# (Kwetsbare) hackers in het politieverhoor

"*De politie heeft – mede vanwege de zwijgende houding van de verdachte – een omvangrijk onderzoek moeten uitvoeren*".[1] In voorgenoemde zaak stond een verdachte terecht voor onder meer het hacken van e-mailaccounts van ondernemers en het versturen van valse facturen naar klanten van deze bedrijven. Cybercrime, met name hacking, is een groeiend probleem in de huidige digitale maatschappij. Door de opkomst van cybercrime krijgen rechercheurs in het politieverhoor[2] te maken met een nieuwe groep verdachten: verdachten van hackdelicten. Hackverdachten zijn veelal mannelijk, jong en kunnen een psychische aandoening als een Autisme Spectrum Stoornis (hierna: autisme) hebben. Zij variëren op het gebied van technische vaardigheden, opleiding en motivatie.
In hackzaken lijkt met name technisch bewijs een grote rol te spelen. Dit roept de vraag op of een verdachtenverklaring noodzakelijk is in het opsporingsonderzoek. En zo ja, hoe ziet het verhoorproces eruit? Hoe zorgen rechercheurs ervoor dat (technisch onderlegde) hackverdachten betrouwbaar verklaren? Tot op heden is nog geen onderzoek gedaan naar het verhoorproces van hackverdachten. Om daar inzicht in te krijgen, is een onderzoek uitgevoerd op basis van interviews met officieren van justitie, advocaten en respondenten die werkzaam zijn bij cybercrimeteams.[3]

## Het belang van het politieverhoor

Verdachtenverklaringen verkregen in politieverhoren dienen nog steeds als een belangrijk bewijsmiddel. Naar verwachting is technisch bewijs niet altijd voldoende om een hackzaak rond te krijgen. Soms speelt een verklaring van een hackverdachte zelfs een cruciale rol in het verloop van het opsporingsonderzoek. Dat is bijvoorbeeld het geval in de situatie waar de politie pas nader onderzoek kan doen zodra een hackverdachte zijn wachtwoord afstaat. Hierbij is het wel van belang dat de politie accurate informatie van de hackverdachte ontvangt. Wanneer rechercheurs onjuiste informatie van de verdachte verkrijgen, kan het onderzoek in de verkeerde richting worden voortgezet of loopt men, zonder ander duidelijk bewijs, vast.

De kans op een accurate verklaring is het grootst wanneer het verhoor op een neutrale wijze wordt uitgevoerd met de toepassing van gepaste verhoortechnieken (Gudjonsson & Pearse, 2011). Verhoortechnieken zijn gesprekstechnieken die worden gebruikt om de verklaringsbereidheid van verdachten te vergroten, zoals het confronteren van de verdachte met bewijsmateriaal en het tonen van bezorgdheid over de (situatie van de) verdachte (Verhoeven & Duinhof, 2017). Risicovolle technieken, zoals het stellen van suggestieve vragen en het voorleggen van fictief bewijs, brengen diverse gevaren met zich mee. Dit kan leiden tot het dichtslaan van een verdachte (Beijer, 2012), het opzettelijk delen van onjuiste informatie of tot het afleggen van een (valse) bekentenis (Kassin et al., 2010). Sinds mei 2021 is daarom een nieuwe richtlijn ingevoerd waarin staat dat verschillende risicovolle technieken niet mogen worden toegepast (Méndez, 2021).

[1] Rb. Rotterdam 4 juli 2021, ECLI:NL:RBROT:2019:5330.

[2] Ondanks de ontwikkelingen met betrekking tot 'investigative interviewing' is in deze bijdrage gekozen voor het woord 'verhoor' in plaats van 'interview'.

[3] Voor het onderzoek, zie: https://www.ubvu.vu.nl/pub/fulltext/scripties/14_2707242_0.pdf.

