

ONGERUBRICEERD

Earth, Life & Social SciencesKampweg 5
3769 DE Soesterberg
Postbus 23
3769 ZG Soesterbergwww.tno.nl

T +31 88 866 15 00

F +31 34 635 39 77

TNO-rapport**TNO 2016 R10924****Toekomstverkenning leugendetectie:
Relevante toepassingen en
implementatievormen in het Nederlandse
veiligheidsdomein**

Datum	september 2016
Auteur(s)	Dr. Sophie van der Zee Dr. Rick van der Kleij Dr. Ir. Henri Bouma Drs. Jeroen van Rest
Aantal pagina's	56 (incl. bijlagen)
Aantal bijlagen	1
Opdrachtgever	Dr. Ir. Bert Don
Projectnaam	Sensoren en Systemen voor Security
Projectnummer	060.20506/01.02.02

Alle rechten voorbehouden.

Niets uit deze uitgave mag worden vermenigvuldigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook, zonder voorafgaande toestemming van TNO.

Indien dit rapport in opdracht werd uitgebracht, wordt voor de rechten en verplichtingen van opdrachtgever en opdrachtnemer verwezen naar de Algemene Voorwaarden voor opdrachten aan TNO, dan wel de betreffende terzake tussen de partijen gesloten overeenkomst.

Het ter inzage geven van het TNO-rapport aan direct belanghebbenden is toegestaan.

© 2016 TNO

ONGERUBRICEERD

Samenvatting

In het veiligheidsdomein is het belangrijk te kunnen bepalen welke informatie waar is en welke niet. Daarom wordt onderzoek gedaan naar waarneembare verschillen in iemands gedrag bij liegen en bij de waarheid spreken. Uit dit onderzoek blijkt dat mensen leugens niet goed kunnen detecteren, ongeacht of dat zij ervaren of getraind zijn in leugendetectie of niet. Ervaring en training in het identificeren van leugenachtig gedrag leidt vooral tot verhoogd zelfvertrouwen van de beoordelaar, maar niet tot verhoogde accuraatheid in het detecteren van leugens. Dit probleem beperkt de toepasbaarheid van leugendetectie in het veiligheidsdomein.

Een doel van dit onderzoek was om te achterhalen of nieuwe wetenschappelijke inzichten en technologische ontwikkelingen de praktische toepasbaarheid van leugendetectie hebben verhoogd. Een ander doel was om te kijken of er behoefte is in de Nederlandse praktijk voor de toepassing van recente leugendetectie-ontwikkelingen. Ook is verkend hoe de *state of the art* op het gebied van leugendetectie effectief is toe te passen in het veiligheidsdomein.

Als onderzoeksmethoden gebruikten wij literatuurstudie en semi-gestructureerde interviews. De interviews vonden plaats met vertegenwoordigers van organisaties die we vooraf hebben aangemerkt als belanghebbenden bij de toepassing van relevante ontwikkelingen op het onderwerp leugendetectie. Dertien interviews vonden plaats met in totaal 20 vertegenwoordigers. In deze interviews spraken wij over het huidige beeld dat de vertegenwoordigers hebben van leugendetectie, het huidige gebruik, het gewenste gebruik en de obstakels die het gewenste gebruik verhinderen.

De literatuurstudie laat zien dat methodologische ontwikkelingen in de afgelopen jaren de betrouwbaarheid en praktische toepasbaarheid van leugendetectie significant hebben verhoogd. Recente studies rapporteren accuraatheden van rond de 70% tot uitschieters van zelfs 90%, waar dit eerder nog nauwelijks boven de 50% lag. Een voorbeeld van een relevante ontwikkeling is de ontdekking dat een meer actieve rol van de interviewer tijdens een verhoor in combinatie met het strategisch inzetten van bewijs, bijvoorbeeld door middel van de *strategic use of evidence*-verhoormethode, de accuraatheid kan verhogen. Deze nieuwe verhoormethode vergroot de gedragsverschillen tussen leugenaars en waarheidssprekers. Ook technologische ontwikkelingen hebben de betrouwbaarheid en potentiële praktische toepasbaarheid vergroot. Een voorbeeld betreft de ontwikkeling van camera's die in combinatie met specifieke software geautomatiseerd verdacht gedrag kunnen herkennen.

Het huidige beeld zoals dat naar voren kwam in de interviews is dat leugendetectie in de praktijk op beperkte schaal wordt toegepast. Niet alle geïnterviewden waren bovendien op de hoogte van de recente ontwikkelingen in het vakgebied. Ondanks de geringe toepassing van leugendetectie in de huidige praktijk blijkt er behoefte te zijn aan de inzet van een betrouwbare leugendetectietest.

Vooral tijdens de eerste fases van onderzoek naar de waarheid ziet de meerderheid van de geïnterviewden voordeel in het gebruik van leugendetectie. Bijvoorbeeld bij het identificeren van onjuiste meldingen en betrouwbaarheidsbepaling van verklaringen van verdachten en getuigen. Bij getuigenverklaringen is er niet alleen behoefte aan het kunnen onderscheiden tussen juiste en onjuiste verklaringen, maar ook aan het kunnen onderscheiden van verschillende soorten onjuiste verklaringen. Een getuige kan namelijk opzettelijk of per ongeluk een onjuiste verklaring afleggen. Dit onderscheid kan juridische consequenties hebben.

De geïnterviewden noemen verschillende obstakels. Wet- en regelgeving staan de toepassing soms ronduit in de weg. Bijvoorbeeld voor de toepassing als bewijs in de rechtszaal. Hiernaast zijn er verschillende operationele belemmeringen die het gebruik van leugendetectie in de praktijk beperken. In het kader van waarheidsvinding is een obstakel dat leugendetectie niet tot de waarheid leidt. Leugendetectie geeft slechts een indicatie van een eventuele leugen. Om de waarheid te achterhalen moeten daardoor alsnog vervolgstappen worden ondernomen. Als de praktijk leugendetectie op grote schaal zou toepassen, moet heel duidelijk zijn hoe het werkt en wat de uitkomsten van de toepassing betekenen. De geïnterviewden zijn het er dan ook over eens dat, ongeacht het type leugendetectie, de resultaten niet ambigu mogen zijn.

In de interviews is ook het *voorkomen* van leugens en ander oneerlijk gedrag onder de aandacht gebracht. Uit de literatuurstudie blijkt dat morele reminders, religieuze reminders en cognitieve belasting ervoor kunnen zorgen dat iemand zich eerlijker gedraagt. Een aantal geïnterviewden ziet kansen om deze nieuwe inzichten in te zetten ter ondersteuning van het dagelijkse werk. Voorbeelden van toepassingsgebieden zijn het voorkomen van verzekerings- of uitkeringsfraude en het voorkomen van valse 112-meldingen.

Op basis van de resultaten van de interviews en inzichten uit de wetenschappelijke literatuur concluderen we dat een complex samenspel van verschillende factoren de toepassingswaarde bepaalt van leugendetectie in de praktijk. Bij elke toepassing is aandacht nodig voor de context waarin leugendetectie wordt gebruikt. Er is niet één techniek – of een combinatie van technieken – die het beste aansluit op de behoeftes van alle partijen, nu en in de toekomst. Maar deze zal per casus moeten worden ontwikkeld.

We concluderen dat de kansen voor toepassing van leugen-detectie bij de publieke veiligheidsorganisaties vooral kunnen liggen bij het:

- vergroten van de effectiviteit bij het afnemen van verhoren van verdachten en het vastleggen van getuigenverklaringen (belanghebbenden o.a. politie, OM en IND);
- ondersteunen van het operationeel optreden bij incidenten door het traceren van potentiële getuigen en het verkrijgen van betrouwbare informatie (belanghebbenden o.a. meldkamers, politie en veiligheidsregio's);
- versterken van de intelligence en opsporing ter bestrijding van zware criminaliteit en terrorisme (belanghebbenden o.a. AIVD, MIVD, NCTV en politie).

Daarnaast zien we nieuwe gebruikswaarde voor private instellingen o.a. voor toegangscontrole van kwetsbare locaties en bedrijfsterreinen, het screenen van sollicitanten voor gevoelige functies en de risico-inschatting bij de intake van cliënten.

Inhoudsopgave

	Samenvatting	2
1	Inleiding	5
1.1	Achtergrond en probleemstelling	5
1.2	Doelstellingen en onderzoeksvraag	7
1.3	Leeswijzer	7
2	Stand van zaken in leugendetectie	8
2.1	Uitdagingen	8
2.2	Ontwikkelingen	9
2.3	De praktijk	13
3	Interviews: Methode	15
4	Interviews: Resultaten	17
4.1	Fase 1: Huidige situatie	17
4.2	Fase 2: Behoeftebepaling en toekomstige ontwikkelingen	24
4.3	Fase 3: Response op huidige ontwikkelingen	34
4.4	Fase 4: Respons op het voorkomen van oneerlijk gedrag	35
5	Discussie	38
5.1	Beperkingen van het onderzoek	38
5.2	Het strategisch belang van kennis over leugendetectie	38
5.3	Kennisinfrastructuur	38
5.4	Aanbevelingen	39
6	Conclusie	43
7	Referenties	47
	Bijlage(n)	
	A Interview protocol	

1 Inleiding

1.1 Achtergrond en probleemstelling

Het bepalen van welke informatie waar is en welke niet speelt in het veiligheidsdomein een belangrijke rol. Op verschillende manieren houden o.a. de volgende instanties zich daar mee bezig: de Nationale Politie, het ministerie van Veiligheid & Justitie, het openbaar ministerie en de Koninklijke Marachaussee. Ook commerciële dienstverleners, zoals verzekeraars en beveiligers, kunnen belang hebben bij waarheidsvinding, zoals bij het herkennen van fraude.

Onder waarheidsvinding verstaan wij het bepalen van het waarheidsgehalte van een bewering. Deze bewering kan mondeling gemaakt zijn, maar bijvoorbeeld ook geschreven. Het strategisch inzetten van interviewtechnieken en bewijsmateriaal kan bijdragen aan waarheidsvinding (May & Granhag, 2016; Soronchinski e.a., 2014). Het waarheidsgehalte van een bewering kan worden bepaald door deze te vergelijken met eerdere beweringen, ofwel uitspraken binnen eenzelfde verklaring, met uitspraken in eerdere verklaringen, met uitspraken in verklaringen van anderen, of met bestaand bewijs (Vredevelde, Van Koppen, & Granhag, 2014). Aan het licht gebrachte inconsistenties, zoals tegenstellingen (meerdere verklaringen die niet allemaal waar kunnen zijn omdat ze tegengestelde informatie bevatten), omissies (jargon voor het niet rapporteren wat wel is gebeurd, oftewel het weglaten van relevante informatie) en commissies (jargon voor het wel rapporteren wat ofwel niet is gebeurd, ofwel niet eerder was gerapporteerd), kunnen dan worden gebruikt om een bewering te toetsen en het waarheidsgehalte te bepalen.

Deze verkennende studie richt zich op een specifiek onderdeel van waarheidsvinding, namelijk *leugendetectie*. Een statement is leugenachtig als deze opzettelijk gemaakt wordt door een individu om een onjuist beeld te creëren bij de ander. Dit onjuiste beeld kan geschetst worden door foutieve informatie aan te bieden, of door het bewust verzwijgen van relevante informatie. Een statement is alleen leugenachtig als de verteller, op het moment van het maken van het statement, zelf doorheeft dat dit statement een onjuist beeld geeft. Anders is het gewoon slechte communicatie of had de verteller zelf een verkeerd beeld van de situatie.

De relevantie van leugendetectie in het veiligheidsdomein wordt in het hierop volgende tekstkader geïllustreerd aan de hand van een recente casus. Daarin zijn met vetgedrukte tekst situaties aangegeven waarin leugendetectie mogelijk een bijdrage had kunnen leveren.

De daders van de aanslagen van 13 november 2015 in Parijs zijn allen EU staatsburgers. Een aantal van hen zijn **naar Syrië gereisd** en van hen is een deel **teruggekomen als vluchteling**, een ander deel mogelijk **als reguliere reiziger**. Een ander, Saleh Abdeslam, was op dat moment nog niet als geradicaliseerde in beeld bij de veiligheidsdiensten. Direct na de aanslagen van 13 november 2015 in Parijs werd hij nog diezelfde avond een half uur **gehoord bij een identiteitscontrole** nabij de Franse grens met België. Ondanks een extra uitvoerige controle, konden daar geen onregelmatigheden worden gevonden. Pas later kon zijn betrokkenheid worden bewezen, en op 18 maart 2016 is hij -na een uitvoerige zoektocht- in Brussel **gearresteerd**. Tegen die tijd was ook duidelijk geworden dat er één of meerdere terroristencellen in België bezig waren om een volgende aanslag te plegen en dat Abdeslam met hen in contact was geweest. Het was de verwachting dat deze cellen hun plannen zouden versnellen naar aanleiding van deze arrestatie: Abdeslam kon immers informatie loslaten over de plannen en de betrokkenen. Helaas lukte het de terroristen om op 22 maart 2016, vier dagen na de arrestatie van Abdeslam, om een nieuwe serie aanslagen te plegen. Abdeslam is zowel voor als na de aanslagen in Brussel ondervraagd. **In de ondervraging voorafgaand aan die tweede serie aanslagen**, bekent hij dat hij plannen maakt voor nieuwe aanslagen. **In de ondervraging na die tweede serie aanslagen** stelt hij echter dat hij geen informatie heeft over deze nieuwe aanslagen. Een extra complicatie bij deze ondervraging kan de strijdigheid zijn tussen enerzijds het opsporingsbelang in relatie tot de aanslagen in Parijs, en anderzijds het intelligence-belang in relatie tot het voorkomen van nieuwe aanslagen. In deze casus zijn minstens zes, mogelijk zeven soorten situaties waar leugendetectie wellicht op één of andere manier een bijdrage had kunnen leveren; deze zijn vet gemaakt. Het onderzoek is op dit moment nog in volle gang, en nieuwe feiten komen nog regelmatig naar boven. Het is nog niet duidelijk of en wanneer Abdeslam loog.

De afgelopen jaren heeft het leugendetectie-onderzoeksveld zich snel ontwikkeld. Dit is gebeurd dankzij technologische ontwikkelingen en interesse uit verschillende andere onderzoeksgebieden. Traditioneel werd het veld namelijk gedomineerd door psychologen, maar de laatste jaren wordt er ook leugendetectie onderzoek gedaan vanuit domeinen als informatica, communicatiewetenschappen en gedrags-economie. Deze ontwikkelingen zijn zichtbaar in de hernieuwde interesse voor onderzoek en in de ontwikkeling van nieuwe detectiemethodes (zie bijvoorbeeld Van der Zee, Van der Kleij, Van Rest, & Bouma, 2016). Onderzoek en de ontwikkeling van nieuwe methoden worden echter niet altijd geleid door vragen over maatschappelijk nut. Onderzoek in een gecontroleerde lab setting is ook niet altijd goed vertaalbaar naar de weerbarstige praktijk waarin veiligheidsprofessionals opereren. Dit leidt tot de indruk dat er in de praktijk van het veiligheidsdomein nog nauwelijks gebruik wordt gemaakt van de (nieuwe) mogelijkheden van het gebruik van de huidige state-of-the-art kennis en technologie op het gebied van leugendetectie.

1.2 Doelstellingen en onderzoeksvraag

Het doel van dit rapport is tweeledig. Ten eerste is het doel om de huidige kennisbasis bij TNO op het onderwerp leugendetectie te bundelen en te versterken. Ten tweede is het doel om veiligheidsorganisaties en -bedrijven in positie te brengen om te profiteren van deze kennis. De vraag die ligt achter dit onderzoek is:

op welke manier kan state-of-the-art kennis en technologie over leugendetectie effectief worden toegepast door veiligheidsprofessionals, zoals bijvoorbeeld politiediensten, ter bevordering van maatschappelijke veiligheid?

Voor dit doeleinde is een selectie gemaakt van potentiële eindgebruikers in Nederland. Bij hen is een inventarisatie gemaakt van hun actuele kennis en gebruik van leugendetectie, van hun behoeftes op dit gebied en van welke obstakels overkomen moeten worden om die behoeftes in te vullen. Hierbij is aandacht geweest voor beschrijving van scenario's, toepassingen en uitdagingen voor waarheidsvinding in complexe omgevingen. Om in te zoomen op de kansen voor de Nederlandse hightech industrie, is daarbij ook specifiek gekeken naar de utiliteit van nieuwe sensortechnieken.

1.3 Leeswijzer

Hoofdstuk 2 beschrijft actuele ontwikkelingen in leugendetectie op basis van de wetenschappelijke literatuur. Hoofdstuk 3 beschrijft de gevolgde aanpak van de gevoerde interviews. Hoofdstuk 4 beschrijft de resultaten van de interviews. Door de interviews is inzicht verkregen in de huidige situatie, behoeftes en toekomstige kansen voor de toepassing van leugendetectie. Hoofdstuk 5 evalueert het onderzoek, doet aanbevelingen en suggesties voor vervolgonderzoek. Hoofdstuk 6 geeft de conclusies van het onderzoek.

2 Stand van zaken in leugendetectie

2.1 Uitdagingen

2.1.1 *Het effect van liegen op gedrag*

Inmiddels is bekend dat liegen geen direct effect heeft op gedrag van de leugenaar – dat wil zeggen, er is geen gedrag dat uniek gerelateerd is aan liegen – maar dat liegen wel op verschillende manieren een indirect effect op gedrag kan hebben op de volgende drie manieren.

- Liegen kan een emotionele reactie opwekken, zoals schuldgevoel en angst maar ook verrukking (Ekman, 1989).
- Liegen kan moeilijker zijn dan de waarheid vertellen en daarmee de cognitieve belasting van een leugenaar verhogen. Liegen kan bijvoorbeeld moeilijker zijn dan de waarheid vertellen omdat leugenaars een leugen moeten fabriceren terwijl ze de waarheid moeten onderdrukken (DePaulo, e.a., 2003), doordat leugenaars er niet vanuit gaan dat ze geloofd worden en dus de gesprekspartner nauwlettend in de gaten zullen houden op tekenen van ongeloof (Buller & Burgoon, 1996), of doordat ze proberen versprekingen te voorkomen (Vrij, 2008).
- Leugenaars kunnen proberen hun leugenachtige gedrag te beheersen om zo eerlijker over te komen. Hoe een leugenaar zijn gedrag probeert aan te passen, hangt af van het beeld dat hij heeft van leugenachtig gedrag (Hurley, Griffin, & Stefanone, 2014; Taylor & Hick, 2007).

De drie voorgenoemde manieren waarop liegen gedrag kan beïnvloeden, kunnen verschillende en ook tegengestelde effecten hebben op gedrag. Zo kunnen schuldgevoel en cognitieve belasting bijvoorbeeld de hoeveelheid handbeweging verminderen, terwijl angstige gevoelens die juist kunnen vermeerderen.

Leugenachtig gedrag en reacties kunnen onderverdeeld worden in drie typen die ofwel met het blote oog waarneembaar zijn, ofwel met behulp van technologie meetbaar zijn. De drie typen zijn non-verbaal gedrag (hoe iemand zich gedraagt), verbaal gedrag (wat iemand zegt en op welke manier) en fysiologische (lichamelijke) reacties zoals verandering in bloeddruk, hartslag en huidgeleiding (Vrij, 2008; Zuckerman, DePaulo, & Rosenthal, 1981).

2.1.2 *Problemen met leugendetectie*

Tien jaar geleden hebben Bond en DePaulo (2006) een meta-analyse uitgevoerd over ongeveer 200 leugenunderzoeken. Zij vonden dat mensen niet goed zijn in het detecteren van leugens, of in ieder geval niet in een labsetting waarin ongetrainde proefpersonen (met of zonder interactie) een inschatting moeten maken van het waarheidsgehalte van de verklaring van een verdachte. Uit hun metastudie bleek dat proefpersonen niet veel beter dan kans niveau scoorden (54%; Bond & DePaulo, 2006). Helaas bleek jarenlange interviewervaring als politieagent (Aamodt & Custer, 2006; Hartwig, Granhag, Strömwall, & Vrij, 2004; Vrij & Mann, 2005) of het trainen van mensen in de juiste leugenachtige gedragingen (Kassin & Fong 1999) niet de oplossing, want ervaring en training leidden wel tot een hoger zelfvertrouwen, maar meestal niet tot betere detectie, vooral niet wanneer de training gericht was op non-verbale of paraverbale leugenindicatoren (Hauch, Sporer, Michael, & Meissner, 2016).

Vrij, Granhag en Porter (2010) hebben verschillende redenen geïdentificeerd waarom mensen niet goed zijn in het detecteren van leugens. Allereerst is er geen enkele gedraging die uniek gerelateerd is aan liegen. Oftewel, er bestaat geen menselijke versie van de neus van Pinocchio (DePaulo e.a., 2003). Ten tweede heeft men vaak onjuiste ideeën over welke gedragingen indicatoren zijn van liegen, zoals bijvoorbeeld het idee dat leugenaars oogcontact vermijden (Hurley e.a., 2014). Dit onjuiste beeld van leugenachtige gedragingen geldt in zekere mate ook voor deceptie onderzoekers, aangezien ongeveer 75% van de bestudeerde gedragingen in leugenonderzoek geheel niet gerelateerd bleken te zijn aan liegen (DePaulo e.a., 2003; Vrij e.a., 2010). Ten derde hebben de gedragingen die wel gerelateerd zijn aan liegen slechts een zwakke correlatie ($d = 0.12 - 0.55$; DePaulo e.a., 2003), waardoor gedragsverschillen tussen waarheidsvertellers en leugenaars kleiner zijn dan vaak wordt gedacht (Hartwig & Bond, 2011). Ten vierde proberen leugenaars om hun leugenachtige gedrag te onderdrukken en eerlijk over te komen (Vrij, 2008). Een vijfde, meer contextuele reden waarom leugendetectie lastig kan zijn, is dat men in de praktijk vaak geen feedback krijgt van juiste of onjuiste leugendetectie (Hartwig, Granhag, Strömwall, & Andersson, 2004). Bijvoorbeeld, als een *screeener* iemand onterecht doorlaat bij een screening op het vliegveld dan komt men dat vermoedelijk hooguit bij uitzondering, en dan slechts op organisatieniveau en pas na verloop van tijd te weten. Zonder tijdige, concrete en accurate feedback is het lastig om beter te worden in leugendetectie.

