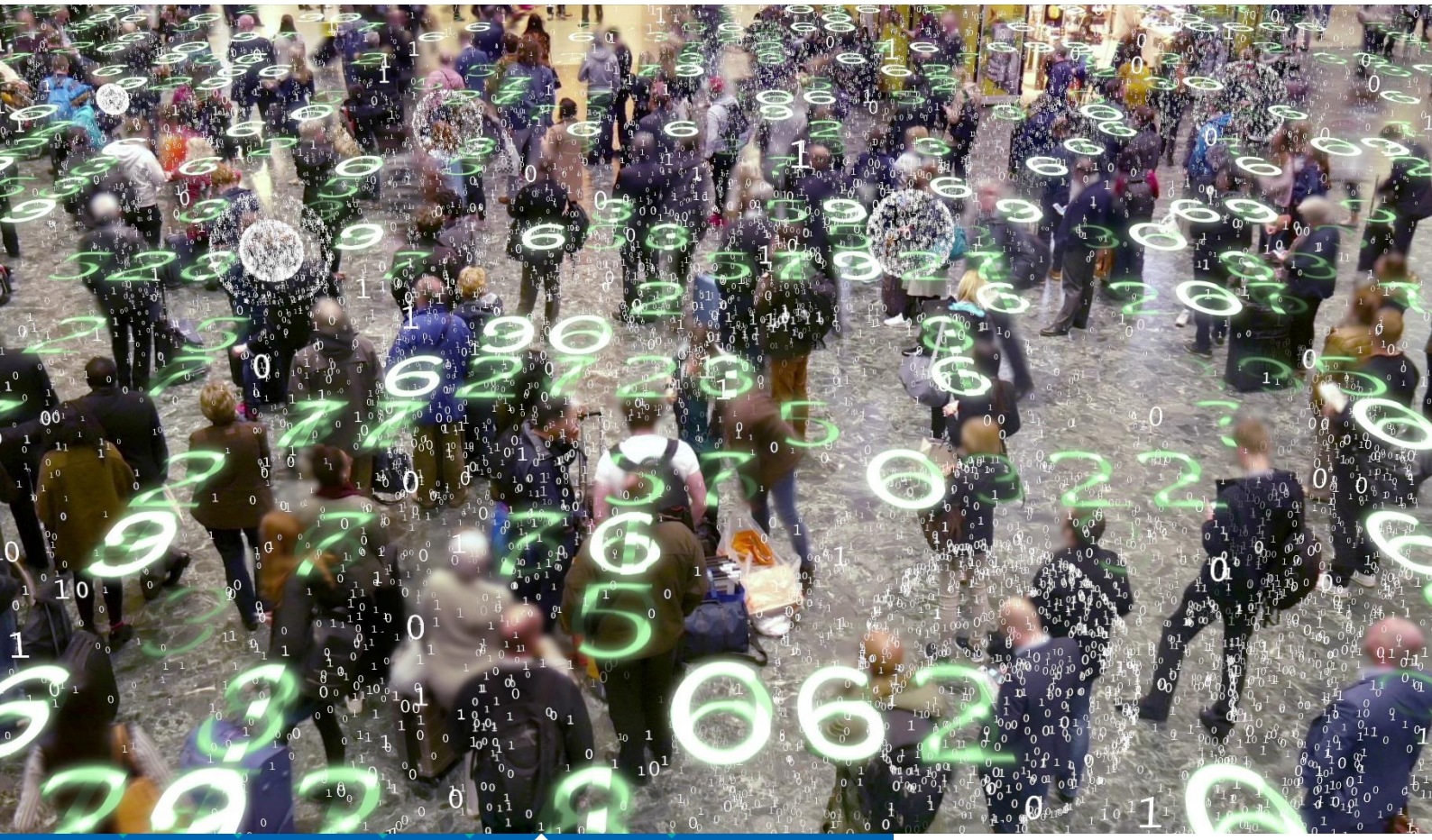
Level-Up!

Kennis voor politiewerk in een digitale samenleving

Auteurs: Jurjen Jansen, Thijs van Valkengoed, Sander Veenstra & Wouter Stol
Onderzoeksgroep Cybersafety



NHL STENDEN hogeschool

POLITIE Politieacademie

Level-Up!

Kennis voor politiewerk in een digitale samenleving

Datum	Juli 2020
Versie	1.1
Uitgever	Cybersafety Research Group
	NHL Stenden Hogeschool / Politieacademie
	www.cybersciencecenter.nl
Vraagarticulatie	Theo van der Plas (portefeuillehouder digitalisering en cybercrime)
Opdrachtgever / subsidieverstrekker	Richard Nijeboer (Platform Intensivering Aanpak Cybercrime [PIAC])
Publicatietitel	Level-Up! Kennis voor politiewerk in een digitale samenleving
Publicatiejaar	2020
Publicatietype	Onderzoeksrapport
Auteurs	Dr. Jurjen Jansen Thijs van Valkengoed BBa Sander Veenstra MSc Prof dr. Wouter Stol
Met dank aan de klankbordgroep	Barry Bout (Districtsrecherche, Oost-Nederland) Gerard van Cuijk (TDO, Zeeland-West-Brabant) Theo Derksen (Politieacademie) Fred Ootes (Teamleider Cybercrime Team, Noord-Holland) Robert Weedage (TDO, Oost-Nederland) Lourens Witteveen (Projectleider Cybercrime, Noord-Holland) Anoniem (Projectleider Cybercrime)

Samenvatting

In dit onderzoek staat kennis van politiemensen aangaande digitale aspecten van politiewerk centraal. Het doel van dit onderzoek is om de politie te helpen ontwikkelen tot een organisatie die optimaal functioneert in een gedigitaliseerde samenleving. Meer specifiek wordt met dit onderzoek duidelijk gemaakt op welke digitale aspecten van politiewerk en bij welke groepen politiemensen sprake is van een kennistekort, en wordt inzichtelijk gemaakt hoe het kennistekort aangepakt kan worden. De centrale vraag in dit onderzoek luidt: Wat is het kennisniveau van politiemensen inzake digitale aspecten van politiewerk en hoe kan een eventueel kennistekort worden bestreden? De functies van politiemensen zijn in dit onderzoek als volgt afgebakend: (1) intake en service, (2) politiemensen in uniformdienst (hierna: blauw), (3) basisteamrecherche, (4) districtsrecherche, en (5) regionale recherche.

Hierna komen vijf onderwerpen aan bod (gebaseerd op de geformuleerde deelvragen): (1) de organisatie van intake en afhandeling van digitale criminaliteit, (2) welke kennis de politiemensen in de vijf functiegroepen zouden moeten hebben, (3) in hoeverre politiemensen aan de kennisvereisten 'voldoen', (4) bij welke groepen politiemensen een eventueel kennistekort zich met name voordoet, en (5) hoe een kennistekort bestreden kan worden.

(1) Organisatie van intake en afhandeling van digitale criminaliteit

Ten eerste hebben we gekeken hoe de intake en afhandeling van digitale criminaliteit en van criminaliteit met een digitale component is georganiseerd binnen de politieorganisatie. Vanuit de literatuur zijn de volgende fasen in het opsporingsproces hierbij te onderscheiden: (1) kennis nemen van een misdrijf (via melding, aangifte of politiestraatwerk), (2) initieel onderzoek (informatie veiligstellen), (3) evaluatie opsporingsonderzoek (beslissen om wel of niet over te gaan tot opsporingsonderzoek), (4) waarheidsvinding (identificeren van verdachten en vergaren van zowel belastend als ontlastend materiaal), (5) evaluatie bewijs (beslissen om opsporingsonderzoek [vroegtijdig] te beëindigen of aanvullend onderzoek te verrichten), en (6) afronding onderzoek (strafrechtelijk dossier opmaken en overdragen aan het Openbaar Ministerie). Vanuit de praktijk wordt een soortgelijke beschrijving gegeven: (1) intake (input), (2) casescreening (beoordelen input), (3) voorbereiden, (4) uitvoering (verrichten van opsporingsonderzoek), en (5) afronding.

Hoe concreet invulling wordt gegeven aan het proces van intake en afhandeling en wie daarbij betrokken zijn is afhankelijk van het type criminaliteit (veel voorkomende criminaliteit, high impact crime, ondermijning) en het soort aanpak (incidentgerichte aanpak, probleemgerichte aanpak, programmatische aanpak). Uit praktijksignalen wordt duidelijk dat intake doorgaans het vertrekpunt vormt voor het opsporingsproces. In de praktijk wordt vooral gewerkt volgens een incidentgerichte en in mindere mate volgens de probleemgerichte of programmatische benadering.

De wijze waarop de intake is georganiseerd kan verschillen per eenheid, maar het overgrote deel van de intakewerkzaamheden wordt verricht door speciaal daarvoor aangestelde medewerkers intake en service. In sommige eenheden wordt ook blauw belast met het opnemen van meldingen en aangiften op het bureau. Na de intake wordt via casescreening de zaak al dan niet toegewezen aan een van de rechercheniveaus.

(2) Welke kennis politiemensen in de vijf functiegroepen moeten hebben

Ten tweede hebben we onderzocht welke kennis de eerder onderscheiden vijf groepen politiemensen zouden moeten hebben inzake digitale aspecten van politiewerk. Per functiegroep zijn daarvoor kennisnormen ontwikkeld. Deze kennisnormen zijn in onderstaande tabellen 1-2 samengevat. We gebruiken de term 'competentie' om ordening aan te brengen. Hoewel vaardigheden ook onder competenties vallen, hebben we die in dit onderzoek niet gemeten.

Tabel 1: Kennisnormen voor intake en service

Competentie
Het kennen van de standaardprocedure voor het opnemen van aangifte
Verschijningsvormen van digitale criminaliteit kennen en weten te herkennen op basis van praktijksignalen
De strafbaarstelling van cyberdelicten weten vast te stellen
Weten dat verbanden bestaan tussen cyberdelicten en weten hoe die verbanden te toetsen tijdens het opnemen van de aangifte
Kennis hebben van het inventariseren van opsporingsrelevante digitale sporen
Weten hoe te adviseren over het veiligstellen van digitale sporen
Kennis hebben van voor 'cyber'intake ontwikkelde handreikingen en op basis daarvan weten hoe de aangever te adviseren over preventie en/of vervolgstappen

Tabel 2: Kennisnormen voor blauw en recherchegroepen

Competentie
Het kennen van de fasen in het optreden op de PD
Het kennen van het juridisch kader voor het optreden op de PD
Het kennen en weten uit te voeren van de eerste maatregelen
Weten hoe onderzoek op de PD te verrichten
Het kennen van de specifieke basisstappen in het geval van een PD (met digitale sporen)
Weten hoe relevante digitale gegevensdragers te herkennen op een digitaal PD
Weten hoe op forensisch technisch verantwoorde wijze relevante digitale gegevensdragers kunnen worden veiliggesteld
Weten hoe onderzoek rondom de PD te verrichten
Informatiegaring op internet (zie Tabel 6.3)
Kennis van communicatie met burgers via internet*
Weten hoe met het oog op opsporing de waarde van de aangedragen informatie te beoordelen†
Weten hoe planmatig/systematisch aan een opsporingsonderzoek gewerkt kan worden†
Weten hoe opsporingsonderzoek te verrichten†
Kennis van specifieke opsporingskennis en -vaardigheden in een gedigitaliseerde samenleving†
Weten hoe onderzoeksbevindingen te analyseren en duiden†
Weten hoe de waarde van bewijs te beoordelen†
Weten hoe eigen onderzoekshandelingen vast te leggen†

**Alleen geldend voor blauw, †alleen geldend voor recherche groepen.*

Daarnaast is een functiegroepoverstijgende kennisnorm onderscheiden, namelijk voor informatiegaring op internet, zie Tabel 3.

Tabel 3: Kennisnormen voor informatiegaring op internet (functiegroepoverstijgend)

Competentie
Kennis van internet en sporen (bijv. Intel, OSINT, IP-adres, en afbreukrisico's)
Kennis van het juridisch kader (bijv. wetsartikelen die aangeven welke informatie je wel/niet mag opzoeken)
Kennis van monitoren en identificeren (bijv. zinvolle zoektermen en gebruik H.U.I.B.)
Kennis van tools (bijv. iRN en Google)
Kennis van bronnen (bijv. welk type informatie te vinden is op diverse internetbronnen en sociale media)
Kennis van taal / jargon / thema's (bijv. bekend met taalgebruik van persoon/groep die wordt onderzocht)

(3) In hoeverre politiemensen aan de kennisvereisten voldoen

Ten derde hebben we gekeken hoe politiemensen op kennisvragen die zijn gebaseerd op bovenstaande normen scoren c.q. welke kennis zij in de praktijk hebben van digitale aspecten van politiewerk. De resultaten zijn gebaseerd op vragenlijstdata van 402 politiemensen (zelfrapportage), verdeeld over de vijf groepen, en worden hierna in zes thema's behandeld (hierna A t/m F). We gaan hierbij alleen in op de belangrijkste resultaten. Voor de leesbaarheid spreken we soms van 'hoge' en 'lage' scores. Dit betekent dat respectievelijk hoger of lager is gescoord dan het gemiddelde. We geven geen oordeel over in hoeverre de kennis toereikend is.

A. Het eerste thema is digitale criminaliteit. Wat opvalt is dat zowel de kennis van als het herkennen van strafbare gedragingen laag is. Dit betekent dat in het opleidingen- en cursusaanbod aandacht besteed moeten worden aan kennis over hoe strafbare gedragingen te herkennen.

B. Het tweede thema is optreden op en rondom een plaats delict (PD). Aspecten die opvallen zijn (a) een gebrek aan kennis van risico's met betrekking tot het vernietigen of besmetten van digitale sporen en (b) een gebrek aan kennis van basisprocedures voor het veiligstellen van digitale gegevensdragers. Ook op het aspect 'toekennen van prioriteit aan welke gegevensdragers belangrijk zijn om als eerste veilig te stellen' wordt laag gescoord. Dit zijn aspecten waar de politieorganisatie op moet inzetten qua kennisvergroting. Daarentegen wordt over het algemeen hoog gescoord op aspecten die te maken hebben met handelingen op een PD en bewijsvoering. Gegevensdragers die mogelijk op een PD aanwezig zijn, worden herkend wanneer het algemene, veelvoorkomende gegevensdragers betreft. Nieuwe, of zelf geknutselde gegevensdragers worden minder herkend. Bij het aantreffen van onbekende gegevensdragers geeft bijna iedereen aan een specialist in te schakelen, wat wordt gezien als een zeer belangrijke handeling.

C. Het derde thema is digitale sporen. Zaken die hier bijzonder de aandacht verdienen zijn: (i) duidelijk maken welke digitale sporen van belang zijn voor opsporingsonderzoek (o.a. toepassing van de zeven gouden W's [wie, wat, waar, waarmee, welke wijze, wanneer, waarom] en herkenning digitale sporen); (ii) duidelijk maken welke digitale sporen kunnen worden uitgelezen; (iii) instructie

geven voor het opstellen van uitleesvragen en inzichtelijk maken welke eisen daaraan zijn verbonden; en (iv) instructie geven over het gebruik van softwarepakketten voor de analyse van digitale sporen en het vastleggen van bevindingen daarover.

Op algemene digitale termen scoren politiemensen over de hele linie hoog, maar specifieke termen als clearweb en deepweb worden niet altijd herkend. Op de kennisvragen over interceptie is ook hoog gescoord. Wat betreft het gebruik van digitale hulpmiddelen is de kennis laag. Slechts twee op de vijf politiemensen zijn bekend met de webapps van de Politieacademie.

D. Het vierde thema is informatiegaring op internet dat uit een aantal subthema's is opgebouwd. Aspecten die binnen het subthema 'vorderen van gegevens' laag scoren en dus aandacht verdienen zijn bekendheid met: OSINT, Intel, verantwoordelijkheden voor informatiegaring op internet, IPv4- en IPv6-adressen. Het subthema 'juridische implicaties voor het zoeken naar informatie op internet' moet in zijn geheel worden versterkt binnen de politieorganisatie. De kennis hieromtrent is over het algemeen aan de lage kant. Daarnaast scoren respondenten laag op kennis van zoektermen en van wat zoekoperatoren zijn. Ook scoort men laag op kennis van welke internetbronnen voor welke informatie geraadpleegd kunnen worden. Wel scoren respondenten over het algemeen redelijk hoog op 'tools' voor het zoeken van informatie op internet.

E. Het vijfde thema is onlinecommunicatie met burgers. Daarop wordt laag gescoord. Respondenten weten over het algemeen niet van welke internettoepassingen burgers gebruik maken en weten ook niet goed welke toepassingen zij kunnen gebruiken om in contact te treden met burgers.

F. Tot slot zijn kennisvragen gesteld binnen het zesde thema 'aangiften van cybercrime'. Over het algemeen zijn de scores hoog. Op enkele onderdelen kan worden geïnvesteerd om dit thema verder te versterken. Specifiek gaat het daarbij om kennis van welke sporen geïnventariseerd kunnen worden voor het vullen van aangiften en hoe veelvoorkomende digitale sporen veiliggesteld kunnen worden. Daarnaast geldt dat medewerkers intake en service in slechts de helft van de gevallen kennis hebben van de zeven W's om de relevantie van digitale sporen te bepalen en scoren laag op wat vluchtige gegevens zijn. Drie op de tien politiemensen zijn onvoldoende op de hoogte van hoe digitale sporen aangeleverd kunnen worden.

(4) Groepen politiemensen waarbij een eventueel kennistekort zich met name voordoet

Ten vierde hebben we gekeken in hoeverre het kennistekort verder gespecificeerd kan worden, namelijk door naar functiegroepniveau en achtergrondkenmerken van politiemensen te kijken. Deze kenmerken betreffen geslacht, leeftijd, wel of geen opleiding/cursus gevolgd op cybergebied en de mate van ervaring met cyberzaken. De analyses voor geslacht en leeftijd toonden weinig significante verschillen en worden hier derhalve buiten beschouwing gelaten. Wel verdient het expliciet aandacht

dat kennistekort niet generatiegebonden is. Hierna gaan we nader in op (A) de vijf functiegroepen, (B) politiemensen met of zonder een opleiding/cursus aangaande digitale criminaliteit, en (C) de mate van ervaring van politiemensen met cyberzaken.

A. Functiegroepen. Over het algemeen geldt dat de recherchegroepen hoger scoren dan blauw, en intake en service. Binnen de recherchegroepen scoren respondenten van de regionale recherche vaak hoger dan respondenten van de districts- en basisteamrecherche. Wel moet hierbij worden opgemerkt dat de effecten veelal klein of klein tot middelmatig zijn.

In een aantal gevallen waren de effecten sterker. Een van de aanbevelingen is om de basisprocedures voor het veiligstellen van digitale gegevensdragers onder de aandacht te brengen. Hoewel alle functiegroepen hiervan kunnen profiteren laat de analyse op groepsniveau zien dat dit het meest noodzakelijk is voor blauw.

Kennis van vluchtige gegevens versterken werd al geopperd voor de groepen intake en service, en blauw. Een analyse op de recherchegroepen laat echter zien dat dit ook noodzakelijk is voor medewerkers van de basisteamrecherche. Deze drie functiegroepen zijn ook gebaat bij meer kennis over OSINT, Intel, en algemene juridische regels voor het zoeken naar informatie op internet. Analyses op functiegroepen lieten zien dat deze kennis gemiddeld genomen aanwezig is bij politiemensen die werkzaam zijn voor de districts- of regionale recherche. Voor twee juridische regels scoorden echter ook respondenten van de districts- of regionale recherche – hoewel hoger dan de andere groepen – beneden gemiddeld. Het gaat hierbij om kennis van de beslisboom waarmee kan worden bepaald of een onderzoek uitgevoerd mag worden volgens de taakstelling van de politie en de wetsartikelen voor informatiegaring op internet.

Eerder werd de suggestie gedaan voor meer opleiding op het gebied van iRN (Internet Research and Investigation Network). Functiegroepanalyse laat zien dat deze kennis reeds meer dan gemiddeld aanwezig is bij de districts- en regionale recherche. Een kennisimpuls is vooral nodig bij medewerkers intake en service, blauw en basisteamrecherche.

B. Opleiding. De opleiding van politiemensen speelt een rol. Bij 51 vragen/stellingen werden significante verschillen gevonden tussen politiemensen die wel of geen opleiding/cursus hebben gevolgd op het gebied van digitale criminaliteit. In alle gevallen scoorden respondenten die een cursus of opleiding hebben gevolgd gemiddeld hoger.

C. Ervaring. Bij zeven vragen/stellingen werden significante verschillen gevonden betreffende ervaring met cyberzaken. Voor deze resultaten geldt dat hoe meer ervaring, hoe hoger de score.

(5) Hoe een kennistekort bestreden kan worden.

Ten vijfde en laatste, hebben we bekeken in hoeverre kennistekort bestreden kan worden.Het bestrijden van het kennistekort op het gebied van basiskennis is geen eenvoudige opgave. Bepaalde

kennis moet elk politiemens paraat hebben. Denk hierbij bijvoorbeeld aan een aanhouding waarbij politiemensen snel en juist moeten handelen. Hoe meer tijd voorradig is om kennis te bemachtigen, hoe kleiner het aandeel van de politiemensen waarbij deze kennis aanwezig moet zijn. Hierbij kan gedacht worden aan opsporingsonderzoek waarin meer tijd is voor verdieping. Tevens werd geconstateerd dat kennis zowel aanwezig moet zijn bij specialisten als generalisten; al is het maar om effectief met elkaar te kunnen communiceren. Belangrijker dan het hebben van kennis is dat politiemensen weten hoe en waar ze die kennis kunnen halen.

Door geïnterviewde experts worden diverse leermethoden aangehaald om het kennistekort aan te pakken. De meest interessante en effectieve leermethode lijkt het praktijkleren; leren door kennis direct toe te passen in de praktijk. Een belangrijke vereiste hierbij is om óók te reflecteren op dat handelen. Het is daarbij van belang een afweging te maken tussen de effectiviteit van een leermethode en de kosten daarvan. Daarnaast kan – waar mogelijk – de techniek ondersteunen, middels *performance support by design*: ondersteuning door tips vanuit een computerprogramma.

Alles overziend concluderen we dat bij het beantwoorden van de vraag wat het kennisniveau van politiemensen inzake digitale aspecten van politiewerk is, aan de ene kant nieuwe vragen worden opgeroepen en aan de andere kant geconstateerd moet worden dat verbetering in de breedte en diepte noodzakelijk is. Immers, op veel digitale aspecten van politiewerk werd niet hoog gescoord. De kennisnormen – een belangrijke uitkomst van dit onderzoek – kunnen helpen om hierin verbetering aan te brengen, omdat we nu – beter dan voorheen – weten waar de deficits zich voordoen en bij welke groep(en). Het verdient de aandacht dat de kennisnormen tijdelijk van aard zijn. De uitkomsten van dit onderzoek kunnen dan ook worden gezien als een tussenstand. Welke digitale kennis politiewerk vereist, verandert continu. Politiewerk in een gedigitaliseerde samenleving vergt meebewegen. De vraag die dat oproept is hoe dat ‘meebewegen’ in kennis het beste gaat. Ons onderzoek laat enkele mogelijkheden zien.

Ten eerste laat ons onderzoek een positief verband zien tussen het gevolgd hebben van een opleiding/cursus over digitaal en de mate van kennis. De causaliteit is daarmee nog niet bepaald. Ofwel mensen die naar een opleiding gaan, hebben al meer dan gemiddelde kennis omtrent digitaal, ofwel het volgen van een opleiding maakt dat mensen een hoger digitaal kennisniveau hebben. In het laatste geval is te concluderen dat opleiden helpt en kan daarop meer worden geïnvesteerd. Nader (experimenteel) onderzoek kan hierover meer helderheid verschaffen. In het eerste geval is het zo dat politiemensen naar een opleiding worden gestuurd die al meer dan gemiddelde kennis hebben, wat vragen oproept over de opleidingsstrategie.

Opleiden kan op diverse wijzen ingevuld worden. Geïnterviewde experts wezen op *learning on the job.* Die route sluit aan bij de praktijk van alledag en bij hoe politiemensen vaak al leren. In dat

licht is aan te raden om een werksituatie te creëren waarin politiemensen op basis van echte zaken in aanraking komen met 'digitaal' en daaraan werken met collega's met diverse (digitale) expertise. Door het met elkaar te doen ontstaat het leren bijna vanzelf. Belangrijk is wel om dit te faciliteren. Enerzijds door medewerkers de ruimte te geven om (ook) te reflecteren op het handelen (als individu en als groep) alsook door een goed portaal en menselijke ondersteuning te bieden waar kennis te halen is.

Ten tweede wezen experts erop dat politiemensen niet altijd alle benodigde kennis paraat hoeven te hebben, als zij maar op het juiste moment over die kennis kunnen beschikken. Daar zijn reeds oplossingen voor, zoals een *Real Time Intelligence Center*, het beschikbaar hebben van apps, het bevragen van collega's, aandachtvestigingen in de briefing, et cetera. Tegelijk zijn dat oplossingen die niet altijd goed werken. Dit onderzoek laat bijvoorbeeld zien dat politiemensen over de gehele linie niet bekend zijn met de apps van de Politieacademie.

Kennis op het juiste moment en tijdig bij politiemensen krijgen kan tevens door middel van het concept *performance support by design*. Denk bijvoorbeeld aan 'technische' ondersteuning bij het opnemen van aangiften. Op dit gebied is bij ons weten nog weinig ervaring opgedaan. Duidelijk is wel dat de strategie om politiemensen te voorzien van informatie op of vlak voor het moment dat zij die nodig hebben, niet zomaar effectief is. Investeren in het beschikbaar krijgen van kennis, bijvoorbeeld door een portaal, *performance support by design*, en menselijke ondersteuning, is essentieel voor politiemensen om hun weg te vinden in de snel veranderende wereld.

Hiermee hebben we twee strategieën aangeduid voor het vergroten van digitale kennis bij politiemedewerkers. De focus moet liggen op intake en service, blauw en in wat mindere mate op de recherche aan basisteams, maar ook anderen zijn niet uitgeleerd zolang de digitalisering voortgaat. De twee strategieën zijn: (een combinatie van) opleiden (inclusief praktijkleren om ervaring op te doen) en kennismanagement. Elk apart of gecombineerd initiatief dient te worden geëvalueerd, want een bewezen effectieve praktijk (dé oplossing) staat niet zomaar klaar.

Tot slot denken wij dat de Nationale Politie gebaat is bij het ontwikkelen van een *roadmap* met betrekking tot het opleiden van politiemensen. Vanwege de snelle digitale ontwikkelingen is het van belang duidelijk te maken waar de politieorganisatie nu staat en waar ze naar toe moet. Het is daarbij belangrijk om 'digitaal' niet te zien als iets dat plaatsvindt naast regulier politiewerk, maar als een geïntegreerd onderdeel van de dagelijkse praktijk. Immers, de scheidslijn tussen online en offline is veelal niet scherp, maar vloeit in elkaar over. Een andere reden is dat cybercrime, gedigitaliseerde criminaliteit en criminaliteit met een digitale component nu zoveel voorkomen dat het niet alleen aan specialisten kan worden overgelaten.

