresultaten kan worden aangenomen dat de Scenario's Onderzoekende Methode wordt toegepast in het verhoor. Verhoorders maken namelijk veelvuldig gebruik van de omsingelingstechniek en bouwen tijdens de confrontatie de toelaatbare druk geleidelijk op. Verder is een tweede aanname dat rechercheurs ook de Directe Stapelmethode gebruiken, omdat in sommige gevallen al het gevonden bewijsmateriaal wordt opgestapeld en vervolgens om een verklaring van de verdachte wordt gevraagd. Tot slot passen de rechercheurs waarschijnlijk ook de Vrije Verklaringsmethode toe, omdat verdachten vaak de ruimte wordt gegeven om eerst zelf met een verklaring te komen. Dat lijkt te komen doordat verhoorders doorgaans over voldoende bewijsmateriaal beschikken, waardoor een verklaring van de verdachte niet noodzakelijk is. Dat is het ideale uitgangspunt voor (hack)verhoren, omdat verhoorders in dat geval geen (risicovolle) technieken meer zouden hoeven toe te passen.

Toch blijkt uit deze studie dat verhoorders (waaronder ook opgeleide rechercheurs) gebruikmaken van verhoortechnieken die risicovol zijn voor (hack)verdachten met betrekking tot het verkrijgen van een valse of onbetrouwbare verklaring of het volledig dichtslaan van een verdachte (Beijer, 2012; Boon et al., 2016; Geijsen, 2018; Geijsen & De Ruiter, 2017; Kassin, 1997). In de richtlijn van de VN staat zelfs beschreven dat technieken als het voorleggen van fictief bewijs en het stellen van suggestieve vragen niet meer mogen worden toegepast (Association for the Prevention of Torture, Center for Human Rights & Humanitarian Law, & Norwegian Centre for Human Rights, 2021). Bovenstaande gevaren spelen een nog grotere rol bij een langdurig verhoor (Drizin & Leo, 2004; Redlich et al., 2011) waar in sommige gevallen bij de cybercrimeteams ook sprake van is (namelijk verhoren van 7 uur lang of de hele dag).

Daarnaast worden er in het verhoor technieken toegepast die positief zouden kunnen zijn met betrekking tot het verklaringsbereid maken van verdachten, zoals het opbouwen van een band met de verdachte en het geven van complimenten. Het verkeerd en te veel inzetten van deze technieken kan echter risicovol zijn voor kwetsbare personen die compliant zijn en de neiging hebben anderen te 'pleasen' (Kassin, 2008; North et al., 2008), al is het maar de vraag wanneer een verhoorder té vriendelijk is. Kwetsbare verdachten lopen verder ook gevaar in het persoonsgericht verhoor, omdat dat dan al vragen worden gesteld die ingaan op de zaak. Kwetsbare verdachten begrijpen, mede vanwege een beperkt inzicht in oorzaak-gevolg relaties, niet dat vragen later tegen hen kunnen worden gebruikt en dat zij mogen zwijgen (Kranendonk,

2017; Uzieblo, 2014). Daardoor bestaat de kans dat zij (onbetrouwbaar) verklaren of ontlastende informatie voor zich houden terwijl dat niet in het eigen belang is (Beijer, 2012).

Hoewel moet worden benadrukt dat het uitvoeren van een verhoor niet makkelijk is, staan de verhoorders uit deze studie mogelijk onvoldoende stil bij de gevaren van het verhoor. De huidige verhoorsituatie van (kwetsbare) hackverdachten bij de cybercrimeteams lijkt risicovol te zijn. Ook andere verdachten die offline delicten plegen, lopen potentieel gevaar. Dat heeft te maken met het feit dat sommige tactische rechercheurs voor een bepaalde periode aan de cybercrimeteams zijn uitgeleend. Wanneer zij teruggaan naar een ander politieteam, bestaat de mogelijkheid dat zij dezelfde technieken toepassen in verhoren van andere delicten.

In het geval van een risicovolle verhoorsituatie is het van belang dat de cyberofficier van justitie controleert of het verhoor op een zorgvuldige manier en volgens de regels wordt uitgevoerd. Hij geeft immers tijdens de opsporing leiding aan de politie (Openbaar Ministerie, 2018). Uit dit onderzoek blijkt echter dat cyberofficieren nauwelijks op de hoogte zijn van wat er tijdens een verhoor gebeurt, omdat ze enkel informatie uit een proces-verbaal of een kort telefoongesprek krijgen. Het is maar de vraag of zij daardoor voldoende de situatie van de verdachte, de werkelijke verhoorsituatie en risico's met betrekking tot de betrouwbaarheid van de verklaring van de verdachte kunnen inschatten. Dit geldt ook voor de rechter die zijn of haar beslissing baseert op het schriftelijke dossier. Naar verwachting wordt een potentieel kwetsbare verdachte vaak niet als dusdanig opgemerkt, waardoor bij de strafeis en de uiteindelijke straf door de rechter geen rekening wordt gehouden met de kwetsbaarheid van de verdachte.

Desalniettemin is het positief voor de verklaringsbereidheid van de verdachte dat het verhoorteam, in overeenstemming met de studie van Van Kuppevelt (2020), vaak wordt samengesteld door een tactische en een technische rechercheur. Zij hebben immers kennis van óf het technische aspect óf het verhoorproces. Ook is het goed dat er soms vaste verhoorkoppels worden ingezet omdat de communicatie dan beter lijkt te verlopen tussen de verhoorders. Dat kan een positief effect hebben op de verhoorsfeer, waardoor een verdachte zich mogelijk meer op zijn gemak voelt om een verklaring af te leggen. Echter zijn er niet altijd vaste koppels, mede omdat in sommige cybercrimeteams tactische rechercheurs zijn uitgeleend en na enkele jaren terug moeten naar de basisteams of de districtsrecherche. De achterliggende reden hiervan is het verbeteren van het kennisniveau omtrent cybercrime binnen de politie. De vraag is echter in hoeverre deze kennis daadwerkelijk naar de politieteams wordt overgedragen en of dit niet nadelig is voor de cybercrimeteams, zeker gezien de beperkte tijd waarover zij beschikken om rechercheurs op te leiden. Zodra de uitgeleende tactische rechercheurs teruggaan, geen cybercrimezaken draaien en geen opfriscursussen doen, kan er veel cyberkennis verloren gaan.