2.2 Ontwikkelingen

Er wordt veel onderzoek gedaan om manieren te identificeren om de detectieaccuraatheden te verhogen. In het afgelopen decennium hebben verschillende ontwikkelingen plaatsgevonden die de betrouwbaarheid van leugendetectie kunnen verhogen of die ervoor zorgen dat leugendetectie beter in de praktijk kan worden toegepast. Waar leugens en de detectie hiervan traditioneel voornamelijk bestudeerd werd door psychologen, heeft leugendetectie inmiddels ook de interesse gewekt van informatici en gedragseconomen. Dankzij de bijdragen van deze onderzoeksgebieden zijn er de afgelopen jaren verschillende onderzoeksmethoden en analysetechnieken gebruikt, welke hebben geleid tot nieuwe inzichten en ontwikkelingen. Van der Zee, Van der Kleij, Van Rest en Bouma (2016) hebben vier recente ontwikkelingen op het gebied van leugendetectie geïdentificeerd die relevant zijn voor de praktijk.¹

2.2.1 *Een actievere rol van de interviewer*

Het idee achter leugendetectie is dat wanneer iemand liegt, diens gedrag verandert en dat deze verandering kan worden waargenomen. In welke mate iemands gedrag verandert wordt mede bepaald door de interviewer en het type, dat worden gesteld. Zo is aangetoond dat het verhogen van de *cognitieve belasting* van de verdachte door het moeilijker maken van het interview, de gedragsverschillen tussen leugenaars en waarheidssprekers vergroot (Vrij e.a., 2011). Dit vergemakkelijkt het detecteren van leugens en zorgt voor een hogere leugendetectie accurateid (van 54% naar 71%; Vrij, Fisher, & Blank, 2015).

¹ Sectie 2.1.2 is in gewijzigde vorm eerder verschenen in Security Management (Van der Zee e.a., 2016).

Omdat bij leugenaars het geheugen en hun verklaring niet overeenkomen, kan de cognitieve belasting van een leugenaar verhoogd worden door vragen te stellen die de leugenaar niet heeft voorbereid, zoals *onverwachte vragen*, *specifieke vragen*, en *vragen in omgekeerde volgorde* (Vrij e.a., 2009; Vrij e.a., 2008).

Omdat waarheidsvertellers wel op hun geheugen kunnen vertrouwen bij het beantwoorden van dit type vragen, ervaren zij een kleinere verhoging in cognitieve belasting dan leugenaars, en kunnen gedragsveranderingen veroorzaakt door cognitieve belasting gebruikt worden om leugens te detecteren. Letten op cognitieve belasting in plaats van leugenachtig gedrag kan ook leugendetectie accuraatheid ten goede komen. In experimenteel onderzoek is aangetoond dat proefpersonen beter waren in het identificeren van leugens als ze de vraag moesten beantwoorden over hoe hard iemand nadacht in plaats van of iemand loog (Vrij, 2004). Naast het stellen van verschillende soorten vragen, kan de cognitieve belasting ook verhoogd worden door de verdachte tijdens het interview een tweede taak uit te laten voeren zoals het behouden van oogcontact met de interviewer (Vrij, Mann, Leal, & Fisher, 2010).

Er zijn ook verschillende verhoormethoden die kunnen bijdragen aan een hogere leugendetectie accuraatheid die niet berusten op het verhogen van de cognitieve belasting van de verdachte. Wanneer twee verdachten tegelijk worden verhoord, het zogeheten *collective interviewing*, geeft de manier waarop zij met elkaar interacteren een inzicht in het waarheidsgehalte van hun verklaring.

Omdat leugenaars graag hun verhaal zo simpel mogelijk houden, zullen leugenaars elkaar minder onderbreken, aanvullen en corrigeren dan waarheidsprekers wanneer geïnterviewd in paren (Vrij e.a., 2012). Daarnaast kan ook bewijsmateriaal ingezet worden om leugenaars te detecteren, bijvoorbeeld met de SUE (Strategic Use of Evidence) techniek. Door het bewijs tegen een verdachte niet aan het begin, maar later of stapsgewijs gedurende het interview te onthullen, is het lastiger voor een verdachte om antwoorden te geven die consistent zijn met het bewijs, waardoor leugenaars makkelijker te detecteren zijn in hun gedrag (Sorochinski e.a., 2014). Daarnaast is gebleken dat je door de illusie te wekken dat je als interviewer meer weet dan je eigenlijk weet, een verdachte aan het praten kan krijgen, wat bevorderlijk kan zijn voor leugendetectie. Deze techniek staat bekend als de Scharff techniek (May & Granhag, 2016). Deze ontwikkeling heeft in surveillance toepassingen geleid tot de opkomst van *predictive profiling* trainingen zoals *Search Detect React*, de Spottersmethode en Observeren Reageren² (van Pel, Verhagen, & Wijn, 2012). De effectiviteit van dit soort trainingen is voor surveillance echter nog niet overtuigend aangetoond.

2.2.2 *Het automatisch meten van leugenachtig gedrag*

Traditioneel concludeert de menselijke interviewer op basis van de aan- of afwezigheid van leugenachtige gedragingen of de verdachte liegt. Menselijke waarneming is echter subjectief en detectie accuraatheden liggen laag (Bond & DePaulo, 2006). Uit onderzoek blijkt dat leken er vaak vanuit gaan dat iemand de waarheid spreekt (*truth bias*; Levine, Park, & McCornack, 1999), terwijl professionals vaker het omgekeerde doen (*lie bias*; Meissner & Kassin, 2002). Om deze subjectiviteit weg te nemen en om de accuraatheid en efficiëntie te vergroten, wordt er steeds meer onderzoek gedaan naar automatische leugendetectie (Bethlem & Casparie, 2008).

² Dit zijn merknamen.

Traditioneel werden de fysiologische reacties (hartslag, bloeddruk en huidweerstand) van verdachten al automatisch gemeten, bijvoorbeeld door middel van een polygraaf. De polygraaf is een verzamelnaam voor apparatuur waarmee verschillende fysiologische reacties zoals bloeddruk, hartslag en ademhaling tegelijkertijd kunnen worden gemeten. De bekendste toepassing van de polygraaf is de *Controlled Question Technique* (CQT), waarin de fysiologische reactie wordt vergeleken op verschillende soorten vragen, namelijk zogenaamde feiten-vragen (om een baseline vast te stellen), delict-vragen en controle -vragen (Counter Intelligence Field Activity, 2004). Nu worden naast fysiologische reacties ook non-verbale gedrag, bijvoorbeeld door automatische video-analyse (Meservy e.a., 2005; Perez-Rosas, Abouelenien, Mihalcea, & Burzo, 2015) en het gebruik van *motion-capture* pakken (Van Der Zee, Poppe, Taylor, & Anderson, 2015), en verbale gedrag, bijvoorbeeld door software pakketten als Linguistic Inquiry and Word Count (LIWC; Pennebaker, Francis, & Booth, 2001), automatisch gemeten.

Technologische ontwikkelingen hebben tot twee belangrijke vernieuwingen geleid, die voorheen geen optie waren: namelijk *real-time analysis*, oftewel het objectief analyseren van gedrag terwijl het gebeurt, en het automatisch combineren van input uit verschillende sensoren, de zogenaamde *multimodale aanpak*. Wanneer zowel het non-verbale gedrag, het verbale gedrag en de fysiologische reacties van een persoon worden gemeten is de kans groter dat een leugen gedetecteerd wordt dan wanneer naar één gedraging gekeken wordt; een leugenaar kan immers niet alle gedragingen tegelijkertijd controleren. Uit experimenteel onderzoek waarin de effectiviteit van leugendetectie gebaseerd op één modaliteit vergeleken werd met een multimodale aanpak, blijkt dat een multimodale aanpak tot een hogere detectieaccuraatheid leidt (Abouelenien, Mihalcea, & Burzo, 2015; Abouelenien, Pérez-Rosas, Mihalcea, & Burzo, 2014). Een indrukwekkend voorbeeld van een real-time multimodale aanpak is de AVATAR screeningtool voor controles op vliegvelden van het Department of Homeland Security in de VS. Terwijl passagiers de vragen van een *virtual agent* beantwoorden gedurende 30 tot 90 seconden, wordt door middel van verschillende sensoren hun gedrag gemeten, geanalyseerd en doorgestuurd naar de tablet van de dienstdoende TSA officer (red. TSA staat voor Transport Security Administration. Dat is een onderdeel van Homeland Security) die op basis van deze informatie kan bepalen welke passagiers verdacht gedrag vertonen. Die worden uitgenodigd voor een vervolginterview. Onderzoek met deze automatische detectiemethode heeft aangetoond dat de AVATAR beter presteert dan TSA officers, en zowel in het lab als op de luchthaven leugendetectie accurateheden bereikt van 85% en hoger (Burgoon, 2015). In hoeverre deze resultaten replicerbaar zijn, zal moeten blijken uit vervolgonderzoek, bij voorkeur uitgevoerd door andere onderzoeksgroepen.

2.2.3 *Liegen over kwade intenties*

De meerderheid van het leugnonderzoek gaat over het liegen over dingen die mensen wel of niet gedaan hebben in het verleden. Er zijn echter ook situaties waarin het belangrijk is om te detecteren of iemand slechte intenties of plannen heeft, zoals bijvoorbeeld het plannen van een terroristische aanslag. De behoefte aan het kunnen detecteren van liegen over intenties komt vooral uit de intelligence hoek. Sinds 2011 wordt het liegen over intenties systematisch in het leugendetectie onderzoeksveld bestudeerd, bijvoorbeeld om te identificeren in hoeverre leugenachtig gedrag verschilt ten opzichte van liegen over activiteiten in het

verleden, en om te testen hoe goed mensen zijn in het detecteren van valse intenties. Uit onderzoek van Vrij en collega's (2011) bleek dat hoewel verklaringen over activiteiten in het verleden meer leugenindicatoren bevatten dan verklaringen over intenties, dat leugens over intenties ($M = .68$; $SD = 0.47$) beter werden gedetecteerd dan leugens over uitgevoerde activiteiten ($M = .61$; $SD = 0.49$). Leugens over intenties kunnen beter gedetecteerd worden wanneer relevante interviewtechnieken worden gebruikt, zoals het stellen van onverwachte vragen (Vrij e.a., 2009), de Scharff techniek (May & Granhag, 2016), het verhogen van cognitieve belasting, en bij het interviewen van twee verdachten tegelijkertijd het geforceerd moeten wisselen van beurt om te spreken (Vrij & Granhag, 2014).

2.2.4 *Daderkennis identificatie*

De bekendste manier om leugens op basis van fysiologische veranderingen te detecteren is de CQT toepassing van de polygraaf. Hoewel deze methode vrij effectief (61-83%; Verschuere e.a., 2011) is in het detecteren van leugens, is het minder goed in het detecteren van waarheden door de hoge mate van loze alarmen (National Research Council, 2003; Bull, Baron, Gudjonsson, Hampson, Rippon & Vrij, 2004). Dit wordt veroorzaakt door een fysiologische stressreactie die niet uniek is voor leugenaars, maar ook ervaren kan worden door onschuldige verdachten die onder deze omstandigheden verhoord worden (Ben-Shakhar & Elaad, 2003).

Een nieuwere toepassing van de polygraaf is de *Concealed Information Test (CIT)*; ook wel de *Guilty Knowledge Test [GKT]*; voor een overzicht zie Verschuere e.a., 2011). In tegenstelling tot de eerder genoemde CQT methode, is niet leugendetectie per se, maar het aantonen van (dader)kennis de kern van CIT. Daderkennis identificatie is gebaseerd op een cognitieve of lichamelijke reactie die optreedt als iemand bekend is met de gepresenteerde informatie (Verschuere, Ben-Shakar, & Meijer, 2011), de zogeheten *orienting reflex*. Deze reflex kan bijvoorbeeld gemeten worden met huidgeleiding of met een EEG (*elektro-encefalogram*) aan de hand van een *P300-wave*, een signaal dat optreedt bij het zien van bekende informatie. In tegenstelling tot leugendetectie waarbij de verdachte een verklaring aflegt die vervolgens een betrouwbaarheidsbepaling krijgt, hoeft de verdachte bij de CIT geen antwoord te geven. In plaats daarvan worden verschillende opties van misdaad gerelateerde informatie getoond en de fysiologische reactie tijdens het zien van deze informatie gemeten. Als de hersenactiviteit aantoont dat een persoon herhaaldelijk de "juiste" antwoordoptie herkent, betekent dit dat deze persoon de informatie herkent. De CIT wordt voornamelijk ingezet bij het aantonen van daderkennis in verdachten. De testresultaten kunnen vervolgens worden ingezet tijdens het verhoor.

Naast het gebruik van EEG wordt er ook succesvol geëxperimenteerd met andere meetmethoden om daderkennis aan te tonen met de *CIT*, zoals het gebruik van warmtecamera's (Park, Suk, Hwang, & Lee, 2013), fMRI (Langleben, Hakun, Seelig, Wang, Ruparel, Bilker, & Gur 2016), het meten van reactietijd (Verschuere, Crombez, De Grootte, & Rosseel, 2010), en het meten van pupil en oogknipper reacties (Seymour, Baker, & Gaunt, 2013).

Het nadeel van de CIT is echter dat al op de *plaats delict* rekening moet worden gehouden met de mogelijke inzet van deze test, aangezien er voldoende misdaad gerelateerde details moeten zijn die bekend zijn bij de politie en bij de dader, maar niet bij het algemene publiek (Verschuere, Ben-Shakar, & Meijer, 2011).

Daarnaast moet een verdachte wel willen meewerken aan de test, anders kan de verdachte de leugendeteciemethode bijvoorbeeld saboteren door zijn ogen te sluiten waardoor hij de aangeboden informatie niet waarneemt.

Naast het identificeren van daderkennis, oftewel kennis over een activiteit in het verleden, kan de CIT ook ingezet worden voor het identificeren van iemands kwade intenties, oftewel geplande activiteiten die mogelijk in de toekomst gaan plaatsvinden. Dit kan behulpzaam kan zijn bij het vergaren van intelligence. Dit onderzoeksveld is nog relatief onontgonnen, maar de eerste wetenschappelijke resultaten zijn veelbelovend. In een experiment van Meijer, Smulders en Merckelbach (2010) kreeg bijvoorbeeld een groep proefpersonen informatie over een op handen zijnde terroristische aanval. Door middel van CIT-verhoren slaagden de onderzoekers erin om succesvol de datum, de locatie en het doelwit van de aanval te achterhalen. In een vergelijkbaar experiment van Meixner en Rosenfeld (2011) waren de onderzoekers in staat om 12 van de 12 proefpersonen met kwade intenties te identificeren en details te leren over de geplande terroristische aanslagen, zonder onschuldigen als schuldig aan te wijzen. In een recentere experimenteel onderzoek op dit onderwerp hebben 20 groepen van vijf proefpersonen een CIT ondergaan om de locatie van een geplande terroristische aanval te achterhalen (Meijer, Bente, Ben-Shakhar, & Schumacher, 2013). In 19/20 groepen kon het correcte land geïdentificeerd worden, in 13/19 de correcte stad, en in 7/13 zelfs de correcte straatnaam. Er zijn nu verschillende experimenten door verschillende labs op dit onderwerp uitgevoerd, en tot nu toe zijn de resultaten gerepliceerd. Zoals bij elke nieuwe onderzoekslijn zal vervolgonderzoek uit moeten wijzen hoe robuust deze resultaten zijn. De huidige resultaten geven in ieder geval wel aan dat de CIT dus niet alleen relevant zou kunnen zijn voor het verhoren van verdachten voor een specifiek delict, maar ook bij het verwerven van intelligence.

2.3 De praktijk

Het detecteren van leugens over activiteiten in het verleden en intenties voor de toekomst heeft de afgelopen jaren een belangrijke vooruitgang meegemaakt. De hogere betrouwbaarheid en praktische toepasbaarheid zijn mogelijk gemaakt door technologische ontwikkelingen, zoals automatische leugendetecie en real-time analyse, en niet-technische ontwikkelingen, zoals het verhogen van de cognitieve belasting en het strategisch inzetten van bewijs. De wetenschappelijke ontwikkelingen lijken echter de praktijk niet altijd te bereiken. Omdat er weinig kennis over toepassing van leugendetecie, of het gebrek daaraan, in Nederland beschikbaar is, richt deze paragraaf zich voornamelijk op voorbeelden uit de Amerikaanse praktijk. Bijvoorbeeld in de meest recente versie van het invloedrijke Amerikaanse *Reid method* verhoorhandboek komen de verhoormethoden gebaseerd op het verhogen van de cognitieve belasting geheel niet aan bod (Inbau, Reid, Buckley, & Jayne, 2011; Vrij & Granhag, 2012). Vice versa worden er in de praktijk methoden toegepast waarvoor geen wetenschappelijk bewijs gevonden is, zoals het op micro-expressies gebaseerde airport security programma SPOT (Kassin, 2012). Op het gebied van leugendetecie is bekend dat de polygraaf met de CQT regelmatig door de Amerikaanse overheid gebruikt wordt, onder andere voor het screenen van eigen personeel (e.g., CIA en NSA personeel) en het is toelaatbaar als bewijs in de Amerikaanse rechtszaal; Meijer & Merckelbach, 2008). De zojuist genoemde voorbeelden komen echter allemaal uit de Amerikaanse praktijk.

Dat de Amerikaanse praktijksituatie en de Nederlandse niet één-op-één vergelijkbaar zijn blijkt onder andere uit de afschaffing van de *Zaanse verhoortechniek*³ in Nederland; een vroeger in Nederland populaire verhoormethode gebaseerd op de Amerikaanse Reid methode⁴. Onder andere na kritiek van wetenschappers zoals Aldert Vrij (Volkskrant, 16 augustus 1996) is deze omstreden verhoortechniek in 1996 in Nederland afgeschaft, terwijl in Amerika de Reid methode nog steeds veelvuldig gebruikt wordt.

Ook met betrekking tot leugendetectie zijn er verschillen tussen Nederland en Amerika. Zo heeft het Nederlandse Hooggerechtshof in 1998 het gebruik van de polygraaf (traditioneel de meest bekende leugendetectiemethode) in rechtszaken opgegeven. Ook in Europese rechtbanken wordt de polygraaf als onbetrouwbaar beschouwd. Binnen Europa kan leugendetectie alleen in enkele landen gebruikt worden als ondersteuning van een argument en niet als op zichzelf staand bewijs. In Amerika wordt leugendetectie bewijs wel regelmatig ingezet aan zowel door de aanklager als aan de kant van de verdediging. Ook zonder te fungeren als bewijsmateriaal in een rechtszaal zou leugendetectie echter een bijdrage kunnen leveren aan een veilige maatschappij.

Om te identificeren in hoeverre de Nederlandse praktijk hier behoefte aan heeft en of recente ontwikkelingen reeds worden toegepast, is een serie interviews afgenomen. De interviews worden in het volgende hoofdstuk besproken.

³ De Zaanse verhoormethode is een interviewtechniek die zich kenmerkt door het laten herbeleven van de misdaadsituatie. Dit kan echter tot valse bekentenissen leiden en is mede daarom in 1996 in Nederland afgeschaft. Voor meer informatie, zie https://nl.wikipedia.org/wiki/Zaanse_verhoormethode

⁴ De Reid techniek is een vergelijkbare Amerikaanse verhoormethode gericht op het laten herbeleven van de misdaadsituatie en bestaat uit een initieel interview gevolgd door een verhoor in het geval van verdenking. Tijdens het verhoor doorloopt de verhoorder 9 stappen om de aan te moedigen een bekentenis af te leggen. Deze methode wordt in Amerika nog veelvuldig gebruikt. Voor meer informatie, zie https://en.wikipedia.org/wiki/Reid_technique

3 Interviews: Methode

Om te bepalen hoe in Nederland gedacht wordt over de recente ontwikkelingen op het gebied van leugendetectie en om te achterhalen in hoeverre leugendetectie momenteel in de Nederlandse praktijk wordt ingezet, zijn interviews gehouden met verschillende relevante publieke en private partijen uit de Nederlandse praktijk. Het doel hiervan is te identificeren in hoeverre leugendetectie ontwikkelingen uit de wetenschappelijke wereld doordringen tot de Nederlandse praktijk, en in welke mate er een behoefte bestaat om deze ontwikkelingen in de praktijk toe te passen.

In totaal zijn er 15 interviewverzoeken uitgestuurd gebaseerd naar organisaties die relevant zijn voor deze vraagstelling. Hieruit zijn 13 interviews voortgekomen met medewerkers van verschillende afdelingen van de Nationale Politie, de Koninklijke Marechaussee, verschillende ministeries, justitiële partijen, veiligheidsorganisaties en verzekeringsmaatschappijen. Deze sampling strategie heeft een divers en representatief beeld van de Nederlandse praktijk opgeleverd.

De 13 interviews zijn gehouden tussen februari en juni 2016. Voor aanvang van deze interviews is er een interview protocol opgesteld (zie Appendix A) en dit protocol is gebruikt als leidraad voor ieder gesprek. Daarnaast was er de mogelijkheid om dieper in te gaan op een aspect als de interviewer of geïnterviewde daar behoefte aan had. Het gehele interview protocol is niet bij elk gesprek doorlopen, ofwel door gebrek aan relevantie van bepaalde vragen, ofwel door tijdgebrek. Interviews duurden tussen de 1.5 en 3 uur per stuk.

Het interviewpanel bestond uit één of twee onderzoekers met een achtergrond in leugendetectie of het identificeren van afwijkend gedrag. De hoofdauteur van dit rapport heeft alle interviews bijgewoond en in 12 van de 13 interviews werd zij vergezeld door een collega. Alle geïnterviewden hadden op het moment van interviewen een relevante functie op het gebied van security en technologie, zoals innovatiemanager of *security officer*. Per interview zijn één, twee of drie mensen geïnterviewd van dezelfde organisatie. In één geval waren de geïnterviewden ook werkzaam bij verschillende organisaties. In dat geval hebben we bij de rapportage van het interview duidelijk onderscheid gemaakt tussen de uitspraken van verschillende geïnterviewden.