Inhoudsopgave

1. Inleiding

Op 31 augustus 2015 werd in de Herijkingsnota Nationale Politie bij de politie een kennistekort inzake digitalisering gesignaleerd (Ministerie van Veiligheid en Justitie, 2015). De daaropvolgende 'Contourennota' van 23 november 2015 benadrukte het probleem.[1] De samenleving digitaliseert, maar de politie heeft daarvan te weinig kennis om haar werk goed te doen. Op 19 mei 2016 verscheen een sterkte- en zwakteanalyse over de opsporing (Huisman, Princen, Klerks, & Kop, 2016).[2] Daarin staat onder andere dat het opnemen van aangiften van cyber-gerelateerde zaken alsook de afhandeling van die zaken ronduit ondermaats zijn vanwege een gebrek aan kennis. Die kennis is weliswaar aanwezig bij specialisten, maar ontbreekt in de volle breedte van de organisatie. Dat is een probleem, want de politie bevindt zich wel degelijk in de volle breedte van haar organisatie in een digitale en snel digitaler wordende omgeving. Ieder lid van de organisatie moet dus in zekere mate uit de voeten kunnen met een gedigitaliseerde werkomgeving; er is geen andere optie.

Het kennistekort aangaande 'digitaal' of 'cyber' bestaat al lang (Stol, Van Treeck, & Van der Ven, 1999; Toutenhoofd, Veenstra, Domenie, Leukfeldt, & Stol, 2009) en wordt blijkens de genoemde berichten er niet minder op. Opvallend genoeg is tot op heden nog niet in beeld gebracht wat het kennistekort precies is en waar het zich binnen de politieorganisatie voordoet. Zonder een duidelijk beeld van het kennistekort kan het niet adequaat worden bestreden. Dit onderzoek moet helpen die leemte op te vullen en gerichte verbetering(en) mogelijk te maken. Dit onderzoek beoogt het kennistekort inzichtelijk te maken en op basis daarvan aanbevelingen doen waarmee de politie het kennisniveau gericht kan vergroten.

Leeswijzer

In hoofdstuk 2 wordt de onderzoeksopzet besproken. Hierin staan de doelstelling en onderzoeksvragen centraal en wordt het onderwerp van onderzoek afgebakend. Vervolgens worden de onderzoeksmethoden verantwoord in hoofdstuk 3. In hoofdstuk 4 worden de resultaten gepresenteerd over de intake en organisatie van de afhandeling van digitale criminaliteit en criminaliteit met een digitale component. In hoofdstuk 5 komen de resultaten aangaande de kennisnormen en bijbehorende vragenlijst aan bod. Tevens wordt in dat hoofdstuk ingegaan op mogelijkheden om een kennistekort aan te pakken. De conclusies en daaruit volgende discussie en beperkingen staan centraal in hoofdstuk 6. In hoofdstuk 7 volgt een slotbeschouwing en worden aanbevelingen gepresenteerd inzake het verbeteren van kennis van digitale aspecten van politiewerk.

[1] De 'contourennota' is de bijlage bij de brief van 23 november 2015 van de minister van Veiligheid en Justitie aan de voorzitter van de Tweede Kamer (kenmerk 707191).

[2] Deze sterkte-zwakte analyse is de bijlage bij de brief van 16 mei 2015 van de minister van Veiligheid en Justitie aan de voorzitter van de Tweede Kamer (kenmerk 765465).

2. Onderzoeksopzet

In dit hoofdstuk worden de doelstelling en onderzoeksvragen gepresenteerd. Ook worden de begrippen die centraal staan in het onderzoek toegelicht. Het hoofdstuk start echter met een beschrijving van het onderwerp en de afbakening van het onderzoek.

2.1 Onderwerp en afbakening

Het onderwerp van onderzoek is de kennis van politiemensen inzake digitale aspecten van criminaliteit bij het opnemen van aangiften en het behandelen van zaken. Dit gaat om (a) kennis aangaande digitalisering (bijv. wat is een IP-adres? en wat is een DDoS-aanval?) – en om (b) kennis aangaande de vraag welke (eerstelijns) handelingen de politie kan verrichten in het kader van digitaal opsporen (bijv. waar vraag ik gegevens op over een IP-adres?).

Het onderzoek heeft betrekking op de politie in Nederland en daarbinnen op vijf functiegroepen: medewerkers intake en service (taakgebied opnemen aangiften), blauw (politiemensen in uniformdienst), en tactisch rechercheurs aan basisteams, districten en eenheden.

2.2 Doelstelling

Het doel van dit onderzoek is om de politie te helpen ontwikkelen tot een organisatie die optimaal functioneert in een gedigitaliseerde samenleving. Daartoe moet het onderzoek laten zien op welke plaatsen in de organisatie en/of bij welke groepen medewerkers sprake is van een kennistekort en waaruit dat bestaat. Daarnaast biedt het onderzoek inzicht in methoden om het kennistekort aan te pakken. Het maatschappelijk doel van het onderzoek is bij te dragen aan een veilige samenleving.

2.3 Onderzoeksvragen en kernbegrippen

De centrale vraag in dit onderzoek luidt: Wat is het kennisniveau van politiemensen inzake digitale aspecten van politiewerk en hoe kan een eventueel kennistekort worden bestreden? De centrale onderzoeksvraag werken we als volgt uit in deelvragen:

1. Hoe is de intake en afhandeling van digitale criminaliteit en van criminaliteit met een digitale component georganiseerd?
2. Welke kennis inzake digitale aspecten van politiewerk moeten de eerder onderscheiden vijf groepen politiemensen hebben (de norm)?
3. Welke kennis inzake digitale aspecten van politiewerk hebben de onderscheiden vijf groepen politiemensen (de realiteit)?
4. In hoeverre is er een kennistekort bij de onderscheiden vijf groepen politiemensen en waar doet dit tekort zich eventueel voor?
5. Indien een tekort is vastgesteld, hoe kan dat worden bestreden?

In de hoofd- en deelvragen komen enkele begrippen naar voren die nadere toelichting verdienen. De volgende werken we hierna uit: (a) kennis, (b) kennistekort, (c) politiemensen, (d) digitale aspecten van politiewerk, en (e) digitale criminaliteit en criminaliteit met een digitale component.

Kennis. Het begrip 'kennis' kunnen we in abstracto definiëren als iedere gedachte die, volgens de persoon die die gedachte heeft, iets inhoudt dat waar of echt is (Stol, 1996). Dit onderzoek gaat over politiekennis aangaande digitalisering (waar heb ik mee te maken?) en politiekennis aangaande de vraag welke handelingen de politie kan verrichten in het kader van digitaal opsporen (wat kan ik doen?). We noemen dat respectievelijk materie- en handelingskennis. Materiekennis is een vereiste voor handelingskennis.

Tekort – als in kennistekort. Het tekort is de mate waarin de materie- of handelingskennis van politiemedewerkers niet voldoet aan de eisen die daaraan vanuit goed politiewerk kunnen worden gesteld. Het is dus een normatief begrip. Het onderzoek vereist dus het opstellen van een norm. Die geldt dan voor dit moment en is niet toekomst-vast, want met wat vandaag voldoende kennis omtrent digitalisering is, kan de politie over enige tijd niet meer uit de voeten. Dat laatste is echter geen belemmering om nu een norm te bepalen en vast te stellen waar het kennistekort nu zit en waaruit het nu bestaat.

Politiemensen. We gebruiken de term politiemensen in plaats van politiemedewerkers, omdat politiemensen korter is en vlotter leest. Het onderzoek gaat over (1) politiemensen die de intake verzorgen, (2) politiemensen in uniformdienst (in dit rapport 'blauw' genoemd)[3], (3) tactisch rechercheurs aan basisteams, (4) tactisch rechercheurs aan districten, en (5) tactisch rechercheurs aan eenheden – in totaal vijf functiegroepen.

Digitale aspecten van politiewerk. Politiewerk volgt de ontwikkelingen in de samenleving. Digitale aspecten van de samenleving zijn dus per definitie ook digitale aspecten van politiewerk. Bovendien wordt wel gesteld dat vrijwel ieder klassiek of offline delict inmiddels een digitale component bevat. Daarnaast heeft politiewerk nog digitale aspecten die specifiek zijn voor de politie, zoals kennis van 'digital forensics' en opsporingsbevoegdheden. In verband met politie en digitalisering worden vaak benamingen gebruikt voor nieuwe vormen van criminaliteit, zoals cybercrime, gedigitaliseerde criminaliteit en computercriminaliteit. In dat opzicht hanteren wij de volgende begrippen: (1) 'cybercrime' is elk delict met ICT als middel en doelwit (bijv. hacken en DDoS-aanvallen), (2) 'gedigitaliseerde criminaliteit' is elk delict waarbij ICT van overwegende betekenis is voor de uitvoering ervan, zonder ICT als doelwit (bijv. internetoplichting en cybersmaad), en (3) 'criminaliteit met een digitale component' is elk delict waarbij digitale sporen kunnen bijdragen aan het oplossen ervan (bijv. een gefilmde mishandeling). Dit onderzoek gaat over kennis van (1), (2), én (3).

[3] Politiemensen in uniformdienst worden ook wel aangeduid als gebiedsgebonden politie (GGP).

Digitale criminaliteit en criminaliteit met een digitale component. Om lange formuleringen te vermijden, reserveren we voor cybercrime in combinatie met gedigitaliseerde criminaliteit de term ‘digitale criminaliteit’. ‘Digitale criminaliteit’ bestaat dus deels uit delicten die in het digitale tijdperk zijn ontstaan (cybercrime) en deels uit oude delicten die qua vorm met de digitalisering zijn meegegaan (gedigitaliseerde criminaliteit). Kortom, we kijken naar twee hoofdvormen: ‘digitale criminaliteit’ en ‘criminaliteit met een digitale component’.

3. Methodische verantwoording

In dit hoofdstuk staat de methodische verantwoording centraal: deskresearch (par 3.1), interviews (par. 3.2.), focusgroep (par. 3.3), en online vragenlijst (par. 3.4). Tevens wordt toegelicht hoe de data-analyse heeft plaatsgevonden (par. 3.5). Voor het overzicht is hieronder een methodenmatrix opgenomen (Tabel 3.1) waarin is te zien op welke wijze de methoden zich verhouden tot de deelvragen die zijn geformuleerd in hoofdstuk 2.[4]

Tabel 3.1: Methodenmatrix

Deelvraag	Deskresearch	Interviews	Focusgroep	Vragenlijst
1. Organisatie?	X	X		
2. Norm?	X	X	X	
3. Kennisniveau?	X			X
4. Tekort?	X			X
5. Aanpak?	X	X		

3.1 Deskresearch

Deskresearch heeft bijgedragen aan het beantwoorden van de vraag hoe de intake en afhandeling van digitale criminaliteit is georganiseerd (deelvraag 1), het vaststellen van de kennisnorm (deelvraag 2) en het verkennen van de mogelijkheden om een eventueel kennistekort te bestrijden (deelvraag 5). Daarvoor is gebruik gemaakt van literatuuronderzoek en documentanalyse. Hoe invulling is gegeven aan deze vormen van deskresearch is hierna verantwoord.

Literatuuronderzoek. Voor het literatuuronderzoek is een twee-sporenaanpak gehanteerd. Allereerst is voortgebouwd op eerder onderzoek van de onderzoeksgroep Cybersafety. Van 2012 tot en met 2016 heeft de onderzoeksgroep een drietal handreikingen geschreven voor politiewerk in een digitale samenleving. In 2012 verscheen een handreiking voor het opnemen van aangiften met een digitale component (Leukfeldt e.a., 2012). Die handreiking is drie jaar later in geactualiseerde vorm opnieuw uitgebracht (Leukfeldt, Kentgens, Prins, & Stol, 2015). De inhoud van de handreiking is vertaald naar de tevens voor dit onderzoek geraadpleegde webapp ‘Cybercrime’, die via de website van de politieacademie beschikbaar is. In 2015 verscheen daarnaast een handreiking voor het herkennen en veiligstellen van digitale gegevensdragers op een plaats delict (Zuurveen, Doodeman, Veenstra, & Stol, 2015). Ook die handreiking is vertaald naar een nog steeds beschikbare en ook voor dit onderzoek geraadpleegde webapp ‘Digitale PD’. Tot slot is in 2016 de handreiking voor opsporing in een gedigitaliseerde samenleving gepubliceerd (Veenstra, Zuurveen, Kerstens, & Stol, 2016). Deze

[4] Halverwege het project heeft overdracht van projectleiderschap plaatsgevonden. Onderzoek naar de organisatie van de intake en afhandeling van digitale criminaliteit en van criminaliteit met een digitale component lag in handen van Sander Veenstra (deelvraag 1). Het vervolg – het vaststellen van de kennisnormen, het meten en preciseren van het kennisniveau en aanbevelingen voor verbetering – lag in handen van Jurjen Jansen (deelvragen 3-5). De conceptkennisnorm is in gezamenlijkheid ontwikkeld (deelvraag 2).

handreikingen bieden 'generalisten' – politiemedewerkers zonder specifieke digitale expertise – handvatten bij het opnemen van aangiften, het optreden op een plaats delict en opsporing in een digitale samenleving.

Daarnaast bouwt het onderzoek voort op het onderzoek van Van Valkengoed (2017) naar digitale kennis onder tactisch rechercheurs van de eenheid Amsterdam. In dat onderzoek is inzicht geboden in de kennis waarover rechercheurs zouden moeten beschikken en de kennis waarover rechercheurs daadwerkelijk beschikken. In het kader van het literatuuronderzoek is geput uit voornoemde publicaties en daaraan ten grondslag liggende literatuur.

Ten tweede is via de mediatheek van de Politieacademie en in diverse digitale wetenschappelijke databanken gezocht naar aanvullende literatuur. Specifiek ging het om databases van NHL Stenden Hogeschool, Open Universiteit en Google Scholar. Om gericht naar aanvullende literatuur te zoeken zijn aan de deelvragen ontleende zoektermen gebruikt. Onder andere de volgende zoektermen zijn afzonderlijk en in combinatie gebruikt, zowel in het Nederlands als Engels: *policing, criminal investigation, process, knowledge, skills, digitized, digital, crime, cybercrime*.

In totaal zijn tien boeken opgevraagd en/of geraadpleegd. De zoekslag leverde daarnaast vijftig aanvullende digitale publicaties op. De literatuur werd gescand op relevantie en betrouwbaarheid. Een publicatie werd als relevant aangemerkt wanneer de inhoud ervan bijdroeg aan de beantwoording van de onderzoeksvragen. Om de betrouwbaarheid van publicaties vast te stellen zijn de datum van publicatie, de auteur/organisatie waarvan de publicatie afkomstig is en de eventuele (verantwoording van de) onderzoeksmethodiek meegewogen. Publicaties over de wijze waarop het opsporingsproces is georganiseerd (deelvraag 1) en welke kennis daarvoor van belang is (deelvraag 2) vertonen sterke gelijkenissen. Omdat het saturatiepunt tijdens het literatuuronderzoek reeds was bereikt, is een deel van de publicaties die daarop betrekking had buiten beschouwing gelaten. Publicaties over digitale aspecten van politiewerk waren in mindere mate voorhanden. In de literatuurlijst is weergegeven van welke publicaties uiteindelijk gebruik is gemaakt.

Documentenanalyse. De onderzoekers hadden geen toegang tot de informatie- en bedrijfsprocessensystemen van de politie. In de voorbereidingsfase van het onderzoek is daarom afgesproken dat relevante kennis- en beleidsdocumenten door de opdrachtgever (het PIAC) en de klankbordgroep zouden worden aangeleverd. In de klankbordgroep namen vertegenwoordigers van vier aan het onderzoek deelnemende regionale eenheden zitting.[5] De deelnemende eenheden waren: Midden-Nederland, Noord-Holland, Oost-Nederland en Zeeland-West-Brabant.

[5] De klankbordgroep is tevens ingezet om te reflecteren op de uitkomsten van het onderzoek en de implicaties ervan voor de politiepraktijk. Hoewel dat een bijdrage heeft geleverd aan de interpretatie van bevindingen, zijn niet alle opmerkingen en suggesties van klankbordgroepleden overgenomen. Door vooraf gemaakte afspraken, zijn de onderzoekers in staat gesteld onafhankelijk onderzoek uit te voeren en daarover te publiceren. De opvattingen in dit rapport zijn dus niet noodzakelijkerwijs de opvattingen van de leden van de klankbordgroep.

De opdrachtgever heeft drie documenten aangeleverd: het inrichtingsplan voor de Nationale Politie en een tweetal beschrijvingen over de werking van de digitale platforms en teams digitale opsporing binnen de politie. Deze documentatie droeg met name bij aan de beantwoording van de eerste deelvraag (over de wijze waarop het [digitale] opsporingsproces is ingericht binnen de politie). Vanuit de klankbordgroep is in dat verband één aanvulling toegestuurd: het betrof een regionaal document waarin een voorstel wordt gedaan om de intake en het proces van 'wegen kiezen en monitoren' van cybercrime-zaken binnen een regionale eenheid te verbeteren. Vertegenwoordigers vanuit de overige eenheden gaven aan dat binnen de eenheden die zij vertegenwoordigen over de intake en afhandeling van digitale criminaliteit geen documenten voorhanden zijn. Ook documenten waarin is beschreven welke kennis nodig is om effectief uitvoering te geven aan politiewerk in een gedigitaliseerde samenleving waren niet bij de opdrachtgever en de klankbordgroep bekend.

Daarnaast is voor de documentenanalyse zoveel mogelijk geput uit kennis en documenten die in het kader van eerdere onderzoeken zijn opgedaan, bijvoorbeeld van TRIO Opsporing (2014) en Campman e.a., (2012). Deze documenten droegen bij aan het inzichtelijk maken van de wijze waarop de intake en afhandeling van (digitale) criminaliteit binnen de politie is georganiseerd (deelvraag 1).

Om meer zicht te krijgen op de voor 'digitale aspecten van politiewerk' benodigde kennis (deelvraag 2) is een inventarisatie gemaakt van relevante opleidingen aan de Politieacademie. De Politieacademie biedt zowel basisopleidingen aan voor intake, blauw en recherchemedewerkers als gespecialiseerde opleidingen op het gebied van ´cyber´.[6,7] Hoewel op de website van de Politieacademie een overzicht is opgenomen van het onderwijsaanbod, was specifieke documentatie over de inhoud van opleidingen, trainingen, e-learnings en modules niet inzichtelijk. Om die reden is een overzicht opgesteld van het onderwijsaanbod waarvan het ogenschijnlijk nuttig was om kennis te hebben van de onderliggende opleidingsdocumenten. Het betrof veertien basisopleidingen, -modules en -trainingen voor intake en servicemedewerkers, blauw en de recherche en zeventien specifieke cyber onderwijsprogramma's (zie bijlage I voor een overzicht).

Tot slot is tijdens de interviews (zie par. 3.2) gebleken dat voor onlinegegevensgaring al een landelijke kennisnorm in ontwikkeling was. Om daarop zoveel mogelijk te kunnen aansluiten is die kennisnorm door de politie beschikbaar gesteld en als uitgangspunt genomen voor dit onderzoek. Het gaat daarbij om een groeidocument van januari 2018.

---

[6] Politieacademie (z.d.). *Bijdragen aan beter politiewerk*. Verkregen via: https://www.politieacademie.nl/onderwijs/Pages/politieonderwijs.aspx

[7] Het onderwijs aan de politieacademie is gebaseerd op door de politiepraktijk gevalideerde beroepsprofielen. Daarin is beschreven welke functiegebonden eisen aan politiewerk worden gesteld. De daarvoor benodigde competenties worden op duale wijze aangeleerd: enerzijds door onderwijs te volgen aan de politieacademie en anderzijds door werkervaring op te doen in een van de politie-eenheden. Opleidingsdocumentatie waarin de beroepsprofielen en aan te leren competenties staan beschreven is dus relevant om inzicht te krijgen in de voor politiewerk in een digitale samenleving benodigde kennis.

3.2 Interviews

Tijdens het onderzoek hebben drie interviewreeksen plaatsgevonden. De eerste reeks interviews had tot doel om inzicht te bieden in de wijze waarop de intake en afhandeling van digitale criminaliteit binnen de politie is georganiseerd (deelvraag 1). De tweede reeks interviews heeft bijgedragen aan het in kaart brengen van de kennis die nodig is voor politiewerk in een gedigitaliseerde samenleving (deelvraag 2). Nadat met een vragenlijst het kennisniveau van politiemedewerkers in kaart was gebracht (zie par. 3.4), zijn tot slot expertinterviews afgenomen om zicht te krijgen op mogelijkheden om het digitale kennisniveau binnen de politie te vergroten (deelvraag 5). Iedere interviewreeks diende een ander doel en is daarom anders opgezet en uitgevoerd. Hierna is per reeks verantwoord hoe de interviews zijn verricht.

3.2.1 In kaart brengen van intake en afhandeling

De wijze waarop de intake en afhandeling van strafzaken is georganiseerd kon deels worden ontleend aan literatuuronderzoek en politiedocumentatie. Op papier vastgelegde processen kunnen echter afwijken van de praktijk. Bovendien is het mogelijk dat de wijze waarop het opsporingsproces is georganiseerd per regionale eenheid verschilt. Om zicht te krijgen op de invulling die in de praktijk aan het proces van intake en afhandeling wordt gegeven zijn zodoende interviews verricht.

Voorafgaande aan de interviews is een interviewprotocol ontwikkeld (zie bijlage II). Om vast te stellen over welke digitale kennis politiemedewerkers in het intakeproces, de geüniformeerde dienst en de recherche moeten beschikken was het essentieel om te weten welke rol zij vervullen in het opsporingsproces. De interviews hadden daarom tot doel om zowel het proces van intake en afhandeling, als de rollen van de daarbij betrokken politiemedewerkers in kaart te brengen. Die doelstelling vormde het uitgangspunt bij de ontwikkeling van het interviewprotocol. Verder is bij de totstandkoming van het protocol gebruik gemaakt van inzichten over de intake en afhandeling die tijdens eerder onderzoek zijn opgedaan (zie naast de in sectie 3.1.1 genoemde publicaties: Toutenhoofd e.a. [2009] en Leukfeldt, Veenstra, Domenie, & Stol [2012]).

Gevraagd is naar mogelijkheden voor de politie om kennis te nemen van (potentiële) strafzaken en de wijze waarop het werkaanbod wordt afgehandeld. Daarbij is specifiek doorgevraagd naar het aangifteproces, het proces van ‘casescreening’, de rol van blauw en de rol van de recherche (op de drie onderscheiden niveaus). Steeds is gevraagd in hoeverre verschil bestaat tussen de intake en afhandeling van klassieke ten opzichte van digitale criminaliteit.

Aan het onderzoek namen zoals eerder aangegeven vier eenheden deel. Het doel was om één interview per eenheid te af te nemen. De leden van de klankbordgroep – die ieder een van de deelnemende eenheden vertegenwoordigde – werd daarom gevraagd om geschikte kandidaten aan te leveren. De aangedragen kandidaten zijn vervolgens benaderd en bleken bereid en beschikbaar

voor een interview. Hier volgt het overzicht opgenomen van de kandidaten die we hebben gesproken:

- een beleidsadviseur van de districtsstaf Utrecht (eenheid Midden-Nederland);
- een tactisch coördinator bij een cybercrimeteam (Operationeel Specialist A, eenheid Noord-Holland);
- een medewerker van het team werkvoorbereiding van de Dienst Regionale Recherche (Operationeel Specialist A, eenheid Oost-Nederland);
- een medewerker intake en service bij het regionaal servicecentrum (eenheid Zeeland-West-Brabant).

De interviews (N = 4) zijn telefonisch afgenomen in de periode september-oktober 2017 en duurden gemiddeld 45 minuten. Drie kandidaten merkten tijdens de interviews op niet het gehele proces van intake en afhandeling op detailniveau te kennen. De beleidsadviseur gaf – gezien zijn functie – aan operationele vragen niet op basis van eigen ervaringen te kunnen beantwoorden. De tactisch coördinator van het cybercrimeteam merkte op dat zij beperkt zicht heeft op politieprocessen die zich buiten het cybercrimeteam afspelen. De medewerker intake en service heeft naar eigen zeggen weliswaar zicht op het intakeproces, maar in mindere mate op de rol en werkwijze van de recherche. Kortom, de interviewkandidaten hebben de interviewvragen vanuit hun eigen (functiegebonden) referentiekader beantwoord.

3.2.2 Ontwikkelen kennisnorm

Het doel van de tweede interviewreeks was om de concept-kennisnormen voor intake en service, blauw en recherche te toetsen aan de praktijk en, waar nodig, te optimaliseren. In totaal zijn elf interviews afgenomen. Het aantal interviewkandidaten per functiegroep is gebaseerd op de omvang en complexiteit van de betreffende norm, alsmede op de mate waarin de normen voor die functiegroep op basis van deskresearch al waren uitgekristalliseerd. Eén interview vond plaats met een expert buiten de politieorganisatie, maar die wel over veel politie-ervaring beschikt. Deze had betrekking op de norm voor blauw en recherche.

De norm voor intake en service is relatief klein van omvang en was in een eerder ontwikkelde handreiking voor het opnemen van aangiften met een digitale component al relatief ver uitgewerkt (Leukfeldt e.a., 2015). Zodoende zijn twee experts op het gebied van intake en casescreening geselecteerd om de kennisnorm voor intake en service te bespreken.

Op basis van deskresearch bleek dat digitale aspecten in het werk van politiemensen in uniformdienst (blauw), vanwege de daar aanwezige digitale sporen, met name betrekking hebben op het optreden op een plaats delict. Op basis van eerdere handreikingen over het optreden op een

plaats delict in een gedigitaliseerde samenleving was ook dat onderdeel al in een vergevorderd stadium (Van Amelsvoort & Groenendal, 2017; Zuurveen e.a., 2015). Voor het toetsen van de norm zijn twee interviewkandidaten geselecteerd: iemand uit de uitvoering en een plaatsvervangend districtschef. Die laatste is benaderd voor een interview omdat zij op het gebied van digitalisering belast is met vakontwikkeling. De achterliggende gedachte was dat zij mogelijk aanvullende digitale aspecten in politiestraatwerk voor het voetlicht zou brengen.

De recherchenorm was de meest uitgebreide, complexe en minst uitgekristalliseerde norm. Voor het toetsen en optimaliseren van de kennisnorm voor de recherche is daarom op voorhand het grootste aantal interviewkandidaten geselecteerd (N = 5). Het betrof twee tactisch experts op het gebied van opsporingsonderzoek naar digitale criminaliteit, twee digitaal-forensisch experts (allen werkzaam bij een Team Digitale Opsporing of digitaal platform[8]) en een cyberofficier van justitie van het Openbaar Ministerie (OM). De laatste vanwege diens leidende rol in de opsporing.