Concluderend heeft dit onderzoek een bijdrage geleverd aan de wetenschappelijke literatuur op het gebied van het politieverhoor. In het verhoor lijken veel zaken goed te gaan, zoals de samenstelling van het verhoorteam en het feit dat een verklaring niet altijd de belangrijkste bewijsbron is. Desalniettemin zijn er ook diverse risico's die kunnen optreden met betrekking tot het gebruik van risicovolle technieken, waaraan op alle aspecten een gebrek aan (technische-, verhoor-, psychologische) kennis en bewustzijn ten grondslag ligt.

6.2 Beperkingen van het onderzoek

Ondanks de wetenschappelijke bijdrage zijn er ook enkele beperkingen aan het onderzoek verbonden, zoals aan de sneeuwbalmethode die is gebruikt om rechercheurs te werven. Hoewel bewust is geprobeerd om verschillende soorten respondenten te interviewen, zijn grotendeels rechercheurs verworven die affiniteit hebben met het uitvoeren van verhoren. Vier van de zeven tactische rechercheurs hadden een verhooropleiding gevolgd. Hoewel vier een groot aantal lijkt, kan het zo zijn dat vooral enthousiaste rechercheurs een verhooropleiding volgen. Dat heeft invloed op de interne validiteit van deze studie, omdat daardoor een vertekend beeld ontstaat van het werkelijk aantal opgeleide rechercheurs binnen de cybercrimeteams. Ook kan het zo zijn dat opgeleide rechercheurs een heel ander beeld schetsen van het verhoor (Boeije, 2014).

Een andere beperking heeft te maken met het online en telefonisch afnemen van de interviews. Hoewel deze methoden een goed alternatief zijn voor het fysieke interview en er ook geen andere mogelijkheid was voor het afnemen van de interviews vanwege de corona-richtlijnen, zijn er toch nadelen aan verbonden. Aangezien de vertrouwensband met de respondenten minder goed kon worden opgebouwd (Nind et al., 2021), is voorafgaand aan de interviews geprobeerd de respondenten op hun gemak te stellen. Aan de respondenten werd verteld dat de eigen mening centraal staat en dat er geen foute antwoorden zijn. Toch kwam het voor dat respondenten minder bereid waren om gevoelige informatie te delen, niet kritisch op zichzelf waren en er sociaal wenselijke antwoorden werden gegeven (Baarda & Van der Hulst, 2017; Boeije, 2014; Nind et al., 2021). Ter illustratie, de respondenten werden stiller wanneer ontoelaatbare verhoortechnieken of verhoorrisico's aan bod kwamen. Om in dat geval toch een antwoord van de respondenten te krijgen, werden zij gedurende het gesprek nogmaals op hun gemak gesteld. Dan werd bijvoorbeeld vermeld dat het stellen van suggestieve vragen voor kan komen en dat de interviewer dat zelf soms ook onbewust doet. Dit heeft invloed gehad op de betrouwbaarheid en interne validiteit van deze studie, waardoor de interviews mogelijk niet de werkelijke verhoorsituatie in kaart hebben gebracht (Baarda & Van der Hulst, 2017). Voor een

vervolgonderzoek is het beter om de interviews voor zover mogelijk fysiek plaats te laten vinden, zeker wanneer gevoelige verhooronderwerpen worden besproken.

Wat tot slot ook invloed heeft gehad op de betrouwbaarheid en interne validiteit van deze studie, heeft te maken met het feit dat verhoorders zich vaak niet realiseren dat zij bepaalde methoden of technieken toepassen; dat lijkt in veel gevallen onbewust te gebeuren. Om toch antwoord te krijgen op de vraag welke methoden en technieken worden toegepast, zijn door de interviewer aan de respondenten diverse voorbeelden gegeven om de vraag te verduidelijken. De respondenten gingen door deze aangedragen suggesties vooral in op de voorbeelden die werden gegeven, waardoor naar verwachting een groot aantal methoden en technieken over het hoofd zijn gezien die ook een rol spelen in het verhoor van hackverdachten. Ondanks deze beperking heeft dit verkennend onderzoek een zeer waardevolle eerste inzicht gegeven in het verhoorproces; en welke methoden en technieken daar onder andere in worden toegepast.

6.3 Aanbevelingen voor de praktijk

Het verhoorproces bij de cybercrimeteams kan risicovol zijn voor (kwetsbare) hackverdachten. Zo komen er langdurige verhoren voor, die moeten worden vervangen door kortere verhoren met meer pauzes. Bovendien worden verschillende risicovolle technieken toegepast die niet in overeenstemming zijn met de richtlijn van de VN. Wanneer tactisch uitgeleende rechercheurs teruggaan naar andere politieteams, worden deze technieken waarschijnlijk ook toegepast in verhoren van andere delicten. Een aanbeveling kan daarom zijn om in Nederland over te stappen op het internationale verhoormodel ‘investigative interviewing’, omdat dit model het risico op valse bekentenissen vermindert (Howes, 2020; Meissner et al., 2014).