Naast de introductie en afsluiting van het gesprek, bestond ieder interview uit vier verschillende fases. Voorafgaand introduceerden alle gespreksdeelnemers zichzelf en de organisatie die zij representeerden. De eerste fase ging over de *huidige situatie*. Tijdens deze fase werden er verschillende vragen gesteld om de huidige situatie bij de betreffende organisatie op het gebied van waarheidsvinding en specifiek leugendetectie vast te stellen. Bijvoorbeeld, 'Waar haalt u uw kennis over leugendetectie vandaan?' en 'Maakt uw organisatie momenteel gebruik van waarheidsvinding of leugendetectie en zo ja, hoe?'. Tijdens deze fase is er ook aandacht besteed aan eventuele obstakels die verhinderen dat leugendetectie gebruikt wordt in de praktijk, waaronder relevante beleidskaders en wetten.

De tweede fase ging over de *behoeftebepaling en toekomstige activiteiten*.

Tijdens deze fase werden behoeftes en wensen op het gebied van leugendetectie bevraagd. Bijvoorbeeld 'In een ideale situatie, hoe zou uw organisatie gebruik maken van leugendetectie?'. Tijdens deze behoeftebepaling is er ook aandacht besteed aan eventuele obstakels, zoals nadelen en situaties waarin leugendetectie niet bruikbaar is. Aan de hand van deze vragen kan vastgesteld worden wanneer leugendetectie juist wel, en wanneer niet nuttig zou kunnen zijn. Vervolgens werd gevraagd hoe deze ideale situatie bereikt zou kunnen worden.

Na het bepalen van de huidige en gewenste situatie heeft de interviewer recente ontwikkelingen op het gebied van leugendetectie met de geïnterviewden doorgenomen om aan te geven welke mogelijkheden er tegenwoordig zijn. De derde fase betrof de *response op huidige ontwikkelingen*. Tijdens deze fase hebben de interviewers gevraagd in hoeverre zij van deze ontwikkelingen op de hoogte waren, en of deze ontwikkelingen interessant zouden kunnen zijn voor hun organisatie.

De vierde fase ging over de *respons op het voorkomen van oneerlijk gedrag*.

Deze fase waarin een nieuwe tak binnen deceptie onderzoek werd besproken is in verband met tijdgebrek slechts tijdens 9 van de 13 interviews aan bod gekomen. In deze 9 interviews bespraken we het voorkomen van leugenachtig en oneerlijk gedrag door subtiele manipulaties van bijvoorbeeld morele waarden of cognitieve belasting. Eerst vertelde de interviewer wat over het vakgebied en onderzoeksresultaten, waarna er gevraagd werd in hoeverre zij van deze ontwikkelingen op de hoogte waren, en of ze eventueel relevant zijn voor hun organisatie. Aan het eind van het interview vond de afsluiting plaats waarin aanvullende opmerkingen gemaakt konden worden en er besproken werd wat er met de interviewuitkomsten zou gebeuren.

Aangezien de meerderheid (i.e., 12 van de 13 interviews) heeft plaatsgevonden met twee interviewers, kon één van de twee interviewers meeschrijven terwijl de ander het gesprek voerde. Op basis van deze aantekeningen is ieder interview uitgewerkt en vervolgens naar de relevante geïnterviewde(n) opgestuurd voor feedback. De interviews zijn niet opgenomen. Voor dit rapport zijn de antwoorden van de verschillende geïnterviewde partijen onder elkaar gezet, gegroepeerd en met elkaar vergeleken. Uit deze vergelijking zijn overeenkomsten en verschillen geïdentificeerd en beschreven. Op deze manier is alle input uit de interviews in dit rapport aan bod gekomen. Waar relevant zijn daarnaast ook quotes toegevoegd.

4 Interviews: Resultaten

Het resultatenhoofdstuk is onderverdeeld in de vier fases van het interview. De resultaten bespreken we hieronder in chronologische volgorde. De input uit alle 13 interviews komt hierin aan bod, zowel generiek, door antwoorden met elkaar te vergelijken, als op interview niveau, door het geven van voorbeelden en quotes, overigens zonder dat deze herleidbaar zijn tot de partijen die door ons zijn geïnterviewd.

4.1 Fase 1: Huidige situatie

De vragen tijdens deze fase zijn erop gericht om een beeld te krijgen van de huidige situatie omtrent waarheidsvinding en leugendetectie binnen de geïnterviewde organisaties.

4.1.1 *Leugendetectie beeld*

Allereerst is er gevraagd naar het huidige beeld dat de geïnterviewden hebben van leugendetectie, en welke aspecten voor hun organisatie van belang zijn. Het type leugendetectie dat het vaakst werd genoemd was de op stress-gebaseerde polygraaf. Zo gaf één van de geïnterviewden aan: *“Ik zie het vooral als dat apparaat uit de film, eentje met draden en een monitor die bijvoorbeeld de hartslag meten.”* De alternatieve toepassing van de polygraaf, de *Concealed Information Test (CIT)* werd ook genoemd. Stress en de fysieke gevolgen daarvan werden ook los genoemd. Eén van de geïnterviewden noemde expliciet *“de geur van transpiratie”*. Een andere technologie die meerdere malen werd genoemd is de *voice stress analysis* waarbij leugens worden geïdentificeerd op basis van verschillen in toonhoogte. Er werd ook onderscheid gemaakt tussen het detecteren van leugens op basis van verbaal en non-verbaal gedrag, en dan vooral gebaseerd op afwijkingen in dit gedrag. Vanuit verschillende publieke en private organisaties is de nadruk gelegd op het belang van verbale leugendetectie dankzij informatie-vergarende verhoortechnieken en het strategisch gebruik maken van bewijs (zoals SUE, het Cognitieve Interview⁵ en de Standaard Verhoorstrategie⁶).

De context waarin leugendetectie wel en niet zou moeten worden toegepast werd ook genoemd. De meesten dachten bij leugendetectie automatisch (1) dat het wordt gebruikt als aanvullend bewijs en (2) dat het in de rechtszaal geen stand houdt. *“Leugendetectie heeft in Nederland momenteel niet echt een plek, dat vind ik zelf ook wel terecht.”* Vanuit de juridische hoek werd ook aangegeven dat leugendetectie onder bewijsmiddelen zou vallen en dat de politie gaat over het verzamelen van het bewijs. In eerste instantie werd niet gedacht aan andere manieren van inzetten dan als bewijs (bijvoorbeeld als stuurinformatie), en er werd ook geen

⁵ Het Cognitieve Interview is een informatie vergarende verhoormethode gebaseerd op geheugenonderzoek om zoveel mogelijk details te verkrijgen zonder de kans op onjuiste herinneringen te vergroten. Oorspronkelijk is deze methode ontworpen voor het verhoren van getuigen en slachtoffers, maar het tegenwoordig wordt het ook soms ingezet voor het verhoren van verdachten. Voor meer informatie, zie https://en.wikipedia.org/wiki/Cognitive_interview

⁶ Deze verhoorstrategie richt zich op het confronteren en omsingelen van mogelijke uitvluchten van de verdachte op basis van inconsistenties tussen de verklaring en eerdere verklaringen en technische bewijsmiddelen. Deze methode wordt onderwezen op de Nederlandse Politieacademie (van Amelsvoort, Rispens, & Grolman, 2015).

rekening gehouden met toekomstige wijzigingen (waardoor het bijvoorbeeld wel zou kunnen standhouden als bewijs). Dit beeld veranderde tijdens het interview. Eén geïnterviewde zei hierover: *“Gebruik het vooral als selectiemiddel, maar als het ook ingezet kan worden als bewijsmiddel is het helemaal mooi. Ik zeg niet dat de menselijke factor er helemaal uit moet, maar de mens speelt vooral een rol in de besluitvorming.”*

Als laatste werden ook de issues omtrent leugendetectie genoemd tijdens het beschrijven van het beeld wat men van leugendetectie heeft. Verschillende issues zijn genoemd, waaronder een lage accuraatheid en problemen met het toepassen van statistieken als het over één individu gaat. Als een leugendetectiemethode bijvoorbeeld een accuraatheid heeft van 75% betekent het dat je het gemiddeld in één van de vier gevallen fout hebt. Maar wanneer dat het geval is blijft onbekend, wat het lastig kan maken om concrete uitspraken te doen over de betrouwbaarheid van de persoon voor je. Dit kan moeilijkheden veroorzaken bij het interpreteren van leugendetectie uitkomsten door de mensen die ermee moeten werken. Ook de invloed van iemands referentiekader genoemd. Daarover werd gezegd: *“Volgens mij moet je een onderscheid maken tussen de mens (de bron), en het verhaal dat wordt verteld (de informatie). Maar ook “als ik dan kijk naar dit soort zaken, dan hebben we minder vaak iemand die in het moment iets deed, we hebben vaker iemand die zelf vindt dat hij normaal bezig is en niks fout heeft gedaan.”* Als iemand niet het gevoel heeft dat hij fout zit of aan het liegen is, is het misschien moeilijker te detecteren.”

4.1.2 Kennisbron

Ten tweede is er gevraagd naar de bron van hun kennis op het gebied van waarheidsvinding en leugendetectie. Grofweg werden er zes soorten informatiebronnen genoemd: film en tv, populair wetenschappelijke artikelen en opiniestukken, contact en samenwerking met wetenschappers en het bedrijfsleven, het lezen van wetenschappelijke artikelen en jurisprudentie, het bezoeken van congressen, workshops en cursussen en als laatste het vergelijken (benchmarking) met andere organisaties of afdelingen.

De meest voorkomende informatiebron zijn tv-series en films. Zowel meer documentaire achtige programma's op Discovery Channel en van de publieke omroep als de populaire tv-series als *Lie to me* en *The mentalist*. Hierbij werd wel regelmatig opgemerkt dat de betrouwbaarheid van deze informatie met een korrel zout werd genomen.

Daarnaast worden opiniestukken en populair wetenschappelijke stukken in de krant en op het internet regelmatig gelezen, van Nederlandse onderzoekers zoals Peter van Koppen, Harald Merckelbach, Aldert Vrij, Ewout Meijer, Bruno Verschuere, Henri Otgaar en Hans Crombach.

Sommigen van de geïnterviewden hebben ook persoonlijk contact met de voorgenoemde onderzoekers. Soms leidt dit contact tot het opzetten van experimenteel onderzoek, of het beproeven van een bepaalde techniek of methode. Een aantal geïnterviewden gaf ook aan in contact te zijn met het bedrijfsleven, bijvoorbeeld met bedrijven die gespecialiseerd zijn in het maken van software, bijvoorbeeld op het gebied van spraak(structuur)analyse.

Verscheidene geïnterviewden gaven aan door middel van wetenschappelijke artikelen op de hoogte te blijven, vooral als deze open-access worden gepubliceerd. Uit de interviews bleek dat de meeste geïnterviewden echter geen of weinig toegang hebben tot afgeschermd tijdschriften waar de meerderheid van de wetenschappelijke artikelen wordt gepubliceerd, waardoor het lastig kan zijn om toegang te krijgen tot deze informatie. Sommigen gaven ook aan deze informatie lastig leesbaar te vinden. Eén geïnterviewde zei hierover: *“Ik lees ook wetenschappelijke publicaties, zeker als deze openlijk toegankelijk zijn. Dan kijk ik na of het (redactie: onderzochte) van deze tijd is.”* Ook het volgen van de jurisprudentie en gerechtelijke uitspraken werd genoemd als informatiebron.

Ongeveer een kwart van de geïnterviewden gaf aan regelmatig wetenschappelijke conferenties te bezoeken waar leugendetectie besproken wordt, zoals SARMAC, EAPL, APLS en IIRG. Naast het op de hoogte blijven van recente ontwikkelingen wordt hier onder andere ook contact gelegd met relevante onderzoekers. Sommige organisaties organiseren ook workshops en cursussen op het gebied van leugendetectie en gedragsherkenning, of stimuleren medewerkers om extern hier een cursus over te volgen. Over de kwaliteit van deze cursussen wordt wel gediscussieerd. Eén geïnterviewde noemde ook dat leugendetectie informeel wordt besproken op de politieacademie en rechercheopleiding. Er worden momenteel echter geen formele cursussen op het gebied van leugendetectie gegeven op de politieacademie.

Als laatste gaven geïnterviewden van zowel publieke als private organisaties aan dat het vergelijken met andere relevante organisaties zowel nationaal als internationaal, of met andere afdelingen binnen de eigen organisatie, een rol speelt in de kennisneming van leugendetectie.

4.1.3 *Huidig gebruik*

Ten derde is er gevraagd naar het huidige gebruik van leugendetectie en waarheidsvinding binnen de eigen organisatie. Bij verzekeringsmaatschappijen wordt gebruik gemaakt van waarheidsvinding. Wat in de gesprekken met andere organisaties opviel, is dat, hoewel medewerkers van de meerderheid van de organisaties aangaven niet officieel of expliciet aan leugendetectie doen, er informeel en impliciet wel het één en ander gebeurt. Zo worden er verhoormethodes ingezet, zoals de Strategic Use of Evidence (SUE) en tactisch gebruik van bewijsmiddelen via de Standaard Verhoorstrategie, om de waarheid tijdens interviews te achterhalen, maar dit wordt niet geïnterpreteerd als het inzetten van leugendetectie. Echter, deze technieken zijn onder andere ontworpen om de kans dat een leugenaar wordt ontmaskerd te vergroten en worden in de leugendetectie literatuur uitgebreid beschreven en getest. Hierover zei een geïnterviewde: *“Van te voren stond ik niet echt stil dat een verhoorder ook onbewust aan leugendetectie doet, maar het dan falsificeren noemt.”* In de rechtszaal worden verklaringen ook vergeleken met het bewijsmateriaal, context en eerdere ervaringen en kan op basis van inconsistenties aan de betrouwbaarheid van een verklaring getwijfeld worden. Daarnaast worden er ook pilots gedraaid om nieuwe leugendetectiemethoden te testen in de praktijk, maar met gemixte of tegenvallende resultaten. Tijdens de interviews kwam ook naar boven dat er vanuit de organisaties zelf regelmatig wordt aangegeven dat er wel behoefte en interesse is in leugendetectie, maar dat het officieel geen onderdeel uitmaakt van training of opleiding.

Voor het gedetailleerder beantwoorden van de vraag in hoeverre Nederlandse praktijkorganisaties gebruik maken van leugendetectie hebben wij de antwoorden gesplitst naar de specifieke context, zoals een verhoorsituatie, het beveiligen van een openbare of semiopenbare ruimte, heimelijk interviewen, een juridische context en een verzekeringscontext. In iedere categorie zijn medewerkers van meerdere organisaties geïnterviewd.

Wij hebben gesproken met specialisten over getuigen- en verdachtenverhoren. Enkele waren verantwoordelijk voor techniek en innovaties en anderen voor opleiding en training. Een rode draad tijdens deze gesprekken was het belang van waarheidsvinding en het kunnen identificeren van onschuldige mensen, net zo veel als het identificeren van schuldige mensen. *“Ik heb liever 1000 boeven onterecht op straat dan één onterecht vast”*. In Nederland wordt buiten universiteiten niet officieel les gegeven op het gebied van leugendetectie, maar wordt het onderwerp soms wel besproken. *“Het zit niet in de opleiding en het wordt dus niet op structurele basis gedaan, maar mogelijk wel bij individuen. Of dat effectief is, is niet bekend. Sommigen zijn er wel van overtuigd dat ze in staat zijn om leugenaars te ontmaskeren, dat is een gevaar. Daarom hebben we meer zicht nodig op ontwikkelingen en wat er wel en niet werkt”*. Vanuit de verschillende onderdelen van de betreffende organisatie kwamen ook andere meningen en ervaringen op het gebied van leugendetectie naar voren. Er wordt bijvoorbeeld verschillend gedacht over in welke scenario's leugendetectie wel en niet ingezet zou kunnen worden. Zo gaf één geïnterviewde aan dat *“leugendetectie alleen relevant is voor getuigen, want verdachten mogen liegen en zich op het zwijgrecht beroepen”*. Dat houdt in dat een verdachte in zijn recht staat als hij niet wil praten en dus ook het recht heeft om te liegen tijdens zitting. Dan wordt leugendetectie meteen een ethisch vraagstuk, mag je technieken toepassen om te bepalen of iemand liegt als deze persoon het recht heeft om te liegen, of ontnem je hem daarmee zijn rechten? Het kan echter ook lastig zijn om leugendetectie toe te passen bij de getuigen, omdat *“bij getuigen het verschil tussen een onwaarheid en een (opzettelijke) leugen moeilijk vast te stellen is. Getuigenverklaringen zijn vaak van slechte kwaliteit en kunnen zo een rol spelen bij gerechtelijke dwalingen.”* Er zijn verschillende proeven gedaan waarin de inzetbaarheid van leugendetectie en betrouwbaarheidsbepaling zijn getest in de praktijk. Zo bleek de CIT moeilijk toepasbaar in de praktijk omdat er ofwel geen geschikte zaken konden worden gevonden, ofwel de verdachte niet wilde meewerken. Ook is de pilot met real-time interview feedback vroegtijdig afgebroken: *“we hebben ook wel eens een test gedraaid met een oortje waarbij je feedback kreeg tijdens het verhoor van een psycholoog die meekijkt (i.e., in real-time).”* Deze test is echter afgebroken omdat *“de flow van het gesprek werd verstoord doordat het oortje afleidde van het verhoor.”* Een ander type feedback, bijvoorbeeld door middel van *“een chatvenster op een tablet, of tactiele feedback”* zou misschien wel kunnen werken. Meer formele leugendetectiemethoden zoals de polygraaf en voice stress analyse worden niet gebruikt in een verhoorcontext vanwege een te lage accuraatheid, een te hoge hoeveelheid loos alarmen en omdat het niet toelaatbaar is als bewijs in de rechtszaal. Eén geïnterviewde noemde dat *“leugendetectie volgens mij onder de onorthodoxe methodes die niet zijn toegestaan in de rechtszaal valt”*, en een ander gaf aan dat *“leugendetectie zwak is voor bewijsvoering, maar zou wel kunnen worden gebruikt als tactische- of stuurinformatie, maar we hebben die technieken ook niet”*.

Voor de veiligheid op een luchthaven is leugendetectie wel relevant, maar niet voor iedere partij die een rol speelt in het proces. *“Nu is er op de luchthaven ook niet de behoefte. Alle passagiers worden toch gescand, dus waarom extra leugendetectie?”*. Op een luchthaven met meerdere veiligheidspartners die verschillende en soms zelfs tegengestelde belangen hebben is het naast het waarborgen van veiligheid ook belangrijk om een continue doorstroom van passagiers door het vliegveld te kunnen leiden, en dan het liefst door zo weinig mogelijk fysieke ruimte in te nemen. Dat betekent dat het misschien wel interessanter is om niet leugens of mensen met kwade intenties te detecteren, maar je juist te richten op het identificeren van waarheden of mensen zonder kwade intenties en voor hen een soort *fast lane* te maken (Van Rest, et al., 2015). Oftewel, een onderverdeling maken tussen *low en high security*. Hierover werd gezegd *“Let op de 99% die wel OK zijn en probeer die te identificeren in plaats van je te richten op diegenen die niet OK zijn. Aanvullende maatregelen bij verhoogde dreiging geldt dan alleen voor die overige 1%”*. Uit de interviews bleek dat men vindt dat leugendetectie nog niet volwassen genoeg is omdat er niet één duidelijke, betrouwbare en goed werkende techniek is.

In het kader van heimelijk interviewen wordt er wel aan waarheidsvinding gedaan, maar niet per se aan leugendetectie zelf. Of in ieder geval, dat wordt niet expliciet zo benoemd. *“We doen zeker aan waarheidsvinding; en leugendetectie, we doen het wel, maar noemen het niet leugendetectie.”* Er is wel interesse in, bijvoorbeeld bij het inwinnen van informatie. Impliciet wordt leugendetectie ook nu al gebruikt in deze situaties. *“Dan beoordeel je impliciet het gedrag van de ander; is hij gehaast? Gestrest?”*. Soms kunnen dit type interviews face-to-face worden gedaan, maar soms bevinden de geïnterviewden zich ook in een ander land en moeten interviews telefonisch gedaan worden, of moet je een beeld krijgen op basis van een geschreven rapport.

Vanuit de justitiële hoek wordt terughoudend gereageerd op het gebruik van leugendetectie, zeker in de context van het gebruik als bewijsmiddel in de rechtszaal. Bijvoorbeeld omdat *“leugendetectie moeilijk is als instrument. Als je slechte vragen stelt, of je pakt het verkeerd in, is het meteen kwetsbaar. Bewijsmiddelen moeten van goede kwaliteit zijn”*. Als obstakel wordt de *onzekerheidsmarge* genoemd, veroorzaakt door de lage accuraatheid en betrouwbaarheid van huidige technieken en methoden. *“Het gaat om een zaak met deze ene persoon, niet om de statistiek. De marge is nu nog aanzienlijk, dat maakt het kwetsbaar”*. Deze terughoudende visie wordt ondersteund door een invloedrijk maar deels verouderd rapport van de British Research Council op het gebruik van de polygraaf in de rechtszaal (Bull e.a., 2004). In Amerika wordt er wel gebruik gemaakt van de polygraaf, *“maar dat is meer iets voor de Amerikanen. Het past beter in hun cultuur en bij hun imago dan bij de Nederlandse.”* De beschuldigende verhoormethoden die in de VS worden gebruikt zijn bijvoorbeeld meer gericht op het verkrijgen van een bekentenis dan de methoden gericht op waarheidsvinding zoals in gebruik in Nederland. Impliciet wordt er in de rechtszaal wel gebruik gemaakt van leugendetectie, bijvoorbeeld door een verklaring te vergelijken met context, ervaring en bewijsmiddelen. Over het inzetten van geurervaring werd het volgende gezegd: *“Bepaalde soorten drugs hebben zo’n sterke en herkenbare geur, dat merk je wel. Als iemand dus aangeeft niks raars geroken te hebben, is dit ontkennen waarschijnlijk een teken van liegen”*.