Tot slot is één interviewkandidaat geselecteerd die in 'onlinegegevensgaring' (OGG) is gespecialiseerd en deel uitmaakte van een landelijke werkgroep die voor dat het online vergaren van gegevens een afzonderlijke kennisnorm heeft ontwikkeld (de zogeheten OGG-5 norm). Het online vergaren van gegevens is een ogenschijnlijk complex onderdeel van politiewerk waarmee – zo bleek tijdens het interview – medewerkers in uiteenlopende functiegroepen (bijv. blauw en recherche) belast zijn. Het inzichtelijk maken van de daarvoor benodigde kennis (per functiegroep) vroeg om een opzichzelfstaand interview.

Voordat de interviewkandidaten werden benaderd, zijn vier interviewprotocollen opgesteld. Drie protocollen voor de afzonderlijke kennisnormen (intake, blauw en recherche) en een protocol voor de kennis die noodzakelijk is om onlinegegevens te verzamelen. De concept-kennisnormen stonden centraal in de interviewprotocollen. De normen bestaan uit competenties die zijn uitgewerkt in (kennis)indicatoren (zie par. 5.1). Per competentie en de daartoe behorende (kennis)indicatoren werd aan de kandidaten gevraagd in hoeverre de competentie volledig was beschreven. Reacties en eventuele aanvullingen konden in het protocol worden verwerkt.

Daarnaast zijn bij verschillende competenties verdiepingsvragen geformuleerd. De verdiepingsvragen zijn onder te verdelen in drie categorieën. Er zijn verdiepingsvragen gesteld om (1) zicht te krijgen op eventuele verschillen tussen de noodzakelijke kennis voor de intake en afhandeling van klassieke- en de intake en afhandeling van digitale criminaliteit, (2) te controleren of inzichten uit deskresearch op de juiste wijze zijn vertaald naar de kennisnormen, en (3) niveauverschillen inzichtelijk te maken voor de onderscheiden functiegroepen (bestaat bijv. verschil tussen de kennis waarover rechercheurs op de basisteamrecherche, de districtsrecherche of de regionale recherche moeten beschikken?). Tijdens de interviews stond, tot slot, de vraag centraal of

[8] Soms ook platform digitaal genoemd.

de kennisnormen over de hele linie volledig waren en zo niet, waaraan het dan ontbrak. De interviewprotocollen zijn opgenomen in bijlage III.

De interviewkandidaten zijn per e-mail en/of telefonisch benaderd en waren allen bereid om mee te werken. De kandidaten kregen minimaal een week voorafgaande aan het interview de betreffende concept-kennisnorm toegestuurd ter voorbereiding. Van november 2017 tot en met januari 2018 zijn volgens deze werkwijze elf interviews met in totaal dertien kandidaten afgenomen. Bij twee van de interviews over de kennisnorm voor de recherche sloot namelijk naast de beoogde tactisch cybercrime-expert ook een digitaal-forensisch expert aan. Van de elf interviews zijn er twee telefonisch en negen face-to-face afgenomen. De interviews duurden ongeveer 60 minuten.

Tot slot verdienen twee methodologische noten in deze sectie de aandacht. Ten eerste, de selectie van interviewkandidaten is gemaakt op basis van de in het onderzoek onderscheiden functiegroepen (intake en service, blauw en recherche). De gedachte daarachter was dat het voor het achterhalen van de voor intake-, blauw-, of recherchewerkzaamheden noodzakelijke kennis van belang is om functiegebonden experts te spreken. Hoewel de interviews bevestigen dat een expert op het gebied van een bepaalde functie vooral daarover kennis heeft, laten de interviews ook zien dat experts over relevante functieoverstijgende kennis beschikken.[9] Dat betekent dat in alle kennisnormen zoveel mogelijk de inzichten zijn verwerkt vanuit alle interviews. Daarmee is de input per functiegroep groter dan slechts het aantal afgenomen functiegebonden interviews. Dat vergroot de betrouwbaarheid van de bevindingen.

Ten tweede bevestigden de interviews voornamelijk wat al in de concept-kennisnormen was opgenomen. Hoewel voor de uitwerking ervan waardevolle inzichten zijn opgedaan, bleken de normen grotendeels volledig. Ongetwijfeld is discussie mogelijk over de inhoud van de normen, maar de bevindingen in dit onderzoek wijzen erop dat de combinatie van deskresearch en interviews leidt tot een betrouwbaar (eerste) overzicht van de voor digitale aspecten in intake-, blauw- en recherchewerk noodzakelijke kennis.

3.2.3 Advies over verhogen kennisniveau

Nadat de vragenlijsten waren afgenomen en geanalyseerd (par. 3.4) kon worden gepreciseerd hoe het kennisniveau aangaande digitale aspecten van politiewerk ervoor staat. Op basis van deze bevindingen zijn vier interviews afgenomen met zes experts. Het doel van deze interviews was om inzichtelijk te maken op welke wijze (de geconstateerde) kennistekorten aangaande digitale aspecten van politiewerk het beste bestreden kunnen worden. Tevens is ingegaan op het concept ‘basiskennis’ om te verkennen waar de ondergrens van de kennisnorm zou moeten liggen. Naar aanleiding van de

[9] Experts op het gebied van recherchewerk hebben bijvoorbeeld waardevolle suggesties aangedragen voor de kennis waarover politiemensen in uniformdienst of medewerkers intake en service moeten beschikken en vice versa.

vragenlijstresultaten zijn specifieke vragen gesteld over internetrechercheren, digitale sporen, en contact met burgers. De interviews hadden een semigestructureerd karakter. Het interviewprotocol is opgenomen in bijlage IV.

De interviewkandidaten zijn zowel binnen als buiten de politieorganisatie geworven. Het voordeel van experts die werkzaam zijn binnen de politie is dat ze weten hoe de politiepraktijk is en veelal een duidelijk beeld hebben van de materie. Het voordeel van experts die werkzaam zijn buiten de politie is dat ze met een open blik konden reflecteren op de vragen die hen werden gesteld; ze werden niet gehinderd door kennis van de politieorganisatie. Bovendien kunnen ervaringen van buiten de politie interessant zijn om toe te passen binnen de politie.

De interviews vonden plaats van 22 juli 2019 tot 24 september 2019. De interviews duurden gemiddeld ongeveer 60 minuten en zijn – met toestemming van de geïnterviewden – opgenomen voor uitwerkingsdoeleinden. Vier experts gaven toestemming om hun functie en organisatie te noemen in het onderzoeksrapport. Twee experts kozen ervoor anoniem te blijven. Hier volgt het overzicht van de kandidaten die we hebben gesproken:

- twee kandidaten van een overheidsorganisatie vergelijkbaar met de politieorganisatie;
- twee onderwijskundig adviseurs bij Directie HRM van de Nationale Politie;
- een staffunctionaris bij de Politieacademie van het cluster Onderwijs en Kennisprofessie;
- een associate lector werkzaam bij het lectoraat Wendbaar Vakmanschap van NHL Stenden Hogeschool.

Daarnaast waren we voornemens om een interviewkandidaat te werven van een commerciële instelling om te leren hoe vanuit die hoedanigheid wordt gekeken naar het structureel verbeteren van kennis van medewerkers binnen grote organisaties. Hiervoor zijn pogingen gedaan bij financiële instellingen en consultancy organisaties. Er kwam echter geen (relevante) respons op die verzoeken.

3.3 Focusgroep

Na het opstellen en optimaliseren van de concept-kennisnormen op basis van deskresearch (par. 3.1) en interviews (par. 3.2), is de concept-kennisnorm vastgesteld door middel van een focusgroepbijeenkomst c.q. groepsinterview, op 21 maart 2018 in Driebergen. De focusgroep draagt bij aan de beantwoording van deelvraag 2. Het gespreksprotocol is opgenomen in bijlage V.

Van contactpersonen binnen de meewerkende eenheden, kregen we in totaal 19 namen (onderverdeeld per doelgroep) van personen die we konden benaderen voor de focusgroep. Uiteindelijk hebben zeven van hen meegewerkt aan de focusgroep, waarbij de kennisnormen voor blauw en recherche zijn vastgesteld. Twee andere deelnemers hebben in dezelfde periode via de e-mail gereageerd om de kennisnorm voor intake en service vast te stellen. De reden om intake en

service niet in de focusgroep mee te nemen was een pragmatische. Allereerst was hier weinig discussie over. Immers, de kennisnorm stond al voor een belangrijk deel vast op basis van het deskresearch en de interviews. Ten tweede zou het lastig zijn om drie protocollen vast te stellen in een focusgroepbijeenkomst van twee uren. Ten derde zou de groep te groot worden dan effectief wordt geacht voor een focusgroep.

Op hoofdlijnen waren de deelnemers aan de focusgroep het eens dat de concept-kennisnormen voldeden aan het beeld dat zij hadden over de kennis die nodig is inzake digitale aspecten van politiewerk. Sommigen gaven echter aan dat dit een 'gewenst' beeld is, maar dat dit in de praktijk niet realistisch is. Op basis van de bevindingen van de focusgroep en de deelnemers die via de e-mail hebben gereageerd zijn enkele kleine aanpassingen gemaakt. Wijzigingen hadden veelal te maken met het weglaten of toevoegen van details en dat bepaalde normen ook voor andere functiegroepen gelden, of juist niet.

Aanvullend op de focusgroep zijn de gegevensdragers die onderdeel zijn van de kennisnorm aan een digitaal expert voorgelegd ter verificatie, aangezien de deelnemers aan de focusgroep hiervan onvoldoende op de hoogte waren. Dit leidde tot een enkele toevoeging en aanpassing.

3.4 Online vragenlijst

Om het kennisniveau inzake digitale aspecten van politiewerk in beeld te brengen, is een online vragenlijst ontwikkeld. De vragenlijst is gebaseerd op de vastgestelde kennisnormen (zie par. 5.2). Bij het opstellen van de vragen is inspiratie geput uit het vooronderzoek van Van Valkengoed (2017). De vragen gaan uitsluitend over digitale aspecten van politiewerk. Dit betekent dat algemene aspecten buiten beschouwing zijn gelaten, zoals 'het kennen van de standaardprocedure voor het opnemen van aangifte'. De reden hiervoor is tweeledig: (1) de algemene kennisindicatoren zijn geen doel van dit onderzoek, en (2) het beperken van de lengte van de vragenlijst. Met de vragenlijst konden we kennis (materie- en handelingskennis) in beeld brengen van vijf groepen politiemensen (intake en service, blauw en recherche op basisteam-, districts- en eenheidsniveau). De vragenlijst is gericht op het beantwoorden van deelvragen 3 en 4, en is opgenomen in bijlage VI.

Een opmerking die we hierbij willen plaatsen is dat we de aanwezige kennis niet hebben 'getoetst', maar dat we aan de respondenten hebben gevraagd de eigen kennis over bepaalde onderwerpen te beoordelen. Dit hebben we vooral gedaan omdat we (a) wilden voorkomen dat de vragenlijst zou lijken op een examen en dus minder uitval zou geven, en (b) de vragenlijst beknopt kon worden gehouden omdat niet elk aspect hoeft te worden geoperationaliseerd in een set vragen/items die kan worden gebruikt om de aanwezige kennis op dat onderwerp/construct te meten. Een nadeel is dat de uitkomst wat globaler is en dus wat minder precies, wat we overigens hebben opvangen door gebruik te maken van een relatief grote steekproef. Bovendien hebben we

respondenten niet alleen gevraagd naar de mate waarin zij zelf denken over kennis te beschikken, maar is hun kennis ook in kaart gebracht aan de hand van praktijksituaties c.q. praktijkhandelingen. Hierdoor houden we tevens rekening met het zogenoemde Dunning-Krugereffect, wat inhoudt dat mensen die incompetent zijn hun competentieniveau vaak overschatten bij zelfbeoordeling (Kruger & Dunning, 1999).

De vragenlijst moest in elk geval leiden tot uitspraken op het niveau van een groep (intake en service, blauw en recherche op basisteam-, districts- en eenheidsniveau). Om te komen tot een betrouwbaarheidsmarge van maximaal plus of min 7 procent (b = 0,07) en een zekerheid van 95 procent (α = 0,05) hebben we berekend dat we een netto steekproef van ongeveer 200 deelnemers per groep nodig hadden.[10] Uitgaande van een response-percentage van 40%, betekende dit dat per groep 500 deelnemers aangeschreven moesten worden (in totaal dus 2.500). In het vooronderzoek van Van Valkengoed (2017) was het response-percentage ongeveer 20%. Een belangrijke response-verhogende maatregel die we hebben ingezet is het stevig verkorten van de vragenlijst. Tevens is een bericht verschenen op het intranet van de deelnemende eenheden over het onderzoek (zie voorbeeld in bijlage VII).

Na de ontwikkeling van de conceptvragenlijst is deze in juni 2018 kwalitatief gepretest onder de vijf functiegroepen van het onderzoek. Om ervoor te waken dat degenen die de vragenlijst testen niet werden uitgenodigd om de uiteindelijke vragenlijst in te vullen, is de pretest afgenomen onder politiemensen van andere eenheden (N = 5). De vragenlijst is in Politie-eenheid Den Haag op papier voorgelegd aan één medewerker uit de doelgroep blauw en één basisteamrechercheur. Vervolgens is de vragenlijst in Politie-eenheid Limburg op papier voorgelegd aan een medewerker intake en service, een districts- en een regionaal rechercheur. De deelnemers kregen de opdracht om tijdens het invullen van de vragenlijst hardop te denken en verduidelijkingsvragen te stellen waar zij dat nodig achtten. Indien er aanleiding was stelde de onderzoeker zelf verduidelijkingsvragen. Daarnaast werd de invulduur bijgehouden. Voor intake en service betrof dit 23 minuten, blauw 36 minuten, basisteamrecherche 31 minuten, districtsrecherche 32 minuten, en voor de regionale recherche 34 minuten. De tijd voor verduidelijkingsvragen is hierbij niet van de totaaltijd afgetrokken. De pretest leidde tot enkele kleine aanpassingen in de vragenlijst. Wijzigingen hadden veelal te maken met het weglaten of toevoegen van details en het verduidelijken van vragen. Een klein aantal vragen is komen te vervallen.

Een senior onderzoeker van Bureau Analyse en Onderzoek (BAO) heeft de uiteindelijke vragenlijst overgezet in een digitale, online versie. Hiervoor is de IBM SPSS Data Collection Interviewer Server gebruikt. De onlineversie van de vragenlijst is vervolgens in september 2018 twee

[10] In de berekeningen zijn de getallen afgerond en hanteren we enkel de belangrijkste principes. De vereiste omvang van een steekproef is namelijk niet van tevoren exact te bepalen. We hanteerden daarom het principe van de verantwoorde schatting (Stol, In 't Velt, & Van Treeck, 2000).

keer kwalitatief gepretest door collega-onderzoekers van de onderzoeksgroep Cybersafety (N = 4). Dit resulteerde in enkele kleine wijzigingen. Een aantal spelfouten is eruit gehaald, de weergave van antwoordcategorieën is bij een enkele vraag aangepast (van naast elkaar naar onder elkaar), twee grote tabellen met stellingen zijn opgedeeld in kleinere tabellen, en in twee gevallen ontbrak de juiste routing. De vragenlijst is gezien het verkennende en beschrijvende karakter van de studie niet kwantitatief gepretest.

De potentiele respondenten zijn geworven in de vier meewerkende regionale eenheden. In overleg met de BAO-medewerker is de steekproef vastgesteld. Het voordeel van deze werkwijze is dat tevens inzicht verkregen kon worden in de totale populatie. Ongeacht de specifieke functies werd bijvoorbeeld duidelijk dat in de vier eenheden 19.279 politiemensen werkzaam zijn (peildatum medio 2018) binnen de vijf functiegroepen. Uitgesplitst naar eenheid is dit: Midden-Nederland (N = 4.937), Noord-Holland (N = 3.675), Oost-Nederland (N = 7.129) en Zeeland-West-Brabant (N = 3.538).

Niet alle medewerkers van de vier eenheden behoren tot één van onze functiegroepen, en binnen die functiegroepen zijn niet alle functies in het onderzoek meegenomen omdat de kennisnorm niet voor alle werkzaamheden relevant is. Aldus omvat de populatie binnen de vier eenheden 9.391 politiemensen (zie Tabel 3.2). Per functiegroep leverde dit het volgende beeld op:

- Intake en service (N = 1.274). Functies die zijn meegenomen in de steekproeftrekking zijn: Assistant Intake en Service A (n = 10), Assistant Intake en Service B (n = 817), Medewerker Intake en Service (n = 407), Generalist Intake en Service (n = 36), Senior Intake en Service (n = 3) en Operationeel Expert Intake en Service (n = 1).[11]
- Blauw (N = 6.280). Functies die zijn meegenomen in de steekproeftrekking zijn: Assistent GGP A (n= 6), Assistent GGP B (n = 111), Medewerker GGP (n = 411), Generalist GGP (n = 3.806), Senior GGP (n = 1.386), en Operationeel Expert GGP (n = 560).[12]
- Opsporing (N = 1.837). Functies die zijn meegenomen in de steekproeftrekking zijn: Medewerker Tactische Opsporing (n= 7), Generalist Tactische Opsporing (n = 844), Senior Tactische Opsporing (n = 815), en Operationeel Expert Tactische Opsporing (n = 171). Wanneer we deze aantallen vertalen naar de onderscheiden functiegroepen, dan zien we het volgende beeld ontstaan: Basisteam Recherche (n = 451), Districtsrecherche (n = 829), en Regionale Recherche (n = 557).

[11] De volgende afdelingen van intake en service zijn niet meegenomen: Team Regionaal Service Centrum, Team Buitengerechtelijke Afdoening, Leiding District Flevoland, Team Korpscheftaken, Team Coördinatie Executietaken, Team Identiteitsonderzoek, en Team ZSM. 'Servicemedewerkers' vallen buiten de doelgroep, want die hoeven niet te putten uit parate kennis, maar maken gebruik van CATI (Computer Assisted Telephonic Interviewing) software (servicemodule of Q&A), aldus een coördinator servicecentrum.

[12] De volgende afdelingen van blauw zijn niet meegenomen: Afdeling Meldkamer (politiedeel), Team Korpscheftaken, Subteam Trajectbegeleiding, Leiding Afdeling Regionale CCB (conflict- en crisisbeheersing), en Afdeling Meldkamer (politiedeel). Nb. GGP staat voor gebiedsgebonden politie.

Tabel 3.2: Steekproefoverzicht per eenheid en doelgroep

Eenheid	Intake en service	Blauw	Recherche	Totaal
Midden-Nederland	377	1.624	503	2.504
Noord-Holland	201	1.333	274	1.808
Oost-Nederland	482	2.192	707	3.381
Zeeland-West-Brabant	214	1.131	353	1.698
Totaal	*1.274*	*6.280*	*1.837*	*9.391*

Omdat binnen BAO de richtlijn wordt gehanteerd dat politiemensen niet te vaak benaderd mogen worden voor deelname aan onderzoek, zijn politiemensen die in 2018 reeds aan een onderzoek hadden meegewerkt uitgesloten voor deelname (N = 1.309). Dit betekent dat de totale steekproef waarop de willekeurige selectie plaatsvond N = 8.082 is. De uiteindelijke sample die een uitnodiging kreeg tot de vragenlijst is willekeurig uit deze steekproef getrokken (zie Tabel 3.3). Hierbij werd getracht om politiemensen te selecteren naar rato per eenheid.

*Tabel 3.3: Sample per doelgroep en eenheid (N = 2.509)**

Doelgroep	Midden-Nederland	Noord-Holland	Oost-Nederland	Zeeland-West-Brabant	Totaal
Intake en service	148	79	189	84	500
Blauw	130	106	175	90	501
Basisteamrecherche	Alle	Alle	Alle	Alle	451
Districtsrecherche	121	69	188	123	500
Regionale recherche	Alle	Alle	Alle	Alle	557

**Notitie. In een aantal gevallen hebben we geen inzicht in exacte cijfers, maar weten we alleen dat 'alle' medewerkers uit bepaalde functiegroepen zijn geselecteerd.*

De dataverzameling startte op maandag 1 oktober 2018 en is afgesloten op vrijdag 19 oktober 2018. De potentiele deelnemers ontvingen een uitnodigingsmail die hen toegang gaf tot de vragenlijst. In totaal hebben 2.366 politiemensen de uitnodiging ontvangen.[13] Na een week ontvingen diegenen die de vragenlijst niet hadden ingevuld een herinneringsmail met het verzoek om dat alsnog te doen. Een week daarna werd een derde en laatste herinnering gestuurd.

Om te voorkomen dat 'common method bias' optreedt (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003) is aan de respondenten duidelijk gemaakt dat de antwoorden anoniem worden verwerkt.[14] Daarnaast instrueerden we de respondenten dat er geen goede of foute antwoorden zijn, maar dat het belangrijk is om hun mening/ervaringen te delen.

[13] Dit is minder dan de totale sample van 2.509. Dit komt omdat het systeem politiemensen die recent hebben meegewerkt aan vragenlijstonderzoek automatisch eruit filtert (aanvullende controle). Dit houdt in dat naast de eerdergenoemde 1.309 nog eens 143 politiemensen op voorhand zijn buitengesloten van het onderzoek.

[14] Common method bias houdt in dat variaties in responses worden veroorzaakt door het instrument, bijvoorbeeld sociaal wenselijkheid, in plaats van door hoe de respondent er echt over denkt.

Uiteindelijk hebben 626 politiemensen de vragenlijstlijst bezocht (bruto responspercentage 26%), waarvan er 484 de lijst volledig hebben ingevuld of zijn doorverwezen naar het einde van de vragenlijst. Van de 484 records zijn 82 uit het databestand verwijderd. Eén is verwijderd omdat de respondent niet tot de gedefinieerde eenheden behoorde. Daarnaast zijn 69 respondenten verwijderd omdat zij niet tot de gedefinieerde functieprofielen behoorden. Deze respondenten kregen na een selectievraag aan het begin van de vragenlijst het bericht dat zij niet tot de doelgroep behoren en zij hebben derhalve de vragenlijst niet kunnen invullen. Tot slot zijn de data van twaalf respondenten buiten beschouwing gelaten, omdat zij niet juist reageerden op de 'stelling' – een controlevraag – waarbij de middelste antwoordcategorie gekozen moest worden.[15] Dit betekent dat de netto respons 402 is, ofwel een netto responspercentage van 17%. Dat is lager dan de beoogde 40% en ongeveer identiek aan het responspercentage in het vooronderzoek van Van Valkengoed (2017).

Voor de vragenlijst is aan de hand van het aantal respondenten de daadwerkelijke foutmarge bij een betrouwbaarheid van 95% berekend. Voor de functiegroepen is de foutmarge als volgt: intake en service 11,9%, blauw 13,3%, basisteamrecherche 9,2%, districtsrecherche 9,2%, en regionale recherche 9,3%. De foutmarge voor de totale groep respondenten is 4,8%. Bij een betrouwbaarheid van 99% is de foutmarge voor de totale groep respondenten 6,3%.

Aan de vragenlijst werkten 242 mannen (60,2%) en 160 vrouwen (39,8%) mee. De gemiddelde leeftijd van de respondenten is M = 49 jaar (SD = 9,9) met een range van 25 tot 65 jaar. Van de 402 respondenten komen 146 uit de eenheid Oost-Nederland (36,3%), 120 uit Midden-Nederland (29,9%), 72 uit Zeeland-West-Brabant (17,9%) en 64 uit de eenheid Noord-Holland (15,9%). 64 respondenten verzorgen de intake (15,9%), 54 respondenten werken in de uniformdienst ('blauw') (13,4%), 91 respondenten zijn tactisch rechercheur bij de basisteamrecherche (22,6%), 100 bij de districtsrecherche (24,9%), en 93 bij de regionale recherche (23,1%).

In Tabel 3.4 is de verdeling van functies per eenheid weergegeven. Qua functie is de verdeling voor de totale sample als volgt: Assistent A (0,7%), Assistent B (7,2%), Medewerker (9,5%), Generalist (38,6%), Senior (35,6%), Operationeel Expert (5,5%), Operationeel Specialist (1,7%), en Anders (1,2%).[16] Naar eenheid, geslacht en aanstelling is de verdeling naar verwachting ten opzichte van de populatie. Qua functiegroepen is de verdeling ook redelijk goed, maar is basisteamrecherche iets oververtegenwoordigd en blauw iets ondervertegenwoordigd.

[15] Deze controlevraag is opgenomen om de betrouwbaarheid van de gegeven antwoorden door de respondenten te beoordelen.

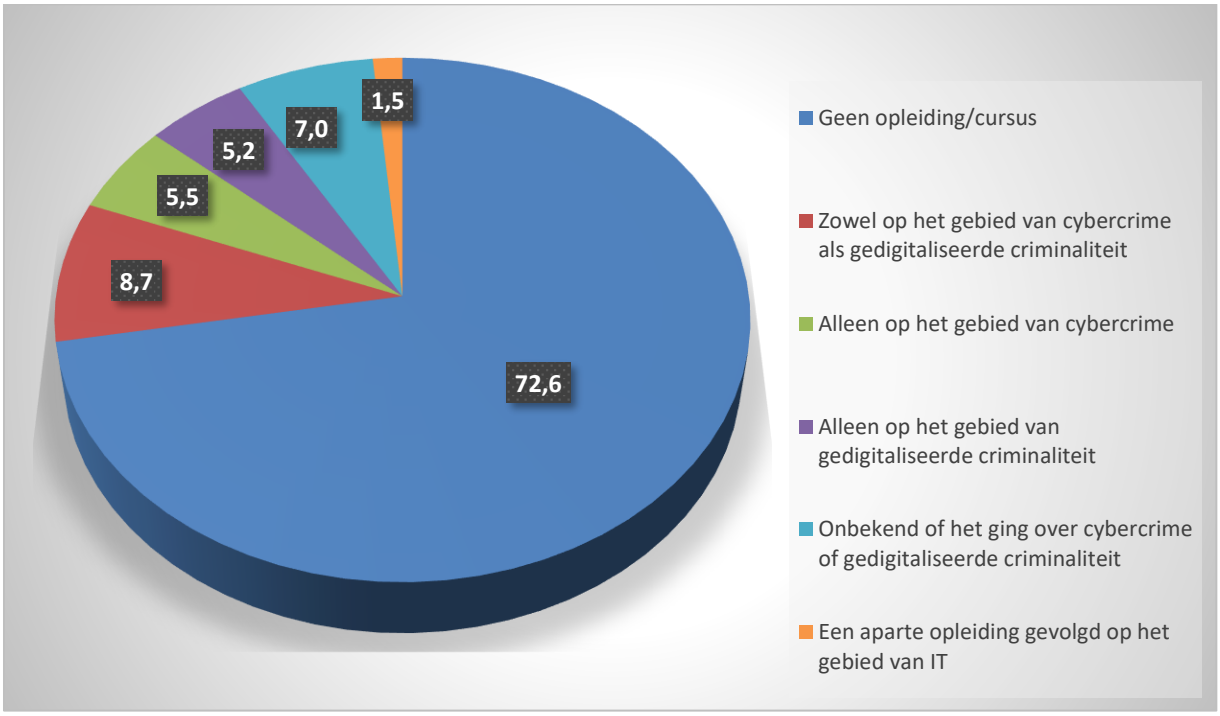
[16] De 'anders' categorie is niet verder uitgevraagd in de vragenlijst.