Los daarvan moet er meer kennis en bewustzijn worden gecreëerd voor de risico’s die verbonden zijn aan het verhoor (en met name aan verhoortechnieken). Hierbij moet ook worden gekeken naar de huidige verhooropleidingen binnen de Politieacademie, omdat zelfs opgeleide rechercheurs risicovolle technieken toepassen. Een mogelijke aanbeveling kan zijn om meer intervisies of terugkomdagen te organiseren, zodat het kennisniveau van verhoorders op peil wordt gehouden. Verder moet binnen de politieorganisatie ook worden geïnvesteerd in het kennisniveau van verhoorders op het gebied van kwetsbare verdachten, bijvoorbeeld door meer rechercheurs een cursus te laten volgen op het gebied van het triggeren en voorkomen van effecten van compliance, acquiescence en suggestibiliteit. Dat is van belang omdat de resultaten van deze studie uitwijzen dat een relatief groot deel van de hackverdachten een psychische problematiek zoals een autismespectrumstoornis lijkt te hebben; en deze verdachten gevoeliger zijn voor het afleggen van een valse of onbetrouwbare verklaring. Ook moeten verhoorders

worden getraind in het herkennen van kwetsbare verdachten door het stellen van vragen over onder andere de psychische gesteldheid, opleiding of de werksituatie van de verdachte en daar voldoende op door te vragen. Zonder herkenning worden kwetsbare verdachten onderworpen aan een normaal verhoor en krijgen zij geen verplichte rechtsbescherming in het politieverhoor.

Ook voor advocaten en cyberofficieren van justitie is een rol weggelegd. Het is goed als zij worden getraind in het herkennen van kwetsbaarheden en zich bewust worden van verhoorrisico's. Specifiek is het ook van belang dat advocaten ondersteuning bieden bij het persoonsgericht verhoor, omdat kwetsbare verdachten daarin een gevaar lijken te lopen. Op deze manier kunnen advocaten en cyberofficieren beter toezien op het verhoor en in het geval van een risicovolle verhoorsituatie een laatste redmiddel voor (kwetsbare) hackverdachten zijn.

6.4 Aanbevelingen voor vervolgonderzoek

Hoewel het politieverhoor een onderbelicht onderwerp is in de wetenschappelijke literatuur, is nog minder onderzoek uitgevoerd naar het verhoor van cybercrimedelicten. Meer onderzoek op dit gebied is gewenst. Specifiek op het gebied van hackzaken moet meer inzicht worden verkregen in het gehele verhoorproces. Daarbij is het wenselijk om (significante) conclusies te trekken omtrent het aantal hackverdachten met een psychische gesteldheid, de mate waarin VIK-vragen worden gesteld en de mate waarin kwetsbare personen als dusdanig worden herkend. Ook is het een aanbeveling om een beter beeld te krijgen van het daadwerkelijke aantal rechercheurs met een verhooropleiding en de samenstelling van de verhoorteams; zo ook wie de leiding neemt in het verhoor van een technisch autistische verdachte. Dit vergt namelijk een combinatie van specifieke vaardigheden zoals het kunnen omgaan met kwetsbare verdachten en de benodigde technische kennis. Uit deze studie blijkt echter dat verhoorders niet over beide kennisniveaus beschikken. Moet in dat geval de technische rechercheur of een gespecialiseerde rechercheur op het gebied van kwetsbare verdachten het voortouw nemen? Bovendien is het een aanbeveling om audio(visuele) verhoren te analyseren, zodat er een objectiever beeld kan worden verkregen van het verhoor van hackverdachten. Op deze manier kunnen overige verhoormethoden en -technieken worden geïdentificeerd, de risico's van het verhoor en de invloed hiervan op de betrouwbaarheid en volledigheid van de verklaring van hackverdachten.

Een laatste aanbeveling voor vervolgonderzoek heeft betrekking op de beperkte representativiteit van deze studie. Hoewel in de huidige verkennende studie is geprobeerd om diverse typen rechercheurs[14] uit verschillende eenheden te interviewen (N = 4), heeft elk team

[14] Hierbij is gekeken naar rechercheurs met en zonder opleiding en technische en tactische rechercheurs.

mogelijk zijn eigen verhoorcultuur of -wijze. Indien meer teams bij het onderzoek worden betrokken, kunnen meer generaliserende uitspraken worden gedaan. Daarbij is het ook een aanbeveling om andere teams (zoals de districtsrecherche, de basisteams en het THTC) bij het onderzoek te betrekken en met elkaar te vergelijken op het gebruik van risicovolle technieken, het kennisniveau en de samenstelling van de teams. In een interview met een advocaat die meer met de districtsrecherche te maken kreeg, werd bijvoorbeeld een ander beeld geschetst van het verhoor bij dit team ten aanzien van de cybercrimeteams.

Literatuurlijst

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

Amelsvoort, A. van & Rispens, I. (2017). *Handleiding verhoor*. Den Haag: Sdu Uitgevers.

Association for the Prevention of Torture, Center for Human Rights & Humanitarian Law, & Norwegian Centre for Human Rights. (2021). *Principles on effective interviewing for investigations and information gathering.* Geraadpleegd van https://www.apt.ch /sites/default/files/inline-files/PoEI_final_2021.06_4.pdf

Baarda, D., & Hulst, M. van der (2017). *Basisboek interviewen. Handleiding voor het voorbereiden en afnemen van interviews.* Groningen/Houten: Noordhoff Uitgevers.

Banach, B., & Kampen, M. van (2020, 28 maart). Cybercrime is groeiend probleem: De digitale snelweg als breekijzer. *De Limburger*. Geraadpleegd van https://www.limburger.nl/cnt/ dmf20200327_00153839

Beijer, G. (2012). *Autisme & verdachtenverhoor. Een onderzoek naar de knelpunten tijdens een verdachtenverhoor met personen met ASS* (Scriptie). Geraadpleegd van http://inserviceautisme.nl/onewebmedia/BeijerScriptieass%26verdachtenverhoor.pdf

Bijleveld, C.C.J.H. (2013). *Methoden en technieken van onderzoek in de criminologie*. Den Haag: Boom Lemma uitgevers.

Blom, M., Oudhof, J., Bijl, R.V., & Bakker, B.F.M. (2008). *Verdacht van criminaliteit. Allochtonen en autochtonen nader bekeken*. Den Haag: WODC.

Boeije, H. (2014). *Analyseren in kwalitatief onderzoek. Denken en doen*. Amsterdam: Boom Lemma uitgevers.