Ook vanuit een praktisch oogpunt kan het lastig zijn om leugendetectie in te gaan voeren in de rechtszaal omdat een verdachte niet mee hoeft te werken aan zijn eigen veroordeling. Hij hoeft ter zitting bijvoorbeeld niet de waarheid te spreken. Daarnaast kan het ook remmend werken, *“geef je nog verklaring af als je aan een leugendetector zit? Je wilt juist dat iemand gaat praten; hij kan [immers] zichzelf tegenspreken of het onderzoek sturen.”*

In een verzekeringscontext wordt leugendetectie bewuster ingezet dan bij de meeste organisaties die wij tijdens dit onderzoek hebben gesproken. Er wordt bijvoorbeeld nagedacht over het inrichten van het proces en de verschillende onderzoeksfases. *“Hoe kun je een proces zo inrichten dat mensen de waarheid vertellen? Het is gefragmenteerd en niet zo georganiseerd, maar we zijn er wel mee bezig. Maar, het is nu nog teveel op basis van onderbuikgevoelens, het moet meer vanuit de wetenschap.”* Het beoordelingsproces van verzekeringsclaims bestaat uit een initiële screening fase waar op basis van kenmerken van de claim en het claim verleden van de klant claims gefilterd worden. Het overgrote merendeel wordt dan gekenmerkt als “eerlijk” en de claim wordt uitgekeerd. Een klein gedeelte van de claims wordt gekenmerkt als verdacht, en deze claims worden in meer detail bestudeerd in de onderzoeksfase. Tijdens de onderzoeksfase wordt leugendetectie ingezet *“om te bepalen of een claim frauduleus is en verder onderzocht moet worden.”* Tijdens deze fase kan het cognitieve interview⁷ telefonisch afgenomen door een groep getrainde interviewers om te bepalen of een claim frauduleus is. Tijdens deze fase is er in het verleden ook geëxperimenteerd met de voice stress analyse waarbij leugens worden gedetecteerd op basis van veranderingen in toonhoogte, maar die bleek niet genoeg toegevoegde waarde te hebben. De voice stress analyse zou eventueel meer op kunnen leveren als deze in de initiële screening fase zou worden ingezet, maar dat mag niet zonder medeweten van de klant. Omdat alle claims in deze initiële fase gescreend worden en niet alleen verdachte claims behandeld worden moet hier rekening gehouden worden met imagoschade, want leugendetectie toepassen op iedere claim kan spanning opleveren met gezien worden als een betrouwbare verzekeraar. *“We hebben de voice stress analyse niet geprobeerd in te zetten tijdens de initiële screening fase omdat dat spanning op zou leveren met het doel om een betrouwbare dienstverlener te zijn. Hoewel klantpanels hebben laten zien dat zij het niet erg zouden vinden als dit gebruikt zou worden. Om leugendetectie te laten werken moet je óf de business case hard maken, óf het moet passend zijn bij de organisatiedoelstellingen. Je kunt eventueel experimenteel onderzoek doen om dit aan te tonen.”*

4.1.4 Relevante beleidskaders

“Tussen droom en daad staan wetten in de weg en praktische bezwaren (citaat uit Willem Elsschot, het huwelijk).”

⁷ Het Cognitieve Interview is een informatie vergarende verhoormethode gebaseerd op geheugenonderzoek om zoveel mogelijk details te verkrijgen zonder de kans op onjuiste herinneringen te vergroten. Oorspronkelijk is deze methode ontworpen voor het verhoren van getuigen en slachtoffers, maar het tegenwoordig wordt het ook soms ingezet voor het verhoren van verdachten. Voor meer informatie, zie https://en.wikipedia.org/wiki/Cognitive_interview

Het meest genoemde beleidskader komt uit het wetboek voor strafvordering die bepaalt dat een verdachte niet mee hoeft te werken aan zijn eigen veroordeling, dat een verklaring in vrijheid afgelegd moet worden (i.e., artikel 29 strafvordering) en dat hij/zij zich eventueel mag beroepen op het zwijgrecht. Daardoor werd het nut van het gebruik van leugendetectie in verhoren met verdachten door verschillende geïnterviewden in twijfel getrokken. Een enkeling ging hierbij nog een stap verder door de eventuele negatieve gevolgen van het gebruik van leugendetectie in verhoren met verdachten uiteen te zetten. Per 1 maart 2016 mag een advocaat namelijk bij alle verhoren aanwezig zijn en als leugendetectiemethoden zoals de CIT (i.e., geheugendetectie) *“vooral goed [zijn] in het aanwijzen van onschuldigen. Dus als je als advocaat je onschuldige cliënt wel mee laat werken, dan lijkt een cliënt die je niet mee laat werken, meteen schuldig. Daarom zal een advocaat eigenlijk nooit adviseren om mee te werken.”* Daarnaast werd ook artikel 27 Strafvordering genoemd, wat betekent dat *“we zonder verdenking niet van alles mogen doen. Leugendetectie resultaten gelden ook niet als bewijs in de Nederlandse rechtszaal.”* Verscheidene geïnterviewden noemden de assumptie dat leugendetectie niet zal standhouden als bewijs in een rechtszaal ook als belemmering voor het gebruik van leugendetectie in de praktijk. In plaats daarvan zou leugendetectie misschien beter aan de voorkant ingezet kunnen worden, als sturende of tactische informatie in plaats van als bewijsmateriaal. Een enkeling dacht hier echter anders over en gaf aan dat leugendetectie, mits goed gedocumenteerd en getest in de praktijk, best onderdeel zou kunnen gaan uitmaken van de forensische toolkit. *“Andere forensische bewijsmiddelen hebben ook een onzekerheidsmarge (i.e., zijn ook niet 100% betrouwbaar), en die gebruiken we ook. Dus waarom zou leugendetectie niet kunnen?”*

Hoewel wet- en regelgeving aan de ene kant een belemmering zou kunnen worden voor het gebruik van leugendetectie in de praktijk, gaven verscheidene geïnterviewden aan dat juist het gebrek aan wet- en regelgeving op het gebied van leugendetectie ook juist een belemmering kan vormen van voor het gebruik ervan in de praktijk. *“Omdat leugendetectie niet verplicht is, is er weinig incentive om het te gebruiken..”* En omdat *“de polygraaf in Nederland niet als bewijs wordt gebruikt, en dan vraag ik me af, wat is de toegevoegde waarde?”* Een ander gaf aan dat leugendetectie waarschijnlijk pas op grote schaal ingezet zal worden in de praktijk als het *“goedgekeurd selectiemiddel”* is met *“duidelijke protocollen en procedures, een beetje zoals DNA onderzoek”*.

Naast wet en regelgeving erkenden alle geïnterviewden ook de ethische bezwaren die mogelijk kleven aan het gebruik van leugendetectie in de praktijk. Vooral bij heimelijke leugendetectie, of ongecontroleerde leugendetectie in de openbare ruimte kan er privacy schending optreden. *“Het gaat namelijk wel om persoonsgegevens en gevoelige data, dus de wet bescherming persoonsgegevens is hier van belang.”* Zoals vaker in security betreft het hier een *“belangenafweging van privacy - en een inbreuk daarop - en security.”* Private partijen zoals verzekeringsmaatschappijen hebben -naast wet en regelgeving- ook te maken met de Gedragscodes vanuit het Verbond van Verzekeraars. *“Wat mag wel en niet op privacy gebied? Vertel klanten wat er waarom gebeurt met hun persoonsgegevens.”* Vanuit dit perspectief hebben verscheidene geïnterviewden geadviseerd om niet zozeer te focussen op het detecteren van leugens, maar juist op het identificeren van die mensen die niets te verbergen hebben.

Door goed gedrag te kunnen identificeren kan men wellicht bijvoorbeeld sneller door airport security, het *fast lane* concept. Door hetzelfde principe, namelijk het kunnen onderscheiden van goed en kwaad, op een andere manier naar buiten te brengen, is de kans op maatschappelijke weerstand kleiner, en dus de kans dat leugendetectie gebruikt mag worden in de praktijk groter. Voorgaand onderzoek naar het introduceren van een fast lane concept heeft echter uitgewezen dat dit concept onder de huidige voorwaarden nog niet kan worden toegepast bij burgerluchtvaart in Nederland en er meer onderzoek op dit onderwerp nodig is om te identificeren welke mogelijkheden er wel zijn (Van Rest, e.a, 2015).

4.2 Fase 2: Behoeftebepaling en toekomstige ontwikkelingen

De vragen tijdens deze fase waren er op gericht om een beeld te krijgen van de behoeftes die de organisaties van de geïnterviewden hebben op het gebied van waarheidsvinding en leugendetectie. Allereerst zijn geïnterviewden expliciet gevraagd naar hun behoeftes en mogelijke toepassingen van leugendetectie in de Nederlandse praktijk. Deze toepassingen zijn uitgesplitst naar context. Vervolgens is gevraagd welke van deze toepassingen prioriteit hebben en wordt besproken welke leugendetectiemethoden bruikbaar zijn in de genoemde contexten. Daarna is gevraagd in welke contexten leugendetectie niet ingezet zou moeten worden en welke nadelen er aan leugendetectie kleven. Als laatste is gevraagd of de betrokken organisaties al de benodigde kennis in huis hebben om leugendetectie in de genoemde contexten in te zetten.

4.2.1 *Behoeftes aan betrouwbaarheidsbepaling*

De geïnterviewden werden gevraagd welke mogelijkheden zij voor leugendetectie zagen onder ideale omstandigheden. Hoewel een enkeling ook aangaf dat *“in een ideale situatie leugendetectie niet nodig zou zijn omdat iedereen dan eerlijk is”*, noemde iedere geïnterviewde meerdere scenario's waarin leugendetectie behulpzaam en een aanvulling op bestaande procedures zou kunnen zijn. We hebben de verschillende behoeftes gegroepeerd per context en hieronder samengevat. De genoemde contexten zijn politieonderzoek, in- en uitreizen, screening, claims, als training- en testmiddel en het identificeren van afwijkend gedrag. Voor de hieronder genoemde voorbeelden en contexten is een valide en betrouwbare leugendetectiemethode waarbij de procedures en de interpretatie van de resultaten geheel duidelijk zijn bij de afnemers van de leugendetectietesten wel een voorwaarde.

4.2.1.1 *Betrouwbaarheidsbepaling in een politieonderzoekcontext*

Het inzetten van leugendetectie om de betrouwbaarheid van een persoon of verklaring te bepalen kan in verschillende contexten relevant zijn, zoals in de *bewaken & beveiligen* context. Specifieker, een betrouwbaarheidsbepaling kan op verschillende momenten tijdens het onderzoeksproces ingezet worden, en zowel bij getuigen als verdachten. Hierover waren de meningen van de geïnterviewden wel verdeeld. Sommige vonden leugendetectie toepasbaar bij zowel getuigen als verdachten, terwijl anderen een sterke voor- of afkeur voor één van de twee had. De geïnterviewden waren het er wel over eens dat onder de huidige omstandigheden, met accuraatheden van 70-75%, de grootste meerwaarde van leugendetectie aan de voorkant van het onderzoeksproces is en niet in bewijsvoering.

Een betrouwbaarheidsindicatie kan dan ingezet worden als tactische- of stuurinformatie om te bepalen welke zaken verder onderzocht worden, bij wie je dan moet zijn voor informatie en wat bepaalt of iemand een verdachte is. Of als er meerdere verdachten zijn op wie je de beperkte onderzoekscapaciteit zou moeten richten.

Tijdens de interviews zijn er verschillende toepassingen genoemd waarin leugendetectie van pas kan komen, voornamelijk aan de voorkant van het onderzoeksproces. De resultaten van de interviews zijn hier samengevat. De toegevoegde waarde van leugendetectie aan de voorkant van het proces begint al bij het beoordelen van een binnengekomen aangifte, (112) melding of een tip, zoals bijvoorbeeld een bommelding of een tip voortkomend uit een afgetapt gesprek. Helaas kunnen hier ook valse aangiftes, onterechte meldingen en *red herrings* (dat wil zeggen, onjuist informatie om het onderzoek in een verkeerde richting te sturen) tussen zitten die geïdentificeerd moeten worden om verspilling van capaciteit te voorkomen. Eén geïnterviewde gaf aan dat een red herring ook geplaatst kan worden door een informant, waardoor er behoefte is aan het bepalen van de betrouwbaarheid van verklaringen van informanten. In verband met beperkte capaciteit kunnen namelijk niet alle aangiftes, meldingen en tips opgevolgd worden. *“Bij een melding wordt er nu een lijstje met vragen doorgelopen en dan een keuze gemaakt. Leugendetectie zou daar misschien bij kunnen helpen.”* De keuze wordt nu ook vaak gebaseerd op zwakke indicatoren en de leugendetectie zou dit kunnen versterken. Het bepalen van de betrouwbaarheid van dit type meldingen en tips kan dus veel tijd en geld besparen en ook de kans vergroten dat een zaak wordt opgelost.

Wanneer besloten is om een onderzoek te openen, bijvoorbeeld door het opvolgen van een melding of een tip, kan leugendetectie ook tactische informatie opleveren bij het identificeren van relevante getuigen. Dit proces kan al plaatsvinden tijdens het initiële buurtonderzoek. *“Met wie moet je praten en met wie niet?”* “Het bepalen welke omstanders (of getuigen) misschien verdacht zijn is bijvoorbeeld relevant bij een brand, *“waarvan we weten dat de dader misschien toe staat te kijken”*. Hier kleeft mogelijk wel een juridisch of ethisch probleem aan: *“Moet er een verdenking zijn voor je leugendetectie in mag zetten?”* In alle contexten geldt het proportionaliteitsprincipe. Zo moet je bijvoorbeeld ook *“de kans en gevolg van een scenario meenemen. Bij een terroristische aanslag is het gevolg groot. Ik kan me wel voorstellen dat het dan interessant is.”*

Geïnterviewden noemden ook voorbeelden van hoe ook later in het onderzoeksproces een betrouwbaarheidsbepaling een positieve bijdrage kan leveren aan het onderzoek. Bijvoorbeeld *“wanneer je in gesprek bent met een relevante getuige, kun je er dan achter komen of de informatie juist is?”* Zowel vanuit de wetenschap (bijvoorbeeld, de *false memory* literatuur), als uit de praktijk (bijvoorbeeld, gerechtelijke dwalingen) is bekend dat ooggetuigen zich kunnen vergissen en per ongeluk een onjuiste verklaring geven, niet uit kwade opzet, maar omdat zij zich de gebeurde evenementen anders herinneren, de zogenaamde *memory distortions*. Verscheidene geïnterviewden gaven aan dat het niet alleen nuttig is om te weten welke getuigenverklaringen waar zijn en welke niet in verband met de richting van het onderzoek, maar ook om in het geval van een onjuiste verklaring te kunnen identificeren of deze per ongeluk was gemaakt (dat wil zeggen, een false memory), of opzettelijk (dat wil zeggen, een leugen).

“Hoe bepaal je het verschil tussen een leugen en een (eerlijke) foute ooggetuigen herkenning? Misschien te testen met de CIT?” Het eerste betreft namelijk een menselijke fout die vroegtijdig geïdentificeerd moet worden om te voorkomen dat het onderzoek de verkeerde kant op gaat, maar het laatste betreft een strafbaar feit waarnaar eventueel gehandeld moet worden, namelijk het bewust verstoren van het onderzoek. Als kanttkening werd er door de geïnterviewden wel opgemerkt dat er voorzichtig gehandeld moet worden wanneer men de betrouwbaarheid van getuigenverklaringen toetst. *“Getuigen kunnen ook slachtoffer zijn.”* Een andere geïnterviewde noemde dat hun medewerking bovendien belangrijk is voor een goed verloop van het onderzoek. Door hen te onderwerpen aan leugendetectie kan mogelijk de medewerking aan het onderzoek verloren gaan.

Verscheidene geïnterviewden gaven ook aan dat een betrouwbaarheidsbepaling van een verklaring van de verdachte meerwaarde kan bieden, al moet hier wel rekening gehouden worden met de Nederlandse wet- en regelgeving die bepaalt dat een verdachte niet mee hoeft te werken aan zijn eigen veroordeling en dus het recht heeft om te zwijgen of te liegen (zie ook 4.1.4. voor een bespreking van de genoemde relevante beleidskaders). Tijdens één van de interviews is besproken dat er echter ook stemmen opgaan om het liegen van verdachten in de rechtszaal in de toekomst mogelijk aan banden te leggen (zie ook Korthals Altes, 2014), al is dit een controversieel onderwerp (zie ook Plasman, 2014). Als laatste gaf een geïnterviewde aan dat een betrouwbaarheidsbepaling bij de verklaring van een verdachte ook juist ingezet kan worden om de verdachte te beschermen. Zo zouden onschuldige verdachten kunnen aantonen dat ze de waarheid spreken en zouden vermoedelijke valse bekentenissen getest kunnen worden en daarmee hopelijk een eventuele gerechtelijke dwaling voorkomen worden.

4.2.1.2 *Betrouwbaarheidsbepaling in een in- en uitreiscontext*

Naast het politieonderzoek kan een betrouwbaarheidsbepaling nuttig zijn in een in- en uitreiscontext. Hierbij kan gedacht worden aan grensbewaking en het screenen van passagiers in de burgerluchtvaart, maar ook aan het screenen van in- en uitreizende jihadisten en binnenkomende asielzoekers. Zoals ook eerder opgemerkt kan leugendetectie in deze context niet alleen ingezet worden om het kleine percentage onbetrouwbare personen eruit te halen, maar juist ook omgekeerd door te bepalen wie juist wel betrouwbaar is zodat deze mensen bijvoorbeeld sneller door de security check heen kunnen (dat wil zeggen, het fast lane-concept). *“Iedereen moet toch door security heen gaan, alleen het niveau van de security verschilt.”* Dan kun je dat beter positief framen (e.g., bij een positieve betrouwbaarheidsbepaling uitkomst mag je sneller door het systeem heen dan normaal is) dan negatief (e.g., je bent verdacht dus moet je door de strengere selectie heen waardoor je trager bent dan normaal) ten opzichte van de norm.

4.2.1.3 *Betrouwbaarheidsbepaling in een screeningcontext*

Tijdens de interviews werd ook genoemd dat leugendetectie ingezet zou kunnen worden ten behoeve van een betrouwbaarheidsbepaling in een bedrijfscontext. Bijvoorbeeld als onderdeel van een pre-employment screening, vooral bij banen waar een security clearance voor nodig is. Het is niet alleen belangrijk om betrouwbaarheid bij “kernwerknemers” te bepalen, maar wellicht ook bij personeel dat indirect toegang heeft tot gevoelige informatie, of zelfs bij personeel van andere bedrijven zoals leveranciers, catering en schoonmaak die mogelijk toegang hebben tot gevoelige informatie.

Door naast een pre-employment screening ook tijdens iemands dienstverband regelmatig betrouwbaarheidstoetsen te doen kunnen bijvoorbeeld ook *insider threat* gevaren geïdentificeerd worden, zoals radicalisering van medewerkers. Naast het toepassen van leugendetectie bij het (herhaaldelijk) screenen van medewerkers van het kernbedrijf en randbedrijven, kan het ook nuttig zijn om de bezoekers van beveiligde locaties te screenen.

4.2.1.4 *Betrouwbaarheidsbepaling in een claimcontext*

Specifiek voor de verzekeringsbranche en de belastingen biedt leugendetectie naast het screenen van personeel en bezoekers extra mogelijkheden. Ingediende verzekeringsclaims moeten beoordeeld worden op hun betrouwbaarheid. Momenteel wordt dat voornamelijk handmatig gedaan en soms op basis van beslisregels die gebaseerd zijn op eerdere aangiften of op het profiel van de indiener. Claims die als verdacht worden aangemerkt, worden vervolgens verder onderzocht. De uitkomsten van dit onderzoek bepalen of de claim als valide wordt aangemerkt en er dus uitbetaald kan worden, ofwel als verdacht. Indien de claim als verdacht wordt aangemerkt, dan wordt er telefonisch een cognitief interview afgenomen waarin uitgezocht wordt of een claim al dan niet terecht was. Zeker bij de initiële schifting van claims zou met behulp van leugendetectie aanzienlijke winst behaald kunnen worden, aangezien uit onderzoek blijkt dat ongeveer 10% van de claims frauduleuze elementen bevatten (verzekeren.net, 2013) terwijl er nu *“minder dan 1% uitgehaald wordt”*.

Het Centrum Bestrijding Verzekeringscriminaliteit heeft vorig jaar berekend dat er in totaal voor ongeveer 900 miljoen euro fraude wordt gepleegd met verzekeringen door het indienen van valse claims (verzekeringen.com, 2014). Een kleine verbetering in het proces van enkele procenten, levert daarom al een enorme besparing op. Een ander gerelateerd scenario waarbij een betrouwbaarheidsbeoordeling van een ingediende melding, claim of aanvraag relevant kan zijn is bij de aanvraag van een uitkering, zoals bijvoorbeeld een bijstandsuitkering of een arbeidsongeschiktheidsuitkering. Deze uitkeringsaanvragen worden momenteel al beoordeeld, maar deze beoordeling zou misschien accurater kunnen worden dankzij het gebruik van leugendetectie. Ook werd in deze context de behoefte uitgesproken om het aantal frauduleuze claims omlaag te brengen (zie H4.4 voor een uitgebreidere bespreking van dit onderwerp).

4.2.2 *Leugendetectie als trainings- en testmiddel*

Tijdens verscheidene interviews werd genoemd dat het soms nodig kan zijn om effectief te kunnen liegen om een bepaalde taak of baan goed uit te kunnen voeren. Bijvoorbeeld wanneer iemand operationeel werk gaat doen en een andere identiteit moet aannemen. In een dergelijke situatie is het van belang dat iemand goed in zijn verhaal zit. Leugendetectie zou kunnen helpen bij de voorbereiding en training van dit type operaties en kan gebruikt worden om te testen in hoeverre er extra training nodig is voor aanvang van een operatie. Verschillende geïnterviewden vonden deze toepassing interessant. Zeker wanneer de andere partij misschien ook over leugendetectietechnologie beschikt kan dit van groot belang zijn. Naast het gebruik van leugendetectie tijdens de voorbereidingen van dit type operaties, zou het ook ingezet kunnen worden om iemands mentale staat en betrouwbaarheid te kunnen testen tijdens de operatie, bijvoorbeeld om te bepalen wanneer de operatie moet worden stopgezet.