Tabel 3.4: Respondenten naar doelgroep en eenheid (N = 402)

Doelgroep	Midden-Nederland	Noord-Holland	Oost-Nederland	Zeeland-West-Brabant	Totaal
Intake en service	17	15	24	8	*64*
	26,6%	23,4%	37,5%	12,5%	*100%*
Blauw	14	10	17	13	*54*
	25,9%	18,5%	31,5%	24,1%	*100%*
Basis	37	10	34	10	*91*
	40,7%	11,0%	37,4%	11,0%	*100%*
District	29	12	32	27	*100*
	29,0%	12,0%	32,0%	27,0%	*100%*
Regio	23	17	39	14	*93*
	24,7%	18,3%	41,9%	15,1%	*100%*

Van de 402 respondenten had de meerderheid (72,6%) geen opleiding of cursus gevolgd op het gebied van digitale criminaliteit. De andere respondenten hebben dus wel enige opleiding gehad of een cursus gevolgd op dit vlak, zie Figuur 3.1. Let op dat de percentages niet tot exact 100 optellen. Dit komt doordat respondenten meer dan een antwoord konden kiezen.

Figuur 3.1: Opleiding/cursus gevolgd op het gebied van digitale criminaliteit



Er is een significant verschil tussen blauw en de andere functiegroepen. Hoewel de meerderheid van de andere functiegroepen in ongeveer 70% van de gevallen geen specifieke opleiding heeft gevolgd, is dit voor blauw bijna 95%. Tevens is een significant verschil gevonden tussen de groepen die weinig tot geen en die veel tot uitsluitend ervaring hebben met zaken op het gebied van digitale criminaliteit. Van de ervaren groep heeft 38,6% een opleiding of cursus gevolgd ten opzichte van 21,3% van de niet-ervaren doelgroep.

Daarnaast hebben we gevraagd in hoeverre de respondenten in de afgelopen vijf jaar te maken hebben gehad met zaken op het gebied van digitale criminaliteit. Bijna de helft van de respondenten (46,8%) gaf aan hier weinig of nooit mee te maken te hebben gehad. Ongeveer eenderde (31,3%) heeft er niet veel, maar ook niet weinig mee te maken gehad. Het resterende kwart van de respondenten (21,9%) heeft er veel mee te maken gehad, waarvan één had ingevuld hiermee uitsluitend in aanraking te komen.

Medewerkers intake en service komen in hun werk significant vaker in aanraking met digitale criminaliteit dan de overige functiegroepen. De basisteamrecherche komt significant meer met digitale criminaliteit in aanraking dan de groepen blauw, districtsrecherche en regionale recherche. Daarnaast komen vrouwen hier significant vaker mee in aanraking dan mannen. Dit geldt ook voor de groep die wel een opleiding/cursus heeft gevolgd op cybergebied ten opzichte van de deelnemers die dit niet hebben gevolgd.

3.5 Data-analyse

De data zijn geanalyseerd met het statistische softwareprogramma SPSS (versie 23). De analyse leverde een algemeen beeld op van het kennisniveau inzake digitale aspecten van politiewerk. In bijlage VIII zijn de gemiddelde scores op de vragenlijstitems opgenomen. Om een specifieker beeld te krijgen, zijn de vragen ook op groepsniveau geanalyseerd. In totaal hebben we vijf van deze analyses uitgevoerd: (1) functiegroep, (2) geslacht, (3) leeftijd, (4) opleiding, en (5) ervaring.[17] Belangrijk om te vermelden is dat niet alle functiegroepen iedere vraag hebben gekregen. Dit houdt in dat niet voor iedere vraag alle analyses mogelijk zijn.

Met functiegroep bedoelen we de vijf die zijn geselecteerd voor het onderzoek (intake en service, blauw en drie rechercheniveaus). Geslacht bestaat uit man en vrouw. Voor leeftijd hebben we twee groepen geïdentificeerd, namelijk politiemensen van 50 jaar en ouder en jonger dan 50 jaar. Deze keuze is gebaseerd op de mediaan, welke ligt bij 50 jaar. Daarmee hebben we twee groepen kunnen vormen die ongeveer even groot zijn (n = 190, n = 212). Voor opleiding geldt dat we vergelijkingen konden maken tussen politiemensen die wel (n = 110) en geen (n = 292) opleiding hadden gevolgd op gebied van digitale criminaliteit. Tot slot, voor ervaring geldt dat we verschillen konden bestuderen tussen politiemensen die (a) geen tot weinig (n = 188), (b) niet weinig, maar ook niet veel (n = 126), en (c) veel tot uitsluitend (n = 88) te maken hebben gehad met zaken op het gebied van digitale criminaliteit in de afgelopen vijf jaar.

[17] We hebben ook analyses gedraaid waarmee we verschillen tussen de deelnemende eenheden konden zien. Op vier vragen na waren er geen significante verschillen tussen de eenheden. Hieruit leiden wij af dat het aannemelijk is dat de resultaten generaliseerbaar zijn voor alle eenheden binnen de Nationale Politie.

Wanneer gemiddelden zijn vergeleken tussen twee groepen (bijv. mannen en vrouwen) is gebruik gemaakt van *t*-toetsen. We hebben hierbij tevens gekeken naar effectgrootte.[18] Indien er drie of meer groepen zijn vergeleken is gebruik gemaakt van variantieanalyse (Anova), denk bijvoorbeeld aan de vijf functiegroepen. Hierbij is ook een post-hoc toets (Tukey HSD) uitgevoerd om te preciseren tussen welke groepen de verschillen zich voordoen. Tevens is getest op de homogeniteit van de varianties (Levene's F). Daar waar de assumptie van gelijke varianties in de populatie is geschonden, is dit vermeld. Omdat met een grote dataset resultaten al snel significant kunnen zijn, gaan we uit van een betrouwbaarheid bij $p < .01$. Dit betekent dat we alleen verschillen presenteren vanaf dit significantieniveau. Bovendien hebben we gekeken naar de effectgrootte bij significante verschillen (Omega kwadraat, ω^2). Een middelmatig of groot effect zegt namelijk meer dan wanneer het effect klein is. We hebben alleen de resultaten gepresenteerd met een middelmatig effect of groter ($\omega^2 \geq .06$).[19]

In sommige gevallen was het nodig om een andere toets te gebruiken, namelijk in het geval van de analyse van dichotome variabelen. In die gevallen hebben we – in geval van het vergelijken van meerdere groepen – gebruikgemaakt van de Fisher's Exact toets. Vervolgens pasten we de Chi-kwadraattoets toe. Ook hierbij hebben we gekeken naar effectgrootte (Cramer's V).[20] De statistische output van deze analyses is opgenomen in een addendum (zie: Jansen & Van Valkengoed, 2019).

[18] De interpretatie van effectgrootte (r) is als volgt: < .1 = zeer klein; r = .1 = klein; r > .1 en r < .3 = klein tot middelmatig; r = .3 = middelmatig; r > .3 en r < .5 = middelmatig tot groot; r = .5 = groot; en r > .5 = zeer groot (Field, 2009).

[19] We spreken van een zeer klein effect bij $\omega^2 < .01$, een klein effect bij $\omega^2 = .01$, een klein tot middelmatig effect bij $\omega^2 > .01$ en < .06, een middelmatig effect bij $\omega^2 = .06$, een middelmatig tot groot effect bij $\omega^2 > .06$ en < .14, een groot effect bij $\omega^2 = .14$, en tot slot een zeer groot effect bij $\omega^2 > .14$ (Field, 2009).

[20] We spreken bij een waarde tussen 0 en 0,45 van een zwakke samenhang, een waarde tussen 0,45 en 0,65 van een tamelijk sterke samenhang, en een waarde tussen 0,65 – 1 van een sterke samenhang (Derckx, e.a., 1994).

4. Intake en afhandeling van digitale criminaliteit

In dit hoofdstuk is uitgewerkt hoe de intake en afhandeling van digitale criminaliteit binnen de politie is georganiseerd. Eerst is beschreven hoe het opsporingsproces volgens de literatuur en politiedocumentatie is ingericht (par 4.1). In paragraaf 4.2 is beschreven hoe het theoretische perspectief zich verhoudt tot de wijze waarop de intake en afhandeling van (digitale) criminaliteit in de praktijk is georganiseerd.

4.1 Het opsporingsproces in theorie

In diverse internationale publicaties is beschreven hoe het politiële opsporingsproces op hoofdlijnen is ingericht. Een gezaghebbend model voor de inrichting van het opsporingsproces is afkomstig van de Association of Chief Police Officers (ACPO) uit het Verenigd Koninkrijk. Het model vormt de basis voor de wijze waarop het opsporingsproces in Engeland is ingericht en er wordt in diverse publicaties naar verwezen (ACPO, 2005; Bryant & Kennedy, 2014; Stelfox, 2009; Tilley, Robinson & Burrows, 2007).

Samengevat doorloopt het opsporingsproces de volgende fasen. (1) Allereerst neemt de politie kennis van een (mogelijk) misdrijf. Dat kan door melding/aangifte, maar bijvoorbeeld ook tijdens politiestraatwerk. (2) Er volgt initieel onderzoek, om zoveel mogelijk informatie over het (mogelijke) misdrijf veilig te stellen. De plaats delict en het ondervragen van getuigen en slachtoffers zijn in deze fase belangrijke informatiebronnen. (3) Op basis van de vergaarde informatie over het incident wordt een besluit genomen over het al dan niet verrichten van opsporingsonderzoek. (4) Tijdens een eventueel opsporingsonderzoek staat het verzamelen en analyseren van informatie centraal. Waarheidsvinding en het in dat kader identificeren van verdachten en vergaren van zowel belastend als ontlastend materiaal is het doel. (5) Het verzamelde bewijs wordt vervolgens geëvalueerd. Er kan worden besloten tot het vroegtijdig beëindigen van het opsporingsonderzoek, het verrichten van aanvullend opsporingsonderzoek of tot het afronden van de zaak omdat vanuit politieperspectief voldoende wettig en overtuigend bewijs is verkregen. (6) Als het onderzoek wordt afgerond wordt een strafrechtelijk dossier opgemaakt en ingestuurd bij het Openbaar Ministerie (OM).

In het landelijk werkingsdocument opsporing (TRIO opsporing, 2014) is op hoofdlijnen beschreven hoe de intake en afhandeling van (digitale) criminaliteit binnen de Nederlandse politie is georganiseerd. We merken op dat de globale inrichting van het opsporingsproces vergelijkbaar is met de procesbeschrijvingen zoals die zijn opgenomen in de literatuur. (1) Opsporing begint altijd met ‘input’. De input is divers van aard. Een incident, een melding, een aangifte, intelligence over een prangend criminaliteitsprobleem of speerpunten in de programmatische aanpak van specifieke veiligheidsproblemen vormen het vertrekpunt voor de opsporing. (2) In de volgende fase wordt de

input beoordeeld. De uitkomst van deze fase is een besluit over het afwijzen, veredelen of toewijzen van een zaak voor opsporing. (3) Als wordt overgegaan tot opsporing, volgt de zogenaamde voorbereidingsfase. Die fase houdt in dat voorbereidende werkzaamheden worden verricht om ervoor te zorgen dat het opsporingsteam direct met het opsporingsonderzoek kan beginnen. (4) Tijdens de uitvoeringsfase staat het planmatig verrichten van het daadwerkelijke opsporingsonderzoek centraal. Er wordt gemonitord of het opsporingsonderzoek volgens plan verloopt en waar nodig wordt bijgestuurd. (5) In de afrondingsfase wordt een strafrechtelijk dossier opgemaakt en wordt informatie over het dossier gedeeld met relevante actoren, zoals de aangever, de politiële informatieorganisatie en/of het OM.

Type criminaliteit en soort aanpak

Voorgaande is een abstracte beschrijving van het opsporingsproces. Hoe concreet invulling wordt gegeven aan het proces van intake en afhandeling en wie daarbij betrokken zijn is volgens het werkingsdocument opsporing afhankelijk van het type criminaliteit en het soort aanpak (TRIO opsporing, 2014).

Er worden drie typen criminaliteit onderscheiden: veel voorkomende criminaliteit (VVC), high impact crime (HIC) en ondermijning. Onder VVC vallen eenvoudige criminaliteitsvormen die een behandeltijd kennen van slechts enkele uren of dagen, zoals vernieling, bedreiging of winkeldiefstal. HIC omvat misdaden met een grote impact op het slachtoffer en/of de maatschappij. Het betreft ernstige varianten van straatroof, overvallen, woninginbraak en geweldsdelicten. De afhandeling ervan vergt meer tijd en deskundigheid van de politie. Ondermijning is een verzamelnaam voor delicten die de integriteit/het functioneren van de rechtstaat bedreigen. Denk bijvoorbeeld aan georganiseerde criminaliteit waarin sprake is van drugshandel, afpersing en/of corruptie. Opsporingsonderzoek naar verschijningsvormen van ondermijning vraagt om langdurige en specialistische politie-inzet.

In samenhang met het type criminaliteit, speelt ook het soort aanpak een rol bij de wijze waarop de intake en afhandeling van zaken is georganiseerd. Er worden drie mogelijke routes onderscheiden (TRIO opsporing, 2014), namelijk: (1) de incidentgerichte aanpak, (2) de probleemgerichte aanpak, en (3) de programmatische aanpak. Bij de incidentgerichte aanpak vormt ‘een incident’, dat bijvoorbeeld is vertaald in een melding of aangifte, het vertrekpunt. Bij de probleemgerichte aanpak vormen specifieke veiligheidsproblemen die door de politie en haar partners worden gesignaleerd het vertrekpunt. Het gaat dan bijvoorbeeld om met elkaar verband houdende delict-reeksen. De aanpak van een dergelijk probleem is integraal. Dit betekent dat niet alleen strafrechtelijke, maar ook door partners uit te voeren interventies worden overwogen. Tot slot is er de programmatische aanpak. Op basis van het Nationaal Dreigingsbeeld werden om de vier jaar

thema's vastgesteld waaraan de politie prioriteit moest geven. Voor de aanpak van elk van die thema's werd een 'programma' – een specifieke aanpak – geschreven waarin staat waarop de politie-inspanningen zich richten. Inmiddels wordt uitgegaan van de Gemeenschappelijke Veiligheidsagenda. Hierin zijn landelijke beleidsdoelstellingen vastgesteld ten aanzien van de taakuitvoering van de politie. Voor cybercrime is afgesproken om niet voor de volledige vier jaar doelstellingen vast te stellen, maar dat vanwege de dynamiek van cybercrime de doelstellingen jaarlijks worden bepaald (Ministerie van Justitie en Veiligheid, 2018).

In het 'toewijzingskader' voor de opsporing wordt besproken hoe de onderscheiden criminaliteitssoorten en aanpakken zich tot elkaar verhouden en welk organisatieonderdeel bij de aanpak daarvan betrokken is (Korps Nationale Politie, 2012). Er zijn vier rechercheniveaus te onderscheiden, namelijk: (1) basisteamniveau, (2) districtsniveau, (3) regionaal niveau, en (4) landelijk niveau. Het toewijzingskader laat zien dat de:

- basisteamrecherche verantwoordelijk is voor de incidentgerichte aanpak van VVC;
- districtsrecherche verantwoordelijk is voor de incidentgerichte aanpak van HIC en de probleemgerichte aanpak van VVC;
- regionale recherche verantwoordelijk is voor de programmatische aanpak van VVC, de probleemgerichte aanpak van HIC, en de incident- en probleemgerichte aanpak van ondermijning;
- landelijke recherche aangewezen is voor de programmatische aanpak van landelijk geprioriteerde HIC en ondermijningsthema's (probleemgericht en programmatisch).

Het toewijzingskader verduidelijkt welke rechercheniveaus betrokken zijn bij de verschillende typen criminaliteit en aanpakken. Hoe dit kader zich verhoudt tot digitale criminaliteit is niet weergegeven en/of beschreven in het landelijk werkingsdocument opsporing. Voor digitale criminaliteit gelden derhalve dezelfde uitgangspunten.

In het beleidsdocument 'Criminaliteit in een digitale samenleving' hebben Campman e.a. (2012) desalniettemin een poging gedaan om het toewijzingskader – zoals dat destijds was opgenomen in het inrichtingsplan voor de Nationale Politie (Korps Nationale Politie, 2012) – te vertalen naar digitale criminaliteit. Daaruit blijkt op hoofdlijnen dat, ten eerste, de incidentgerichte aanpak van veel voorkomende digitale criminaliteit zich toespitst op digitale criminaliteitsvormen die zich voordoen binnen de geografische grenzen van het basisteam (locatiegebonden), gepleegd worden door 'alleenplegers' en qua complexiteit op basisteamniveau af te handelen zijn. Gedacht moet worden aan hacken in de relationele sfeer waarbij verdachte en slachtoffer woonachtig zijn binnen de geografische grenzen van het basisteam.

Ten tweede maken we uit het document op dat de districtsrecherche verantwoordelijk is voor de incidentgerichte aanpak van cybercrime met grote impact (bijv. hacken van een grootschalige database van een lokaal bedrijf) en de probleemgerichte aanpak van veel voorkomende digitale criminaliteit (bijv. een reeks van delicten met een digitale component op een middelbare school). Het betreft delicten die zich afspelen binnen het district (locatiegebonden), gepleegd worden door hetzij een alleenpleger, hetzij een crimineel samenwerkingsverband en qua complexiteit op districtsniveau af te handelen zijn.

Ten derde constateren we dat de regionale recherche zowel kan worden belast met de incidentgerichte als de probleemgerichte aanpak van digitale criminaliteitsvormen met hoge impact en ondermijning (bijv. malware bij een regionaal energiebedrijf). Daarnaast kan de regionale recherche worden ingezet bij de thematische aanpak van alle onderscheiden criminaliteitssoorten (VVC, HIC, ondermijning). Het gaat dan bijvoorbeeld over de aanpak van stelselmatige woninginbraken waarbij sociale media worden gebruikt, 'grooming' door regionaal actieve loverboys of (digitaal) witwassen.[21] De uitingsvormen van digitale criminaliteit waarmee de regionale recherche zich bezighoudt onderscheiden zich doordat zij regionaal van aard zijn, gepleegd worden door alleenplegers of criminele samenwerkingsverbanden, en/of doordat zij dermate complex zijn dat zij op regioniveau afgehandeld dienen te worden en/of op regionaal niveau prioriteit genieten.

Tot slot zien we dat opgeschaald wordt tot een landelijke aanpak als sprake is van locatie onafhankelijke uitingsvormen van digitale criminaliteit met grote impact of als sprake is van digitale uitingsvormen van ondermijning. Daarbij kan zowel sprake zijn van de incidentgerichte, probleemgerichte als programmatische (geprioriteerde) benadering.

Het toewijzingskader voor digitale criminaliteit heeft geen 'voorschrijvende' status. Volgens Campman e.a. (2012) dient het toewijzingskader slechts als handreiking. Er bestaan immers vele uitingsvormen van digitale criminaliteit en er zijn vele methoden en technieken om digitale delicten te plegen. Ervaringen met het toewijzingskader moeten het document verder aanscherpen. Een geüpdatete versie is echter niet aangereikt en/of gevonden gedurende het onderzoek. Wel heeft het onderzoek van Van Valkengoed (2017) het door Campman e.a. voorgestelde toewijzingskader bevestigd.

Het toewijzingskader voor de opsporing laat op hoofdlijnen zien dat met name de omvang (geografisch, capaciteit) van een zaak en de complexiteit van het gevraagde werk bepalen welk rechercheniveau wordt belast met het opsporingsonderzoek. Algemeen geldt – voor zowel klassieke delicten als cybercrime – hoe omvangrijker en complexer de criminaliteit en het soort aanpak, hoe hoger het rechercheniveau. Overigens is het op alle rechercheniveaus mogelijk om, waar nodig, digitale expertise te mobiliseren. Daarvoor zijn digitale platforms en Teams Digitale Opsporing (TDO)

[21] Grooming kan worden geïnterpreteerd als 'digitaal kinderlokken'.

ingericht (De Jong, 2015a; De Jong, 2015b). De digitale platforms, waarbinnen gespecialiseerde politiemedewerkers werkzaam zijn, vormen het eerste aanspreekpunt wanneer tijdens de uitvoering van een opsporingsonderzoek digitale expertise vereist is. Er wordt opgeschaald naar TDO als de kennis en kunde binnen het platform ontoereikend is.

In literatuur en beleidsdocumenten is beschreven hoe het opsporingsproces is georganiseerd. Onduidelijk is vooralsnog hoe aan dat proces in de praktijk invulling wordt gegeven. Daar wordt in paragraaf 4.2 nader op ingegaan.

4.2 Het opsporingsproces in de praktijk

Om in kaart te brengen hoe de intake en afhandeling van zaken in de praktijk is georganiseerd, zijn naast de documentenanalyse vier interviews afgenomen. Grotendeels bevestigen de interviews de globale inrichting van het opsporingsproces zoals besproken in paragraaf 4.1. In de praktijk worden de volgende vijf fasen onderscheiden: (1) intake (input), (2) casescreening (beoordelen input), (3) voorbereiden, (4) uitvoering, en (5) afronding. Of en zo ja hoe invulling wordt gegeven aan de voorbereidingsfase in het kader van een opsporingsonderzoek verschilt per eenheid en/of is zaakafhankelijk. We gaan op de vijf genoemde fasen nader in.

Fase 1 van 5: input (het intakeproces)

Door de interviews wordt duidelijk dat intake – het opnemen van meldingen of aangiften – doorgaans het vertrekpunt vormt voor het opsporingsproces. In de praktijk wordt dus vooral gewerkt volgens de incidentgerichte en in mindere mate volgens de probleemgerichte of programmatische benadering. Daarvoor vormen intelligence over specifieke veiligheidsproblemen of op specifieke dreigingen gebaseerde programma's immers de input (TRIO Opsporing, 2014).

De wijze waarop de intake is georganiseerd kan verschillen per eenheid, maar het overgrote deel van de intakewerkzaamheden wordt verricht door speciaal daarvoor aangestelde medewerkers intake en service. In sommige eenheden worden ook politiemensen in uniformdienst (blauw) belast met het op het bureau opnemen van meldingen en aangiften. In elk geval is blauw belast met de intake op locatie, bijvoorbeeld naar aanleiding van een incident op straat. Daarnaast kunnen, als de aard en complexiteit van de aangifte daar om vraagt – zoals bij complexe cyberzaken – specialisten worden betrokken om te ondersteunen bij het opnemen van aangiften.

Aangevers hebben verschillende mogelijkheden voor politiecontact. Zo kan telefonisch contact worden opgenomen met de politie, kan melding/aangifte gedaan worden via internet of op het politiebureau en bestaat de mogelijkheid om op locatie melding en/of aangifte te doen. Per eenheid kunnen verschillende aanvullende mogelijkheden bestaan. Zo kan in sommige eenheden

aanvullend contact met de politie worden gezocht via WhatsApp, per e-mail, via Facebook en/of via videobellen (de zogeheten 3D aangifte).

Het intakeproces is gelijk voor klassieke criminaliteit (al dan niet met een digitale component) en gedigitaliseerde criminaliteit of cybercrime. Dezelfde medewerkers zijn er mee belast en dezelfde mogelijkheden voor politiecontact kunnen worden benut.

Fase 2 van 5: Het beoordelen van input (casescreening)

De wijze waarop invulling wordt gegeven aan de fase 'beoordelen input' in het opsporingsproces hangt af van de gehanteerde aanpak. In de praktijk is vooral sprake van de incidentgerichte benadering. Na een melding of aangifte vindt dan de zogenaamde 'casescreening' plaats. Meldingen en aangiften worden 'gescreend' om te bepalen of tot actie wordt overgegaan.

Volgens geïnterviewden bepaalt de aard van een *melding* wat ermee gebeurt. Aan spoedmeldingen die binnenkomen bij de meldkamer wordt ogenblikkelijk opvolging gegeven. Executieve politiemedewerkers worden direct ter plaatse gestuurd. Aan zogeheten 'nu' meldingen wordt op korte termijn (binnen een half uur) opvolging gegeven, zoals bij winkeldiefstal. Tot slot zijn er de 'later' meldingen. Dit zijn meldingen waarvoor niet meteen actie vereist is, maar die vooral nuttig zijn voor de informatiepositie van de politie. Hoewel dergelijke meldingen meestal slechts worden opgeslagen in het bedrijfsprocessensysteem van de politie en er verder niets mee wordt gedaan, worden de meldingen idealiter wel gescreend. De 'later' meldingen kunnen namelijk aanleiding zijn tot het doen van aangifte. Als een burger bijvoorbeeld melding maakt in plaats van aangifte doet, dan kan de politie – als sprake is van een misdrijf – de burger vragen om daar alsnog aangifte van te doen. Met het oog op cybercrime merkt een van de geïnterviewde politiemensen op dat het medewerkers intake en service soms aan kennis ontbreekt om te bepalen of sprake is van een cyberdelict. Dan wordt de melding opgenomen in de veronderstelling dat geen sprake is van een misdrijf, terwijl wel degelijk sprake is van een aangiftewaardig cyberdelict. Het screenen van meldingen kan dus, zeker bij digitale criminaliteit, nuttig zijn.

Aangiften worden gescreend op (lokale) beleidsprioriteiten en opsporingsindicatie. De aangiftescreening kan leiden tot verschillende uitkomsten. Allereerst kan een zaak worden teruggestuurd naar de medewerker die de aangifte heeft opgenomen. Hem of haar wordt dan verzocht om de aangifte te verbeteren en/of aan te vullen. Ten tweede kan een aangifte bij gebrek aan opsporingsindicatie of prioriteit worden 'opgelegd'. De zaak wordt dan niet in behandeling genomen. Als de aangifte voldoende aanknopingspunten bevat om tot opsporing over te gaan, wordt besloten door welk opsporingsteam (basis, districts- of eenheidsniveau) een zaak wordt opgepakt en met welke prioriteit. In de praktijk is dat vaak de basisteamrecherche, maar als de omvang en

complexiteit daar om vragen, dan kan de zaak ook worden doorgestuurd aan de districts- of eenheidsrecherche. Het eerder besproken toewijzingskader wordt daarbij als uitgangspunt gebruikt.