Boekhoorn, P. (2019). *De aanpak van cybercrime door regionale eenheden van de politie. Van intake van cybercrime naar opsporing en vervolging*. Den Haag: Politie & Wetenschap.

Bogaart, S. (2018, 25 januari). Cybercrimeteams succesvol in de strijd tegen online criminaliteit. *JenVMagazine 1*. Geraadpleegd van https://magazines.rijksoverheid.nl /jenvjenvmagazine/2018/01/reportage-cyberfraude

Boon, R., Odinot, G., Horselenberg, R., & Geijsen, K. (2016). Van verhoor naar forensisch interview. Naar een effectieve interviewstandaard voor de politie. *Het Tijdschrift voor de Politie, 78*(4), 20-25.

Cachia, M., & Millward, L. (2011). The telephone medium and semi-structured interviews: A complementary fit. *Qualitative Research in Organizations and Management: An International Journal, 6*(3), 265-277.

Centraal Bureau voor de Statistiek. (2020). *Veiligheidsmonitor 2019*. Den Haag / Heerlen / Bonaire: Centraal Bureau voor de Statistiek.

Centraal Bureau voor de Statistiek. (2021, 1 maart). *Verdachten; delictgroep, geslacht, leeftijd en migratieachtergrond* [Dataset]. Geraadpleegd van https://www.cbs.nl/nl-nl/cijfers/detail/81947NED

Chiesa, R., Ducci, S., & Ciappi, S. (2009). *Profiling hackers. The science of criminal profiling as applied to the world of hacking*. Boca Raton: Auerbach Publications.

Clarke, C., Milne, R., & Bull, R. (2011). Interviewing suspects of crime: The impact of PEACE training, supervision and the presence of a legal advisor. *Journal of Investigative Psychology and Offender Profiling, 8*(2), 149-162.

Decorte, T., & Zaitch, D. (2016). *Kwalitatieve methoden en technieken in de criminologie*. Leuven: Acco.

Drizin, S.A., & Leo, R.A. (2004). The problem of false confessions in the post-DNA world. *North Carolina Law Review, 82*(3), 891-1007.

Duker, M.J.A. & Stevens, L. (2009). Het politiële verdachtenverhoor: Meer aandacht gewenst voor de totstandkoming van een betrouwbare verdachtenverklaring. In M.J. Borgers, M.J.A. Duker & L. Stevens (Reds.), *Politie in beeld. Liber amicorum Jan Naeyé* (pp. 77-103). Nijmegen: Wolf Legal Publishers.

Evers, J.C. (2015). *Kwalitatieve analyse: Kunst en kunde*. Amsterdam: Boom Lemma uitgevers.

Farrington, D.P. (1986). Age and crime. *Crime and Justice, 7*, 189-250.

Garrett, B.L. (2010). The substance of false confessions. *Stanford Law Review, 62*(4), 1051 -1119.

Geijsen, K. (2018). *Persons at risk during interrogations in police custody* (Proefschrift). Geraadpleegd van https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/95127.PDF

Geijsen, K., & Ruiter, C. de (2017). Het Nederlandse politieverhoor van verdachten anno 2017. *Strafblad, 14*(2), 157-162.

Geijsen, K., Ruiter, C. de, & Kop, N. (2018). Identifying psychological vulnerabilities: Studies on police suspects' mental health issues and police officers' views. *Cogent Psychology, 5*(1). doi: 10.1080/23311908.2018.1462133

Geijsen, K., Vanbelle, S., Kop, N., & Ruiter, C. de (2018). The interrogation of vulnerable suspects in the Netherlands: An exploratory study. *Investigative Interviewing: Research and Practice*, *9*(1), 34-51.

Gorp, B. van (2007). Het reconstrueren van frames via inductieve inhoudsanalyse uitgangspunten en procedures. *KWALON, 12*(2), 13-18.

Grabosky, P. (2017). The evolution of cybercrime, 2006-2016. In T.J. Holt (Red.), *Cybercrime through an interdisciplinary lens* (pp. 15-36). New York: Routledge.

Gudjonsson, G.H., & Pearse, J. (2011). Suspect interviews and false confessions. *Current Directions in Psychological Science, 20*(1), 33-37.

Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber -crime units: An empirical analysis. *Police Practice and Research, 19*(6), 519-536.

Hennink, M., Hutter, I., & Bailey, A. (2011). *Qualitative research methods*. London: Sage Publications.

Hoge Raad. (1979, 2 oktober). ECLI:NL:PHR:1979:AB7396. Geraadpleegd op 1 maart 2021 van https://www.navigator.nl/document/id341979100270770nj1980243dosred?ctx=WKNL_CSL_92

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

Holt, T.J., Burruss, G.W., & Bossler, A.M. (2010). Social learning and cyber deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice, 33*(2), 31-61.

Howes, L.M. (2020). Interpreted investigative interviews under the PEACE interview model: Police interviewers' perceptions of challenges and suggested solutions, *Police Practice and Research, 21*(4), 333-350.

Hulst, R.C. van der & Neve, R.J.M. (2008). *High-tech crime: Inventarisatie van literatuur over soorten criminaliteit en hun daders*. Den Haag: WODC.

Jafarkarimi, H., Sim, A.T.H., Saadatdoost, R., & Hee, J.M. (2015). Individual characteristics and hacking, piracy, online gambling and pornography use among students: A study in Malaysia. *International Journal of Cyber Behaviour, Psychology and Learning, 5*(2), 30-43.

Janghorban, R., Latifnejad Roudsari, R., & Taghipour, A. (2014). Skype interviewing: The new generation of online synchronous interview in qualitative research. *International Journal of Qualitative on Health and Well-being, 9*(1). doi: 10.3402/qhw.v9.24152

Johnson, D.R., Scheitle, C.P., & Ecklund, E.H. (2019). Beyond the in-person interview? How interview quality varies across in-person, telephone, and Skype interviews. *Social Science Computer Review,* 1-17. doi: 10.1177/0894439319893612

Kassin, S.M. (1997). The psychology of confession evidence. *American Psychologist, 52*(3), 221-233.