4.2.3 *Monitoren om afwijkend gedrag te identificeren*

Tijdens de interviews werden er ook een aantal andere toepassingen van leugendetectie methodologieën genoemd, vooral in de context van “*verstoren en voorkomen*”. Het op afstand monitoren van individuen of groepen mensen, bijvoorbeeld door een persoon of slimme camera's, kan gebruikt worden om afwijkend gedrag te identificeren. Afwijkend gedrag, bijvoorbeeld in reactie op *prikkelen*, kan een indicator zijn van kwade intenties of risicovol gedrag (Van Rest, Roelofs, & Van der Kleij, 2014). Deze afwijkingen vroegtijdig signaleren zou kunnen helpen om een ongewenste situatie te voorkomen. Een geïnterviewde zei hierover “*intenties identificeren kan dreiging wegnemen, in de voorfase, en daarmee een risico of misdrijf voorkomen.*”

4.2.4 *Welke leugendetectietoepassing heeft prioriteit?*

Tijdens het interview is er expliciet gevraagd welke toepassingen van leugendetectie prioriteit hebben om doorontwikkeld te worden. Om te bepalen welk type leugendetectie voor deze toepassingen relevant is, moeten zowel de modaliteit (dat wil zeggen, face-to-face, telefonisch, op basis van geschreven tekst door de persoon zelf, of op basis van geschreven tekst door een ander zoals een rapportage) als het type interactie (dat wil zeggen, interview vs. zonder interactie; openlijk vs. heimelijk) en de context (dat wil zeggen, bewaken & beveiligen, verzekeringen) en organisatie randvoorwaarden (tijd, systemen, experts e.d.) meegenomen worden. Deze informatie geeft een inzicht in welke methodes en technieken in verschillende scenario's toegepast kunnen worden. De relevantie van technieken verschilt dan ook tussen de geïnterviewden. Los van het type leugendetectie is ook gevraagd welke overige ontwikkelingen prioriteit hebben. Er is een grote behoefte aan ontwikkelingen die kunnen bijdragen aan het verhogen van de accuraatheid, zoals door een geïntegreerde leugendetectiemethode, het verlagen van de invasiviteit (bijvoorbeeld door metingen op afstand), en het uitvoerig testen van protocollen in zowel het lab als de praktijk. De ideale leugendetectiemethode is zo duidelijk mogelijk, bijvoorbeeld “*een selectiemiddel dat groen of rood toont. Als het rood toont, dan komt er een team om nader onderzoek uit te voeren en bij groen niet. Zeker bij het gebruik van technologie moet het wel duidelijk zijn waar het rood en groen op gebaseerd zijn.*” Deze geïnterviewde legde ook het verband met een blaascontrole om de hoeveelheid geconsumeerde alcohol te meten. “*Hoe accurater een machine is, hoe meer die mag doen. Vertrouwen in de techniek is dan van belang. De uitkomst kan eventueel nog terzijde geschoven worden door de agent.*” Er is dus behoefte aan een methode of apparaat om leugens te kunnen detecteren waarvan het heel duidelijk is hoe deze werkt, en hoe de resultaten geïnterpreteerd moeten worden. Naast deze duidelijke behoefte werd er ook door meerdere personen aangegeven dat het belangrijk is om te kunnen identificeren of iemand per ongeluk of expres een onjuiste verklaring heeft gegeven.

4.2.5 *Welk type leugendetectie is relevant?*

Afhankelijk van de toepassing waarin leugendetectie plaatsvindt kan gebruik gemaakt worden van verschillende technieken die bepaalde leugenachtige gedragingen juist wel of juist niet mee kunnen nemen. Hieronder worden de uitkomsten van de interviews gecombineerd met onze vakkennis en worden de verschillende leugendetectietoepassingen en implicaties daarvan uiteengezet. Als laatste wordt ook het effect van context expliciet meegenomen in de overweging welke leugendetectiemethoden toepasselijk zijn. Niet alle informatie hieronder is dus in de interviews besproken.

4.2.5.1 Face-to-face leugendetectie (eventueel via videoverbinding)

Bij dit type leugendetectie kan beschikt worden over de rijkste data en de meeste technieken om leugens te kunnen detecteren. Er is namelijk sprake van non-verbaal gedrag (dat wil zeggen, hoe iemand zich gedraagt), para-verbaal gedrag (hoe iemand iets zegt), verbaal gedrag (wat iemand zegt en welke woorden hij gebruikt) en eventueel zelfs fysiologische metingen die een objectief inzicht kunnen bieden in de ervaren stress en cognitieve belasting. Bij alle data, maar specifiek ook bij deze laatste categorie, moet er wel rekening mee gehouden worden dat hoewel het mogelijk is om vast te stellen of iemand gestrest is, de oorzaak van deze stress niet bekend is. *“Het moet duidelijk zijn voor de agent die het toepast wat de uitkomst van zo’n leugendetectie test precies betekent. Bijvoorbeeld, een verhoogde hartslag kan betekenen dat iemand spanning voelt, maar dit betekent niet direct dat het een leugen is.”* Deze persoon kan bijvoorbeeld ook haast hebben of nerveus zijn om een andere reden. Dit gegeven is belangrijk om in gedachten te houden om eventuele valse beschuldigingen te voorkomen en moet dus bekend zijn bij eenieder die de leugendetectie techniek zou gebruiken. *“Om te voorkomen dat de resultaten verkeerd worden geïnterpreteerd en er verkeerde conclusies worden getrokken is het dus belangrijk dat de methode zo duidelijk mogelijk wordt ontworpen.”* Leugendetectie op basis van face-to-face interacties of video opnames is bijvoorbeeld relevant tijdens het verhoren van verdachten en getuigen, tijdens het buurtonderzoek (eventueel met bodycam), airport security screenings, pre-employment screenings, het interviewen van informanten, etc.

Non-verbale indicatoren van liegen kunnen op verschillende manieren gemeten worden, zowel met als zonder het gebruik van technologie. Zo kan bijvoorbeeld de interviewer zelf het non-verbale gedrag van de geïnterviewde observeren, of een derde persoon kan deze taak overnemen door mee te kijken en feedback terug te koppelen naar de interviewer. Hiermee is in het verleden geëxperimenteerd, maar deze pilot is mislukt omdat de terugkoppeling van de feedback in real-time via een oortje verliep en te storend bleek voor de interviewer. Een andere manier of moment om feedback te geven, bijvoorbeeld achteraf of op een computerscherm, zou er eventueel voor kunnen zorgen dat deze methode succesvoller is. Daarnaast is het ook mogelijk om non-verbaal gedrag met behulp van technologie te meten en analyseren. Dit kan grofweg op twee manieren, namelijk *intrusive*, bijvoorbeeld door het gebruik van motion-capture pakken (Van Der Zee e.a., 2015) of *unobtrusive*, bijvoorbeeld door middel van beeldanalyse of infra-rood camera’s (Perez-Rosas e.a., 2015). Zowel menselijke observaties als unobtrusive technieken kunnen beide openlijk of heimelijk ingezet worden. Bij intrusive technieken is dit lastiger omdat er apparatuur voor nodig is die fysiek contact maakt met de verdachte, al zou het eventueel kunnen als er een goede coverstory is voor waarom deze technologie gebruikt wordt. Bijvoorbeeld, de interviewer kan de verdachte vertellen dat het polsbandje fysiologische reacties meet en dat dit gebruikt wordt om ervoor te zorgen dat het interview niet te stressvol wordt, terwijl de data dan heimelijk gebruikt wordt voor leugendetectie doeleinden. Aan dit bedrog kleven wel ethische en mogelijk wettelijke nadelen. Zo is er bijvoorbeeld *“een formeel moment waarop iemand als verdacht wordt aangemerkt. Dus vooraf leugens detecteren bij een potentiële verdachte is lastig zonder verdenking. Deze informatie mag dan niet als bewijs gebruikt worden omdat het dan onterecht verkregen bewijs betreft.”* *“Bij het heimelijk detecteren van leugens is eventueel ook toestemming van de Rechter Commissaris nodig.”*

Tot slot, alle analyses kunnen ofwel achteraf gedaan worden, ofwel in real-time waardoor de interviewer de feedback meteen mee kan nemen in het interview.

Face-to-face of op video opgenomen interviews bevat ook audio waardoor paraverbale gedragingen zoals toonhoogte en gesprekshaperingen kunnen geanalyseerd worden. Analyse kan plaatsvinden ofwel door een mens, ofwel door audio analyse. Feedback over de betrouwbaarheid van een verklaring op basis van deze paraverbale indicatoren kan ofwel achteraf, ofwel in real-time worden gegeven. Deze analyse is altijd niet-invasief.

Verbale leugendetectie in face-to-face gesprekken of video-opnames kan zowel door een mens, als door technologie gedaan worden. Wanneer de analyse van verbale leugenindicatoren met behulp van technologie plaatsvindt, is de analyse gebaseerd op een al dan niet automatische transcriptie van de audio opname. In deze context gaf één van de geïnterviewden aan dat het verbeteren van het omzetten van spraak naar tekst in het Nederlands prioriteit heeft. Het automatisch omzetten van spraak naar tekst voor dit type analyses werkt momenteel namelijk beter in het Engels dan in het Nederlands. Op basis van audio opnames kunnen twee soorten verbale leugenindicatoren getest worden, namelijk woordgebruik en type details. Woordgebruik wordt al regelmatig automatisch gemeten (Hauch, Blandón-Gitlin, Masip, & Sporer, 2014) met het software programma LIWC (Pennebaker e.a., 2001), terwijl type details vaak nog handmatig aan de hand van een codeersysteem wordt geannoteerd (Vrij, 2015).

In plaats van de verschillende type leugenindicatoren los van elkaar te bestuderen is het ook mogelijk om een multimodale leugendetectiemethode te gebruiken. Hierbij worden non-verbale, paraverbale, verbale en eventueel fysiologische metingen gecombineerd om samen een accuratere betrouwbaarheidsbepaling te kunnen doen. Een gecombineerde aanpak kan eventueel door een mens, bijvoorbeeld de interviewer of een derde persoon gedaan worden door tijdens het interview op alle soorten gedragingen van de ander te letten, maar door de vele en verschillende soorten input kan het lastig zijn om deze taak goed uit te voeren, vooral wanneer dit gecombineerd wordt met het uitvoeren van het interview. Daarnaast zijn sommige van deze leugenindicatoren, zoals woordgebruik, lastig om zelf op te merken. Daarom is deze multimodale aanpak waarschijnlijk het meest succesvol wanneer deze uitgevoerd wordt met behulp van meerdere sensoren en technieken. Verschillende geïnterviewden zagen het voordeel van een multimodale leugendetectiemethode en gaven aan dat het ontwikkelen van een betrouwbare variant prioriteit heeft.

4.2.5.2 *Leugendetectie op basis van audio (e.g., telefonisch)*

Leugendetectie op basis van audio kan gebruik maken van de hierboven beschreven paraverbale en verbale leugenindicatoren, maar niet van de non-verbale of fysiologische indicatoren. Leugendetectie kan uitgevoerd worden door ofwel de mens, ofwel met behulp van technologie, en feedback kan zowel in real-time als achteraf worden gegeven afhankelijk van het scenario. Dit type leugendetectie is bijvoorbeeld relevant bij het detecteren van valse telefonische meldingen, aangiften en verzekering claims (Leal, Vrij, Warmelink, Vernham, & Fisher, 2015), maar bijvoorbeeld ook bij het bepalen van de betrouwbaarheid van informatie uit getapte gesprekken.

4.2.5.3 *Leugendetectie op basis van geschreven tekst*

Leugendetectie op basis van geschreven teksten kan onderverdeeld worden in twee categorieën. Ofwel de geïnterviewde heeft de tekst zelf geschreven, ofwel het is een samenvatting of rapportage opgemaakt door de interviewer of een derde. Bij beide categorieën kan er gekeken worden naar het type details die de verklaring bevat. Daarnaast leveren zelfgeschreven verklaringen mogelijk nog twee andere type indicatoren op: 1) woordgebruik, en 2) schrijf- of typegedrag. Er bestaat bijvoorbeeld software waarin muisklikken en ander typegedrag die indicatief kunnen zijn voor liegen gemeten wordt (Derrick, Meservy, Jenkins, Burgoon, & Nunamaker Jr., 2013). In dit geval kan een technologische leugendetectie aanpak waarschijnlijk tot meer informatie en een betere accuraatheid leiden dan een menselijke aanpak.

4.2.5.4 *Context-specifieke leugendetectie*

De situaties beschreven in de bovenstaande paragrafen betreffen vaak een (één-op-één) interactie of interview. Er zijn echter ook situaties waarin interacties met meerdere mensen relevant zijn. Specifiek voor het interviewen van meerdere verdachten tegelijkertijd zijn er interviewmethoden en analysetechnieken ontworpen die de interactie tussen geïnterviewden tijdens het verhoor analyseren. Uit experimenteel onderzoek is gebleken dat paren die de waarheid spreken complexere verhalen hebben, elkaar vaker onderbreken en het vaker met elkaar oneens zijn (Vrij e.a., 2012).

Specifiek bij het bepalen van de betrouwbaarheid van verzekeringsclaims kan er gewerkt worden aan “het combineren van databronnen om de kennisregels te verscherpen (Morley, Ball, & Ormerod, 2006). Dit helpt bij de automatisering van het screeningsproces” en kan ervoor zorgen dat claims sneller (i.e., het verhogen van de efficiëntie) en beter (i.e., het verhogen van de effectiviteit) gecategoriseerd kunnen worden. Zo kunnen bijvoorbeeld details van de claim of van diegene die de claim heeft ingediend meegenomen worden bij het bepalen van de betrouwbaarheid van een claim. Een geïnterviewde gaf ook dat deze branche voordeel kan halen bij het verbeteren van *fuzzy search* technieken waarmee je bepaalde targetwoorden kan identificeren, ook wanneer deze verkeerd zijn geschreven. Deze fuzzy search methode zou nuttig kunnen zijn als blijkt dat het gebruik van bepaalde woorden een indicator zijn van liegen in deze context. Omdat het in de verzekeringsbranche om grote bedragen gaat kan een kleine verbetering in effectiviteit of efficiëntie al een groot effect hebben.

4.2.6 *Zijn er ook scenario's waarin leugendetectie niet bruikbaar of wenselijk is?*

Om een accuraat beeld te krijgen van de mogelijkheden van leugendetectie in de Nederlandse praktijk is het belangrijk om niet alleen te vragen naar de scenario's waarin het gebruik wel wenselijk is, maar ook in welke scenario's dit juist niet het geval is. Door dit expliciet te maken, kan voorkomen worden dat leugendetectie-ontwikkelingen plaatsvinden die door de praktijk als onwenselijk worden gezien. De antwoorden op deze vraag kunnen grofweg in twee categorieën worden ingedeeld: 1) scenario's die ethisch bezwaarlijk zijn, en 2) scenario's die praktisch bezwaarlijk zijn.

Vanuit een ethisch perspectief werd er opgemerkt dat het toepassen van leugendetectie alleen ingezet moet worden “als toepassing in veiligheidsscenario's en niet in het algemeen, want liegen is ook sociaal wenselijk”. Dit is een relevant – maar in de praktijk ook lastig – punt omdat je bij het ontwikkelen van methodes

en technieken niet altijd controle hebt over waar het ontwikkelde nog meer voor gebruikt gaat worden door anderen. Een andere geïnterviewde zei: *“Moet je dit wel willen? Maar dat is meer een vraag voor de politiek dan voor ons.”*

“Deze ontwikkelingen zullen namelijk langzaam doorgaan en dan moet het politieke debat bepalen waar het heen gaat. Dit zou kunnen leiden tot een verschillende aanpak in verschillende landen.” Zowel in een security context als in een verzekeringscontext zal de framing van het inzetten van leugendetectie in de praktijk van groot belang zijn. Over het gebruik van leugendetectie in een verzekeringscontext zei één van de geïnterviewden: *“Transparantie over de inzet van dat soort middelen naar klanten is cruciaal. De inzet van leugendetectie ten behoeve van fraudeopsporing raakt ook de meerderheid van de relaties die te goeder trouw handelen. Je zal goed moeten afwegen en uitleggen waarom je het middel inzet en op welke wijze je omgaat met privacy en gevoelens van klanten. Uiteindelijk zal fraude detectie in bredere zin ook ten goede komen aan klanten die te goeder trouw zijn.”* Eenzelfde reactie kan verwacht worden in de context van airport security screening en bijvoorbeeld ook in tijdens buurtonderzoek of gesprekken met de wijkagent: *“Ik zou geen leugendetectie gebruiken als een wijkagent praat met iemand, alleen al vanwege de beeldvorming en de issues met vertrouwen die het op kan leveren. Stel dat het uitkomt, welk effect het dan heeft op de publieke opinie.”* Daarom kan een positieve framing (i.e. bijvoorbeeld, het benadrukken dat met leugendetectie een voordeel is te behalen, zoals de mogelijkheid om door sneller dan normaal door de security check te mogen in plaats van gestraft te worden met een extra check waardoor je langzamer dan normaal door de check gaat) bijdragen aan een succesvolle implementatie van leugendetectie in de praktijk.

Als praktisch bezwaar werd door een geïnterviewde aangegeven waarom bepaalde leugendetectiemethodes niet gebruikt worden in de praktijk: *“CIT was te moeilijk toe te passen in de praktijk en SCAN (Scientific Content Analysis)⁸ is niet wetenschappelijk onderbouwd”* (Bogaard, Meijer, Vrij, & Merckelbach, 2016). Ook problemen met leugendetectie in de bewijs sfeer werden in dit kader genoemd. Vanwege een te lage accuraatheid en problemen met de interpretatie van expertverklaringen *“zou ik op korte termijn wegblijven bij het gebruik als bewijs in de rechtszaal.”* Zeker als bewijs bij verdachten, want *“die mogen namelijk liegen.”* *“Wat als dit type bewijs verkeerd wordt gebruikt of geïnterpreteerd en dat het daardoor mis gaat?”* Daarnaast moet je ook *“uitkijken in de opleiding, dat de gebruikers er niet iets te enthousiast mee aan de haal gaan.”* *“Wat doe je met de uitslag van een systeem voor leugendetectie? We zijn niet bang voor kwade opzet bij het eigen personeel, wel voor incompetentie.”*

4.2.7 Welke nadelen en kwetsbaarheden heeft leugendetectie?

Dit rapport gaat over het gebruik van leugendetectie ten behoeve van waarheidsvinding. Eén van de nadelen van leugendetectie die tijdens deze interviews naar boven is gekomen, is dat je *“met leugendetectie alsnog de waarheid niet boven water krijgt; je hebt alleen een indicatie dat iets misschien niet waar is. Dus voor waarheidsvinding helpt het niet per se.”* Oftewel, om de waarheid te achterhalen is meer nodig dan alleen leugendetectie, zoals bijvoorbeeld onderzoek naar verhoormethoden en het construeren van line-ups, maar het kan daar wel bij helpen.

⁸ Methoden voor een betrouwbaarheidsbepaling van verklaringen op basis van woordgebruik. Voor meer informatie, zie https://en.wikipedia.org/wiki/Statement_analysis

Daarnaast is leugendetectie *“een ethisch vraagstuk en is het (momenteel) niet als bewijs te gebruiken. Ik ben ook bang voor verkeerde interpretatie. Soms zegt iemand iets wat hij gelooft, en is het toch niet waar”*, de false memories.

Onderzoek naar het kunnen onderscheiden van opzettelijk leugenachtige verklaringen en onopzettelijk onjuiste verklaringen gebaseerd op false memories kan dan ook bijdrage aan het veilig implementeren van leugendetectie in de praktijk.

Een praktisch nadeel van leugendetectie is dat een verdachte, eventueel met behulp van zijn of haar advocaat, erachter kan komen hoe de leugendetectiemethode werkt. Eén geïnterviewde noemde bijvoorbeeld dat er papieren rondgaan van advocatenbureaus met advies van wat wel en niet te doen tijdens een verhoor. Wanneer leugendetectie tijdens het verhoor ingezet zou worden is het dus waarschijnlijk dat advocaten hun cliënten gaan adviseren over het gebruik van tegenmaatregelen om de leugendetectie te omzeilen. Een voorbeeld van een tegenmaatregel bij de polygraaf met CQT methode is het manipuleren van de baseline-maat door het opwekken van een fysiologische stressreactie tijdens controle- en feitenvragen, bijvoorbeeld door op de tong te bijten (Iacono, 2008). Effectieve tegenmaatregelen kunnen de accurateheid van een leugendetectiemethode verminderen (Ganis, Rosenfeld, Meixner, Kievit, & Schendan, 2011). Daarom zou het optimaal zijn als de leugendetectiemethode bestand is tegen het gebruik van tegenmaatregelen. De methode wordt moeilijker te misleiden als er verschillende type leugenindicatoren gemeten worden en samen leiden tot een uitkomst (dat wil zeggen, een multimodale aanpak). Het is immers lastiger om verschillende gedragingen tegelijkertijd te controleren dan als je je maar op één leugenindicator (bijvoorbeeld, non-verbaal gedrag of type details) hoeft te concentreren. Het is echter niet noodzakelijk dat een leugendetectiemethode volledig bestand is tegen het gebruik van tegenmaatregelen: *“Elk middel heeft namelijk een halfwaardetijd, en dat is de tijd dat een middel effectief ingezet kan worden. Daarom is het belangrijk om een brede gereedschapskist te hebben met verschillende technieken waar je uit kunt kiezen.” “Liever veel kleine stapjes in leugendetectie dan één grote stap.”* Deze stapsgewijze verbetering zou bovendien de halfwaardetijd kunnen verlengen.

In de meerderheid van deceptieonderzoeken wordt gekeken naar gedragsverschillen op groepsniveau. Hoewel deze onderzoeken een relevant inzicht bieden in het effect van liegen op gedrag, is deze informatie alleen niet per se voldoende voor toepassing in de praktijk. Mensen verschillen namelijk in de manier waarop zij zich gedragen. Om de toepasbaarheid van leugendetectie te vergroten, moet de techniek in staat zijn om uitspraken te doen over het betrouwbaarheidsgehalte van een uitspraak van één, vaak onbekend, individu. Om gedragsverschillen tussen leugens en waarheden te identificeren voor deze ene individu kan het vaststellen van baseline gedrag daarom nuttig zijn. Dit is echter lastig gebleken.