Een 'bypass' – een anders ingericht proces – voor de casescreening van digitale criminaliteit is niet aanwezig. Volgens een van de geïnterviewden is het echter zo dat cybercrimezaken relatief vaak worden opgelegd in het casescreeningsproces. Daarvoor zijn verschillende redenen voor. Door een gebrek aan kennis van de medewerker intake en service kan opsporingsindicatie in de aangifte ontbreken, maar ook capaciteit en andere prioriteiten op rechercheteams spelen een rol. Een andere geïnterviewde geeft aan dat cybercrimezaken relatief weinig voorkomen en dat dergelijke zaken, als zij zich aandienen, dermate complex zijn dat ze doorgaans worden afgehandeld door rechercheteams op districts- of eenheidsniveau.

In de praktijk wordt vooral gewerkt volgens de incidentgerichte benadering. Daarom is de wijze waarop de casescreening is ingericht bij de probleemgerichte en programmatische aanpak van (digitale) criminaliteit onderbelicht gebleven tijdens de interviews. Uit het landelijk werkingsdocument opsporing kan echter worden opgemaakt dat de input voor de opsporing bij die benaderingen op een andere wijze worden beoordeeld (TRIO opsporing, 2014). Voor de probleemgerichte aanpak vormt in- en/of extern verzamelde informatie over een criminaliteitsprobleem de input. Die input wordt door de informatieorganisatie verrijkt tot een 'preweegdocument'. Daarin wordt het probleem op basis van de beschikbare informatie beschreven, zodat zicht ontstaat op mogelijkheden om dat probleem aan te pakken. Op basis van het preweegdocument (de input) beoordeelt een stuurploeg of een projectvoorstel moet worden geschreven voor de aanpak van het probleem. Vervolgens beoordeelt de stuurploeg op basis van het projectvoorstel welke interventiestrategie wordt gehanteerd. Voorgaande informatie wordt verwerkt tot een operationeel plan van aanpak. De stuurploeg besluit – met inachtneming van beschikbare capaciteit en doorlooptijd – op basis daarvan of al dan niet wordt overgegaan tot het verrichten van een opsporingsonderzoek. Bij de programmatische aanpak, tot slot, bepaalt een strategische stuurploeg op basis van het Nationaal Dreigingsbeeld het programma waarop actie wordt ondernomen. In het programma zijn de kaders beschreven voor de aanpak van een op basis van het Nationaal Dreigingsbeeld geprioriteerd veiligheidsprobleem. Het programma vormt daarmee de input voor de te verrichten opsporingswerkzaamheden.

Fase 3 van 5: Voorbereiden

Of, door wie en hoe in de praktijk aan de voorbereidingsfase invulling wordt gegeven is zaakafhankelijk. Dat blijkt zowel uit het werkingsdocument opsporing als uit de interviews. Bij kleinschalige zaken met een incidentgerichte benadering doet de recherche het voorbereidende werk bijvoorbeeld zelf. Dan wordt doorgaans niet gewerkt met een op schrift gesteld plan van

aanpak voor het opsporingsonderzoek. Bij grotere zaken en/of zaken met een probleemgerichte aanpak kan de informatieorganisatie, het team werkvoorbereiding en/of een integraal samenwerkingsverband een rol spelen in de voorbereiding op het opsporingsonderzoek. Bij zulke zaken wordt in de voorbereidingsinformatie zoveel mogelijk informatie verzameld. Die informatie wordt verwerkt in een plan van aanpak. Dit plan wordt opgesteld voor de aanpak van het centrale veiligheidsprobleem.

Fase 4 van 5: Uitvoeren

In de uitvoeringsfase staat het daadwerkelijk verrichten van opsporingsonderzoek centraal. In deze fase wordt de uitvoering van een onderzoek bovendien gemonitord op het effect, capaciteit en doorlooptijd. Waar nodig wordt bijgestuurd, bijvoorbeeld als het onderzoek te weinig effect resulteert, een buitenproportionele hoeveelheid capaciteit vraagt of de doorlooptijd irreëel is (TRIO Opsporing, 2014). Hoe daadwerkelijk invulling wordt gegeven aan het opsporingsonderzoek en de monitoring daarvan is afhankelijk van het type zaak en de gehanteerde opsporingsbenadering. De geïnterviewden reproduceren niet wat daarover in het toewijzingskader staat (zie ook sectie 4.1.1), maar stellen, kort samengevat, dat vooral de omvang en complexiteit van een zaak bepaalt op welk niveau de zaak wordt behandeld.

Op basisteamniveau worden voornamelijk kleinschalige en weinig complexe zaken gedraaid. In de praktijk wordt onderscheid gemaakt tussen twee soorten zaken. Allereerst zijn er de zogeheten ‘9-uurs’ zaken, die door medewerkers in de reguliere basispolitiezorg worden afgehandeld.[22] Het gaat dan om kleinschalige onderzoeken die binnen negen uur kunnen worden afgerond. Denk bijvoorbeeld aan uitgaansgeweld met een bekende dader. Daarnaast zijn er zaken waarvoor aanvullend, maar geen grootschalig of complex opsporingsonderzoek nodig is. Dergelijke ‘korte klap-zaken’ worden toebedeeld aan de basisteamrecherche.

De basisteamrecherche wordt doorgaans bemand door een of een aantal vaste krachten (een ervaren tactisch rechercheur/coördinator) en een steeds roulerend aantal medewerkers uit blauw, die binnen de basisteamrecherche ervaring opdoen met opsporingsonderzoek.

De basisteamrecherche verricht onderzoek naar zaken van uiteenlopende aard. Het betreft onderzoeken naar zowel klassieke misdrijven (al dan niet met een digitale component) als onderzoeken naar digitale criminaliteit. In de praktijk is het volgens de geïnterviewden echter wel zo dat het op basisteamniveau veelal ontbreekt aan de kennis die nodig is om een cybercrimezaak te draaien. Cybercrimezaken worden daardoor in kleine mate op basisteamniveau afgehandeld. Als er al een opsporingsonderzoek naar cybercrime plaatsvindt bij de basisteamrecherche, dan betreft het

[22] Voor 1 maart 2017 werd gesproken van ‘6-uurs’ zaken. Dit is gewijzigd naar 9 uur in verband met het recht van een verdachte op bijstand van een raadsman.

relatief eenvoudige zaken (zoals een zaak waarbij het e-mailaccount van een ex-partner is gehackt). Veelal worden cybercrimezaken dus op een hoger niveau afgehandeld.

Net als de basisteamrecherche, kan ook de districtsrecherche zowel worden belast met klassieke criminaliteit (al dan niet met een digitale component), als gedigitaliseerde criminaliteit en cybercrime. De aard, omvang en impact van een zaak bepalen of de districtsrecherche wordt ingeschakeld. HIC-zaken waarnaar op districtsniveau onderzoek wordt gedaan zijn overvallen, zware mishandelingszaken, brandstichtingen of – in geval van cybercrime – de hack van een bedrijf.

De mate waarin de districtsrecherche is toegerust op het afhandelen van digitale criminaliteit is eenheidsafhankelijk. Eén van de geïnterviewden geeft aan dat de districtsrecherche in zijn eenheid multidisciplinair is georganiseerd. Zowel tactisch rechercheurs als digitaal experts nemen daarin zitting. In die eenheid wordt van de districtsrecherche verwacht dat zij in staat zijn om opsporingsonderzoek te verrichten naar digitale criminaliteit. In de meeste andere eenheden is de districtsrecherche op dezelfde wijze georganiseerd als de basisteamrecherche. Digitale expertise is daar niet geborgd binnen rechercheteams op districtsniveau. Het kennistekort dat daardoor ontstaat leidt er volgens een van de geïnterviewden toe dat digitale criminaliteit maar in geringe mate wordt afgehandeld door de districtsrecherche. Veelal wordt in de betreffende eenheid het speciaal ingerichte cybercrimeteam (op eenheidsniveau) ingezet om uitvoering te geven aan de opsporing van ’cyberzaken’.

Dat ogenschijnlijk complexe cyberzaken niet of nauwelijks op basis- of districtsniveau worden afgehandeld is volgens de geïnterviewden in sommige gevallen onnodig. Niet zelden overschatten rechercheurs volgens hen de benodigde kennis en vaardigheden voor de opsporing van digitale criminaliteit. Eén van de geïnterviewden legt uit dat een cyberopsporingsonderzoek voor 70 tot 80 procent gelijk is aan klassiek opsporingsonderzoek. In de tien latere interviews over de voor de opsporing van digitale criminaliteit benodigde kennis, werd deze bewering unaniem bevestigd. Hetzelfde proces van informatieverzameling – bijvoorbeeld door gegevens te vorderen – is namelijk van toepassing. In plaats van NAW-gegevens (naam, adres, woonplaats) bij een kenteken, worden in cyberonderzoek echter NAW-gegevens opgevraagd bij een IP-adres. Dat soort ‘digitale terminologie’ (IP-adres) leidt tot onnodige ‘koudwatervrees’. Bovendien beschikt de recherche op basisteam- en districtsniveau in alle eenheden over de mogelijkheid om een beroep te doen op digitaal experts (vanuit digitale platforms en/of TDO).

Voor de afhandeling van digitale criminaliteit kan in iedere eenheid worden opgeschaald naar de eenheidsrecherche, ofwel de Dienst Regionale Recherche (DRR). Volgens het inrichtingsplan van de politie bestaat de DRR uit de afdelingen Generieke Opsporing, Thematische Opsporing, Vreemdelingenpolitie en Specialistische Ondersteuning (Ministerie van Veiligheid en Justitie, 2012). Gezamenlijk zijn deze afdelingen belast met de opsporing van zeer uiteenlopende

criminaliteitsvormen, van milieucriminaliteit tot mensenhandel en fraude. Ook digitale criminaliteit kan worden belegd bij de recherche op eenheidsniveau. In de tien regionale eenheden gebeurt dat bij een speciaal daarvoor ingericht (thematisch) cybercrimeteam. De cybercrimeteams zijn multidisciplinair samengesteld: ze bestaan uit een mix van ervaren tactisch rechercheurs en digitaal experts. Daarnaast nemen een aantal periodiek roulerende rechercheurs vanuit de basisteams- en de districtsrecherche zitting in de cybercrimeteams. Zij doen daar ervaring op met opsporingsonderzoek naar digitale criminaliteit, zodat zij hun kennis bij terugkomst kunnen benutten en uitleren in de rechercheteams op basis- en districtsniveau. In de twee eenheden zonder cybercrimeteams wordt de bestrijding van cybercriminaliteit opgepakt door reguliere, sowieso al multidisciplinair samengestelde eenheidsrechercheteams.

Fase 5 van 5: Afronden

Op basis van de interviews zijn op hoofdlijnen twee manieren te onderscheiden waarop een opsporingsonderzoek kan worden afgerond. Deze afrondingsmogelijkheden zijn gelijk voor alle soorten criminaliteit en zijn zowel op basis-, districts- als op eenheidsniveau van toepassing.

Allereerst is het mogelijk dat een zaak niet wordt opgelost. Het opsporingsonderzoek wordt dan vroegtijdig beëindigd en dus niet ingestuurd bij het OM. Een gebrek aan aanknopingspunten voor opsporing en/of een gebrek aan bewijs tegen de verdachte(n) zijn daar debet aan. Bij cybercrimezaken is dat niet uitzonderlijk, omdat de recherche in dergelijke onderzoeken bijvoorbeeld stuit op een doodlopend spoor in het buitenland. Eén van de geïnterviewden merkt op dat een dergelijke zaak eventueel ‘op de plank’ kan worden gelegd, omdat zich in de toekomst wellicht alsnog sporen aandienen en de zaak dan kan worden hervat. De politie probeert op voorhand zoveel mogelijk te voorkomen dat capaciteit wordt geïnvesteerd in zaken die niet worden opgelost, door in het proces van casescreening en voorbereiding een selectie te maken van kansrijke zaken. Ten tweede kan een zaak worden opgelost: er is dan voldoende bewijs tegen de verdachte(n) om een zaak aan te dragen bij het OM. Het OM beraadt zich daarna over de vervolging van de verdachte(n).

In het landelijk werkingsdocument is, ter aanvulling, beschreven dat het intern en, waar nodig, extern delen van informatie en het voltooien van dossiers tijdens de afrondingsfase centraal staat (TRIO Opsporing, 2014). Het strafrechtelijk dossier is vaak het belangrijkste eindproduct van het opsporingsonderzoek, maar ook andere producten – zoals een ontnemingsdossier – kunnen van belang zijn. Informatie over de zaak wordt vervolgens gedeeld met de aangever en/of direct bij de zaak betrokkenen, samenwerkingspartners van zowel binnen als buiten de politie en, waar passend, de media. Daarnaast wordt informatie over de zaak voor intelligencedoeleinden gedeeld binnen de politie, bijvoorbeeld door het te verwerken in de bedrijfsprocessensystemen en/of presentaties en rapportages.

5. Kennisnormen: theorie en praktijk

In paragraaf 5.1 komt aan bod welke kennis noodzakelijk is voor politiewerk in een gedigitaliseerde samenleving (de kennisnormen; theorie). Op basis van een meting onder 402 politiemensen, is vervolgens beschreven in hoeverre politiemensen over de noodzakelijke kennis beschikken, welke kennis tekortschiet en waar de kennistekorten zich voordoen (par. 5.2; praktijk). In paragraaf 5.3 zijn suggesties van experts opgenomen over de wijze waarop het kennistekort kan worden bestreden.

5.1 Kennisnormen voor de aanpak van digitale criminaliteit

In deze paragraaf is achtereenvolgens beschreven over welke kennis medewerkers intake en service (sectie 5.1.1), blauw (sectie 5.1.2), en rechercheurs (sectie 5.1.3) moeten beschikken om effectief uitvoering te geven aan de aanpak van digitale criminaliteit.

Noot vooraf

Het in kaart brengen van noodzakelijke kennis voor 'digitale aspecten van politiewerk' staat centraal. Klassiek en digitaal politiewerk kunnen echter niet los van elkaar gezien worden. De wijze waarop de intake en afhandeling van digitale criminaliteit is georganiseerd is immers grotendeels gelijk aan de intake en afhandeling van klassieke delicten (zie hoofdstuk 4). Digitale aspecten van politiewerk zijn (grotendeels) geïntegreerd in het reguliere politieproces. Het reguliere politieproces vormt daarom het vertrekpunt voor de opgestelde kennisnormen. De kennisnormen zijn daarmee meteen voorzien van een logische structuur. Het betekent echter wel dat de kennisnormen niet uitsluitend uit 'digitale kennis(indicatoren)' bestaan, maar dat in de normen ook klassieke indicatoren zijn opgenomen. Voor de begrijpelijkheid van de (opbouw van de) normen en omdat kennis voor de aanpak van digitale criminaliteit onderdeel is van het reguliere politieproces is dat onvermijdelijk. Hoewel klassieke indicatoren dus wel zijn opgenomen in de normen, worden deze niet getoetst aan de praktijk.

De kennisnorm voor medewerkers in het intakeproces is grotendeels gebaseerd op de handreiking voor de intake van delicten met een digitale component (Leukfeldt, Kentgens, Prins, & Stol, 2015) en de webapp cybercrime van de Politieacademie.[23] De kennisnorm voor blauw is gebaseerd op de handleiding optreden plaats delict (Van Amelsvoort & Groenendaal, 2017), een onderzoek naar het herkennen en veiligstellen van digitale apparatuur (Zuurveen, Doodeman, Veenstra, & Stol, 2015), en de OGG-5 (onlinegegevensgaring) norm. De kennisnorm voor recherche is gebaseerd op algemene (inter)nationale literatuur over het verrichten van opsporingsonderzoek. Voor de beschrijving van specifieke 'digitale' kennis en vaardigheden is geput uit Vademecum Interceptie (Kennis- en Expertisecentrum Cybercrime, 2014), de OGG-5 norm, competentieonderzoek cybercrimeopsporing (Van Valkengoed, 2017) en uit een handreiking voor het herkennen, vinden en

[23] Door politiemensen te raadplegen via: https://webapps.politieacademie.nl/cybercrime

benutten van digitale sporen (Veenstra, Zuurveen, Kerstens, & Stol, 2016). Daarnaast is geput uit interviews (zie par. 3.2). Tot slot zijn de concept-kennisnormen besproken aan de hand van een groepsinterview (zie par. 3.3).

De kennisnormen worden hierna in verschillende tabellen gepresenteerd. We gebruiken hierbij de term 'competentie' als ordenend principe. Deze zijn weergegeven in de tabeltitel. Daarbij worden voor overzichtsdoeleinden – mede gelet op de paragraaf 5.2 – competentienummers aangegeven. Deze nummers zijn voorzien van een letter (I, B, R) die weerspiegelen op welke functiegroep de competentie betrekking heeft (respectievelijk intake en service, blauw, recherche). De kennisindicatoren – ofwel de uitwerking van de competenties – zijn geplaatst in de tabel. Let op dat onder competenties ook vaardigheden verstaan kunnen worden. We gaan echter niet in op vaardigheden.

5.1.1 Kennisnorm voor intake en service

In onderstaande tabellen (5.1a-5.1g) zijn per competentie de indicatoren beschreven die gelden voor medewerkers intake en service.

Tabel 5.1a: Indicatoren competentie I.1: Het kennen van de standaardprocedure voor het opnemen van aangifte

- Kent de standaardprocedure voor het opnemen van een aangifte. De procedure kent de volgende stappen:
  - Geef de aangever de ruimte te vertellen wat er is gebeurd
  - Bepaal of een aangifte wordt opgenomen
    - De medewerker intake en service moet in staat zijn om te bepalen of sprake is van een civielrechtelijke dan wel strafrechtelijke zaak.
  - Bepaal of het nodig is een expert in te schakelen om de aangifte op te nemen
  - Beschrijf de situatie
  - Noteer de gegevens van de aangever en het delict (gespecificeerd in verschillende bullets, zoals, datum en tijd, persoonsgegevens, plaats waar het feit is gepleegd, et cetera)
  - Bepaal om welk delict het gaat
  - Bepaal welke wetsartikelen van toepassing kunnen zijn (door te toetsen of aan de elementen uit de delictsomschrijving wordt voldaan)
  - Beschrijf de werkwijze van de verdachte(n)
  - Laat de aangever zo veel mogelijk bewijsmiddelen vastleggen
  - Analyseer de informatie
  - Formaliseer de aangifte
- Van sommige delicten is bekend dat zij maar (heel) beperkt door middel van opsporing en/of vervolging zijn aan te pakken (bijv. Microsoft Scam). Bepaal in hoeverre het zodoende noodzakelijk is om een uitvoerig proces-verbaal op te stellen. Van die delicten kan (voor intelligencedoeleinden) wel melding/aangifte worden opgenomen, maar het is zinloos om van die delicten een uitgebreid proces-verbaal op te stellen.
- Ken je eigen beperkingen en schakel, waar nodig, een expert in (bijv. vanwege de aard en/of complexiteit van een aangifte).

Tabel 5.1b: Indicatoren competentie I.2: Verschijningsvormen van digitale criminaliteit kennen en weten te herkennen op basis van praktijksignalen

- Het kennen van verschijningsvormen van cybercrime en gedigitaliseerde criminaliteit en het herkennen van digitale componenten in klassieke zaken. Er zijn vier hoofdcategorieën:
  - Hacken en andere criminaliteit gericht op computers
  - Internetfraude en andere criminaliteit met een financieel oogmerk
  - Bedreiging en andere vormen van persoonsgerichte criminaliteit
  - Kinderpornografie en andere zedendelicten
- De medewerker intake en service moet in staat zijn om te bepalen of sprake is van een civielrechtelijke dan wel strafrechtelijke zaak.

*Tabel 5.1c: Indicatoren competentie I.3: De strafbaarstelling van cyberdelicten weten vast te stellen**

- Specifiek op het gebied van cybercrime en gedigitaliseerde criminaliteit gaat het over:
  - Hacken en andere criminaliteit gericht op computers
    - Hacken
    - Gegevensdiefstal
    - Stoornis veroorzaken
    - Gegevens vernielen
    - Defacing
    - Malware, zoals ransomware
  - Internetfraude en andere criminaliteit met een financieel oogmerk
    - Oplichting
    - Identiteitsmisbruik
    - Phishing
    - Skimming
    - Fraude via veiling- en verkoopsites
    - Voorschotfraude
    - Merkfraude
    - Diefstal
    - Witwassen
    - Heling van computergegevens
    - Afpersing of chantage
    - Illegaal downloaden
    - Spam
  - Bedreiging en andere vormen van persoonsgerichte criminaliteit
    - Stalking of belaging
    - Smaad of laster
    - Belediging
    - Discriminatie
    - Bedreiging
    - Cyberpesten (in eerste aanleg niet strafbaar)
    - Zonder toestemming verspreiden van teksten via internet
    - Zonder toestemming verspreiden van foto's via internet
  - Kinderpornografie en andere zedendelicten
    - Kinderpornografie
    - Grooming
- Het is tijdens het opnemen van de aangifte niet alleen belangrijk om te bepalen welke wetsartikelen van toepassing zijn, maar ook om te toetsen of aan de elementen uit de delictsomschrijving wordt voldaan.

**Notitie. Uit het hoofd kennen van wetsartikelen is onnodig.*

Tabel 5.1d: Indicatoren competentie I.4: Weten dat verbanden bestaan tussen cyberdelicten en weten hoe die verbanden te toetsen tijdens het opnemen van de aangifte

- Het voert te ver om alle mogelijke verbanden uit te werken. Het is ook niet van belang alle verbanden te kennen. Wel is van belang om te toetsen of het delict waarvan aangifte wordt gedaan mogelijk verband houdt met andere delicten. Hacken is een basisdelict dat bijvoorbeeld verband kan houden met gegevensdiefstal of afpersing. Belangrijk om te doen is in dit verband:
  - Het zo volledig mogelijk in kaart brengen van de modus operandi (MO) van de verdachte (welke handelingen heeft de verdachte achtereenvolgens verricht en waarom?).
  - Het op basis van de MO bepalen in hoeverre de verschillende handelingen strafbaar zijn.
  - Vaststellen of (ook) sprake is van andere delicten dan waarvan in eerste instantie aangifte is gedaan.

Tabel 5.1e: Indicatoren competentie I.5: Kennis hebben van het inventariseren van opsporingsrelevante digitale sporen

- Op basis van de 7W-vragen kunnen identificeren welke digitale sporen van belang kunnen zijn voor het opsporingsonderzoek (in hoeverre kunnen digitale sporen bijdragen aan het beantwoorden van: wie, wat, waar, waarmee, welke wijze, wanneer en waarom).
- Kennen van veelvoorkomende digitale sporen (volgens handreiking en webapp):
  - IP-adres verdachte
  - E-mailadres, e-mailbericht en e-mailheader
  - Gebruikersnaam verdachte
  - Internetadres (domeinnaam)
  - Telefoonnummer
  - Advertentienummer(s)
  - Afbeeldingen
  - (Chat)logfiles
  - Unieke gegevens van goederen (serienummer)
  - Betaalgegevens (rekeningnummers, afschriften, kwitanties, creditcard-, contactgegevens)
    - Gebruikte valuta, betaalmiddel/-wijze
    - Cryptovaluta; bijv. bitcoinadressen (wallets)
    - Moneygram / Western Union registratienummers
- De medewerker intake en service moet herkennen of sprake is van ‘vluchtige gegevens’ waarbij – om te voorkomen dat digitale sporen verloren gaan – snel handelen vereist is. Vluchtige gegevens zijn digitale sporen die (vermoedelijk) op korte termijn niet meer te achterhalen zijn, zoals camerabeelden of gegevens uit een router. Als sprake is van vluchtige gegevens moet een expert worden ingeschakeld.
- Bij twijfel over de relevantie van digitale sporen is van belang dat de medewerker intake en service een expert raadpleegt.

Tabel 5.1f: Indicatoren competentie I.6: Weten hoe te adviseren over het veiligstellen van digitale sporen

- De medewerker intake en service moet weten hoe veelvoorkomende sporen (zie vorige competentie) kunnen worden veiliggesteld.
- De medewerker intake en service moet gebruik kunnen maken van beschikbare hulpmiddelen om aangevers te adviseren over het veiligstellen van digitale sporen:
  - Kennen van de webapp cybercrime van de PA
  - Kennen van internetsporen.nl
- Aanleveren van digitale sporen kan digitaal, (bijv. cd/usb), met print screens, prints op papier of foto’s.
- Bij twijfel over de wijze waarop digitale sporen kunnen worden veiliggesteld is van belang dat de medewerker intake en service een expert raadpleegt.

Tabel 5.1g: Indicatoren competentie I.7: Kennis hebben van voor 'cyber'intake ontwikkelde handreikingen en op basis daarvan weten hoe de aangever te adviseren over preventie en/of vervolgstappen

- Preventieadviezen of advisering over vervolgstappen is delictspecifiek. Het voert daarom te ver om alle adviezen hieruit te werken. In algemene zin worden in de webapp cybercrime van de politieacademie preventietips beschreven. In de handreiking voor de intake van delicten met een digitale component zijn delictspecifieke adviezen beschreven.
  - Kennen van de webapp cybercrime van de PA
  - Kennen van de handreiking voor de intake van delicten met een digitale component
- De aangever kunnen verwijzen naar relevante informatie, zoals de site veiliginternetten.nl.
- De aangever toelichten wat de te verwachten vervolgstappen van de politie zijn. Ook transparant zijn als de politie een zaak vermoedelijk niet in behandeling neemt en toelichten waarom. Dat is bij uitstek bij cyberzaken nog wel eens het geval (anonimisering, gepleegd vanuit buitenland et cetera).

5.1.2 Kennisnorm voor blauw (politiemensen in uniformdienst)

In onderstaande tabellen (5.2a-5.2i) zijn per competentie de indicatoren beschreven die gelden voor politiemensen in uniformdienst (blauw).

Tabel 5.2a: Indicatoren competentie B.1: Het kennen van de fasen in het optreden op de PD

- Fase 1: voorafgaand aan het bezoek aan de PD zoveel mogelijk informatie vergaren over de PD
- Fase 2: het nemen van de eerste maatregelen, gericht op het beschermen van sporen op de PD
- Fase 3: het verrichten van onderzoek op en rondom de PD

Tabel 5.2b: Indicatoren competentie B.2: Het kennen van het juridisch kader voor het optreden op de PD

- Het verrichten van onderzoek op de PD valt onder artikel 3 van de politiewet 2012 (algemene politietaak).
- Meestal is het onnodig om voor het betreden van plaatsen bij een PD-onderzoek bevoegdheden toe te passen, omdat betrokkenen vrijwillig medewerking verlenen (en daarvoor een standaardformulier tekenen). Als er geen sprake is van vrijwilligheid, is de inzet van een aan het betreden van de PD gerelateerde bevoegdheid noodzakelijk.
- De first responder moet bij elke handeling zelf na kunnen gaan of hij/zij bevoegd is. Bij twijfel: raadpleeg een (H)OvJ ([hoofd] officier van justitie).
- Om na te gaan of de first responder bevoegd is, is het noodzakelijk om de meest voorkomende aan het betreden van een PD gerelateerde bevoegdheden te kennen.