Kassin, S.M. (2008). False confessions. Causes, consequences, and implications for reform. *Current Directions in Psychological Science, 17*(4), 249-253.

Kassin, S.M. (2017). False confessions. *WIRE's Cognitieve Science, 8*(6), 1-11.

Kassin, S.M., Appleby, S.C., & Torkildson Perillo, J. (2010). Interviewing suspects: Practice, science and future directions. *Legal and Criminological Psychology, 15*(1), 39-55.

Kassin, S.M., Drizin, S.A., Grisso, T., Gudjonsson, G.H., Leo, R.A., & Redlich, A.D. (2010). Police-induced confessions: Risk factors and recommendations. *Law and Human Behavior, 34*(1), 3-38.

Kassin, S.M., & Gudjonsson, G.H. (2004). The psychology of confession evidence: A review of the literature and issues. *Psychological Science in the Public Interest, 5*(2), 35-69.

Kassin, S.M., & Kiechel, K.H. (1996). The social psychology of false confessions: Compliance, internalization, and confabulation. *Psychological Science, 7*(3), 125–128.

Kassin, S.M., & Wrightsman, L.S. (1985). Confession evidence. In: S.M. Kassin & L.S. Wrightsman (Reds.), *The psychology of evidence and trial procedure* (pp. 67-94). Beverly Hills, CA: Sage Publications.

Klap, H., Leukfeldt, E.R., & Stol, W. (2012). Cybercrime en politie. Een schets van de Nederlandse situatie anno 2012. *Justitiële Verkenningen, 38*(1), 25-39.

Klein Douwel, M. (2021, 11 maart). Onzekerheid bij wetenschappers na NWO-hack: Financier geeft geen duidelijkheid, aanvragen liggen stil. *De Volkskrant*. Geraadpleegd van https://www.volkskrant.nl/wetenschap/onzekerheid-bij-wetenschappers-na-nwo-hack financier-geeft-geen-duidelijkheid-aanvragen-liggen-stil~b3d7c8aa/

Koops, B.-J., & Oerlemans, J.-J. (2007). Formeel strafrecht en ICT. In: B.-J. Koops & J.-J. Oerlemans (Reds.), *Strafrecht en ICT* (pp. 117-208). Den Haag: Sdu.

Kranendonk, P.R. (2017). Verdachten met een LVB in het politieverhoor. De invloed van verhoormethoden op de inhoud van verklaringen. *Justitiële Verkenningen, 43*(6), 74-91.

Kuppevelt, K. van (2020). *De verhoorpraktijk van cybercrimeverdachten. Een onderzoek naar het verhoorgedrag van verhoorders van cybercrimeverdachten* (Scriptie).

Laan, A.M. van der, & Blom, M. (2006). *Jeugddelinquentie: risico's en bescherming. Bevindingen uit de WODC Monitor Zelfgerapporteerde Jeugdcriminaliteit 2005*. Den Haag: WODC.

Ledingham, R., & Mills, R. (2015). A preliminary study of autism and cybercrime in the context of international law enforcement. *Advances in Autism, 1*(1), 2-11.

Leukfeldt, E.R., Domenie, M.M.L., & Stol, W.P. (2010). *Verkenning cybercrime in Nederland 2009*. Den Haag: Boom Juridische uitgevers.

Lobe, B., Morgan, D., & Hoffman, K.A. (2020). Qualitative data collection in an era of social distancing. *International Journal of Qualitative Methods, 19*, 1-8.

Lo Iacono, V., Symonds, P., & Brown, D.H.K. (2016). Skype as a tool for qualitative research interviews. *Sociological Research Online, 21*(2), 1-15.

Marcum, C.D., Higgins, G.E., Ricketts, M.L., & Wolfe, S.E. (2014). Hacking in high school: Cybercrime perpetration by juveniles. *Deviant Behavior, 35*(7), 581-591.

Meissner, C.A., Redlich, A.D., Michael, S.W., Evans, J.R., Camilletti, C.R., Bhatt, B., & Brandon, S. (2014). Accusatorial and information-gathering interrogation methods and their effects on true and false confessions: A meta-analytic review. *Journal of Experimental Criminology, 10*(4), 459-486.

Ministerie van Justitie en Veiligheid. (2018). *Veiligheidsagenda 2019-2022*. Den Haag: Ministerie van Justitie en Veiligheid.

Nationaal Cyber Security Centrum. (2012). *Cybercrime: Van herkenning tot aangifte.* Den Haag: Nationaal Cyber Security Centrum.

National Crime Agency. (2017). *Pathways into cybercrime.* London: National Cyber Crime Unit / Prevent Team.

Navarro, J.N., & Marcum, C.D. (2020). Deviant instruction: The applicability of social learning theory to understanding cybercrime. In: T.J. Holt & A.M. Bossler (Reds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 528-545). Cham, Switzerland: Palgrave Macmillan.

Nind, M., Meckin, R., & Coverdale, A. (2021). *The NCRM wayfinder guide to adapting interview practices for Covid-19*. Southampton: National Centre for Research Methods.

North, A.S., Russell, A.J., & Gudjonsson, G.H. (2008). High functioning autism spectrum disorders: an investigation of psychological vulnerabilities during interrogative interview. *The Journal of Forensic Psychiatry & Psychology, 19*(3), 323-334.

Odinot, G., Boon, R., & Wolters, L. (2015). Het episodisch geheugen en getuigenverhoor: Wat weten politieverhoorders hiervan? *Tijdschrift voor Criminologie, 57*(3), 279-299.

Openbaar Ministerie. (2018). *Het OM in beeld*. Geraadpleegd van https://www.om.nl/binaries /om/documenten/brochures/om-brochures/om-in-beeld/2019/het-om-inbeeld/om_ corporate_brochure+%284%29.pdf

Payne, K.-L., Russell, A., Mills, R., Maras, K., Rai, D., & Brosnan, M. (2019). Is there a relationship between cyber-dependent crime, autistic-like traits and autism? *Journal of Autism and Developmental Disorders, 49*(10), 4159-4169.