Onderzoek heeft aangetoond dat mensen niet alleen onderling verschillen in de manier waarop zij zich gedragen, maar dat ook het type leugen, de ontvanger, de reactie van de ontvanger (Buller & Burgoon, 1996), pakkans, wat er op het spel staat als het bedrog uitkomt (i.e., de stakes) en veranderingen over tijd gedrag kunnen beïnvloeden (Vrij, 2008). Onderzoek naar het vaststellen van een relevante baseline zou de toepasbaarheid van leugendetectie in de praktijk kunnen vergroten.

4.2.8 *Hebt u de benodigde leugendetectie kennis al in huis ?*

De gehouden interviews waren semigestructureerd wat in dit geval inhoudt dat niet alle vragen tijdens alle interviews zijn gesteld. In slechts drie interviews met in totaal vier geïnterviewden is gesproken over de vraag of de benodigde kennis voor de ontwikkelingen in leugendetectie al in huis zijn. Alle vier de geïnterviewden gaven aan dat de benodigde kennis en methodologie momenteel nog niet of nauwelijks in huis is. Hoewel dit antwoord vanwege de kleine hoeveelheid respondenten een incompleet beeld geeft, geeft het, gecombineerd met de bevindingen uit Fase 1 waaruit bleek dat de meerderheid van de geïnterviewden niet goed op de hoogte was van de huidige mogelijkheden omtrent leugendetectie, wel een indicatie dat relevante Nederlandse organisaties qua bemensing en apparatuur momenteel niet in staat zijn om leugendetectie op te pakken.

4.3 **Fase 3: Response op huidige ontwikkelingen**

Na de inventarisatie van de huidige situatie en eventuele behoeftes op het gebied van leugendetectie werd tijdens de interviews tijd besteed aan het doorspreken van een recente publicatie betreffende recente ontwikkelingen op het gebied van leugendetectie, verhoortechnieken, automatisch meten, liegen over intenties en daderkennis testen (Van Der Zee e.a., 2016). Dit onderwerp is bij 10 van de 13 interviews aan bod gekomen. Uit de interviews bleek namelijk, zoals ook verwacht, dat de meerderheid van de geïnterviewden niet op de hoogte was van de recente wetenschappelijke ontwikkelingen op dit gebied. Dit kan toepassing van leugendetectie in de praktijk in de weg staan. Een gebrek aan up-to-date kennis zou bovendien een beperking kunnen betekenen van de generaliseerbaarheid van de resultaten van dit onderzoek, betreffende de mogelijkheden en toepassingen. Vandaar dat wij, na het doorspreken van deze ontwikkelingen, gevraagd hebben in hoeverre deze kennis de toepasbaarheid van leugendetectie in de praktijk voor hen heeft veranderd.

Van de 10 interviews waarin deze recentelijke ontwikkelingen zijn besproken, waren deelnemers van drie van deze interviews van alle ontwikkelingen op de hoogte, twee waren gedeeltelijk op de hoogte en vijf waren vrijwel niet op de hoogte. Het onderzoek naar liegen over intenties was het meest onbekend, namelijk bij zeven van de 10 interviews. Geïnterviewden waren het vaakste bekend met de recente ontwikkelingen op het gebied van automatisch meten van leugenachtig gedrag, namelijk tijdens vijf van de 10 interviews.

Vervolgens is er tijdens acht interviews antwoord gegeven op de vraag of deze kennis iets veranderd aan hun mening over de implementatie mogelijkheden van leugendetectie in de praktijk. Dat bleek bij de meesten het geval. *“Ik was positief verrast, want ik dacht dat de accuraatheid lager lag.”* Tijdens zes van deze acht semigestructureerde interviews werd er aangegeven dat als de huidige wetenschappelijke resultaten (bijvoorbeeld 75% accuraatheid) ook in de praktijk zouden worden gehaald, dat leugendetectie dan bruikbaar voor hen zou zijn. Voor sommigen was een percentage van 75% voldoende, terwijl anderen verder beredeneerden wat een leugendetectie accuraatheid van 75% in de praktijk voor gevolg zou hebben. Eén geïnterviewde zei hierover: *“Als je daarnaast nog verifieerbare informatie kunt toevoegen, gaat de accuraatheid verder omhoog. Dus het wordt altijd meer dan 75% accuraatheid, want het gaat nooit om één stuk bewijs, het is een additioneel element.”*

Ook werd gezegd dat 75% *“in de buurt komt bij de 80/20 regel; niks is perfect, maar bij security is 80% acceptabel.”* Dit standpunt werd beaamt door een andere geïnterviewde: *“In combinatie met andere bewijsmiddelen, waarom zou het dan niet kunnen? Als rechter heb je de vrijheid om bewijsmiddelen in te zetten om tot een overtuiging te komen. Dan is het wettig bewijs en kan het helpen.”* Dat betekent dat een belangrijke volgende stap is om te testen of de leugendetectorresultaten die momenteel in het lab worden gehaald, of die ook gelden in praktijksituaties. De geïnterviewden die aangaven dat accuraatheden van 70-75% onvoldoende zouden zijn om in de praktijk gebruikt te worden noemden een te lage accuraatheid als reden. Zowel omdat het *“met 70% geen stand houdt als bewijsmiddel in de rechtszaal”* en vanwege de hoge mate van *“vals positieven, onschuldigen die als schuldig aangewezen worden. Je wilt alleen iemand beschuldigen van liegen als je het 100% zeker weet.”*

De besproken ontwikkelingen veroorzaakten verschillende reacties bij de geïnterviewden. Het kunnen identificeren van intenties heeft bijvoorbeeld leugendetectorie relevanter gemaakt voor specifieke contexten zoals airport security. *“Intenties identificeren kan dreiging wegnemen in de voorfase en daarmee een risico of misdrijf voorkomen.”* Het kunnen aantonen van daderkennis leidde ook tot nieuwe ideeën, zoals bijvoorbeeld het kunnen identificeren of een bepaald stuk malware geschreven is door een verdachte, maar ook als ondersteuning bij het identificeren van (professioneel) vervalste paspoorten die moeilijk te onderscheiden zijn van echte paspoorten. Er is ook de hoop uitgesproken dat daderkennis-identificatie (CIT) misschien ingezet kan worden om een onderscheid te maken tussen *false memories* en opzettelijke leugens.

De twee interviews waarin werd aangegeven dat deze recentelijke ontwikkelingen leugendetectorie niet bruikbaar maken in de praktijk gaven beide een te lage accuraatheid en het probleem van los alarmen aan als reden. *“Een accuraatheid van 70% houdt geen stand als bewijsmiddel in de rechtszaal.”* Deze geïnterviewde ging verder niet in op het eventuele gebruik van leugendetectorie voor het vergaren van tactische informatie in plaats van als bewijs in de rechtszaal. De andere geïnterviewde deed dat wel en gaf aan wel mogelijkheden voor de toepassing van leugendetectorie in de praktijk te zien als bijvoorbeeld de focus verlegd wordt van het identificeren van leugens (en daarbij de kans dat je iemand vals beschuldigd) naar het identificeren van betrouwbare verklaringen. *“Je wilt alleen iemand beschuldigen van liegen als je het 100% zeker weet. Je kunt het wel gebruiken als reden tot doorvragen in plaats van iemand te confronteren met een leugen en te ‘beschuldigen’. Het gaat dus om het accentverschil tussen een leugen of onschuld bepalen.”* *“Daarnaast kan ook het detecteren van opvallend of afwijkend gedrag in plaats van leugens interessant zijn.”*

4.4 Fase 4: Respons op het voorkomen van oneerlijk gedrag

Fase 4 van het interview begon met een uitleg over het voorkomen van leugens en ander oneerlijk gedrag. Met de geïnterviewden werd besproken dat de laatste jaren, mede dankzij interesse vanuit het vakgebied *behavioral economics* in deceptieonderzoek, een onderzoekslijn is ontstaan waarbij de focus niet ligt op het detecteren van leugens, maar juist op het voorkomen van leugens en ander oneerlijk gedrag. Als leugens namelijk succesvol voorkomen kunnen worden, hoeft de leugen niet eens gedetecteerd te worden.

Onderzoek heeft aangetoond dat bijvoorbeeld *moral reminders* (Mazar, Amir, & Ariely, 2008), *religieuze reminders* (Desai & Kouchaki, 2016) en *cognitieve belasting* (Van 't Veer, Stel, & van Beest, 2014) ervoor kunnen zorgen dat iemand zich eerlijker gedraagt. In experimenteel onderzoek is bijvoorbeeld aangetoond dat het bovenaan (dus vooraf) in plaats van onderaan (en dus achteraf) laten ondertekenen leidt tot eerlijker ingevulde verklaringen en formulieren (Shu, Mazar, Gino, Ariely, & Bazerman, 2012).

Dit onderwerp is besproken tijdens negen van de 13 interviews, waarvan slechts één iemand aangaf op de hoogte te zijn van het onderzoek op dit gebied. Deze persoon kende niet alleen de literatuur, maar paste strategieën die zijn voortkomen uit dit onderzoek ook toe in de praktijk. In een verhoorcontext worden wel gerelateerde strategieën gebruikt, bijvoorbeeld door *“voorafgaand aan een interview samen af te spreken dat je eerlijk gaat zijn tegen elkaar. Maar, je weet niet of deze methode bij alle mensen werkt. En het is lastig goed uit te voeren in de praktijk.”* Daarnaast zijn er ook organisaties die door middel van afschrikking mensen eerlijker willen maken, bijvoorbeeld door het beschrijven van de mogelijke negatieve gevolgen van een actie (bv. boetes of mogelijk gevangenisstraf). *“Maar of dat ook echt afschrikwekkend werkt, weten we niet.”*

Hoewel het voorkomen van oneerlijk gedrag dus niet zo bekend was bij de partijen met wie we hebben gesproken, waren ze wel allemaal enthousiast over een eventuele implementatie hiervan in de praktijk. Sommigen zagen een mogelijke interne toepassing, bijvoorbeeld voor het handhaven van een integere bedrijfsvoering: *“De struggle tussen goed en slecht gedrag vind ik bijzonder interessant. Een ambiance kunnen creëren om niet teveel in de verleiding te komen. Wij staan open voor nieuwe inzichten die kunnen bijdragen aan onze integere bedrijfsvoering.”* Andere geïnterviewden zagen juist kansen om deze methodes in te zetten ter ondersteuning van hun dagelijkse werk, bijvoorbeeld door mensen te stimuleren geen valse aangiftes te doen, meldingen te maken, uitkeringen aan te vragen of verzekeringsclaims in te dienen. Men bleek echter ook geïnteresseerd in een toepassing in het politieonderzoek, bijvoorbeeld door de cognitieve belasting te verhogen door de verdachte (of juist een getuige) te laten multi-tasks tijdens het verhoor waardoor het lastiger wordt om te liegen. Een geïnterviewde opperde dat het interessant zou zijn om een ‘eerlijke verhoorkamer’ in te richten op basis van de uitkomsten uit wetenschappelijk onderzoek naar de preventie van deceptie en oneerlijk gedrag. Een enkeling zag de toepassing nog breder. *“Aan de ene kant heb je de vraag wat je kunt doen om criminelen zelf te stimuleren eerlijker gedrag te vertonen. Oftewel, hoe voorkom je crimineel gedrag? Maar aan de andere kant zijn er ook allerlei partijen omheen die criminaliteit faciliteren, zoals bijvoorbeeld autoverhuurbedrijven.”* Juist bij die randpartijen valt ook winst te behalen. Sommige geïnterviewden waren zelfs enthousiast genoeg om hiermee verder te willen gaan. *“Erg in geïnteresseerd, nudging⁹. Stond eerder al op het punt dit uit te proberen, maar bloedde toen dood. Misschien is dit een aanleiding op het weer op te gaan pakken.”* Al met al geven deze reacties aan dat er interesse is in de Nederlandse praktijk om het promoten en het stimuleren of

⁹ Nudging is gedragsbeïnvloeding waardoor mensen op positieve manier, vaak onbewust, gestimuleerd worden om gewenst gedrag te vertonen. Het betreft een leefstijlbeïnvloeding op basis van 'keuzearchitectuur'. Oftewel, de omgeving wordt zodanig ingericht dat mensen, geheel vrijblijvend, de gewenste keuze aantrekkelijker vinden. Een 'nudge' is een duwtje in de goede richting. Voor meer informatie, zie <https://nl.wikipedia.org/wiki/Nudging>

nudgen van eerlijk gedrag uit te willen proberen. Een enkeling gaf ook prioriteit aan deze ontwikkeling. Net als bij leugendetectie geldt dan natuurlijk wel dat “*validatie en praktische toepasbaarheid dan belangrijk zijn.*” Daarnaast moet je ervoor waken dat “*de verhoorder niet gaat denken dat doordat deze nudge technieken zijn toegepast, nu iedereen de waarheid spreekt.*”

5 Discussie

5.1 Beperkingen van het onderzoek

Aangezien de geïnterviewde personen allemaal in relevante functies binnen relevante organisaties werken in zowel de private als publieke sector, biedt dit rapport inzicht in de huidige Nederlandse praktijksituatie met betrekking tot leugendetectie. Hoewel deze interviews een interessant en relevant beeld hebben opgeleverd van de huidige kennis en behoeften op het gebied van leugendetectie, betreft onze steekproef slechts 13 interviews met in totaal 20 personen. Voorzichtigheid is dan ook geboden bij de vertaling van onze bevindingen naar de gehele Nederlandse praktijk. Door medewerkers van verschillende publieke en private organisaties te spreken hebben we een gevarieerd beeld gekregen, maar omdat we niet medewerkers van alle relevante organisaties hebben gesproken zal het beeld niet compleet zijn. Ook is het natuurlijk mogelijk dat medewerkers binnen dezelfde organisatie anders over leugendetectie denken en dat we op die manier relevante informatie hebben gemist. Ook kan dit beeld natuurlijk nog veranderen over tijd. Dit zijn aangrijpingspunten om de dialoog tussen onderzoek en praktijk ook na deze interviewsessies voort te zetten en daarmee het praktisch nut van leugendetectie te vergroten.

5.2 Het strategisch belang van kennis over leugendetectie

Handel en economie zijn belangrijke pijlers van onze maatschappij. Daarbij past het om naar innovatieve manieren te zoeken om beveiliging te organiseren die zo weinig mogelijk frictie opleveren voor de maatschappij en de economie. Ook verlangen we dat onze eigen rechtspraak –bijvoorbeeld in het kader van Den Haag Stad van Vrede en Recht- aan de hoogste normen voldoet. Op straat en bij evenementen wensen we een politie die informatie-gestuurd optreedt, om daarmee efficiënt en proportioneel te kunnen handelen.

Aan de hand van de resultaten van dit rapport kunnen we stellen dat leugendetectie in verschillende veiligheidsdomeinen op verschillende wijzen daar aan kan bijdragen. Zo is de concrete aanleiding voor deze studie bijvoorbeeld gelegen in de ontwikkelingen op het gebied van luchtvaartbeveiliging. Hierbinnen wordt vooral gezocht naar het slim filteren van passagiersstromen. Dat vereist een heel ander toepassingsconcept dan bijvoorbeeld in een verhoorkamer gewenst –en mogelijk- is.

5.3 Kennisinfrastructuur

Op basis van de ervaringen van de eerste auteur kunnen we stellen dat de academische omgeving in hoge mate is gefragmenteerd op het onderwerp leugendetectie. Incidenteel vindt er wel samenwerking tussen verschillende wetenschappers en tussen wetenschappers en praktijk plaats, maar een grootschalig structureel samenwerkingsverband ontbreekt. Daarmee is Nederland niet uniek, pas vorig jaar is er voor het eerst een internationaal wetenschappelijk congres georganiseerd dat puur over de preventie en detectie van deceptie gaat (Decepticon, 2015). Tegelijkertijd toont dat wel de actuele en hernieuwde interesse aan in het onderwerp.

Op dit moment vinden geïnteresseerde Nederlandse eindgebruikers en onderzoekers elkaar slechts op ad hoc basis. Dit lijken ze soms zelfs te doen in een sfeer van gedogen en persoonlijke interesses, niet omdat de betreffende organisaties daar een strategisch belang aan hechten. Dit strookt niet met de belangen van de betreffende organisaties, zoals deze uit deze interviews naar voren zijn gekomen. Dit wordt deels verklaard door het imago van “pseudowetenschap” dat momenteel aan leugendetectie kleeft.

De uitdagingen in dit onderzoeksveld zijn groot. Een van de belangrijkste randvoorwaarden om deze op te lossen is de beschikbaarheid van validatieomgevingen –inclusief van testdata– die voldoende representatief zijn voor de praktijk, of zelfs onderdeel zijn van de praktijk. Daarbij moet onder ogen worden gezien dat resultaten bij de ene veiligheidsorganisatie, door de complexiteit van het onderwerp, niet vanzelfsprekend ook bij de andere veiligheidsorganisatie van toegevoegde waarde hoeven te zijn.

5.4 Aanbevelingen

In dit onderzoek zijn behoeftes geïdentificeerd van relevante organisaties in de publieke en private sector. Een aantal van deze behoeftes kunnen worden vervuld door de toepassing van recente ontwikkelingen. Andere behoeftes vereisen aanvullend onderzoek of de doorontwikkeling van technologie of methodiek. Op basis van ons onderzoek doen wij de volgende aanbevelingen aan de wet- en regelgevende overheid, potentiële publieke en private gebruikers van leugendetectie, en onderzoekinstellingen en universiteiten. Deze aanbevelingen kunnen dienen als strategische onderzoeksagenda.

5.4.1 *Aanbevelingen aan de wet- en regelgevende overheid:*

1. **Ontwikkel *privacy-by-design* richtlijnen:** Het principe van *privacy-by-design* stelt dat privacy-belangen vanaf de eerste ontwikkelingen gedurende de gehele levensduur van een systeem worden meegenomen. Gegeven de aard van de gegevens die worden gebruikt bij leugendetectietesten en de impact die de toepassing van leugendetectie kan hebben op het leven van mensen, is het verstandig om daar een aantal duidelijke richtlijnen voor op te stellen en dit te doen per toepassingsgebied.
2. **Herzie wet- en regelgeving:** Voor toepassing in de praktijk van leugendetectie kan aanpassing nodig zijn van wet- en regelgeving. In de Amerikaanse rechtszaal is het resultaat op een leugendetectie-test toelaatbaar als bewijs. Vanuit de Nederlandse justitiële hoek wordt terughoudend gereageerd op het gebruik van leugendetectie. Een verdachte hoeft niet mee te werken aan zijn eigen veroordeling. De verdachte hoeft ter zitting niet de waarheid te spreken. Leugendetectie resultaten gelden bovendien niet als bewijs in de Nederlandse rechtszaal. Als obstakel wordt de onzekerheidsmarge genoemd, veroorzaakt door de lage accuraatheid en betrouwbaarheid. Een hogere accuraatheid en betrouwbaarheid van nieuwe methoden kunnen aanleiding zijn om relevante wetgeving te herzien.

5.4.2 *Aanbevelingen aan potentiële publieke en private gebruikers van leugendetectie:*

3. **Investeer in detectie van oprechte verklaringen:** In bepaalde context kan het detecteren van oprechte en betrouwbare verklaringen meer nut hebben dan het detecteren van leugens en onbetrouwbare verklaringen.

Investerings in deze toepassingen kunnen bovendien bijdragen aan een meer positief beeld van leugendetectie door de maatschappij. Een voorbeeld is het snelle baan-principe voor betrouwbare personen op een luchthaven. Daarmee kunnen schaarse middelen gericht worden ingezet op de overige groep.

4. **Wees transparant:** De maatschappelijke acceptatie van leugendetectie is beperkt, en wordt sterk beïnvloed door hoe de media het in beeld brengt. Houd dan dus rekening bij de inzet van leugendetectie met weerstand in de maatschappij. Deze is mogelijk gebaseerd op onjuiste of verouderde informatie. Gebruik leugendetectie – of de detectie van terechte verklaringen – dus zorgvuldig. Besteed daarnaast aandacht aan zorgvuldige en transparante communicatie, waaronder ook een heldere beschrijving van wat de technologie precies wel en niet doet, en wat daarvan de consequenties zijn voor de personen die er mee in aanraking komen.
5. **Zorg dat de toepassing past bij de context:** Zorg dat de leugendetectiemethode past bij de context waarin het wordt gebruikt. Dat betekent dat in de context van online aangiften en meldingen mogelijk een andere leugen-detectiemethode dient te worden gebruikt dan in verhoorsituaties.
6. **Hinder mensen niet:** Voor een aantal toepassingen – zoals screening – is het belangrijk om op afstand leugens te kunnen detecteren. Maar zelfs in meer gecontroleerde omgevingen, zoals in een verhoorkamer, is het gemakkelijker en minder bedreigend om leugendetectie *non-intrusive* te kunnen uitvoeren. Het op afstand meten kan bijvoorbeeld met camera's en automatische video-analyse technieken.
7. **Stel richtlijnen en protocollen op en train gebruikers:** Het opstellen van richtlijnen, protocollen en trainingen helpt gebruikers in hun begrip van de methode en wat de resultaten juist wel en juist niet betekenen. Daarnaast moet er duidelijkheid zijn over de beperkingen en de mogelijkheden van leugendetectie, met het oog op het gebruik van de resultaten.
8. **Herzie verhoorhandboeken:** In verhoorhandboeken komen veel van de leugendetectie- of leugenvermindering-inzichten in het geheel niet aan bod. Het opnemen van recente ontwikkelingen in verhoorhandboeken kan helpen om de kloof tussen wetenschap en praktijk te dichten.
9. **Test de gevoeligheid van methoden voor tegenmaatregelen:** Test hoe gevoelig de huidige methoden voor leugendetectie zijn voor manipulaties (dat wil zeggen het gebruik van counter measures door kwaadwilligen). Denk na over mogelijkheden om dit te voorkomen, bijvoorbeeld via de inzet van gecombineerde methoden (zie ook aanbeveling #11).