Hulpverlening

- Als sprake is van een voor het leven of de gezondheid van mens en dier bedreigende situatie, valt het PD-optreden doorgaans onder de hulpverleningstaak van de politie (Art. 3 & 7, pw 2012). In dat kader is het betreden van plaatsen meestal rechtmatig.

Strafvorderlijk betreden van een PD

- Er zijn drie doelen voor het strafvorderlijk betreden van een PD:
  - Het betreden van een PD ter inbeslagneming (zoeken en veiligstellen van sporen, sporendragers en andere vatbare voorwerpen)
  - Het betreden van een PD om te schouwen (sporen lezen)
  - Het betreden van een PD voor aanhouding (zoeken naar en aanhouden van een verdachte)
- Als geen sprake is van vrijwilligheid, is het uit het hoofd kennen van bevoegdheden die gerelateerd zijn aan het betreden van de PD essentieel. Op basis daarvan kan de first responder beoordelen of/hij of zij bevoegd is tot het betreden van de PD.

Tabel 5.2b (vervolg): Indicatoren competentie B.2: Het kennen van het juridisch kader voor het optreden op de PD

Relevante bevoegdheden voor <u>het betreden van de PD ter inbeslagneming</u> • Inbeslagneming (art. 96 lid 1 Sv) *Geeft de bevoegdheid PD's te betreden en sporen, sporendragers en andere vatbare voorwerpen die met het blote oog zichtbaar zijn in beslag te nemen. Meer dan 'zoekend rondkijken', bijvoorbeeld verplaatsen van voorwerpen, zoals een vloerkleed, om te zoeken naar sporen, is niet toegestaan op basis van 96 lid 1 Sv.* • Bevriezen van de PD-situatie (art. 96 lid 2 Sv) *Belangrijk om de integriteit van sporen op de PD veilig te stellen, zodat de PD op een later moment door een daartoe bevoegde autoriteit kan worden doorzocht ([H]OvJ).* • Doorzoeken van woningen en kantoren van geheimhouders (art. 110 Sv) *Het doorzoeken van woningen en kantoren van geheimhouders is voorbehouden aan de Rechter-Commissaris (RC). Bij heterdaad of verdenking van een misdrijf als omschreven in art. 67 lid 1 Sv geeft art. 97 Sv de mogelijkheid aan de (H)OvJ – mits de RC daarvoor een mondelinge machtiging heeft gegeven - om bij dringende noodzakelijkheid en als het optreden van de RC niet kan worden afgewacht de doorzoeking uit te voeren.* *Relevante bevoegdheden voor <u>het betreden van de PD voor een schouw</u>* • Schouwen (art. 151 Sv en 192 Sv) *'Het in ogenschouw nemen van de plaatselijke toestand of enig voorwerp. Het zoeken naar sporen en sporendragers met het doel deze in beslag te nemen valt niet onder de schouw' (p.31).* *Relevante bevoegdheden voor <u>het betreden van de PD ter aanhouding</u>* • Betreden PD ter aanhouding (art. 55 Sv) • Onderzoek aan de kleding van de verdachte (art. 56 Sv) en de voorwerpen die de verdachte bij zich draagt (art. 7 lid 3 PW 2012) • Inbeslagneming van daarvoor vatbare voorwerpen die de verdachte bij zich draagt (art. 95 Sv) *Overige relevante bevoegdheden* • Uitlevering vorderen van voor inbeslagneming vatbare voorwerpen bij niet verdachten (art. 96a Sv) • Ordemaatregelen (art. 124 en 125 Sv) o Ter beveiliging en afzetting van de PD kunnen ordemaatregelen worden getroffen. • Art. 96b Sv o Geeft de opsporingsambtenaar in het geval van heterdaad of buiten heterdaad bij feiten waarvoor een voorlopige hechtenis kan worden opgelegd, de mogelijkheid een voertuig te doorzoeken. • Art. 49 Wet Wapens en Munitie (WWM). o Geeft aanvullende bevoegdheden voor een doorzoeking (ook in een woning) bij WWM-overtredingen. • Art. 9 van de Opiumwet (Ow) o Geeft diverse mogelijkheden voor binnentreden ter inbeslagname bij Opiumwetdelicten. • Art. 125i SV e.v. o Geeft bevoegdheden voor in beslagname van gegevens die zijn vastgelegd op een gegevensdrager.

Tabel 5.2c: Indicatoren competentie B.3: Het kennen en weten uit te voeren van de eerste maatregelen

Ter plaatse gaan	• Goed geïnformeerd zijn over wat op de PD kan worden aangetroffen. • Aanrijden naar de PD met rechercheogen en -oren: letten op verdachte personen en/of voertuigen en vastleggen/doorgeven relevante informatie. • Zet de wifi en bluetooth uit op de gegevensdragers die je zelf bij je draagt (zoals een smartphone). Wanneer je een wifi-hotspot hebt ingeschakeld, schakel deze uit. • 'Stil' benaderen van de PD, om vluchtgedrag te voorkomen.

Tabel 5.2c (vervolg): Indicatoren competentie B.3: Het kennen en weten uit te voeren van de eerste maatregelen

Oriënteren op de PD-situatie	• Oriënteer ter plaatse de PD van enige afstand. Voorkom 'besmetting' van het gehele gebied waar het feit is gepleegd en/of sporen zijn achtergelaten (kleiner maken PD is makkelijker dan groter maken, zonder dat sporen verloren gaan). • Hoewel de oriëntatie bij voorkeur op enige afstand plaatsvindt, zijn uitzonderingssituaties mogelijk. De politiemedewerker moet weten wanneer de PD met spoed dient te worden betreden (bijv. bij een kermend slachtoffer). • Herkennen van sporen(dragers).
Primaire taken op de PD	• Informeren OC (zodat juiste inzet van mensen en middelen kan volgen) • Bevriezen situatie (zorg dat de toestand op de PD blijft zoals hij is). • Noodgedwongen handelingen verrichten In principe wordt de PD niet betreden door de first responder, in verband met risico op het vernietigen, beschadigen of besmetten van sporen. Echter, de PD kan worden betreden als maatregelen moeten worden getroffen 'die absoluut geen uitstel dulden' (p.46): o Hulpverlening slachtoffer o Beëindigen gevaarlijke situatie o Aanhouden van nog aanwezige verdachte o Verwijderen van publiek o Beschermen van belangrijke fysieke en digitale sporen die anders verloren gaan *Dit betekent in essentie dat een first responder altijd de PD betreedt. • Stelregels bij noodgedwongen eerste handelingen: o Gebruik onderzoekshandschoenen o Markeer de looproute terwijl je loopt. Voorkom dat je nog eens apart het looppad moet afbakenen, nadat je al een sporendrager van de PD hebt gehaald. o Verplaats geen voorwerpen • Een first responder verricht geen noodgedwongen eerste handelingen als, gezien de aard van de zaak, de FO ter plaatse komt. Dat is het geval bij: o Elke vermoedelijke niet natuurlijke dood o Overvallen waarbij sprake is van wederrechtelijke vrijheidsberoving en/of grof geweld o Brand of ontploffing met zwaar lichamelijk letsel o Gijzeling en ontvoering o Misdrijven met een terroristisch oogmerk o Geweldsdelicten met aanmerkelijke kans op overlijden slachtoffer(s) o Zedendelicten (verkrachting, seksueel binnendringen en aanranding) o Delicten met mogelijke ernstige maatschappelijke en/of economische gevolgen o Delicten met mogelijke gevolgen voor de integriteit en het imago van het openbaar bestuur, politie en Openbaar Ministerie *Hoewel de first responder niet zelf de beslissing neemt kan het zijn dat hij/zij – in overleg met experts – wel actie moet ondernemen; denk bijvoorbeeld aan vluchtige gegevens.

*Tabel 5.2d: Indicatoren competentie B.4: Weten hoe onderzoek op de PD te verrichten**

Kennen van het werkproces voor onderzoek op de PD: • Oriënteren en opstellen van hypotheses en scenario's (wat is er naar alle waarschijnlijkheid gebeurd en hoe) • Voorbereiden van het onderzoek op de PD o Prioriteit bepalen o Volgordelijkheid van werkzaamheden bepalen o Onderzoeksmethodologie bepalen o Externe hulp overwegen/inschakelen

**Notitie. Deze competentie is voorbehouden aan recherche/opsporing; niet voor blauw. Uitzondering is het voorbereiden van eenvoudige PD's.*

Tabel 5.2d (vervolg): Indicatoren competentie B.4: Weten hoe onderzoek op de PD te verrichten

Uitvoeren PD-onderzoek: toetsen en waar nodig bijstellen hypotheses
• Gebruik bij PD-onderzoek altijd een lamp (scheerlicht)
• Stel het sporenbeeld vast en stel, waar nodig, de hypothese bij:
  o Vergaar informatie over het gebruik van middelen (wapen, muts, et cetera)
  o Vergaar informatie over 'daderkenmerken' (snoepen, eten, drinken, urineren)
  o Vergaar informatie over motieven
 	
Afronden PD-onderzoek
• Vastleggen resultaten in proces-verbaal:
  o Bevindingen over de toedracht van het delict
  o De onderzoekshandelingen die zijn verricht
  o De aangetroffen en veiliggestelde sporen

Tabel 5.2e: Indicatoren competentie B.5: Het kennen van de specifieke basisstappen in het geval van een PD met digitale sporen

• Ga zelf bij elke handeling na of je daartoe bevoegd bent. Bij twijfel: raadpleeg een (H)OvJ. • Als je statisch geladen bent kan dat de gegevensdragers die je aanraakt beschadigen. Raak daarom eerst met je blote handen een geaard voorwerp aan (bijv. een kraan, een kale water- of cv-leiding). • Maak enkele overzichtsfoto's van de situatie waarin je de gegevensdrager(s) aantreft. • Houd rekening mee dat alles wat je zegt en doet via de aanwezige digitale apparatuur kan worden opgenomen en afgeluisterd. Zijn er gegevensdragers met daarin een cameralens of is er een webcam? Plak voor je eigen veiligheid en die van je collega's de lens af (je kan uiteraard nog steeds worden afgeluisterd). • Wanneer anderen dan politie-experts willen helpen met het veiligstellen van gegevensdragers of anderszins technische bijstand willen verlenen: weiger dit. • Noteer wie zich op welke plaats bevond toen je op de PD arriveerde. Zorg ervoor dat personen op de PD geen digitale gegevensdragers gebruiken en dat ze niets aanraken. Houd hen uit de buurt van elektriciteit leverende apparatuur (zoals generatoren en accu's), meterkasten, (elektriciteits)kabels en kill-switches. Vraag naar hun identiteitsbewijs. • Het is belangrijk om te voorkomen dat de first responder zelf sporen achterlaat (DNA, vingersporen) en daarmee het sporenbeeld verstoort en/of sporen vernietigt. Doe daarom de handschoenen aan die speciaal voor dit doel in je uitrusting zitten. • Het dragen van handschoenen voorkomt niet dat sporen worden vernietigd. Het is daarom belangrijk om een gegevensdrager zo vast te pakken dat het risico op het beschadigen of vernietigen van sporen zo klein mogelijk is (pak een smartphone dus niet bij het touchscreen).

Tabel 5.2f: Indicatoren competentie B.6: Weten hoe relevante digitale gegevensdragers te herkennen op een digitaal PD

Computers o Desktop o Laptop o Server o Mediabox en HD/dvd-recorder o Gameconsole o Tablet en E-reader (singleboard computers zoals een RaspberryPi, BananaPi, et cetera) *Mobiele telefoons* o Gsm-telefoon o Smartphone

Tabel 5.2f (vervolg): Indicatoren competentie B.6: Weten hoe relevante digitale gegevensdragers te herkennen op een digitaal PD

Opslagapparatuur/datadragers
- Externe harde schijf/NAS (interne harde schijf)
- Tapedrive
- Diskette, cd-rom of dvd
- Geheugenkaart
- USB-stick

LAN-verbindingsapparatuur
- Modem en router
- LAN, Switch en PowerPlug
- GSM-Alarm (in een datacenter: Netflow en/of andere logging van systemen; bijv. IDS)

Overige gegevensdragers
- Digitale foto- en videocamera
- Digitale fotolijst
- Muziekspeler
- Draagbare navigatieapparatuur
- Automotive systems (computerapparatuur/gegevensdragers die zijn geïntegreerd in auto's)
- Printer, scanner, kopieer- en faxapparaten

Nieuwe gegevensdragers
- Smartwatch
- NFC-ringen
- Chromecast Dongel (AppleTV)
- Google Glass
- Mouse Jiggler

*Randapparatuur**
- Muis, toetsenbord, webcam en beeldscherm/monitor
- Docking station
- Externe diskette-, cd- of dvd-speler

- Kunnen omgaan met onbekende gegevensdragers betekent: expert inschakelen
- Het zich ervan bewust zijn dat digitale sporen(dragers) niet los gezien kunnen worden van klassieke sporen. Het in samenhang inventariseren van klassieke en digitale sporen en het op basis van het volledige sporenbeeld kunnen stellen van prioriteiten om sporen veilig te stellen is van belang.

**Notitie. Randapparatuur zijn geen gegevensdragers die uit te lezen data bevatten (tot op heden). Kenmerken van deze apparatuur kunnen echter van belang zijn in een onderzoek (soms alleen al een foto ervan). Ook kan DNA/dacty, geurproef belangrijk zijn (mits goed veiliggesteld).*

Tabel 5.2g: Indicatoren competentie B.7: Weten hoe op forensisch technisch verantwoorde wijze relevante digitale gegevensdragers kunnen worden veiliggesteld

- Kennen van de basisprocedure voor het veiligstellen van digitale gegevensdragers
  - Stel vast welk(e) device(s) op de PD aanwezig zijn
  - Stel de volgorde van veiligstellen vast (in verband met op afstand wissen / belang van sporen)
  - Stel de status van de gegevensdrager vast (aan/uit, wel of niet beveiligd et cetera)
  - Stel de gegevensdragers – op volgorde van prioriteit en afhankelijk van status – veilig
  - Schakel waar nodig hulp van een digitaal expert in

Tabel 5.2h: Indicatoren competentie B.8: Weten hoe onderzoek rondom de PD te verrichten

• Executieve politiemedewerkers moeten in staat zijn tot 'digitaal buurtonderzoek'. Digitaal buurtonderzoek is onderdeel van een 'normaal' buurtonderzoek. Centraal staat het inventariseren van relevante digitale gegevensdragers. Met 'digitaal' wordt dus gedoeld op fysieke middelen die digitale gegevens kunnen bevatten, dus niet bijvoorbeeld het inbreken in digitale netwerken. Dat kan door daar in de omgeving alert op te zijn (hangen er bijv. camera's), maar er ook expliciet naar te vragen aan omstanders (is het incident gefilmd, is er mogelijk een router aangestraald et cetera).

Tabel 5.2i: Indicatoren competentie B.9: Kennis van communicatie met burgers via internet

• Executieve politiemedewerkers moeten ook digitaal in contact kunnen staan met hun wijk/doelgroep. Ze moeten weet hebben van de internettoepassingen die burgers gebruiken en de middelen die ze (dus) zelf kunnen gebruiken om – anders dan voor opsporingsdoeleinden - in contact te zijn met verschillende doelgroepen. De internettoepassingen moeten ze kunnen gebruiken. • Executieve politiemedewerkers, en dan bij uitstek wijkagenten, moeten ook beschikken over een relevant onlinenetwerk.

5.1.3 Kennisnorm voor rechercheurs

In onderstaande tabellen (5.3a-5.3j) zijn per competentie de indicatoren beschreven die gelden voor de drie recherchegroepen. Indien de competenties voor specifieke recherchegroepen gelden (basisteam, district, regio) dan staat dit erbij vermeld. Omdat sommige competenties overlappen met competenties voor intake en service en/of blauw wordt verwezen naar de betreffende tabellen in secties 5.1.1. en 5.1.2.

*Tabel 5.3a: Indicatoren competentie R.1: Verschijningsvormen van digitale criminaliteit kennen en weten te herkennen, en de strafbaarstelling van cyberdelicten weten vast te stellen**

• Zie tabellen 5.1b en 5.1c.

**Notitie. Uit het hoofd kennen van wetsartikelen is onnodig.*

Tabel 5.3b: Indicatoren competentie R.2: Weten hoe op te treden op en rondom een plaats delict

• Zie kennisnormen PD in sectie 5.1.2.

Tabel 5.3c: Indicatoren competentie R.3: Weten hoe met het oog op opsporing de waarde van de aangedragen informatie te beoordelen (bijv.: aangifte/intelligence)

• Aanwijzingen voor de opsporing kunnen filteren uit de input die is aangedragen • Op basis van de 7W vragen kunnen identificeren welke digitale sporen van belang zijn voor het opsporingsonderzoek (in hoeverre kunnen digitale sporen bijdragen aan het beantwoorden van: wie, wat, waar, waarmee, welke wijze, wanneer en waarom). • Kunnen herkennen of sprake is van 'vluchtige gegevens' waarbij – om te voorkomen dat digitale sporen verloren gaan – snel handelen vereist is. Vluchtige gegevens zijn digitale sporen die (vermoedelijk) op korte termijn niet meer te achterhalen zijn, zoals camerabeelden of gegevens uit een router. Als sprake is van vluchtige gegevens moet een expert worden ingeschakeld. • Het zich bewust zijn van andere strategieën dan 'opsporing'. Een bestuursrechtelijke aanpak en/of verstoringstechnieken zijn – zeker bij sommige digitale criminaliteitsvormen - wellicht kansrijker. *Het nemen van beslissingen hierover vindt echter plaats op hoger niveau.

Tabel 5.3d: Indicatoren competentie R.4: Weten hoe planmatig/systematisch aan een opsporingsonderzoek gewerkt kan worden

• Iedere tactisch rechercheur moet zijn/of haar opsporingswerkzaamheden planmatig/systematisch verrichten. • Als aan een opsporingsonderzoek een plan van aanpak (PVA) ten grondslag ligt, moet de rechercheur weten welke activiteit(en) aan hem/haar is toebedeeld. De in het PVA beschreven activiteit(en) moeten dan leidend zijn in de werkzaamheden. Alsnog geldt indicator 1: de specifieke taak moet planmatig/systematisch worden uitgevoerd.

*Tabel 5.3e: Indicatoren competentie R.5: Weten hoe opsporingsonderzoek te verrichten**

• Neem altijd de eigen veiligheid, de veiligheid van slachtoffers, getuigen en verdachten in acht • Vergaar informatie door gebruik te maken van verschillende bronnen. *Volgens Stelfox (2009) kan informatie aanwezig zijn in mensen of als data/sporen in systemen (zie ook Hess Orthman & Matison Hess, 2013)* o Informatie van mensen ➢ Buurtonderzoek ➢ Horen van melders, getuigen, slachtoffers, ➢ Onderzoek aan lichaam en kleding van verdachte(n) ➢ Verhoren van verdachte(n) ➢ Gebruik van (geheime) informanten/inlichtingen ➢ Observatie (menselijk/technisch, bijv. CCTV) ➢ Stelselmatige informatie-inwinning ➢ Infiltratie ➢ Gebruik van compositietekeningen, uitvoeren van confrontaties ➢ Inzet publiek bij identificatie o Informatie in systemen ➢ Gebruik van intelligence (aangiften, dossiers en databases binnen politie) ➢ Informatievergaring op internet ➢ Vorderen van gegevens ➢ Interceptie telecomgegevens ➢ Sporen in gegevensdragers • Kent hulpmiddelen en webapps voor het verrichten van opsporingsonderzoek o Webapp 'cybercrime' o Webapp 'digitale PD' o Webapp 'H.U.I.B (internetbevraging)' o Internetsporen.nl • Ken je eigen beperkingen en schakel waar nodig experts in. Met name in cybercrime-onderzoek, waarin vooral geput moet worden uit digitale sporen, is dat essentieel.

**Notitie. Voor niveauverschillen: zie de specifieke competentiebeschrijvingen voor uitlezen, informatievergaring, vorderen en interceptie.*

Tabel 5.3f: Indicatoren competentie R.6: Kennis van specifieke opsporingskennis en -vaardigheden in een gedigitaliseerde samenleving

Benutten van sporen uit gegevensdragers	• Inbeslagneming o Het kunnen herkennen van gegevensdragers o Kennen van bevoegdheden tot inbeslagname van gegevensdragers (zie PD) o Het, waar nodig in overleg met een digitaal expert, kunnen bepalen welke gegevensdragers relevant zijn voor inbeslagname

Tabel 5.3f (vervolg): Indicatoren competentie R.6: Kennis van specifieke opsporingskennis en -vaardigheden in een gedigitaliseerde samenleving

Benutten van sporen uit gegevensdragers (vervolg)	• Het benutten van digitale sporen in opsporingsonderzoek: o De juiste expert in kunnen schakelen. *Nb.: Schakel bij twijfel over de (on)mogelijkheden om sporen op een gegevensdragers te benutten altijd de hulp van een digitaal expert in* *Nb.: Weet dat het maken van een forensische kopie van de sporen op een gegevensdrager het werk is voor digitaal experts.* o Stap 1: stel, eventueel samen met een digitaal expert, vast welke gegevensdragers beschikbaar zijn voor uitlezen en prioriteer waar nodig o Stap 2: inventariseer, eventueel samen met een digitaal expert, welke mogelijk relevante sporen kunnen worden uitgelezen. ➢ Veel voorkomende gegevens die met behulp van computers, smartphones of tablets – de meest frequent veiliggestelde gegevensdragers – kunnen worden achterhaald zijn: ▪ Persoonsgegevens (gebruikersgegevens, contactenlijst, gesprekkenlijst, telefoonnummer, e-mailadressen, sociale media-accounts) ▪ Berichten ▪ Bestanden ▪ Beeldmateriaal ▪ Locatiegegevens ▪ Informatie voor het maken van een tijdlijn ▪ Browsergeschiedenis ▪ Overige (telefoon)gegevens (serienummers, IP-/MAC-adressen, aangestraalde verbindingen) o Stap 3: overweeg nut en noodzaak van uitlezen o Stap 4: overweeg of uitgelezen gegevens tijdig kunnen worden aangeleverd o Stap 5: stel op basis van de inventarisatie van mogelijk bruikbare sporen gerichte uitleesvragen aan de digitaal expert *Nb.: Houd rekening met jurisprudentie. Het 'volledig uitlezen' van een telefoon is bijvoorbeeld niet zonder meer toegestaan (in verband met inbreuk op privacy)* o Stap 6: ken de eisen die worden gesteld aan de uitleesaanvraag en conformeer de aanvraag hieraan o Gebruik kunnen maken van software, zoals Hansken (forensische zoekmachine), voor de analyse van digitale sporen o Eigen beperkingen kennen: betrek digitaal experts bij het interpreteren van resultaten uit het onderzoek aan gegevensdragers o Verslag kunnen leggen van de bevindingen (zie dossiervorming) ➢ Rapporteer zowel belastend als ontlastend materiaal ➢ Zorg ervoor dat het verslag voor de leek begrijpelijk is ➢ Leg het verslag, waar nodig, voor aan een digitaal expert
Het vorderen van gegevens	• Weten wat (mogelijk) te vorderen sporen zijn. Vorderbare sporen zijn (niet limitatief): o Persoonsgegevens o Beeldmateriaal o Gegevens over internet of telefonie ➢ Identificerende gegevens ➢ Verkeersgegevens ➢ Gegevens over de inhoud van communicatie o Financiële gegevens o Reisgegevens o Administratieve kenmerken • Het kunnen uitzoeken waar en hoe gegevens gevorderd kunnen worden

Tabel 5.3f (vervolg): Indicatoren competentie R.6: Kennis van specifieke opsporingskennis en -vaardigheden in een gedigitaliseerde samenleving

Het vorderen van gegevens (vervolg)	• Het kennen van eigen beperkingen en het waar nodig inschakelen van experts. Zowel bij het opstellen van de vordering, als bij het interpreteren van de resultaten van een vordering. • Werk gestructureerd: o Stap 1: maak op basis van de startinformatie in het onderzoek een overzicht van mogelijk vorderbare sporen o Stap 2: stel vast waar en hoe digitale sporen te verkrijgen zijn (vrijelijk, of door vordering op basis van een bevoegdheid) o Stap 3: bepaal, waar nodig, welke bevoegdheid nodig is (in overleg met leiding en/of OM) o Stap 4: overweeg nut en noodzaak van vorderen ➢ Overweeg proportionaliteit en subsidiariteit ➢ Overweeg bruikbaarheid van de te vorderen gegevens ➢ Overweeg noodzaak van vorderen voor het opsporen van de verdachte en/of bewijsvoering tegen de verdachte ➢ Overweeg tijdigheid van de te vorderen gegevens ➢ Overweeg mogelijk afbreukrisico van vorderen o Stap 4: overweeg het bevriezen van vluchtige gegevens o Stap 5: volg het voorgeschreven vorderingsregime (uit kunnen zoeken wat dat is) ➢ Ken/gebruik de standaardformulieren in bedrijfsprocessensystemen van de politie (BVH/Summ-IT), zodat wordt voldaan aan de eisen die aan een vordering worden gesteld (zie ook de specials in Agora)[24] o Stap 6: Analyseer en waardeer de gevonden informatie
*Interceptie**	• Ken de mogelijkheden voor het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel (interceptie) o Weet dat interceptiemogelijkheden bestaan om 'tapkenmerken' te verkrijgen (bijv. met behulp van de IMSI-catcher ('international mobile subscriber identity') of een bestandsanalyse van basisstationverkeersgegevens). Het verkrijgen van tapkenmerken heeft uiteindelijk tot doel om een tap te kunnen plaatsen. o Weet dat 'verkeersgegevens' kunnen worden onderschept. Het gaat dan om een tap zonder dat de inhoud van de communicatie wordt verkregen (bijv. alleen wanneer gebeld is, naar welk nummer en hoe lang). o Weet dat interceptiemogelijkheden bestaan 'ter plaatsbepaling', bijvoorbeeld om te achterhalen waar een verdachte zich bevindt. o Weet dat interceptiemogelijkheden bestaan om de actuele en toekomstige inhoud van telefonie en/of internetcommunicatie te tappen. • Uit kunnen zoeken hoe interceptiemogelijkheden toegepast kunnen worden en wie daarbij betrokken moeten worden. • Het kennen van eigen beperkingen en het waar nodig inschakelen van experts. Zowel bij het aanvragen en toepassen van interceptiemogelijkheden, als bij de interpretatie van interceptieresultaten.