Verhoorrisico's spelen een nog grotere rol bij kwetsbare verdachten (Gudjonsson, 2003; Kaal, Moonen, & Rispens, 2021; Kranendonk, z.d.). In de OM-instructie AVR-verhoor (2021) wordt iemand als kwetsbaar aangemerkt wanneer hij of zij minderjarig is en/of een verstandelijke beperking, een cognitieve functiestoornis, dan wel een psychiatrische stoornis heeft. Hackverdachten kunnen ook kwetsbaar zijn. In de literatuur wordt beschreven dat een deel van de cyberdaders, waaronder hackers, autisme heeft en/of minderjarig is (Ledingham & Mills, 2015; National Crime Agency, 2017). Kwetsbare verdachten hebben veelal beperkt inzicht in oorzaak-gevolg relaties en kunnen daardoor geen goede inschatting maken van de gevolgen van hun verklaringen. Bovendien zijn zij gevoelig voor druk, hebben zij de neiging om please-gedrag te vertonen (compliance), stemmen zij vaak in met vragen van verhoorders (acquiescence) en zijn zij vatbaarder voor suggestieve vragen (Gudjonsson, 2003; Kaal et al., 2021). Ook het teveel inzetten van gangbare technieken, zoals het complimenteren van de verdachte om hem verklaringsbereid te maken, kan risicovol zijn voor kwetsbare verdachten (Kaal et al., 2021).

Vanwege bovenstaande kenmerken vereist het verhoren van kwetsbare hackverdachten een specifieke aanpak. Om te voorkomen dat deze verdachten worden onderworpen aan een 'normaal' verhoor, waarbij de kans op druk door het gebruik van risicovolle technieken hoger ligt, moeten kwetsbaarheden worden herkend. Dit kan door gebruik te maken van persoonlijke vragen uit de 'Vragenlijst Indicatie Kwetsbaarheid' (VIK-vragen) uit de Handleiding Verhoor (2021). Bij een vermoeden van kwetsbaarheid[4] kan het verhoor worden aangepast aan de problematiek van de verdachte, wordt deze verplicht een advocaat toegewezen, en kan het politieteam een gespecialiseerde verhoorder inzetten (Van Amelsvoort & Rispens, 2021).

## Onderzoeksopzet

Het is essentieel dat het politieverhoor op zo'n manier wordt uitgevoerd dat het betrouwbare informatie oplevert. Echter, onderzoek naar de Nederlandse verhoorpraktijk is schaars. Nog minder onderzoek is gedaan naar het verhoren van verdachten van cybercrime, meer specifiek hackverdachten. Juist in hackzaken is het uitvoeren van een correct verhoor belangrijk vanwege het belang van een accurate verklaring voor de voorspoedige voortgang van het opsporingsonderzoek en de potentiële kwetsbaarheid van hackers.

Het doel van het onderzoek was daarom om eerste inzichten te verkrijgen in het verhoor van hackverdachten. Hiervoor zijn 18 semi-gestructureerde interviews afgenomen met 2 officieren van justitie, 4 advocaten en 12 respondenten die werkzaam zijn bij 4 verschillende cybercrimeteams (waarvan 7 tactische en 3 technische rechercheurs en 2 teamleiders).

De focus van dit artikel ligt op de samenstelling van het verhoorteam, de perceptie van eerdergenoemde deskundigen omtrent de potentiële aanwezigheid van kwetsbaarheden bij hackverdachten en de verhoortechnieken die cybercrimeteams in de verhoorpraktijk toepassen. In het bredere onderzoek kwamen tevens onderwerpen aan bod als persoonskenmerken van hackverdachten, verhoormethoden, het kennisniveau en de vaardigheden van rechercheurs op het gebied van het verhoor van hackverdachten en de verschillen tussen rechercheurs met en zonder gespecialiseerde verhooropleiding.

[4] Verhoorders mogen alleen een inschatting maken en geen diagnose opstellen, aangezien dit niet de taak van de politie is (Van Amelsvoort & Rispens, 2021).

## Onderzoeksresultaten

Uit de onderzoeksresultaten blijkt dat verdachtenverklaringen niet altijd de belangrijkste bewijsbron zijn in hackzaken, al lijkt de verklaringsbereidheid van hackverdachten relatief hoog te liggen. Dat zou onder andere kunnen komen door vaste verhoorkoppels en de samenstelling van het koppel. In het geval van een technisch onderlegde hackverdachte, bestaat dat koppel vaak uit een tactische en een technische rechercheur. Een rechercheur benoemde het volgende voordeel 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. (…) Dat is eigenlijk tweedelig. Punt 1 zie je vaak dat er een soort klik ontstaat, omdat je weet 'hé wij spreken dezelfde taal'. En de andere kant is ook van shit ik kom hier niet weg 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."*[5] Ook krijgt een hackverdachte volgens respondenten veelal de ruimte om zelf met een verhaal te komen.