Platje, E., Cornet, L.J.M., & Kogel, C.H. de (2017). Intelligentie, executieve functies en licht verstandelijke beperking in justitiecontext. *Justitiële verkenningen, 43*(6), 49-62.

Politie. (z.d.). *Van IT'er naar cybercrime-specialist bij de politie.* Geraadpleegd van https://kombijde.politie.nl/politie-als-werkgever/testimonial-cybercrime

Politie. (2020, 26 juni). *Lange celstraf voor kopstuk phishing-bende*. Geraadpleegd van https://www.politie.nl/nieuws/2020/juni/26/08-veroordeling-nieuwerkerk.html

Politieacademie. (z.d.-a). *Verhoren van kwetsbare verdachten.* Geraadpleegd van https://www.politieacademie.nl/onderwijs/onderwijsaanbod/pages/opleiding.aspx?code=4300913&interessegebied=6&thema=63

Politieacademie. (z.d.-b). *Verdieping op verhoor*. Geraadpleegd van https://www.politieacademie.nl/onderwijs/onderwijsaanbod/pages/opleiding.aspx?code=4302569&interessegebied=6&thema=60

Politieacademie. (z.d.-c). *Professioneel verhoor verkort.* Geraadpleegd van https://www.politieacademie.nl/onderwijs/onderwijsaanbod/pages/opleiding.aspx?code=4302567&interessegebied=6&thema=60

Politieacademie. (2020). *Onderzoeksprogramma 2020 Politieacademie.* Geraadpleegd van https://www.politieacademie.nl/kennisenonderzoek/Onderzoek/Documents/Onderzoeksprogramma%20PA%202020_def.pdf

Redlich, A.D., Kulish, R., & Steadman, J.H. (2011). Comparing true and false confessions among persons with serious mental illness. *Psychology, Public Policy, and Law, 17*(3), 394-418.

Rokven, J.J., Weijters, G. & Laan, A.M. van der (2017). *Jeugddelinquentie in de virtuele wereld: Een nieuw type daders of nieuwe mogelijkheden voor traditionele daders*. Den Haag: WODC.

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

Smit-Arnold Bik, M. (2020). Recherchewerk, een veranderend vakgebied. *PROCES, 2020*(5), 350-353.

Snook, B., Eastwood, J., & Barron, W. (2014). The next stage in the evolution of interrogations: The PEACE Model. *Canadian Criminal Law Review, 18*(2), 219-239.

Stambaugh, H., Beaupre, D.S., Icove, D.J., Baker, R., Cassaday, W., & Williams W.P. (2001). *Electronic crime needs assessment for state and local law enforcement*. Washington: National Institute of Justice.

Steinmetz, K.F. (2015). Becoming a hacker: Demographic characteristics and developmental factors. *Journal of Qualitative Criminal Justice and Criminology, 3*(1), 31-60.

Stevens, L., & Verhoeven, W.-J. (2011). Wat is er mis met een 'goed gesprek'? Een exploratief onderzoek naar pressie tijdens politiële verdachtenverhoren en risico's op valse bekentenissen. *Delikt en Delinkwent: Tijdschrift voor strafrecht, 2*(9), 114-131.

Stol, W. (2010). Kennis cybercrime schiet tekort. *Het Tijdschrift voor de Politie, 72*(9), 19-20.

Stol, W., & Jansen, J. (2014). *Cybercrime en de politie*. Den Haag: Boom Lemma Uitgevers.

Straub, J., Leerdam, J., Autar, J., & Sanches, G. (2020, 10 januari). Jeugdcriminaliteit bestrijden? Kijk de kunst af in Rotterdam. *Het Parool*. Geraadpleegd van https:///www.parool.nl/nieuws/jeugdcriminaliteit-bestrijden-kijk-de-kunst-af-in-rotterdam~b237707 7/?referrer=https%3A%2F%2Fwww.google.com%2F.

Sullivan, D. (2021, 16 maart). Tampa Twitter hacker agrees to three years in prison. *Tampa Bay Times*. Geraadpleegd van https://www.tampabay.com/news/crime/2021/03/16 /tampa-twitter-hacker-agrees-to-three-years-in-prison-in-plea-deal/

Turgeman-Goldschmidt, O. (2005). Hacker's accounts: Hacking as a social entertainment. *Social Science Computer Review, 23*(1), 8-23.

Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker. *International Journal of Cyber Criminology, 2*(2), 382-396.

Uzieblo, K. (2014). Kwetsbare verdachten. In R. Schellingen & N. Scholten (Reds.), *Het verdachtenverhoor: Meer dan het stellen van vragen* (pp. 201–220). Mechelen: Wolters Kluwer Belgium NV.

Verhoeven, W.-J. (2014). Mediëren verhoortechnieken de verandering in verklaringsbereidheid van verdachten? *Tijdschrift voor Criminologie, 56*(4), 10-38.

Verhoeven, W.-J., & Duinhof, E. (2017). *Effectiviteit van het verdachtenverhoor. Een veldstudie naar de relatie tussen verhoortechnieken, de verklaring van verdachten en de aanwezigheid van de advocaat in zware zaken*. Apeldoorn: Politie & Wetenschap.

Voskuil, K. (2019, 11 december). Politie neemt 145 fulltimers aan in strijd tegen cybercriminelen. *Algemeen Dagblad*. Geraadpleegd van https://www.ad.nl/binnenland/politie-neemt-145-fulltimers-aan-in-strijd-tegencybercriminelen~abe8424a

Wagen, W. van der, Oerlemans, J.-J., & Weulen Kranenbarg, M. (2020). Inleiding. In: W. Van der Wagen, J.-J. Oerlemans & M. Weulen Kranenbarg (Reds.), *Basisboek Cybercriminaliteit. Een criminologisch overzicht voor studie en praktijk* (pp. 13-18). Den Haag: Boom criminologie.