5.4.3 *Aanbevelingen aan onderzoekinstellingen en universiteiten:*

10. **Zorg voor betere disseminatie van onderzoeksresultaten:** Resultaten van onderzoek zouden beter verspreid kunnen worden. Het toegankelijker maken van onderzoeksresultaten voor de praktijk kan bijvoorbeeld door het schrijven van opiniestukken of populair wetenschappelijke artikelen, maar ook door presentaties bij stakeholders. Daarnaast kunnen er workshops, congressen en evenementen worden georganiseerd waarop resultaten kunnen worden gedeeld.
11. **Combineer verschillende technieken en methoden:** Combineer verschillende technieken en methoden tot een toepassing-specifieke leugendetectiemethode. Non-verbale, paraverbale, verbale en eventueel

fysiologische metingen kunnen gecombineerd worden om samen een accuratere betrouwbaarheidsbepaling te kunnen doen. Voor verdachten is het bovendien gemakkelijker om één kenmerk te misleiden dan meerdere. Deceptie-onderzoekers kijken nu vaak naar geïsoleerde leugenindicatoren en technieken, maar voor de praktijk is het nuttiger om deze gefragmenteerde onderzoeksresultaten te combineren tot een optimaal functionerende methode die moeilijk te misleiden is met een zo hoog mogelijke detectie-accuraatheid.

12. **Valideer onderzoek in de praktijk:** Test gecombineerde en context-specifieke leugendetectiemethoden altijd eerst in de praktijk, met de juiste doelgroep, in een realistische omgeving, ingepast in een verhoormethode en met consequenties. Om dit te bereiken zal er allereerst een meer gestructureerde samenwerking tussen wetenschap en praktijk moeten worden opgezet. Vervolgens zal er een ecologisch valide testomgeving moeten worden ontworpen (field lab) waarmee op grote schaal data kan worden verzameld en gedeeld. Evaluatie en terugkoppeling zijn essentieel in dit proces. Hierdoor kan de praktische toepasbaarheid van leugendetectie op den duur worden vergroot.
13. **Gebruik technologie om prestaties te verbeteren:** Mensen blijken niet zo goed te zijn in het herkennen van leugens. En hoewel trainingen op het gebied van verhoormethoden effectief blijken te zijn, is dit in mindere mate het geval voor trainingen gericht op het herkennen van leugenachtig gedrag. Daarnaast blijken mensen systematische vooroordelen te hebben en subjectieve keuzes te maken. Het gebruik van sensoren en technologie wordt aanbevolen omdat leugendetectie hiermee objectiever kan worden uitgevoerd en omdat de accurateid wordt verhoogd.
14. **Onderzoek toepassingen van een individuele baseline.** Mensen verschillen in de manier waarop zij zich gedragen. Om de toepasbaarheid van leugendetectie te vergroten, moet de techniek in staat zijn om uitspraken te doen over het betrouwbaarheidsgehalte van een uitspraak van één, vaak onbekend, individu. Om gedragsverschillen tussen leugens en waarheden te identificeren voor deze ene individu kan het vaststellen van een baseline van gedrag daarom nuttig zijn. Dit is echter lastig gebleken omdat gedrag door verschillende factoren wordt beïnvloed (zie bv. Buller & Burgoon, 1996; Vrij, 2008). Onderzoek naar het vaststellen van een relevante baseline zou de toepasbaarheid van leugendetectie in de praktijk kunnen vergroten.
15. **Onderzoek de toepassing van leugendetectie in verhoormethoden:** Er zijn diverse niet-technische oplossingen die het gemakkelijker maken om leugens te detecteren tijdens verhoor, bijvoorbeeld door het strategisch aanbieden van bewijs of door het verhogen van de cognitieve belasting. In Nederland wordt op de Politieacademie bijvoorbeeld onderwezen in de Standaard Verhoorstrategie, een verhoormethode die zich richt op het 'omsingelen' van de mogelijke uitvluchten van de verdachte (Van Amelsvoort, Rispens, & Grolman, 2015). Door de verklaring van de verdachte te vergelijken met eerdere verklaringen en technische bewijsmiddelen kunnen onjuistheden en leugens achterhaald worden. Met deze en andere verhoormethoden worden echter niet alle onjuistheden en leugens achterhaald, wat een belemmering kan vormen voor de waarheidsvinden. Meer onderzoek naar het verhogen van de effectiviteit van verhoormethoden en het combineren van verhoormethoden met leugendetectie is daarom wenselijk.
16. **'Voorkomen is beter dan genezen':** Morele en religieuze reminders en cognitieve belasting kunnen ervoor zorgen dat iemand zich eerlijker gedraagt.

Een vertaling is nodig van deze kennis naar de praktijk. Hoe kan deze kennis worden toegepast, bijvoorbeeld in een verhoorsituatie, ter voorkoming van fraude, of in het digitale domein?

6 Conclusie

Deze studie heeft verkend hoe leugendetectie effectief kan worden toegepast door veiligheidsprofessionals in de publieke en private sector. Hiertoe zijn actuele ontwikkelingen op het gebied van leugendetectie bekeken. Ook is onderzocht de mogelijkheid van toepassing van deze ontwikkelingen in relevante domeinen. Door het voeren van interviews met woordvoerders van veiligheidsdiensten, inlichtingendiensten, relevante ministeries en verzekeraars is een beeld ontstaan van de huidige situatie, behoeften, obstakels, relevante toepassingsscenario's en toekomstige implementatievormen van leugendetectie.

Het afgelopen decennium hebben verschillende wetenschappelijke ontwikkelingen plaatsgevonden die de betrouwbaarheid van leugendetectie of de praktische toepasbaarheid kunnen verhogen. De hogere betrouwbaarheid en praktische toepasbaarheid is mogelijk gemaakt door technologische ontwikkelingen, zoals automatische leugendetectie en real-time analyse. Ook niet-technische innovaties op het gebied van methoden hebben bijgedragen aan de hogere betrouwbaarheid en praktische toepasbaarheid, zoals door het verhogen van de cognitieve belasting tijdens een verhoor of het strategisch inzetten van bewijs.

De huidige praktijksituatie op het gebied van leugendetectie zoals in kaart gebracht via de interviews, wordt gekenschetst door verschillende meningen en ervaringen op het gebied van leugendetectie. De meerderheid van de geïnterviewden was niet op de hoogte van recente ontwikkelingen op het gebied van leugendetectie. Wat verder opviel, is dat wet- en regelgeving de toepassing van leugendetectie in de huidige praktijk soms ronduit in de weg staan. Bijvoorbeeld voor de toepassing als bewijs in de rechtszaal. Een verdachte hoeft namelijk niet mee te werken aan zijn eigen veroordeling, wat er in de praktijk op neer komt dat een verdachte zich mag beroepen op het zwijgrecht of zelfs een leugenachtige verklaring af mag leggen. Dit in tegenstelling tot getuigen en getuigendeskundigen die wel de waarheid moeten spreken in de rechtszaal. De gestructureerde aanwezigheid van een advocaat bij verhoren sinds 1 maart 2016 kan het toepassen van leugendetectie ook tijdens verhoor lastiger maken aangezien advocaten soms hun cliënten adviseren in het gebruik van tegenmaatregelen die de accuraatheid van een leugendetectiemethode kunnen aantasten. Naast wettelijke kaders zijn ook ethische bezwaren genoemd die mogelijk kleven aan het gebruik van leugendetectie in de praktijk, zoals het proportionaliteitsbeginsel: de mate van inbreuk op het individueel belang moet proportioneel zijn ten opzichte van het beoogde legitieme doel van de genomen maatregel. Vooral bij heimelijke leugendetectie en het gebruik in een ongecontroleerde setting kan de privacy van individuele burgers in geding zijn.

Het beeld komt naar voren dat private partijen, zoals banken en verzekeraars, verder zijn in de toepassing van leugendetectie dan de publieke partijen. Verzekeringsmaatschappijen zetten leugendetectiemethoden in voor screeningdoeleinden om te bepalen of een claim verder onderzocht moet worden. Hiermee worden financiële besparingen gerealiseerd. Voor publieke partijen ontbreekt nu echter vaak de financiële prikkel om leugendetectie te gebruiken. Het is bovendien veelal geen beleid. De leugendetectiemethoden die worden toegepast, worden ook niet altijd als zodanig herkend, bijvoorbeeld door het strategisch inzetten van bewijs als verhoormethode.

De polygraaf, hoewel bekend, wordt veelal niet gebruikt vanwege een lage accuraatheid, een te hoge hoeveelheid valse alarmen en omdat het resultaat niet goed bruikbaar of toelaatbaar zou zijn in de praktijk, zoals in de rechtszaal. Er zijn pilots gedraaid met leugendetectiemethoden die minder valse alarmen kennen, zoals de schuldige kennis test (CIT), maar die bleken in de huidige vorm niet goed toepasbaar in de praktijk.

In de interviews is ook gesproken over kansen voor de praktijk die volgen uit de nieuwe mogelijkheden op het gebied van leugendetectie. Uit de interviews komen verschillende toepassingsgebieden naar voren, zoals betrouwbaarheidsbepalingen in bedrijfscontext, zowel bij de wervings- en selectieprocedure als bij het detecteren van insider threat. Hoewel leugendetectie soms al ingezet wordt in een fraudecontext, zou dit op grotere schaal of in andere contexten kunnen, zoals bij het aanvragen van uitkeringen, visa en voor het indienen van verzekeringsclaims en belastingaangifte. In de publieke sector zou leugendetectie ingezet kunnen worden voor het screenen van passagiers in de burgerluchtvaart, van binnenkomende asielzoekers of bijvoorbeeld bij het in- en uitreizen van jihadisten. Daarnaast kan leugendetectie ingezet worden tijdens het onderzoeksproces van de politie of het OM, bijvoorbeeld als tactische of sturingsinformatie. Tijdens de interviews werd aangegeven dat er een grote behoefte is aan een betrouwbaarheidsindicatie aan de voorkant van het proces. Hoe bepaal je of je een melding serieus moet nemen? Welke getuigen zijn belangrijker, en hoe betrouwbaar is een getuigenverklaring, hierbij rekening houdend dat als een verklaring onjuist blijkt te zijn, dit per ongeluk of expres gedaan kan zijn. Als laatste werd ook genoemd dat leugendetectie ingezet kan worden als trainingstool en voor testdoeleinden, bijvoorbeeld in een operationele situatie (dat wil zeggen undercover gaan) om te verifiëren of iemand goed genoeg in zijn verhaal zit.

Concrete technieken en methoden zijn echter momenteel veelal niet voorhanden. Het belang van waarheidsvinding en het kunnen identificeren van onschuldige mensen, net als het identificeren van leugens, staat echter bij bijna alle geïnterviewden buiten kijf. Hierbij moet wel rekening worden gehouden met het feit dat leugendetectie wel aan kan geven dat bepaalde informatie niet waar is, maar het vertelt je nog niet wat dan wel de waarheid is. Daarnaast moet er rekening gehouden worden met de faalbaarheid van leugendetectiesystemen wat zal betekenen dat er altijd mensen ten onrechte worden geïdentificeerd als leugenaars. Daarom vond de praktijk juist een positieve framing van leugendetectie interessant die gericht is op het identificeren van mensen die niets te verbergen hebben, in plaats van het (soms onterecht) identificeren van leugenaars. Deze aanpak verkleint de kans op maatschappelijke weerstand en vergroot dus de kans dat leugendetectie gebruikt mag worden in de praktijk. Een voorbeeld hiervan is bijvoorbeeld het *fast lane* concept in de context van aviation security. Iedereen moet door een security check heen, maar als jij als eerlijk uit de bus komt, mag jij er sneller doorheen. Zo word je beloond voor goed gedrag, in plaats van gestraft voor slecht gedrag, rekening houdend met een hoog aantal onterecht gestraften (i.e., loos alarmen). Uit eerder onderzoek is echter gebleken dat onder de huidige voorwaarden, het fast lane concept nog niet toepasbaar is in de Nederlandse burgerluchtvaart.

Een belangrijke bevinding is dat de relevantie van leugendetectie door een complex samenspel van verschillende factoren wordt bepaald. Er is niet één techniek – of een combinatie van technieken – die het beste aansluit op de behoeftes van alle partijen, nu en in de toekomst. Om te bepalen welk type leugendetectie relevant is, moeten zowel de modaliteit (dat wil zeggen, face-to-face, telefonisch, op basis van geschreven tekst door de persoon zelf, of op basis van geschreven tekst door een ander zoals een rapportage) als het type interactie (dat wil zeggen, met of zonder interactie); (openlijk vs. heimelijk), het type sensor (camera vs. EEG, mens vs. technologie, real-time feedback vs. achteraf feedback, invasief vs. op afstand meten) en de toepassingscontext (dat wil zeggen, luchthaven, politieverhoren, intake van vluchtelingen, bewaken & beveiligen, verzekeringen, sollicitatiegesprek) meegenomen worden. Deze informatie geeft een inzicht in welke methodes en technieken bijvoorbeeld in verschillende scenario's toegepast kunnen worden. Bijvoorbeeld bij een online ingediende (belasting)aangifte of verzekeringsclaim volstaat een leugendetectie techniek op basis van door de persoon zelf geschreven tekst. Hierbij kan gekeken worden naar woordgebruik en het type details dat wordt genoemd. Bij een interview met een getuige of verdachte in een verhoorkamer kan daarnaast ook gebruik gemaakt worden van leugendetectie op basis van paraverbaal en non-verbaal gedrag, en van fysiologische reacties. Als dit interview op straat plaatsvindt is er een mobielsensor platform, zoals een bodycam met warmtecamera's en eye-tracking apparatuur, nodig om eenzelfde meting te kunnen doen.

Volgens de geïnterviewden ligt de prioriteit bij ontwikkelingen die kunnen bijdragen aan het verhogen van de accuraatheid, zoals een geïntegreerde leugendetectiemethode, het verlagen van de invasiviteit (bijvoorbeeld door metingen op afstand), en het uitvoerig testen van protocollen in zowel het lab als de praktijk. Als leugendetectie op grote schaal in de praktijk zou worden toegepast moet heel duidelijk zijn hoe het werkt, wat de uitkomsten betekenen en wat de foutenmarge betekent. De geïnterviewden zijn het er dan ook over eens dat, ongeacht het type leugendetectie, de interpretatie van de resultaten niet ambigu mag zijn. Het moet voor elke gebruiker direct duidelijk zijn hoe de resultaten dienen te worden geïnterpreteerd. Ook moet het duidelijk zijn in hoeverre de leugendetectiemethode bestand is tegen manipulaties, zeker nu een advocaat aanwezig is bij het verhoor die zijn cliënt hierin kan adviseren. Om een leugendetectiemethode weerbaarder te maken is het ook mogelijk om, in plaats van de verschillende type leugen-indicatoren los van elkaar te bestuderen, een multimodale leugendetectiemethode te gebruiken. Hierbij worden non-verbale, paraverbale, verbale en eventueel fysiologische metingen gecombineerd om samen een accuratere betrouwbaarheidsbepaling te kunnen doen. Deze multimodale aanpak is waarschijnlijk het meest succesvol wanneer deze uitgevoerd wordt met behulp van meerdere sensoren en technieken. Verschillende geïnterviewden zagen het voordeel van een multimodale leugendetectiemethode en gaven aan dat het ontwikkelen van een betrouwbare variant prioriteit heeft boven enkelvoudige technieken.

Naast een behoefte aan het detecteren van oneerlijk gedrag bleek ook uit de interviews dat er interesse is om oneerlijk gedrag te voorkomen. Uit wetenschappelijk onderzoek is bekend dat morele en religieuze reminders en cognitieve belasting ervoor kunnen zorgen dat iemand zich eerlijker gedraagt.

Verschillende geïnterviewden zagen kansen om deze methodes in te zetten ter ondersteuning van hun dagelijkse werk. Dit zou kunnen worden toegepast in een verzekeringscontext, maar zou ook relevant kunnen zijn in een interview setting, of bijvoorbeeld voor het indienen van aangiften en claims, het aanvragen van uitkeringen en het doen 112-meldingen.

7 Referenties

- Aamodt, M. G., & Custer, H. (2006). Who can best catch a liar? A meta-analysis of individual differences in detecting deception. *Forensic Examiner, 15*, 6-11.
- Abouelenien, M., Mihalcea, R., & Burzo, M. (2015). Trimodal Analysis of Deceptive Behavior. *Proceedings of the 2015 ACM on Workshop on Multimodal Deception Detection*, 9-13.
- Abouelenien, M., Pérez-Rosas, V., Mihalcea, R., & Burzo, M. (2014). Deception Detection Using a Multimodal Approach. *Proceedings of the 16th International Conference on Multimodal Interaction*, 58-65.
- Ben-Shakhar, G., & Elaad, E. (2003). The Validity of Psychophysiological Detection of Information With the Guilty Knowledge Test: A Meta-Analytic Review. *Journal of Applied Psychology, 88*, 131-151.
- Bethlem, T., & Casparie, S. (2008). Gezocht: de Waarheid. Nieuwe ontwikkelingen op het gebied van leugendetectie. Rapportage Politie Amsterdam-Amstelland.
- Bogaard, G., Meijer, E. H., Vrij, A., & Merckelbach, H. (2016). Scientific Content Analysis (SCAN) Cannot Distinguish Between Truthful and Fabricated Accounts of a Negative Event. *Frontiers in Psychology, 7*, Article 243.
- Bond, C. F. Jr., & DePaulo, B. M. (2008). Individual Differences in Judging Deception: Accuracy and Bias. *Psychological Bulletin, 134*, 477-492.
- Bond, C. F., & DePaulo, B. M. (2006). Accuracy of deception judgements. *Personality and Social Psychology Review, 10*, 214-234.
- Bull, R., Baron, H., Gudjonsson, G., Hampson, S., Rippon, G., & Vrij, A. (2004). A review of the current scientific status and fields of application of Polygraphic Deception Detection. *Final report from The British Psychological Society Working Party*.
- Buller, D. B., & Burgoon, J. K. (1996). Interpersonal deception theory. *Communication Theory, 6*, 203-242.
- Counterintelligence Field Activity, Department of Defense (2004). Federal Psychophysiological Detection of Deception: Examiner Handbook.
- Decepticon 2015: International Conference on Deceptive Behavior. Cambridge, UK. <http://2015.decepticon.academy>
- DePaulo, B. M., Lindsay, J. L., Malone, B. E., Muhlenbruck, L., Charlton, K., & Cooper, H. (2003). Cues to deception. *Psychological Bulletin, 129*, 74-118.
- Derrick, D. C., Meservy, T. O., Jenkins, J. L., Burgoon, J. K., & Nunamaker, J. F. Jr. (2013). Detecting deceptive chat-based communication using typing behavior and message cues. *ACM transactions on management information systems, 4*, Article 9.
- Desai, S., & Kouchaki, M. (2016). Moral symbols: A necklace of garlic against unethical requests. *Academy of Management*, online pre-print.
- Ekman, P. (1989). Why lies fail and what behaviours betray a lie. In J. C. Yuille (Ed.), *Credibility assessment* (pp. 71-82). Dordrecht, the Netherlands: Kluwer.
- Ganis, G., Rosenfeld, J. P., Meixner, J., Kievit, R. A., & Schendan, H. E. (2011). Lying in the scanner: Covert countermeasures disrupt deception detection by functional magnetic resonance imaging. *NeuroImage, 55*, 312-319.
- Hartwig & Bond Jr., C. F. (2011). Why Do Lie-Catchers Fail? A Lens Model Meta-Analysis of Human Lie Judgments. *Psychological Bulletin, 137*, 643-659.
- Hartwig, M., Granhag, P.A., Strömwall, L. A. & Andersson, L. O. (2004). Suspicious minds: Criminals' ability to detect deception. *Psychology, Crime and Law, 10*, 83-95.