**Notitie. De uitvoering van interceptiemogelijkheden is voorbehouden aan de recherche op districtsniveau of hoger. Deze competentie geldt niet voor rechercheurs op basisteamniveau. Het kennen van interceptiemogelijkheden is echter van toepassing op zowel basis-, districts- als eenheidsniveau*

[24] BVH staat voor Basisvoorziening Handhaving en is een incidentregistratiesysteem dat wordt gebruikt door de Nederlandse politie. Summ-IT is een politieregistratiesysteem van de Nederlandse politie. Agora is een voorziening voor samenwerken binnen de Nederlandse politie.

Tabel 5.3g: Indicatoren competentie R.7: Weten hoe onderzoeksbevindingen te analyseren en duiden

• Nadat (digitale) sporen zijn verzameld, is het belangrijk om de onderzoeksbevindingen te analyseren en te duiden. • Het identificeren/uitsluiten van verdachte(n) staat centraal. Gebruik/toets zowel belastende als ontlastende scenario's om tunnelvisie tegen te gaan. • Gebruik kunnen maken van software, zoals Hansken, voor de analyse van digitale sporen. • Eigen beperkingen kennen: betrek digitaal experts bij het interpreteren van resultaten uit digitaal onderzoek.

Tabel 5.3h: Indicatoren competentie R.8: Weten hoe de waarde van bewijs te beoordelen (evidential evaluation)

• Gebruik kunnen maken van een bewijsmatrix om te bepalen of er voldoende bewijs is verzameld om (elementen uit) een strafbaar feit aan te tonen.

Tabel 5.3i: Indicatoren competentie R.9: Weten hoe eigen onderzoekshandelingen vast te leggen

• Het ter verantwoording van onderzoeksresultaten systematisch vastleggen van eigen onderzoekshandelingen. • Het in 'lekentaal' verslag leggen van onderzoeksresultaten. • Zorg voor overdraagbaarheid: iedere collega moet het proces-verbaal snappen en interpreteren zoals het is bedoeld. Leg het proces-verbaal waar nodig ter controle voor aan een collega. • Eigen beperkingen kennen: schakel voor zorgvuldige verslaglegging van digitaal onderzoek, waar nodig, een digitaal expert in (voorkom fouten zoals foutieve weergave van IP-adressen).

5.1.4 Kennisnorm informatiegaring op internet

In onderstaande tabellen (5.4a-5.4f) zijn de indicatoren voor informatiegaring op internet weergegeven. Deze zijn geldend voor alle functiegroepen. Hierbij is overigens wel sprake van niveauverschil, maar het verschil manifesteert zich op persoons- en niet op organisatieniveau. Het niveauverschil hangt af van de taakstelling (en opleiding) van de medewerker, ongeacht in welk team hij/zij zich bevindt.

Tabel 5.4a: Indicatoren Informatiegaring op internet: Kennis van internet en sporen

• Kent voorbeelden van het gebruik van internetbronnen en sociale media binnen de politieorganisatie, zoals informatie zoeken in internetbronnen (Intel/OSINT), communiceren met burgers via website, Facebook, Twitter, Instagram, et cetera, (Webcare) Facebook advertising ten behoeve van opsporing bij een (moord)onderzoek, et cetera.[25] • Weet waar in de politieorganisatie de verantwoordelijkheid ligt om internetbronnen en sociale media te gebruiken voor voorgaande (opsporings)doelen en kent daarmee ook de eigen rol. • Stelt zich actief op de hoogte van aanwijzingen (beleid, procedures), tips en trucs vanuit de politieorganisatie over het omgaan met internetbronnen (zowel ten behoeve van onderzoek, opsporing als communiceren). • Kent het onderscheid tussen: OSINT, Cybercrime en Internetrechercheren en kent de verbanden daartussen.

[25] Intel staat voor intelligence. OSINT staat voor opensource intelligence.

Tabel 5.4a (vervolg): Indicatoren Informatiegaring op internet: Kennis van internet en sporen

- Is digibewust; weet wat internet is en hoe het werkt:
    - Weet dat je bij het navigeren in sociale media / internetbronnen, sporen achterlaat
    - Weet wat voor sporen je achterlaat als je op internet aan het zoeken bent
    - Weet dat onlinebronnen en sociale media op allerlei manieren relaties met elkaar leggen en dat jouw sporen dus aan elkaar worden 'geknoopt'
    - Kent het onderscheid tussen clearweb, deepweb, en darkweb[26]
- Weet dat een informatiespoor achter blijft wanneer hij een website bezoekt en kent de afbreukrisico's voor een politieonderzoek.
- Is zich continu bewust van de kans op afbreukrisico's en herkent situaties waarin deze kunnen optreden.
- Weet dat hij bij het gebruik van internetbronnen / sociale media werk en privé gescheiden van elkaar moet houden.
- Weet hoe hij bij het gebruik van internetbronnen / sociale media werk en privé gescheiden van elkaar moet houden.
- Weet wat een IP-adres is.
- Kent het verschil tussen interne en externe IP-adressen.
- Weet hoe een IPv4- en IPv6-adres eruitzien en waarom nieuwe IP-adressen zijn gemaakt.
- Kent het begrip en de organisatie rondom domeinnamen.
- Weet dat je sporen op internet veilig kunt stellen, zoals sporen van chats, e-mail, fora, onlinegames, et cetera.

Tabel 5.4b: Indicatoren Informatiegaring op internet: Kennis van het juridisch kader

- Kent de juridische implicaties en (on)mogelijkheden van het zoeken naar informatie op Internet (de globale lijn).
- Is bekend met de beslisboom (hulpmiddel op intranet) om te bepalen of een onderzoek uitgevoerd kan worden binnen de kaders van PW3 (art. 3 Politiewet 2012), of dat overleg gepleegd moet worden met een informatie-officier of de OvJ.
- Is zich bewust van de kwaliteit van gevonden informatie op internet en het (afbreuk)risico dat dit kan opleveren. Het internet bevat ook informatie afkomstig van derden die zich voordoen als een specifiek persoon.
    - Niet zomaar conclusies trekken op basis van informatie die je vindt. Het kan dienen als achtergrondinformatie.
- Kent de relevante artikelen van de (Politie)wet, die aangeven welke informatie je wel/niet mag opzoeken en wanneer stelselmatige observatie geoorloofd is:
    - Kan voorbeelden noemen van informatie die hij wel/niet mag opzoeken
    - Kan voorbeelden noemen van stelselmatige observatie met gebruikmaking van internetbronnen
    - Kan voorbeelden noemen van handelingen die kunnen leiden tot stelselmatige observatie op internet, zoals: met één zoekslag een min of meer compleet beeld krijgen van een persoon; herhaalde zoekacties naar een persoon.
- Weet wat een BOB-middel (bijzondere opsporingsbevoegdheden) is en wanneer dit noodzakelijk is in relatie tot Intel, OSINT / opsporing met gebruikmaking van internet.
- Begrijpt dat er een omslagpunt is van Politiewet art. 3 (taakomschrijving van de politie met betrekking tot surveillance) naar de opsporing (art. 27 strafvordering) en wat dit betekent voor het gebruiken van internetbronnen.
- Is bekend met privacywetgeving in relatie tot het zoeken en vastleggen van informatie van internet.

[26] Met clearweb worden open geïndexeerde bronnen bedoeld, ofwel publiektoegankelijke websites. Met deepweb worden plekken op internet bedoeld die afgeschermd zijn van het publiek. Deze plekken zijn alleen toegankelijk via authenticatie. Het darkweb kan gezien worden als plekken binnen het deepweb die opzettelijk aan het zicht zijn onttrokken. Anonimiteit is hierbij cruciaal.

Tabel 5.4b (vervolg): Indicatoren Informatiegaring op internet: Kennis van het juridisch kader

- Kent voorbeelden waarbij er sprake is van een meer dan geringe inbreuk op iemands privacy en weet wat hij zelf mag doen en wat hij moet doorsturen naar een ander.
- Weet dat hij contact en communicatie bij surveilleren/zoeken in internetbronnen moet vermijden.
- Weet bij informatieverzoeken of hij zelf naar informatie kan/moet zoeken of dat hij dit moet overlaten aan een collega (op een hoger niveau).

Tabel 5.4c: Indicatoren Informatiegaring op internet: Kennis van monitoren en identificeren

- Weet wat zoektermen zijn en levert zinvolle zoektermen aan (UIL'tjes: Unique Identifying Labels) zodat een identificatie-/traceeractie gestart kan worden. Zinvolle zoektermen komen vooral uit de context van het politiewerk en de specifieke kennis van de medewerker (bijv. op thema's zoals voetbal, evenementen, drugs, jeugdcriminaliteit, et cetera).
- Kan op basaal niveau gegevens vinden over subjecten en objecten.
- Beperkt de zoektijd van een informatieverzoek tot maximaal een half uur.
- Gebruikt H.U.I.B. (Half uur internet bevraging):
    - Volgt de stappen in H.U.I.B. om in een beperkt aantal bronnen een zoekslag te doen of gebruikt de methodiek van H.U.I.B.
    - Vult de invulvelden in H.U.I.B. met de gevonden informatie.
- Bepaalt of de gevonden informatie vastgelegd moet worden in BVH.
- Legt informatie vast door middel van een print screen.
- Legt de domeinnaam vast (in een informatieverslag of in een proces-verbaal [PV]).
- Download een pdf uit H.U.I.B. en maakt deze beschikbaar voor collega's.
- Voegt de PDF uit H.U.I.B. toe aan het PV van aangifte en/of voegt de informatie toe aan BVH.

Tabel 5.4d: Indicatoren Informatiegaring op internet: Kennis van tools (iRN, Google)

- Weet dat je door gebruik te maken van iRN, veiliger zoekt op Internet.
- Scheidt iRN en politiesystemen om besmetting van politiesystemen te voorkomen.
- Weet waarvoor iRN gebruikt wordt (voor politiezaken) en waarvoor het bruikbaar is:
    - Doet geen privé dingen op een iRN computer.
    - Gebruikt geen privéaccounts om in bronnen in te loggen, bijvoorbeeld Facebook, et cetera.
- Heeft basiskennis van de configuratie van de iRN computer, namelijk:
    - Linux besturingssysteem (geen Windows- of MAC-besturingssysteem).
    - Libre Office in plaats van Microsoft office, et cetera.
- Kent de kenmerken, de mogelijkheden en de risico's van het gebruik van iRN en Google.
- Kent de wijze van gebruik van iRN:
    - Weet hoe hij moet inloggen op iRN.
    - Weet hoe hij gebruik kan maken van iRN mail.
    - Weet hoe hij gebruik kan maken van iRN Cloud en gedeelde mappen.
- Weet dat hij op een iRN computer met de browser Firefox moet werken.
- Heeft basiskennis van de wijze waarop een zoekmachine als Google werkt.
- Kent de meest gebruikte internationale zoekmachines (bijv. Google, Yahoo, Bing, Bai, Yandex, DuckDuckGo)
- Kent de basis zoekoperatoren van Google, zoals:
    - AND, OR.
    - Exacte woorden via 'xxx', 'zzz'.
    - Specifieke site via 'site:'
- Weet dat je dezelfde (basis) zoekoperatoren ook kunt gebruiken in andere internetzoekmachines.

*Tabel 5.4e: Indicatoren Informatiegaring op internet: Kennis van bronnen**

• Kent de belangrijkste kenmerken van genoemde internetbronnen en sociale media. • Kent de wijze waarop mensen gebruik maken van genoemde internetbronnen en sociale media. • Weet welk type informatie je kunt vinden op diverse internetbronnen en sociale media. • Weet welke bron welke informatie bevat, bijvoorbeeld: Facebook = persoonlijke berichtjes en foto's; Instagram = foto's; SnapChat = foto's (bewerkt met filters); Twitter = berichtjes en reacties; YouTube = video; et cetera. • Weet dat er continu ontwikkelingen zijn in het landschap van sociale media / internetbronnen. • Kent websites met vrij toegankelijke informatie over personen en organisaties, zoals: detelefoongids.nl en postnl.nl/postcode-zoeken. • Weet hoe je als politiemedewerker redelijk veilig informatie kunt vinden op deze internetbronnen, zonder sporen achter te laten.

**Notitie. Onder bronnen wordt verstaan: Open geïndexeerde bronnen (clearweb) waarbij het zoeken naar informatie voldoet aan de kenmerken: (a) vrij toegankelijk, (b) er is geen account nodig en er wordt geen account gebruikt om informatie te vinden, (c) met klein afbreukrisico (relatief anoniem te raadplegen), en (d) "vluchtig" informatie zoeken, ad hoc / "eenmalig".*

Tabel 5.4f: Indicatoren Informatiegaring op internet: Kennis van taal / jargon / thema's

• Is bekend met het taalgebruik (straattaal) / jargon van de context (persoon/groep) die hij onderzoekt.

5.2 Kennis in de praktijk

In deze paragraaf zijn de vragenlijstresultaten gepresenteerd. De resultaten zijn gepresenteerd aan de hand van de geïdentificeerde kennisnormen uit paragraaf 5.1. Daaraan zijn nummers toegekend, zodat duidelijk is op welke normen de resultaten betrekking hebben. De nummers zijn tevens voorzien van een letter (I, B, R) die weerspiegelen op welke functiegroep de norm betrekking heeft (respectievelijk intake en service, blauw, recherche). Bij het presenteren van de resultaten geven we soms aan dat de scores hoog of laag zijn. Dit betekent respectievelijk hoger of lager dan het gemiddelde op de betreffende antwoordschaal. Wij bepalen in dit onderzoek niet de cesuur, en spreken dus niet van voldoende/onvoldoende, goed/fout, toereikend/ontoereikend, et cetera.

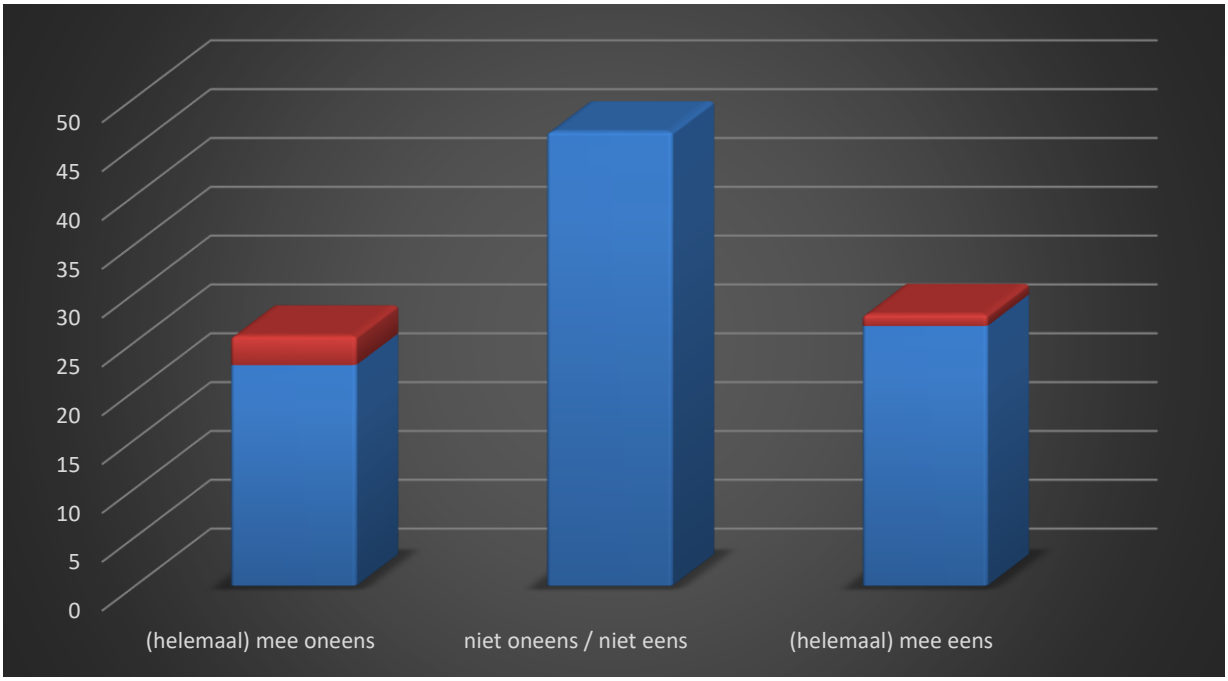
Waar van toepassing worden verschillen tussen de functiegroepen getoond ($p < 0{,}01$). Deze verschillen worden getoond in een tekstkader om het overzicht te bewaren en de snelheid van het lezen te bevorderen. We geven daarbij aan of scores per groep hoger of lager zijn dan bij andere groepen. Hoger wil in dit verband zeggen dat politiemensen hun eigen kennis hoger schatten en vice versa.

Naast significantie is ook gekeken naar effectgrootten en samenhang. Vanaf een middelmatig effect wordt hiervan verslag gedaan. Ter verduidelijking hebben we in die gevallen het woord 'effect' dikgedrukt. Dit betekent dat wanneer effecten klein tot middelmatig zijn en/of de samenhang zwak is, geen extra informatie wordt getoond. De statistische output die deze claims onderbouwen is opgenomen in een addendum (Jansen & Van Valkengoed, 2019).

5.2.1 Verschijningsvormen van digitale criminaliteit

Verschijningsvormen van digitale criminaliteit kennen en kunnen herkennen op basis van praktijksignalen is aan alle functiegroepen is voorgelegd (I.2, I.3., R.1). Allereerst is een algemene stelling voorgelegd: 'Ik weet wat voor strafbare gedragingen vallen onder de term digitale criminaliteit.' Bijna de helft (46,5%) gaf aan het hiermee niet oneens, maar ook niet eens te zijn, zie Figuur 5.1. Ongeveer een kwart (27,8%) is het (helemaal) eens met de stelling en het resterende kwart (25,6%) is het hiermee (helemaal) oneens.

Figuur 5.1: Kennis van strafbare gedragingen digitale criminaliteit (N = 402)



Politiemensen die een opleiding of cursus hebben gevolgd op het gebied van digitale criminaliteit (M = 3,26) scoren significant hoger dan politiemensen die dit niet hebben (M = 2,91). Daarnaast scoren politiemensen met geen tot weinig ervaring met zaken op het gebied van digitale criminaliteit (M = 2,82) significant lager dan politiemensen die niet weinig, maar ook niet veel (M = 3,12) en die veel tot uitsluitend (M = 3,24) ervaring hebben met dergelijke zaken.

Vervolgens zijn vier casussen aan de respondenten voorgelegd die betrekking hebben op digitale criminaliteit, zie bijlage VI. Voor elke casus werd gevraagd van welk strafbaar feit of feiten sprake is. Per casus konden respondenten kiezen uit zes antwoorden, of aangeven dat er in de casus geen strafbaar feit was opgenomen.

Gemiddeld over de vier casussen heeft ongeveer twee derde van de respondenten één of alle juiste antwoorden aangekruist (per casus), zonder daarbij een onjuiste antwoordoptie aan te vinken. De resterende respondenten (30,9%) hebben minimaal één onjuist antwoord gegeven (per

casus). Per casus ziet dit er als volgt uit. Casus 1: juist (40,5%), één van twee juist (20,4%), onjuist (39,1%). Casus 2: juist (46,3%), één van twee juist (31,6%), onjuist (22,1%). Casus 3: juist (26,9%), één van twee juist (44,5%), onjuist (28,6%). Casus 4: juist (17,2%), twee van drie juist (38,3%) één van drie juist (10,7%), onjuist (33,8%). Kortom, het gros van de respondenten is in staat om digitale criminaliteit te herkennen in voorgelegde casuïstiek.

5.2.2 Optreden op en rondom een plaats delict

De vragen omtrent het optreden op en rondom een plaats delict (PD) zijn alleen voorgelegd aan de functiegroepen blauw en recherche (B.5, B.6, B.7, B.8, R.2). De resultaten in deze sectie zijn gebaseerd op N = 338 respondenten.

Allereerst is een aantal stellingen opgenomen over een PD met digitale sporen, zie Tabel 5.5. De respondenten geven over het algemeen aan (helemaal) eens te zijn met de stellingen dat bij twijfel over bevoegdheden een expert moet worden ingeschakeld en dat tijdens een buurtonderzoek ook aandacht moet zijn voor het inventariseren van digitale sporen. De stellingen die gaan over weten welke risico's bestaan met betrekking tot het besmetten/vernietigen van sporen en over de basisprocedures van het veiligstellen van digitale gegevensdragers, zijn wisselend beantwoord.

Tabel 5.5: Optreden rondom een PD (in procenten, N = 338)

		(helemaal) mee oneens		(helemaal) mee eens
1.	Ik weet welke risico's er zijn met betrekking tot het besmetten/vernietigen van digitale sporen.	32,0	30,5	37,6
2.	Bij twijfel over bevoegdheden om handelingen te verrichten op een PD met digitale sporen moet een expert worden ingeschakeld.	3,0	1,8	95,3
3.	Ik ken de basisprocedure voor het veiligstellen van digitale gegevensdragers.	35,2	31,7	33,1
4.	Tijdens een buurtonderzoek moet ook aandacht zijn voor het inventariseren van digitale sporen.	3,3	9,5	87,3

Voor de eerste, derde en vierde stelling zijn significante verschillen gevonden tussen de functiegroepen. Voor de eerste en derde stelling geldt dat blauw (M = 2,90; M = 2,33) lager scoort dan districtsrecherche (M = 3,15; M = 3,10) en regionale recherche (M = 3,19; M = 3,06). Bij de derde stelling is sprake van een middelmatig **effect**. Bij de vierde stelling scoort regionale recherche (M = 4,35) hoger dan basisteamrecherche (M = 3,96).

Voor de eerste stelling werd ook een significant verschil gevonden tussen mannen (M = 3,12) en vrouwen (M = 2,76), waarbij mannen gemiddeld hoger scoorden. Politiemensen die een opleiding of cursus hebben gevolgd op het gebied van digitale criminaliteit scoren significant hoger op stelling één en drie (M = 3,52; M = 3,33) dan politiemensen die dit niet hebben (M = 2,82; 2,73). Voor opleiding is bij stelling één het **effect** middelmatig tot groot en bij de derde middelmatig.

Vervolgens is een aantal kennisvragen opgenomen met betrekking tot handelingen op een PD met digitale sporen. Aan de respondenten werd gevraagd in hoeverre zij dachten dat deze handelingen juist of onjuist zijn. In Tabel 5.6 zijn de handelingen opgenomen en hoe respondenten daarop hebben geantwoord. De onjuiste handelingen zijn voorzien van de kleur grijs. Met uitzondering van de handeling 'met blote handen een geaard voorwerp aanraken in verband met mogelijk statisch geladen zijn' scoren de respondenten goed op handelingen die verricht moeten worden. Bij de handelingen die 'niet' verricht moeten worden, zijn de respondenten verdeeld wanneer het gaat om 'hulp vragen aan de eigenaren van de ICT'. Hoewel dit normaal gesproken 'fout' is, kan het bij nader inzien in sommige gevallen wel correct zijn. Denk bijvoorbeeld aan een zaak die zich afspeelt in een serverruime van een groot datacentrum.

Tabel 5.6: Handelingen op een PD (in procenten, N = 338)

Als ik een PD met digitale sporen betreed dan moet ik:		**Onjuist**	**Juist**
1.	Met blote handen een geaard voorwerp aanraken in verband met mogelijk statisch geladen zijn.	87,6	12,4
2.	Zo spoedig mogelijk alle elektronische apparatuur uitschakelen.	90,8	9,2
3.	Handelingen verrichten om te voorkomen dat sporen op afstand worden gewist.	4,4	95,6
4.	Erop toezien dat digitale sporen niet worden besmet.	2,4	97,6
5.	Hulp vragen aan de eigenaren van de ICT.	56,2	43,8
6.	Hulp vragen aan omstanders.	97,3	2,7
7.	Van tevoren op de eigen gegevensdrager(s) wifi en bluetooth uitzetten.	13,3	86,7

Bij meerdere antwoordopties zijn significante verschillen gevonden. Het uitzetten van wifi en bluetooth (7) werd door regionale recherche vaker juist gescoord dan blauw en werd door districtsrecherche vaker juist gescoord dan basisteamrecherche. Hulp vragen aan ICT-eigenaren (5) werd vaker incorrect beantwoord door basisteamrecherche dan districtsrecherche.

Politiemensen die een opleiding of cursus hebben gevolgd op het gebied van digitale criminaliteit kiezen vaker het juiste antwoord op de eerste en het incorrecte antwoord op vijfde handeling dan politiemensen zonder een dergelijke opleiding of cursus.

De respondenten kregen daarna een aantal juist-onjuist vragen met betrekking tot gegevensdragers die worden aangetroffen op een PD, zie Tabel 5.7. Voor alle vragen geldt dat de meerderheid van de respondenten de vragen goed had. De twee vragen die het best zijn beantwoord, betreffen de twee stellingen die 'juist' zijn geformuleerd. Op vragen die 'niet juist' zijn geformuleerd werden minder eenduidig beantwoord.

Tabel 5.7: Acties betreffende digitale gegevensdragers (in procenten, N = 338)

		Onjuist	Juist
1.	Er moet worden vastgesteld welke gegevensdragers aanwezig zijn op de PD.	1,2	98,8
2.	Gegevensdragers moeten worden veiliggesteld van groot naar klein.	70,7	29,3
3.	Het is niet belangrijk om de status van gegevensdragers vast te stellen (bijv. of ze aan of uit staan).	92,2	7,1
4.	Digitaal experts kunnen worden ingeschakeld bij het veiligstellen van digitale gegevensdragers.	0,9	99,1
5.	Gegevensdragers die snel kunnen worden uitgelezen moeten als eerste worden veiliggesteld.	60,7	39,3
6.	Digitale gegevensdragers mogen alleen worden veiliggesteld door collega's die een forensische opleiding hebben afgerond	72,5	27,5

Bij een uitspraak werd in de functiegroepanalyse een significant verschil gevonden. Het gaat om de uitspraak over het (onjuist) eerst veiligstellen van gegevensdragers die snel uitgelezen kunnen worden. De groep blauw (M = 1,59) gaf vaker het incorrecte antwoord ten opzichte van de groepen districtsrecherche (M = 1,31) en regionale recherche (M = 1,33).

Politiemensen die geen opleiding of cursus hebben gevolgd op het gebied van digitale criminaliteit (M = 1,44) kozen ook significant vaker voor de incorrecte optie was dan politiemensen die dit wel hebben (M = 1,27).

De volgende drie juist-onjuist vragen hebben betrekking op bewijsvoering, zie Tabel 5.8. Meer dan 90% van de respondenten hebben de vragen over bewijsvoering correct beantwoord.