Wagen, W. van der, Zand-Kurtovic, E.G. van 't, Matthijsse, S.R., & Fischer, T.F.C. (2019). *Cyberdaders: Uniek profiel, unieke aanpak*? Den Haag: WODC, Ministerie van Justitie en Veiligheid.

Walsh, D., & Bull, R. (2012). Examining rapport in investigative interviews with suspects: Does its building and maintenance work? *Journal of Police and Criminal Psychology, 27*(1), 73-84.

Weulen Kranenbarg, M. (2018). *Cyber-offenders versus traditional offenders: An empirical comparison* (Proefschrift). Geraadpleegd van http://dare.ubvu.vu.nl/handle/1871/55530

Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? *The Howard Journal, 44*(4), 387-399.

Zebel, S., Vries, P. de, Giebels, E., Kuttschreuter, M., & Stol, W. (2013). *Jeugdige daders van cybercrime in Nederland: Een empirische verkenning*. Enschede / Den Haag: Universiteit Twente / WODC.

Bijlage 1. Toestemmingsformulier gegevensverstrekking

Hierbij verklaar ik dat ik bereid ben informatie te verstrekken voor het onderzoek uitgevoerd in opdracht van de Vrije Universiteit Amsterdam (VU): "*Verdachte hackers in het politieverhoor"*. Indien het interview reeds is afgenomen mag de data (volgens de veiligheidseisen) in het onderzoek worden gebruikt in het kader van een scriptie en publicatie.

- Ik heb van de onderzoeker schriftelijke en mondelinge informatie gekregen over de inhoud, methode en het doel van het onderzoek. Ik heb mijn vragen kunnen stellen en die zijn naar tevredenheid beantwoord. Ik begrijp waarover het onderzoek gaat.
- Ik begrijp dat mijn (auditief opgenomen en uitgewerkte) gegevens niet aan derden worden verstrekt. Mijn (anonieme/pseudonieme) gegevens kunnen wel met betrokken onderzoekers van dit project worden gedeeld.
- Ik stem vrijwillig in met deelname aan dit onderzoek en ben ervan op de hoogte dat de gegevens vertrouwelijk en anoniem worden behandeld. Ik heb voldoende tijd gehad om te beslissen of ik mee wil doen. Ik begrijp dat als ik niet meer mee wil doen, ik het gesprek op ieder moment stop kan zetten. Daarnaast kan ik tot 10 dagen na het interview mijn deelname intrekken, waarna het interview zal worden verwijderd en niet zal worden gebruikt voor het onderzoek.
- Ik begrijp dat ik mijn vragen altijd kan stellen aan de onderzoekscoördinator, Heleen Goes, via e-mail (j.h.goes@student.vu.nl) of (*telefoonnummer*).

Naam:	Datum:
…….	…….
Handtekening respondent:	Handtekening onderzoeker:
…….	…….

Bijlage 2. Vragenlijst van de interviews

Beste respondent, mijn naam is Heleen Goes en ik ben 21 jaar oud. Momenteel doe ik de master Opsporingscriminologie aan de Vrije Universiteit in Amsterdam. Voor mijn afstudeerproject doe ik nader onderzoek naar het verhoor van verdachte hackers. Cybercrime is een fenomeen waar burgers steeds meer mee te maken krijgen, maar in Nederland is er tot op heden nog maar weinig bekend over het verhoorproces bij verdachte hackers. U als respondent heeft unieke kennis over dit onderwerp en daarom is uw deelname aan het onderzoek van groot belang, en wil ik u ook hartelijk danken voor uw medewerking.

Om diepgaande inzichten te verkrijgen in het verhoor van hackers, zal uw perceptie omtrent het verhoor van hackers centraal staan. Het gaat dus echt om uw ervaring op het gebied van het verdachtenverhoor met hackers. Verder is het goed om te benadrukken dat het geen toetsend onderzoek betreft, maar dat het gaat om een verkennende en beschrijvende studie. Zodoende zijn er dus geen goede of foute antwoorden. Ook zal er op een vertrouwelijke en anonieme manier met uw informatie worden omgegaan. Zaakspecifieke informatie zal geanonimiseerd worden zodat de informatie niet herleidbaar is naar verdachten. Als er vragen zijn mag u die uiteraard altijd tussendoor stellen.

1. Achtergrond respondent

- Hou oud bent u?
- Hoe lang werkt u al bij de politieorganisatie?
    - Eerdere functies (bijvoorbeeld in de ICT)?
    - Hoe lang bent u al werkzaam op het gebied van cybercriminaliteit?
- Kunt u iets vertellen over uw vooropleiding?
- Welke opleidingen heeft u binnen de politie gevolgd?
    - Verhooropleiding?
    - Opleiding omtrent kwetsbare verdachten?
    - Opleiding omtrent cybercrime?
- Wat is uw huidige functie en wat houdt deze functie in?

2. Cybercrimeteams

- Kunt u me wat vertellen over uw cybercrimeteam?
    - Specialisatie in een bepaald delict?
    - Grootte van het team?

  - Hoe lang bestaat hij al?
  - Samenstelling van het team (verschillende type experts)?
- Kunt u me iets vertellen over mogelijke verschillen of overeenkomsten tussen uw team en andere cybercrimeteams in Nederland?
- Met wat voor verschillende type verdachten krijgt uw cybercrimeteam te maken?
- Hoe veel ervaring heeft uw cybercrimeteam met het verhoren van hackers?
  - Welke ervaring heeft u zelf met het verhoren van hackers?

Verdachtenverhoor met verdachte hackers – zijn of haar ervaring met die zaken centraal.