Uit de interviews bleek dat rechercheurs diverse verhoortechnieken toepassen om informatie van de hackverdachte te verkrijgen. Zo stelt een rechercheur: *"Ja tuurlijk is een bekentenis een doel uiteindelijk. Dat helpt natuurlijk wel met de bewijsvoering, want ook bij een op waarheid gestoelde verklaring kun je dat weer toetsen. En nou dan heb je gewoon een verhaal klaar."* Respondenten benoemen onder meer het opbouwen van een band met de verdachte, het benoemen van de consequenties indien de verdachte niet wil meewerken in het verhoor, het confronteren van de verdachte met bewijsmateriaal, het doen van een belofte, het innemen van een autoritaire houding en het stellen van suggestieve vragen. Het geven van complimenten wordt volgens een deel van de respondenten gedaan wanneer de hackverdachte zijn verhaal bijstelt om hem op die manier te motiveren om verder te vertellen, maar 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. (…) Ik weet dat techneuten dat leuk vinden om te horen."* Een groot deel van de rechercheurs was van mening dat er geen risico's verbonden zijn aan hun verhoorstrategie. Een onbetrouwbare verklaring wordt door hen vooral gezien als een risico voor de verdachte zelf: *"Vaak is een mens waardeloos qua bewijsvoering. Daar los van denk ik ook, dat onbetrouwbare verklaring vind ik ook prima, kunnen we dat weer weerleggen. Heb ik net zo lief. Ik heb graag een lulverhaal, want dan kunnen we dat helemaal afschieten."*

Wat betreft de potentiële kwetsbaarheid van hackverdachten, blijkt uit deze studie dat de meerderheid van de rechercheurs het vermoeden heeft dat zij in een verhoor weleens te maken hebben gehad met een hackverdachte met een vorm van psychische problematiek als autisme. De meeste rechercheurs lijken deze verdachten echter niet als kwetsbaar te bestempelen. Uit de interviews kon verder worden opgemaakt dat rechercheurs zich niet bewust zijn van het belang en het doel van het stellen van VIK[6]-vragen. In verschillende gesprekken kwam naar voren dat rechercheurs snel door VIK-vragen heengaan en deze in sommige gevallen zelfs volledig overslaan. Het volgende citaat illustreert de redenering van een rechercheur om minder persoonsgerichte

[5] Zie voor een verdere uitwerking hiervan het gehele onderzoeksrapport (zie voetnoot 3).

[6] VIK: Vragenlijst Indicatie Kwetsbaarheid; deze vragen uit de Handleiding Verhoor kunnen bijdragen aan het herkennen van kwetsbaarheden.

vragen te stellen en zich zoveel mogelijk op de zaak te richten: *"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 slaat nergens op. Het moet zin hebben die vragen."*

## Conclusie en aanbevelingen

Hackzaken kunnen complex zijn en het politieverhoor van hackverdachten kan dus ook lastig zijn, zeker aangezien weinig bekend is over het verhoren van hackers. De samenstelling van verhoorkoppels in hackzaken verschilt met andersoortige verhoren, en ook worden andere technieken gebruikt om de verdachte aan te zetten om te verklaren (bijvoorbeeld complimenten over hun technische werkzaamheden). Het onderzoek toont aan dat het verhoor van hackverdachten bij cybercrimeteams grotendeels op een neutrale en correcte manier lijkt te verlopen en dat rechercheurs veelal gepaste technieken gebruiken. Toch komt het ook voor dat rechercheurs risicovolle verhoortechnieken toepassen, zoals het doen van een belofte. De combinatie van het toepassen van risicovolle technieken en het gebrek aan bewustzijn over verhoorrisico's kan leiden tot ongewenste situaties; bijvoorbeeld tot het dichtslaan van verdachten, valse bekentenissen, of onbetrouwbare informatie (Beijer, 2012; Kassin et al., 2010; Kranendonk, z.d.). Dit kan voor zowel de politie als voor verdachten nadelig zijn. Wanneer een hackverdachte dichtslaat en de politie geen ander duidelijk bewijs voorhanden heeft, kan een (mogelijk) schuldige verdachte vrijuit gaan. Daarnaast besteden cybercrimeteams hierdoor onnodig tijd, geld en capaciteit aan het rechercheren op basis van onjuiste informatie. Deze gevaren kunnen nog sneller ontstaan bij kwetsbare hackverdachten. Het onderzoek laat zien dat er een gebrek aan herkenning lijkt te zijn, en mogelijkerwijs daarmee samenhangend een gebrek aan kennis en bewustzijn over (de omgang met) kwetsbare verdachten. Het is daarom belangrijk om op te merken dat rechercheurs uit deze studie onvoldoende stilstaan bij mogelijke gevaren van het politieverhoor van verdachten van hackdelicten.