- Hauch, V., Blandón-Gitlin, I., Masip, J., & Sporer, S. L. (2015). Are Computers Effective Lie Detectors? A Meta-Analysis of Linguistic Cues to Deception. *Personality and Social Psychology Review, 19*, 307-342.
- Hauch, V., Sporer, S. L., Michael, S. W., & Meissner, C. A. (2016). Does Training Improve the Detection of Deception? A Meta-Analysis. *Communication Research, 43*, 283-343.
- Hurley, C. M., Griffin, D. J., & Stefanone, M. A. (2014). Who Told You That? Uncovering the Source of Believed Cues to Deception. *International Journal of Psychological Studies, 6*, 19-32.
- Iacono, W. G. (2008). Effective Policing: Understanding How Polygraph Tests Work and Are Used. *Criminal Justice and Behavior, 35*, 1295-1308.
- Inbau, F., Reid, J., Buckley, J., & Jayne, B. (2011). *Criminal Interrogation and Confessions*. Jones & Bartlett Publishers.
- Kassin, S. M. (2012). Paradigm shift in the study of human lie-detection: Bridging the gap between science and practice. *Journal of Applied Research in Memory and Cognition 1*, 118–119.
- Korthals Altes, W. F. (2014). Stop het liegen. *Ivoren Toga*. Toegankelijk op: <http://ivorentoga.nl/archieven/2591>
- Langleben, D. D., Hakun, J. G., Seelig, D., Wang, A. L., Ruparel, K., Bilker, W. B., Gur, R. C. (2016). Polygraphy and functional magnetic resonance imaging in lie detection: a controlled blind comparison using the concealed information test. *The Journal of Clinical Psychiatry*, page numbers not yet available.
- Leal, S., Vrij, A., Warmelink, L., Vernham, Z., & Fisher, R. P. (2015). You cannot hide your telephone lies: Providing a model statement as an aid to detect deception in insurance telephone calls. *Legal and Criminological Psychology, 20*, 129-146.
- Levine, T. R., Park, H. S., & McCornack, S. A. (1999). Accuracy in detecting truths and lies: Documenting the “veracity effect”. *Communication Monographs, 66*, 125-144.
- May, L., & Granhag, P. A. (2016). Using the Scharff-technique to elicit information: How to effectively establish the “illusion of knowing it all”? *The European Journal of Psychology Applied to Legal Context*.
- Mazar, N., Amir, O., & Ariely, D. (2008). The Dishonesty of Honest People: A Theory of Self-Concept Maintenance. *Journal of Marketing Research, 45*, 633-644.
- Meijer, E. H., Bente, G., Ben-Shakhar, G., & Schumacher, A. (2013). Detecting concealed information from groups using a dynamic questioning approach: simultaneous skin conductance measurement and immediate feedback. *Frontiers in Psychology, 4*, article 68.
- Meijer, E.H., & Merckelbach, H. (2008). Leugendetectie: oude waarheden en nieuwe technologie. *Justitiële Verkenningen, 34*, 42-53.
- Meijer, E. H., Smulders, F. T. Y., & Merckelbach, H. L. G. J. (2010). Extracting Concealed Information from Groups. *Journal of Forensic Sciences, 55*, 1607-1609.
- Meissner, C. A., & Kassin, S. M. (2002). “He’s guilty!”: Investigator Bias in Judgments of Truth and Deception. *Law and Human Behavior, 26*, 469-480.
- Meixner, J. B., & Rosenfeld, J. P. (2011). A mock terrorism application of the P300-based concealed information test. *Psychophysiology, 48*, 149–154.
- Meservy, T. O., Jensen, M. L., Kruse, J., Burgoon, J. K., Nunamaker, J. Jr., Twitchell, D. P., Tsechpenakis, G., & Metaxas, D. N. (2005). Deception

- Detection through Automatic, Unobtrusive Analysis of Nonverbal Behavior. *IEEE Intelligent Systems*, 20, 36-43.
- Morley, N. J., Ball, L. J., & Ormerod, T.C. (2006). How the detection of insurance fraud succeeds and fails. *Psychology, Crime & Law*, 12, 163-180.
- National Research Council (2003). *The polygraph and lie detection; committee to review the scientific evidence on the polygraph*. Division of behavioral and social sciences and education. Washington (DC), The National Academic Press, 2003.
- Park, K. K., Suk, H. W., Hwang, H., Lee, J-H. (2013). A functional analysis of deception detection of a mock crime using infrared thermal imaging and the Concealed Information Test. *Frontiers in Human Neuroscience*. 7, article 70
- Perez-Rosas, V., Abouelenien, M., Mihalcea, R., & Burzo, M. (2015). Deception Detection using Real-life Trial Data. *ICMI '15 Proceedings of the 2015 ACM on International Conference on Multimodal Interaction*, 59-66.
- Plasman, P. (2014). Stop het liegen (niet). *Ivoren Toga*. Toegankelijk op: <http://ivorentoga.nl/archieven/2659>
- Pollina, D. A., Dollins, A. B., Senter, S. M., Brown, T. E., Pavlidis, I., Levine, J. A., & Ryan, A. H. (2006). Facial Skin Surface Temperature Changes During a "Concealed Information" Test. *Annals of Biomedical Engineering*, 34, 1182-1189.
- Poppe, R., Van Der Zee, S., Heylen, D., & Taylor, P. J. (2014). AMAB: Automated measurement and analysis of body motion. *Behavior Research Methods*, 46, 625-633.
- Seymour, T. L., Baker, C. A., & Gaunt, J. T. (2013). Combining blink, pupil, and response time measures in a concealed knowledge test. *Frontiers in Psychology*, 3, 1-15.
- Shu, L. L., Mazar, N., Gino, F., Ariely, D., & Bazerman, M. H. (2012). Signing at the beginning makes ethics salient and decreases dishonest self-reports in comparison to signing at the end. *PNAS*, 109, 15197-15200.
- Soronchinski, M., Hartwig, M., Osborne, J., Wilkins, E., Marsh, J., Kazakov, D., Granhag, P. A. (2014). Interviewing to Detect Deception: When to Disclose the Evidence? *Journal of Police and Criminal Psychology*, 29, 87-94.
- Taylor, R., & Hick, R. F. (2007). Believed cues to deception: Judgements in self-generated serious and trivial situations. *Legal and Criminological Psychology*, 12, 321-332.
- TNO. (2014). *Trends Transities TNO – Strategisch plan 2015 – 2018*. TNO.
- Van Amelsvoort, A., Rispens, I., & Grolman, H. (2015). *Handleiding verhoor* (6de editie). Amsterdam: Stapel & De Koning.
- Van der Zee, S., Poppe, R., Taylor, P. J., & Anderson, R. (2015). To freeze or not to freeze: A motion-capture approach to detecting deception. *Conference Proceedings of the Rapid Screening Technologies, Deception Detection and Credibility Assessment Symposium, 48th HICSS* (5-8 January, 2015).
- Van der Zee, S., Van der Kleij, R., Van Rest, J., Bouma, H. (2016). *Ontwikkelingen in leugendetectie*. Security Management, 26 - 29.
- Van Pel, B., Verhagen, B., & Wijn, R. (2012). Predictive profiling of proactief beveiligen: Security questioning & prikkelen. *Security Management*, 9, 40-43.
- Van Rest, J., Everts, M., Van Rijn, M., & Van Paassen, R. (2012). Het ontwerp van privacy by design. *Privacy & Identiteit*.
- Van Rest, J., Hasberg, M.-P., Lousberg, M., Meijer, G.-J., Van der Kleij, R., Wijn, R., & Van der Jagt, O. (2015). *Challenges of transforming to risk-based aviation security*. TNO.

- Van Rest, J., Roelofs, M., & Van der Kleij, R. (2014). Gebruiken van kennis over afwijkend gedrag. *Security Management*, 9, 28-30.
- Van 't Veer, A. E., Stel, M., & van Beest, I. (2014). Limited capacity to lie: Cognitive load interferes with being dishonest. *Judgment and Decision Making*, 9, 199-206.
- Verschuere, B. J., Ben-Shakar, G., & Meijer, E. H. (2011). *Memory detection: Theory and application of the concealed information test*. Cambridge: Cambridge University Press.
- Verschuere, B., Crombez, G., De Grootte, T., & Rosseel, Y. (2010). Detecting concealed information with reaction times: Validity and comparison with the polygraph. *Applied Cognitive Psychology*, 23, 1-11.
- Verzekeren.net (2013). Steeds meer valse claims bij verzekeringen. Toegankelijk op: <http://www.verzekeren.net/nieuws/valse-claims-verzekeringen/>
- Verzekeringen.com (2014). Strengere aanpak tegen fraude met verzekeringen door valse claims. Toegankelijk op: <https://www.verzekeringen.com/nieuws/strengere-aanpak-tegen-fraude-verzekeringen-valse-claims>
- Volkskrant, 16 augustus 1996. Deskundigen verwerpen 'Zaanse verhoormethode'. Te vinden op: <http://www.volkskrant.nl/archief/deskundigen-verwerpen-zaanse-verhoormethode~a418209/>
- Vredevelde, A., Van Koppen, P. J., & Granhag, P. A. (2014). The Inconsistent Suspect: A Systematic Review of Different Types of Consistency in Truth Tellers and Liars. In R. Bull (Ed), *Investigative Interviewing*, (pp 183-207). New York, US: Springer Science + Business Media.
- Vrij, A. (2015). Verbal Lie Detection Tools- Statement Validity Analysis, Reality Monitoring and Scientific Content Analysis. In: P.A. Granhag, A. Vrij, and B. Verschuere (Eds.), *Detecting Deception: Current Challenges and Cognitive Approaches*, John Wiley & Sons.
- Vrij, A. (2008). *Detecting lies and deceit: Pitfalls and opportunities*. Chichester, England: Wiley.
- Vrij, A. (2004) Why professionals fail to catch liars and how they can improve. *Legal and Criminological Psychology*, 9, 159-183
- Vrij, A., et al. (2012). Collective interviewing of suspects. *Journal of Applied Research in Memory and Cognition*, 1, 41-44.
- Vrij, A., & Granhag, P. A. (2014). Eliciting Information and Detecting Lies in Intelligence Interviewing: An Overview Of Recent Research. *Applied Cognitive Psychology*, 28, 936-944.
- Vrij, A., Granhag, A. P., & Porter, S. (2010). Pitfalls and opportunities in nonverbal and verbal lie detection. *Psychological Science in the Public Interest*, 11, 89-121.
- Vrij, A., Jundi, S., Hope, L., Hillman, J., Gahr, E., Leal, S., Warmelink, L., Mann, S., Vernham, Z., & Granhag, P.A. (2012). Collective interviewing of suspects. *Journal of Applied Research in Memory and Cognition*, 1, 41-44.
- Vrij, A., Leal, S., Granhag, P. A., Mann, S., Fisher, R. P., Hillman, J., & Sperry, K. (2009). Outsmarting the liars: The benefit of asking unanticipated questions. *Law and Human Behaviour*, 33, 159-166.
- Vrij, A., & Mann, S. (2005). Police use of nonverbal behaviour as indicators of deception. In R. E. Riggio, & R. S. Feldman (Eds.), *Applications of nonverbal communication* (pp. 63-94). Mahwah, NJ: Lawrence Erlbaum Associates.
- Vrij, A., Mann, S., Fisher, R., Leal, S., Milne, B., & Bull, R. (2008). Increasing cognitive load to facilitate lie detection: The benefit of recalling an event in reverse order. *Law and Human Behaviour*, 32, 253-265.

- Vrij, A., Mann, S., Leal, S., & Fisher, R. (2010): 'Look into my eyes': can an instruction to maintain eye contact facilitate lie detection?, *Psychology, Crime & Law*, 16, 327-348.
- Vrij, A., Mann, S., Vernham, Z., & Brankaert, F. (2015). Translating theory into practice: Evaluating a cognitive lie detection training workshop. *Journal of Applied Research in Memory and Cognition*, 4, 110-120.
- Zuckerman, M., DePaulo, B. M., & Rosenthal, R. (1981). Verbal and nonverbal communication of deception. In L. Berkowitz (Ed.), *Advances in experimental social psychology*, volume 14, (pp. 1-57). New York, US: Academic Press.

A Interview protocol

S4S WP2.2 Waarheidsvinding: interview protocol

Datum

Naam geïnterviewde(n)

Organisatie geïnterviewde(n)

Naam interviewer(s)

Introductie tot het doel van het interview

TNO ziet interessante ontwikkelingen met het oog op leugendetentie ter bevordering van waarheidsvinding. We willen achterhalen of er behoefte is in Nederland aan leugendetectie, met het oog op het richten van onze kennisontwikkelingen.

Wat is het verschil tussen waarheidsvinding en leugendetectie?

Onder waarheidsvinding verstaan wij het bepalen van het waarheidsgehalte van een bepaald statement. Dit statement kan mondeling gemaakt zijn, maar bijvoorbeeld ook geschreven. Een statement is leugenachtig als deze opzettelijk gemaakt wordt door een individu om een onjuist beeld te creëren in de ander. Dit onjuiste beeld kan geschetst worden door foutieve informatie aan te bieden, of door het verzwijgen van relevante informatie. Een statement is alleen leugenachtig als de verteller, op het moment van het maken van het statement, zelf doorheeft dat dit statement een onjuist beeld geeft. Anders is het gewoon slechte communicatie of had de verteller zelf een verkeerd beeld van de situatie. Waarheidsvinding is dan ook breder dan leugendetectie, omdat het naast leugenachtige verklaringen ook onjuiste informatie moet identificeren.

Waarom met u in gesprek?

Wij spreken met verschillende partijen die mogelijk interesse hebben in leugendetectie ter bevordering van waarheidsvinding. U vertegenwoordigt zo'n partij. Het doel van deze gesprekken is om erachter te komen waar in de praktijk wel en geen behoefte aan is. Er wordt namelijk veel leugenunderzoek uitgevoerd, maar dat is niet allemaal één-op-één toepasbaar in de praktijk, terwijl dit bij uitstek een onderwerp met hoge praktische relevantie is. Er worden momenteel wel allemaal interessante leugendetectiemethodes¹⁰ ontworpen en verbeterd, en wij zijn benieuwd welke hiervan voor u mogelijk interessant zijn en hoe die verder ontwikkeld moeten worden om ook praktisch nut te hebben.

Wat is het doel van dit onderzoek door TNO?

¹⁰ Voor het bepalen van het waarheidsgehalte van een statement kunnen drie soorten indicatoren gebruikt worden, namelijk verbale en non-verbale gedragingen en fysiologische reacties. Deze kunnen tegenwoordig ook automatisch worden gemeten, zodat het mogelijk is om direct (in real-time) een beslissing te nemen over het waarheidsgehalte van een statement. Er wordt zowel onderzoek gedaan naar het verkennen van het waarheidsgehalte van statements over activiteiten in het verleden (handig voor bijvoorbeeld politie interviews), als voor geplande activiteiten en intenties (handig voor screening).

Het doel van onze kennisinvestering is enerzijds om de huidige kennisbasis bij TNO op het onderwerp te bundelen en te versterken, en anderzijds om veiligheidsorganisaties en bedrijven in positie te brengen om te profiteren van deze kennis. De vraag die ligt achter dit onderzoek is op welke manier leugendetectie effectief kan worden toegepast door veiligheidsprofessionals, zoals bijvoorbeeld politiediensten, ter bevordering van de maatschappelijke veiligheid?

Doel van het interview?

Het doel van dit interview is om samen met u te inventariseren of, en zo ja, waarom en hoe organisaties gebruik maken van waarheidsvinding; of daarbij gebruik wordt gemaakt van ondersteunende sensoren en technieken; met welk resultaat; wat de gewenste en toekomstige situatie is m.b.t. waarheidsvinding; en welke stappen moeten worden gedaan om de gewenste situatie te bereiken. Het doel van dit gesprek is niet om uw werk te evalueren. We hopen met dit gesprek juist een beter beeld te krijgen van de huidige en toekomstige behoeftes aan en mogelijkheden van waarheidsvinding in de praktijk.

A. Gesprekspartner achtergrond:

- Achtergrond gesprekspartner.
- Rol / functie in de organisatie.

B. Huidige situatie leugendetectie:

- Wat is het doel / missie van uw organisatie?
- Hoe past waarheidsvinding in het bereiken van die doelstelling?
- Wat zijn uw ideeën over waarheidsvinding en leugendetectie?
- Waar haalt u uw kennis over waarheidsvinding vandaan? (Opleiding en training, onderzoek, media, etc.)
- Maakt uw organisatie momenteel gebruik van waarheidsvinding of leugendetectie?
 - Zo nee:
 - Waarom niet?
 - Welke obstakels zijn er?
 - Zo ja:
 - Waarom?
 - Op welke manier?
 - In welke omstandigheden wordt er gebruik van gemaakt?
 - Waar moet je dan rekening mee houden?
 - Met welk effect?
 - Hoe wordt de effectiviteit vastgesteld? (Worden meerdere mensen ingezet? Worden andere technieken gebruikt? Hoe kan aanvullend bewijs worden verkregen?)
- Maakt uw organisatie gebruik van sensoren en technieken om leugens te detecteren?
 - Zo nee:
 - Waarom niet?
 - Welke obstakels zijn er?
 - Zo ja:
 - Welke sensoren en technieken worden gebruikt?
 - Waarom?

- In welke omstandigheden wordt er gebruik van gemaakt?
 - Waar moet je dan rekening mee houden?
 - Met welk effect?
 - Hoe wordt de effectiviteit vastgesteld? (Worden meerdere mensen ingezet? Worden andere technieken gebruikt? Hoe kan aanvullend bewijs worden verkregen?)
 - Zijn er duidelijke operationele eindgebruikers (functionarissen) aan te wijzen binnen uw organisatie die (mede) aan waarheidsvinding doen?
 - Zijn er leugendetectiemethoden (zoals sensoren en technieken) bekend die bewust niet worden gebruikt?
 - Zo ja:
 - Waarom?
 - Zijn er relevante beleidskaders waarmee rekening moet worden gehouden bij dit onderwerp?
 - Zo ja:
 - Is daar mogelijk spanning mee?
- 17.

C. Behoeftebepaling

- In een ideale situatie, hoe zou uw organisatie gebruik maken van leugendetectie? (Denk ook aan: verhoor, screening, toegangscontrole, interview, insider threat, stelen van de baas, surveilleren op straat, op OV knooppunt, etc.)
 - a. In welke scenario's?
 - b. Wat voor type leugendetectie zou dan relevant zijn?
 - c. Heeft u hiervoor de juiste kennis al in huis? (verhoorders, ICT, hardware/software, etc.)
 - d. Indien afwijkend met huidig gebruik: Welke obstakels ondervindt uw organisatie met betrekking tot gebruik van leugendetectie? (Onderzoek of er verkeerde assumpties tussen zitten)
- Zijn er ook scenario's waarin leugendetectie niet bruikbaar is?
- Welke nadelen heeft leugendetectie (met sensoren) naar uw beleving?
- Zijn er inherente kwetsbaarheden (e.g., gebruik van countermeasures) aan (technische) leugendetectie?
 - a. Is er tegen te trainen?
 - b. Wat als de tegenstander weet hoe het werkt?
- Welke technieken zijn naar jullie mening wel mogelijk en welke technieken zijn niet mogelijk?
 - a. Wel mogelijk
 1. Omdat
 - b. Niet mogelijk
 1. Omdat

D. Toekomstige situatie met betrekking tot waarheidsvinding:

- Hoe denkt u dat leugendetectie verbeterd zou kunnen worden?
 - Welke toepassingen ziet u?
 - Waarom?
- Wat denkt u dat er bereikt moet worden voordat leugendetectie (op grote schaal) ingezet kan worden in uw organisatie?
 - Welke stappen zouden hiervoor gezet moeten worden?

- Wat zou betrouwbare leugendetectie betekenen voor uw organisatie/manier van werken?
 - De vorm van leugendetectie kan in verschillende vormen worden geïmplementeerd. Soms is er volledige controle over de omgeving, en soms is er geen controle over de omgeving. Welk van de onderstaande generieke implementatievormen en randvoorwaarden zouden kunnen passen bij uw organisatie? Waarom wel/niet?
 - Verhoorkamer (bijvoorbeeld verdachtenverhoor)
 - Video-opnames tijdens het gesprek
 - Gesprek bij een balie (bijvoorbeeld op vliegveld)
 - Sluis, poortjes of kiosk (bijvoorbeeld security filter)
 - Tele-presence of video conference (bijvoorbeeld interview op afstand)
 - Volledig gecontroleerd (bijvoorbeeld verhoorkamer met polygraaf)
 - Semi-gecontroleerd (bijvoorbeeld toegangscontrole)
 - Ongecontroleerd (bijvoorbeeld toezicht openbare ruimte)
 - Heimelijk
 - Welke ontwikkelingen hebben prioriteit? (e.g., accuraatheid omhoog, goedkoper, makkelijker toe te passen, etc.)
 - Vindt u dat er sprake van urgentie op dit onderwerp?
 - Zo nee:
 - Waarom niet?
 - Zo ja:
 - Waarom?
 - Staat u er voor open om met ons te verkennen of we er samen een versnelling in kunnen aanbrengen?
 - Welke andere organisaties denkt u dat hiervoor nodig zijn?
 - Wat denkt u dat er bereikt moet worden voordat leugendetectie (op grote schaal) ingezet kan worden ter bevordering van een veilige samenleving?
 - De vraag is op welke manier waarheidsvinding effectief kan worden toegepast door politiediensten, beveiligingsdiensten en particuliere beveiligers. Hoe denkt u dat TNO bij kan dragen aan een effectieve toepassing van waarheidsvinding in de praktijk?
- 18.

E. Response op recente ontwikkelingen:

Wij hebben zojuist een overzichtsartikel geschreven voor Security Management waarin we de recente ontwikkelingen op het gebied van leugendetectie beschrijven (geef exemplaar). Veelbelovende ontwikkelingen zijn:

1. Actieve rol van de interviewer.
2. Automatisch meten van leugenachtig gedrag (multimodaal en in real-time).
3. Liegen over kwade intenties.
4. Daderkennis identificatie.

Dankzij methodologische en technologische ontwikkelingen is de accuraatheid van leugendetectie omhoog gegaan (rond 70-75%, oftewel driekwart), en is de praktische toepasbaarheid verhoogd (in real-time meten en feedback, ook over intenties en het vaststellen van daderkennis en intel).

- Was u op de hoogte van deze recente ontwikkelingen en resultaten?
- Als de huidige wetenschappelijke resultaten (bijvoorbeeld 75%) ook in de praktijk worden gehaald, zou dat dan bruikbaar zijn voor u?

- Zo nee:
 - Waarom niet?
- Zo ja:
 - Op welke manier?
 - Welke ontwikkeling heeft dit mogelijk gemaakt?

F. Het voorkomen van leugens:

- Denkt u dat er ook een afschrikwekkende werking uit kan gaan van leugendetectie?
 - Uit onderzoek weten we dat het naast het detecteren van oneerlijk gedrag ook mogelijk is om actief het gedrag van mensen te beïnvloeden en mensen eerlijker te maken door ofwel het stimuleren van eerlijk gedrag, of door het ontmoedigen van oneerlijk gedrag. Mensen liegen bijvoorbeeld minder als ze bang zijn om gepakt te worden, als ze een hoge cognitieve belasting ervaren, of wanneer zij voor het invullen van een formulier een verklaring tekenen dat zij alle informatie juist zullen invullen. Was u hiervan op de hoogte?
 - Houdt uw organisatie zich hier momenteel mee bezig?
 - Zou het eventueel interessant zijn voor uw organisatie?

G. Afsluiting gesprek

- Zijn er verder nog opmerkingen die u wilt maken over waarheidsvinding?
- Heeft u nog vragen over waarheidsvinding waarop u een antwoord zou willen hebben?
- Is uw beeld van waarheidsvinding tijdens het gesprek gewijzigd?
- Welke vervolgstappen zijn volgens u zinvol?
- Waardeert u het als we u blijven betrekken?
- Afronding:
 - Bedank voor het gesprek.
 - Geef aan dat ze het uitgewerkte interview mogen inzien om eventuele fouten te corrigeren.
 - De uitgeschreven interviews worden niet publiek gemaakt, maar dienen als de basis voor een groepsanalyse.
 - Het uiteindelijke rapport wordt openbaar toegankelijk. Resultaten worden op groepsniveau gepresenteerd. Indien gewenst kunnen we uw organisatie niet expliciet benoemen.