3. Hacken en persoonskenmerken

- Wat verstaat u onder hacken?
- Wat voor verschillende type hackers ziet u terug in de verhoorkamer?
  - Hackers met weinig technische kennis die lijken op traditionele criminelen?
  - Hackers met veel technische kennis en computervaardigheden?
- Welke overeenkomsten of verschillen zijn er volgens u tussen hackers en plegers van traditionele delicten? Of hackers en andere plegers van online delicten?
- Kunnen hackers volgens u worden aangemerkt als een kwetsbare verdachte?
  - Wat is volgens u een kwetsbare verdachte?
  - Jongeren / hoog IQ / autisme / andere stoornis?
  - In de literatuur staat omschreven dat hackers autistisch zijn, ziet u dat ook terug in de verhoorkamer? En zo ja, hoe ziet u dat dan terug?

Eventuele achtergrondkenmerken waar nog naar gevraagd kan worden:

- Belangrijke kenmerken = leeftijd / sekse / opleiding (IT-opleiding) / etniciteit / kennis en computervaardigheden / persoonlijkheidskenmerken (intelligentie, autisme, zelfcontrole of andere persoonlijkheidskenmerken) / motivatie.
- Minder relevante kenmerken = werk en sociaaleconomische status / vrijetijdsbesteding.

4. Verhoor van hackers

- In hoeverre verschilt het verhoor van verdachte hackers ten opzichte van een verhoor met andere verdachten? Zo ja, wat maakt het verhoor anders bij deze verdachtengroep?
- Kunt u me iets vertellen over de opbouw van het verhoor van hackers (welke fasen)?
  - Sociaal verhoor / zaakgerichtsverhoor

- Ik las in de Handleiding Verhoor dat er allerlei verhoormethoden zijn voor het verhoor. Wat gebruiken jullie daaruit bij het verhoor met verdachte hackers, en waarom?
    - Standaard Verhoorstrategie
    - Vrije verklaringsmethode
    - Directe stapelmethode
    - Bewijsvraagmethode
- Welke verhoortechnieken worden in het verhoor met verdachte hackers gebruikt? Kunt u ook toelichten waarom deze technieken worden gebruikt?
    - Voorbeelden van geschikte verhoortechnieken = het belonen van gedrag, het opbouwen van vertrouwen, het krijgen van een goede verstandshouding, het confronteren met bewijs, het confronteren met verklaringen van andere verdachten en het benadrukken van consequenties van het niet meewerken.
    - Voorbeelden van minder geschikte verhoortechnieken = het toepassen van trucs, het stellen van suggestieve vragen, het uiten van bedreigingen en beloften doen.
- Welke risico's zitten verbonden aan het gebruiken van bepaalde verhoormethoden of verhoortechnieken bij het verhoor van verdachte hackers?
    - Betrouwbaarheid en volledige verklaring van verdachte?
    - Wordt er in de keuze voor een verhoormethode of verhoortechniek rekening gehouden met het feit dat een hacker eventueel een kwetsbare verdachte is?
- Wordt er in de keuze voor een verhoormethode of verhoortechniek rekening gehouden met het feit dat een hacker eventueel een kwetsbare verdachte is?
    - Wat is uw ervaring met een advocaat bij een kwetsbare verdachte?
- In hoeverre zijn verdachte hackers bereid om een verklaring af te leggen of beroepen ze zich vaak op hun zwijgrecht? Indien dat het geval is, gebruikt u dan andere technieken?
    - Zitten daar ook risico's aan verbonden?
    - Heeft de advocaat daar ook invloed op? Wat is uw ervaring met advocaten?
- En bent u weleens afhankelijk van een verdachte omdat er geen andere bewijsmiddelen zijn? Indien dat het geval is, gebruikt u dan andere technieken?
    - Zitten daar ook risico's aan verbonden?
    - *Oftewel: is er een verschil wanneer er van te voren veel of weinig bewijs is?*
- Welke verhoormethoden of -technieken zouden volgens u gebruikt moeten worden in het verhoor van hackers, die momenteel nog niet worden toegepast?
    - Indien geen kennis methoden en technieken: Hoe zou het verhoor volgens u ingestoken moeten worden?

5. Samenstelling

- Kunt u me wat vertellen over de samenstelling van het verhoorteam bij een hackdelict?
    - Reguliere verhoorders?
    - Experts op het gebied van de ICT?
    - Ondersteuning rechtspsycholoog?
- Hoe en door wie wordt deze samenstelling bepaald?
- In hoeverre is het volgens u nodig dat er een expert op het gebied van ICT in het verhoor wordt ingezet bij hackdelicten?
- Is de samenstelling van het verhoorteam overeenkomend met andere teams (of de districtsrecherche bij een cybercrimedelict)?
- In welke gevallen werkt de samenstelling van het verhoorteam goed, en wanneer werkt de samenstelling minder goed volgens u?
- Denkt u dat de samenstelling van het verhoorteam invloed kan hebben op het verhoor?
    - Kennis over kwetsbare verdachten?
    - Kennis op het gebied van cybercrime?
    - Kennis op het gebied van het verhoor (voor IT-expert)?

6. Kennisniveau

- Over welke kennis beschikt u omtrent cybercrime en computervaardigheden?
    - Is er een opleiding hieromtrent en heeft u die gevolgd?
    - Beschikken andere mensen uit het team over dezelfde kennis op dit gebied?
    - Denkt u dat andere teams (of de districtsrecherche) over dezelfde kennis en vaardigheden beschikken?
- Over welke kennis beschikt u omtrent het verhoren van kwetsbare verdachten?
    - Heeft u de opleiding ‘Verhoren van kwetsbare verdachten’ gevolgd?
    - Beschikken andere mensen uit het team over dezelfde kennis op dit gebied?
    - Denkt u dat andere teams (of de districtsrecherche) over dezelfde kennis en vaardigheden beschikken?

7. Tot slot

- Wat zijn knelpunten in het verhoor van hackers?
- Wat kan bijdragen aan het optimaliseren van het verhoor van hackers?
- Zijn er nog dingen die u belangrijk vindt om te vermelden, die nog niet aan bod zijn gekomen?