Een aanbeveling is daarom om binnen de politie (en specifiek binnen cybercrimeteams) meer kennis en bewustzijn te creëren voor algemene risico's in het verhoren van hackverdachten. Daarnaast is het ook belangrijk dat de politie investeert in het kennisniveau van verhoorders op het gebied van kwetsbare verdachten, bijvoorbeeld door meer rechercheurs binnen cybercrimeteams een cursus te laten volgen met betrekking tot de oorzaken en het voorkomen van negatieve effecten van risicovolle technieken zoals please-gedrag, acquiescence (berusting) en suggestibiliteit. Gezien het verhoogde risico op deze effecten bij kwetsbare verdachten, en het feit dat huidige en eerdere studies uitwijzen dat een relatief groot deel van de groeiende groep veelal minderjarige hackverdachten leidt aan psychische problemen, is meer kennis hieromtrent essentieel. Ook moeten verhoorders worden getraind in het herkennen van kwetsbare verdachten door het stellen van VIK-vragen en daarbij voldoende door te vragen. Tot slot kan worden aanbevolen om meer intervisies, cursussen of terugkomdagen te organiseren, zodat het kennisniveau van verhoorders op peil wordt gehouden en nieuwe typen verdachten en hun mogelijke kwetsbaarheid goed in beeld komen.

**Over de auteurs**

Heleen Goes MSc is wetenschappelijk medewerker bij het WODC, j.h.goes@wodc.nl.

Robin Kranendonk MSc is promovenda, Vrije Universiteit Amsterdam en Nederlands Studiecentrum Criminaliteit en Rechtshandhaving; p.r.kranendonk@vu.nl.

Dr. Marleen Weulen Kranenbarg is universitair docent Criminologie, Vrije Universiteit Amsterdam, M.WeulenKranenbarg@vu.nl

## Literatuurlijst

Amelsvoort, A. van, & Rispens, I. (2021). *Handleiding verhoor*. Den Haag: Sdu Uitgevers.

Beijer, G. (2012). *Autisme & verdachtenverhoor. Een onderzoek naar de knelpunten tijdens een verdachtenverhoor met personen met ASS* [Scriptie].

Gudjonsson, G.H. (2003). *The psychology of interrogations and confessions: A handbook*. West Sussex: John Wiley & Sons.

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

Kaal, H., Moonen, X., & Rispens, I. (2021). Verhoor van personen met een (vermoede) licht verstandelijke beperking. In M. Bockstaele, F. Declercq, R. Kranendonk, K. Geijsen, & A. Dijk, van (Reds.), *Verhoor van kwetsbare volwassenen - Cahiers Politiestudies 2021-1, 58* (pp. 153-166). Antwerpen: Gompel & Svacina.

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.

Kranendonk, P.R. (z.d.). [Lopend promotieonderzoek naar de invloed van verhoortechnieken op de verklaring van verdachten met een licht verstandelijke beperking].

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.
Méndez, J.E. (2021). *Principles on effective interviewing for investigations and information gathering*. Geraadpleegd van: http://www.interviewingprinciples.com.
National Crime Agency. (2017). *Pathways into cybercrime.* London: National Cyber Crime Unit /Prevent Team.
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.