Tabel 5.8: Bewijsvoering (in procenten, N = 338)

		Onjuist	Juist
1.	Uitsluitend klassieke of uitsluitend digitale sporen meenemen van een PD is voldoende om een sporenbeeld te maken.	97,6	2,4
2.	Voor het vaststellen van het sporenbeeld op de PD is het belangrijk om zowel klassieke als digitale sporen veilig te stellen.	0,3	99,7
3.	Op een PD weegt het veiligstellen van klassieke sporen altijd zwaarder dan het veiligstellen van digitale sporen.	92,6	7,4

Op de derde stelling gaven vijftigplussers (M = 1,04) significant vaker het incorrecte antwoord dan politiemensen onder de vijftig jaar (M = 1,11).

Daaropvolgend kregen de respondenten de vraag welke stap(pen) ze zouden zetten wanneer ze een voor hen onbekende gegevensdrager aantreffen op een PD. Er werden zeven antwoordopties gegeven waarvan twee correct zijn (een specialist inschakelen en gebruikmaken van de webapp 'Digitale PD'). Iets meer dan de helft (54,1%) kruiste een of beide correcte opties aan (zonder een onjuiste optie aan te klikken). De overige respondenten hadden minimaal een onjuist antwoord gegeven. Echter, 'specialist inschakelen' werd wel door 95,9% gekozen als een te nemen stap. De

webapp werd in minder mate aangekruist (22,5%). Een onjuiste actie die het vaakst werd genoemd is 'Ik stel deze veilig zoals ik dat gewend ben te doen met andere, voor mij bekende, gegevensdragers' (32,8%).

Bij drie antwoordopties kwamen significante verschillen naar boven. Politiemensen die geen opleiding of cursus hebben gevolgd op het gebied van digitale criminaliteit kozen significant vaker de onjuiste actie over veiligstellen dan politiemensen die wel een opleiding of cursus hebben gevolgd. Het (onjuist) registreren van een serienummer werd vaker door blauw aangegeven dan door regionale recherche. Blauw kiest significant vaker het juiste antwoord om de webapp digitale PD te raadplegen dan de regionale recherche. Dit geldt ook voor de jongere groep ten aanzien van de vijftigplussers. Politiemensen die niet veel, maar ook niet weinig ervaring hebben met zaken op het gebied van digitale criminaliteit kozen significant vaker het juiste antwoord om de webapp Digitale PD te raadplegen dan politiemensen die geen tot weinig ervaring hebben met dergelijke zaken.

Vervolgens werd aan de respondenten gevraagd om een zestal gegevensdragers te herkennen die politiemensen kunnen tegenkomen op een PD. Vier gegevensdragers werden over het algemeen herkend: smartphone (100%), tapedrive (93,5%), NAS/server (86,7%) en activity tracker (86,4%). De twee andere gegevensdrager werden minder herkend: switch (43,8%) en omgebouwde desktop (35,2%).

5.2.3 Digitale sporen

De resultaten binnen deze sectie hebben betrekking op digitale sporen en zijn alleen beantwoord door de drie recherchegroepen (N = 284) (R.3, R.5, R.6). Allereerst is aan de respondenten een aantal stellingen voorgelegd met betrekking tot digitale sporen en opsporingsonderzoek, zie Tabel 5.9. Wat opvalt is dat de respondenten bij de eerste drie stellingen voornamelijk de middelste antwoordcategorie hebben gekozen. Als het gaat om inzicht in eigen beperkingen en handelen bij onvoldoende kennis scoren de respondenten hoger.

Tabel 5.9: Digitale sporen (in procenten, N = 284)

		(helemaal) mee oneens		(helemaal) mee eens
1.	Ik weet welke digitale sporen van belang zijn voor opsporingsonderzoek.	23,2	45,8	31,0
2.	Ik weet hoe de 7 W's (wie, wat, waar, waarmee, welke wijze, wanneer, waarom) kunnen worden toegepast om de relevantie van digitale sporen te bepalen.	26,4	66,9	33,1
3.	Alternatieven dan het strafrecht kunnen effectiever zijn bij de bestrijding van digitale criminaliteit.	8,8	52,8	47,2

Tabel 5.9 (vervolg): Digitale sporen (in procenten, N = 284)

		(helemaal) mee oneens		(helemaal) mee eens
4.	Ik ken mijn eigen beperkingen bij het verrichten van een opsporingsonderzoek naar digitale criminaliteit.	3,9	11,6	88,4
5.	Ik weet hoe ik moet handelen wanneer ik bij het verrichten van opsporingsonderzoek naar digitale criminaliteit onvoldoende kennis heb.	14,1	28,2	71,8
6.	Ik weet wat 'vluchtige gegevens' zijn.	14,4	29,9	70,1

Bij de vijfde en zesde stelling zijn significante verschillen gevonden tussen de functiegroepen. Bij stelling vijf scoort districtsrecherche (M = 3,79) hoger dan basisteamrecherche (M = 3,42). Bij stelling zes scoort de basisteamrecherche (M = 3,12) lager dan districtsrecherche (M = 3,84) en regionale recherche (M = 3,99) en is het **effect** groot.

Wat betreft de analyse van politiemensen die wel of geen opleiding of cursus hebben gevolgd op het gebied van digitale criminaliteit werden bij de eerste, tweede, vijfde en zesde stelling significante verschillen gevonden. In alle gevallen scoorde de groep die een opleiding of cursus heeft gevolgd (M = 3,34; M = 3,27; M = 3,91; M = 3,91) hoger dan de groep die dit niet heeft (M = 2,93; M = 2,96; M = 3,59; M = 3,55).

De zeven op de tien rechercheurs die weten wat wordt bedoeld met vluchtige gegevens (N = 199) werd een aanvullende stelling gepresenteerd. Op de stelling 'ik weet hoe te handelen wanneer er sprake is van digitale vluchtige gegevens' antwoordde 41,7% (helemaal) mee eens. Een derde (34,7%) was een neutrale mening toegedaan en een kwart (23,6%) was het er (helemaal) mee oneens.

De volgende stellingen gaan over kennis van het benutten van sporen uit gegevensdragers, zie Tabel 5.10. Wat opvalt in de tabel is dat er veel spreiding is over de verschillende antwoordcategorieën terwijl dezelfde competentie centraal staat.

Tabel 5.10: Kennis van het benutten van sporen uit gegevensdragers (in procenten, N = 284)

		(helemaal) mee oneens		(helemaal) mee eens
1.	Ik ken de bevoegdheden tot inbeslagname van gegevensdragers.	12,7	26,1	61,3
2.	Ik weet welke gegevensdragers op een PD relevant zijn voor inbeslagname.	15,5	37,3	47,2
3.	Ik weet welke gegevensdragers kunnen worden uitgelezen.	16,5	41,2	42,3
4.	Ik weet welke digitale sporen kunnen worden uitgelezen.	22,9	46,5	30,6
5.	Ik weet tijdens een onderzoek wanneer het nuttig/noodzakelijk is om gegevensdragers uit te lezen.	12,0	38,0	50,0
6.	Ik weet hoeveel tijd het kost om een gegevensdrager uit te laten lezen.	26,8	24,3	48,9
7.	Ik weet hoe lang het duurt om het resultaat van een uitleesaanvraag te ontvangen.	27,1	26,8	46,1

Tabel 5.10 (vervolg): Kennis van het benutten van sporen uit gegevensdragers (in procenten, N = 284)

		(helemaal) mee oneens		(helemaal) mee eens
8.	Ik weet hoe gerichte uitleesvragen opgesteld moeten worden waarmee de digitaal expert aan de slag kan.	33,8	26,4	39,8
9.	Ik weet welke eisen zijn verbonden aan uitleesvragen.	47,5	32,4	20,1
10.	Ik weet hoe ik softwarepakketten moet gebruiken om digitale sporen te analyseren.	69,0	19,4	11,6
11.	Ik weet hoe ik de bevindingen van digitaal sporenonderzoek moet vastleggen (dossiervorming).	36,3	23,9	39,8
12.	Ik weet dat het maken van een forensische kopie van de sporen op een gegevensdrager is voorbehouden aan daarvoor opgeleide politiemensen.	12,7	9,5	77,8
13.	Bij twijfel over de interpretatie van de analyseresultaten moet een digitaal expert worden ingeschakeld.	4,6	8,1	87,3

Bij de tweede, vierde en zevende stelling zijn significante verschillen gevonden tussen de functiegroepen. Bij de tweede stelling scoorde districtsrecherche (M = 3,49) hoger dan basisteamrecherche (M = 3,11). Bij de vierde en zevende stelling scoorde regionale recherche (M = 3,20; M = 3,38) hoger dan basisteamrecherche (M = 2,84; M = 2,92).

Er zijn veel significante verschillen gevonden tussen politiemensen die wel en geen opleiding of cursus hebben gevolgd op het gebied van digitale criminaliteit. Met uitzondering van de vijfde en elfde stelling werden alle stellingen significant hoger gescoord door de groep die wel een opleiding of cursus heeft gevolgd.

De stellingen die nu volgen gaan over kennis van het vorderen van gegevens, zie Tabel 5.11. Uit de tabel wordt duidelijk dat de kennis hiervan in wisselende mate aanwezig is. Bij twijfels over (on)mogelijkheden tot vordering en prioritering van te vorderen gegevens geven de meeste respondenten aan dat een expert moet worden ingeschakeld.

Tabel 5.11: Kennis van het vorderen van gegevens (in procenten, N = 284)

		(helemaal) mee oneens		(helemaal) mee eens
1.	Ik weet hoe ik uit moet zoeken welke digitale sporen gevorderd kunnen worden.	23,6	31,3	45,1
2.	Ik weet hoe ik vorderbare digitale sporen kan herkennen.	37,0	43,3	19,7
3.	Bij twijfel over de (on)mogelijkheden om digitale sporen te vorderen moet een expert worden ingeschakeld.	1,8	5,3	93,0
4.	Bij twijfel over het geven van prioriteit aan het vorderen van digitale sporen moet een expert worden ingeschakeld.	3,2	7,4	89,4

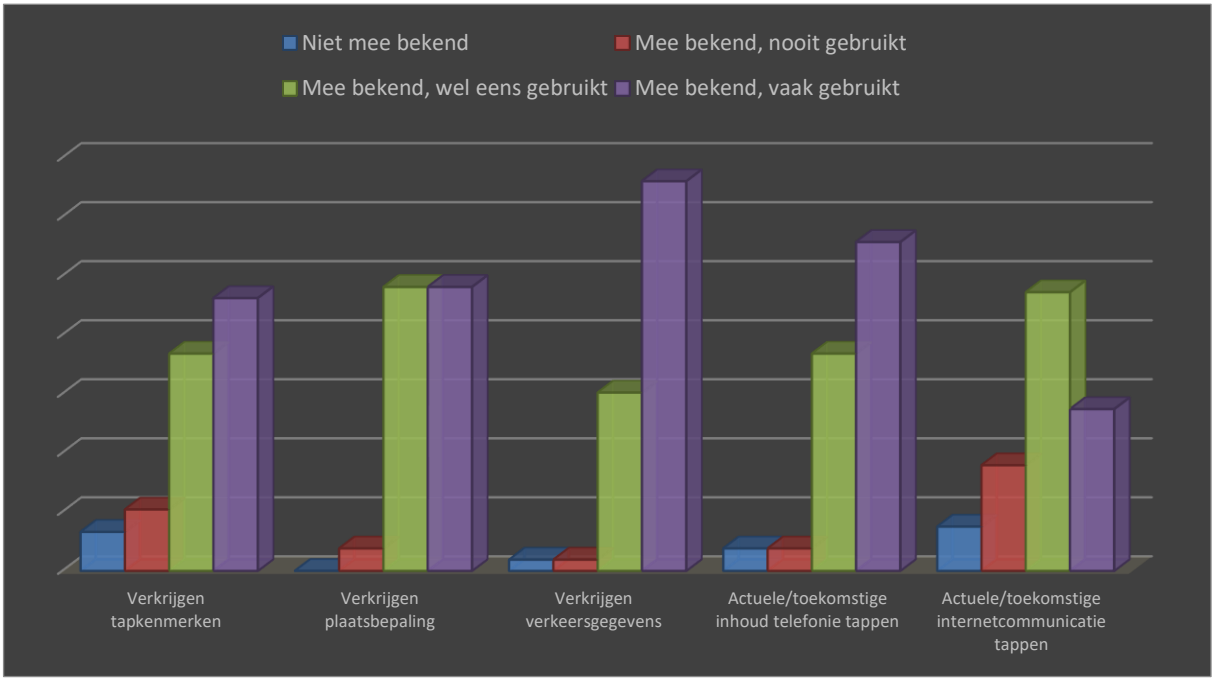
Bij de eerst en tweede stelling scoren mannen (M = 3,30; M = 2,86) significant hoger dan vrouwen (M = 2,97; M = 2,56). Dit geldt ook voor politiemensen die een opleiding of cursus hebben gevolgd op het gebied van digitale criminaliteit (M = 3,45; M = 3,01) ten opzichte van politiemensen die dit niet hebben (M = 3,09; M = 2,67).

De volgende stellingen gaan over kennis met betrekking tot interceptie. Allereerst is een selectievraag gesteld in hoeverre men weet wat interceptie is. Op de stelling ‘ik weet wat interceptie is’ antwoordde 73,6% (helemaal) mee eens. Nadere analyse laat zien dat basisteamrecherche (M = 3,95) hierop significant lager scoort dan districtsrecherche (M = 4,13) en regionale recherche (M = 4,30).

De daaropvolgende stelling had betrekking op of men de mogelijkheden van interceptie kent. Deze stelling is alleen voorgelegd aan de functiegroepen districtsrecherche en regionale recherche, die de vorige stelling antwoordden met (helemaal) mee eens (N = 165). 64,2% was het hier (helemaal) mee eens (N = 106). Deze 106 respondenten hebben vervolgens twee aanvullende stellingen en vijf vervolgvragen gekregen met betrekking tot specifieke vormen van interceptie.

Met de stelling ‘ik weet hoe interceptiemogelijkheden toegepast moeten worden’ was 81,1% het (helemaal) mee eens. Op de stelling ‘bij twijfel over de (on)mogelijkheden van interceptie moet een expert worden ingeschakeld’ werd door 97,2% (helemaal) mee eens geantwoord. De antwoorden op de specifieke interceptiekenmerken zijn weergegeven in Figuur 5.2. Over het algemeen zijn de respondenten bekend met de verschillende interceptiemogelijkheden en heeft de meerderheid deze ook toegepast. Interceptiemogelijkheden om actuele en toekomstige inhoud van internetcommunicatie te tappen en interceptiemogelijkheden om tapkenmerken te verkrijgen (met als doel om een tap te plaatsen) zijn het minst bekend. Respectievelijk 7,5% en 6,6% kennen deze mogelijkheden niet.

Figuur 5.2: (in procenten, N = 106)



De volgende vragen die respondenten kregen, gingen over hulpmiddelen, zie Tabel 5.12. De vragen met betrekking tot webapps van de Politieacademie zijn voorafgegaan aan een selectievraag of men hiermee bekend is. 42,0% gaf aan deze te kennen (n = 169). Opvallend is dat blauw hier significant meer mee bekend is dan intake en service. Wat duidelijk wordt op basis van zowel de selectievraag als de tabel is dat een grote hoeveelheid respondenten de bevraagde hulpmiddelen niet kent. Eveneens is het aandeel dat de hulpmiddelen wel kent, maar nooit heeft gebruikt vrij groot.

Tabel 5.12: Kennis van hulpmiddelen (in procenten)

Hulpmiddel	Ik had nog nooit van deze website/app gehoord	Ik kende de website/app al, maar heb deze nog nooit geraadpleegd	Ik kende de website/app al, en heb deze wel eens geraadpleegd	Ik kende de website/app al, en heb deze vaak geraadpleegd
1. Website internetsporen.nl (N = 402)	66,9	20,6	11,7	0,7
2. Webapp Cybercrime (N = 169)	31,4	55,0	13,0	0,6
3. Webapp Digitale PD (N = 169)	58,6	38,5	3,0	0
4. Webapp H.U.I.B. (N = 169)	74,6	17,2	8,3	0

Tot slot is een aantal algemene termen voorgelegd, zie Tabel 5.13. Over het algemeen weten de respondenten wat met de bevraagde termen wordt bedoeld. Clearweb en deepweb zijn het minst bekend.

Tabel 5.13: Kennis van algemene internettermen (in procenten, N = 402)

Ik weet wat bedoeld wordt met:	(helemaal) mee oneens		(helemaal) mee eens
1. Internetrechercheren	8,5	14,4	77,1
2. Clearweb	74,1	12,7	13,2
3. Deepweb	57,0	11,9	31,1
4. Darkweb	12,9	27,1	72,9
5. IP-adres	1,2	5,7	93,0
6. Domeinnaam	5,2	11,9	82,8

Bij de eerste drie termen zijn significante verschillen gevonden tussen de functiegroepen. Voor de eerste twee termen geldt dat intake en service (M = 3,52; M = 1,72) lager scoort dan districtsrecherche (M = 3,98; M = 2,40) en regionale recherche (M = 4,06; M = 2,38). Voor de derde term geldt dat regionale recherche (M = 3,04) hoger scoort dan intake en service (M = 2,17) en basisteamrecherche (M = 2,40).

Politiemensen die een opleiding of cursus hebben gevolgd op het gebied van digitale criminaliteit scoren significant hoger op de tweede, derde en vierde term (M = 2,53; M = 2,99; M = 3,95) ten opzichte van politiemensen die dit geen opleiding of cursus hebben gevolgd (M = 2,02; M = 2,48; M = 3,66).

5.2.4 Informatiegaring op internet

De resultaten binnen deze sectie hebben betrekking op informatiegaring op internet en zijn door alle respondenten (N = 402) beantwoord (I.8, B.9, R.7). Als eerste zijn stellingen voorgelegd die betrekking hebben op het vorderen van gegevens, zie Tabel 5.14. Een ruime meerderheid van de respondenten beschikt naar eigen zeggen over basale kennis rondom internet en sporen ten behoeve van informatiegaring op internet, namelijk: dat er sporen worden achtergelaten bij zoeken naar online-informatie, werk en privé gescheiden moeten blijven, dat sporen die op verschillende plekken gevonden worden met elkaar in verband gebracht kunnen worden, het mogelijk is om online gevonden sporen veilig te stellen en hoe men informatie op internet moet vergaren. De overige stellingen kennen wisselende antwoorden.

Tabel 5.14: Kennis van internet en sporen ten behoeve van informatiegaring (in procenten, N = 402)

		(helemaal) mee oneens		(helemaal) mee eens
1.	Ik weet hoe ik informatie moet vergaren op internet, bijvoorbeeld via zoekmachines en open bronnen.	8,5	22,4	69,2
2.	Ik weet wat OSINT (open source intelligence) inhoudt.	37,3	17,2	45,3
3.	Ik weet wat Intel (intelligence) inhoudt.	36,8	25,4	37,8
4.	Ik weet waar in de politieorganisatie de verantwoordelijkheid ligt voor informatievergaring op internet.	33,6	33,8	32,6
5.	Van een politiemedewerker wordt verwacht dat hij/zij zich actief op de hoogte stelt over ontwikkelingen in het omgaan met internetbronnen.	13,9	40,5	45,5
6.	Onderzoek op internet kent in potentie een groot afbreukrisico voor politieonderzoek.	12,2	34,3	53,5
7.	Bij het zoeken naar online-informatie laat je sporen achter.	2,5	7,2	90,3
8.	Ik weet welke sporen worden achtergelaten bij het zoeken naar online-informatie.	30,1	30,6	39,3
9.	Sporen die tijdens het zoeken naar informatie op verschillende plekken op internet worden achtergelaten kunnen met elkaar in verband worden gebracht.	2,7	16,2	81,1
10.	Bij het gebruik van internet moeten werk en privé van elkaar worden gescheiden.	2,0	8,7	89,3
11.	Ik weet wat het verschil is tussen interne en externe IP-adressen.	26,4	23,4	50,2
12.	Ik weet wat een IPv4-adres is.	65,2	10,7	24,1
13.	Ik weet wat een IPv6-adres is.	65,4	11,4	23,1
14.	Het is mogelijk om op internet gevonden sporen veilig te stellen.	4,5	22,1	73,4

Bij de tweede, derde, vierde, vijfde, zesde, achtste, twaalfde, dertiende en veertiende stelling zijn significante verschillen gevonden tussen de functiegroepen. Bij de tweede is het **effect** zeer groot, bij de derde, zesde, dertiende en veertiende middelmatig tot groot en bij twaalf middelmatig.

Op de tweede stelling scoren regionale recherche (M = 3,69) en districtsrecherche (M = 3,41) hoger dan intake en service (M = 2,44), blauw (M = 2,59) en basisteamrecherche (M = 2,66). Op de derde en dertiende stelling scoren regionale recherche (M = 3,42; M = 2,75) en districtsrecherche (M = 3,25; M = 2,75)

hoger dan intake en service (M = 2,36; M = 2,11) en basisteamrecherche (M = 2,66; M = 2,13). Op de zesde stelling scoort regionale recherche hoger (M = 3,96) dan de overige groepen. Op de veertiende stelling scoort intake en service lager (M = 3,39) dan de drie recherchegroepen.

Op de vierde stelling scoort regionale recherche hoger dan intake en service en basisteamrecherche. Op de vijfde stelling scoort regionale recherche hoger dan blauw. Op de achtste stelling scoort districtsrecherche hoger dan blauw. Op de twaalfde stelling scoort districtsrecherche (M = 2,78) hoger dan intake en service (M = 2,13) en basisteamrecherche (M = 2,14) en scoort regionale recherche (M = 2,75) hoger dan basisteamrecherche.

Daarnaast zijn er significante verschillen gevonden tussen mannen en vrouwen en leeftijd. Mannen scoren significant hoger dan vrouwen bij stelling drie, zes, twaalf en dertien. Op stelling één scoort de jongere groep significant hoger dan de oudere groep. Tevens zijn significante verschillende gevonden tussen politiemensen die wel of geen opleiding of cursus hebben gevolgd op het gebied van digitale criminaliteit. De groep met een cursus of opleiding scoort ten opzichte van die zonder hoger op stelling twee, drie, vier, vijf, acht, elf, twaalf en dertien. Tot slot scoren politiemensen die veel tot uitsluitend ervaring hebben met zaken op het gebied van digitale criminaliteit significant lager op stelling zes dan politiemensen die geen tot weinig en niet veel, maar ook niet weinig ervaring hebben met dergelijke zaken.

De volgende stellingen gaan over kennis over juridische implicaties van zoeken naar informatie op internet, zie Tabel 5.15. Op deze stelling zijn de antwoorden weinig eenduidig.

Tabel 5.15: Kennis van de juridische implicaties van zoeken naar informatie op internet (in procenten, N = 402)

		(helemaal) mee oneens		(helemaal) mee eens
1.	Ik ken de algemene juridische regels van zoeken naar informatie op internet.	42,3	31,6	26,1
2.	Ik ken de beslisboom waarmee kan worden bepaald of een onderzoek uitgevoerd mag worden binnen de kaders van de taakstelling van de politie (artikel 3 Politiewet 2012).	54,5	26,9	18,7
3.	Ik weet dat er mogelijk verschil is in kwaliteit van gevonden informatie op internet.	20,9	22,6	56,5
4.	Ik ken de wetsartikelen die regels stellen voor informatievergaring op internet.	52,0	33,6	14,4
5.	Ik weet dat er bij een zoektocht op internet snel sprake kan zijn van stelselmatige observatie.	30,6	21,6	47,8
6.	Ik ken de privacywetgeving in relatie tot het zoeken en vastleggen van informatie van internet.	40,8	37,6	21,6
7.	Ik weet dat contacten leggen tijdens zoeken in internetbronnen altijd moet worden vermeden.	24,1	29,9	46,0
8.	Ik weet bij informatieverzoeken (vordering) of ik die zelf mag uitvoeren of dat die bevoegdheid bij een ander ligt.	26,9	28,1	45,0

Bij alle stellingen zijn significante verschillen gevonden tussen de functiegroepen. Gezien de hoeveelheid verschillen verwijzen we voor de gemiddelden naar Jansen en Van Valkengoed (2019).

Op de eerste stelling scoort regionale recherche hoger dan intake en service, blauw en basisteamrecherche, en scoort districtsrecherche hoger dan intake en service en blauw. Op de tweede stelling scoort districtsrecherche hoger dan intake en service, blauw en basisteamrecherche. Op de tweede en derde stelling scoort regionale recherche hoger dan intake en service. Op de vierde stelling scoren regionale recherche en districtsrecherche hoger dan intake en service en blauw. Op de vijfde stelling scoort regionale recherche hoger dan intake en service en blauw, en scoort districtsrecherche hoger dan intake en service. Op de zesde stelling scoort regionale recherche hoger dan blauw en basisteamrecherche. Op de zevende stelling scoort regionale recherche hoger dan intake en service, blauw en basisteamrecherche. Op de achtste stelling scoort regionale recherche hoger dan de groep blauw. De **effecten** van stelling één, twee, vier, vijf en zeven zijn middelmatig tot groot.

Politiemensen die een opleiding of cursus hebben gevolgd op het gebied van digitale criminaliteit scoren significant hoger dan politiemensen die dit niet hebben voor stellingen één, twee, vier, vijf en zeven.

De volgende twee stellingen gaan over kennis van monitoren en identificeren, zie Tabel 5.16. Respondenten hebben wisselend geantwoord op deze stellingen, waarbij meer dan helft van de respondenten weinig of geen kennis heeft van zinvolle zoektermen.

Tabel 5.16: Kennis van monitoren en identificeren (in procenten, N = 402)

		(helemaal) mee oneens		(helemaal) mee eens
1.	Ik weet wat bruikbare zoektermen zijn om informatie op internet te vinden.	30,1	36,3	33,6
2.	Ik weet wat zinvolle zoektermen zijn om een identificatie-/ traceeractie te laten starten.	55,7	29,9	14,4

Op de eerste stelling scoren jongere politiemensen (M = 3,19) significant hoger dan oudere (M = 2,85). Dit geldt ook voor politiemensen die een opleiding of cursus hebben gevolgd op het gebied van digitale criminaliteit (M = 3,31) ten opzichte van politiemensen die dit niet hebben (M = 2,90). Ook scoren politiemensen met een opleiding of cursus hoger op stelling twee (M = 2,72 versus M = 2,38).

De volgende vier stellingen gaan over kennis van tools voor het zoeken naar informatie op internet, zie Tabel 5.17. Net zoals in voorgaande tabel, zijn ook hier wisselende antwoorden zichtbaar.

Tabel 5.17: Kennis van tools voor het zoeken naar informatie op internet (in procenten, N = 402)

		(helemaal) mee oneens		(helemaal) mee eens
1.	Ik weet voldoende om met zoekmachines zoals Google te werken.	11,2	25,9	62,9
2.	Ik weet wat de risico's zijn van het gebruik van zoekmachines, zoals Google.	16,7	27,1	56,2

Tabel 5.17 (vervolg): Kennis van tools voor het zoeken naar informatie op internet (in procenten, N = 402)

		(helemaal) mee oneens		(helemaal) mee eens
3.	Ik weet dat ik zoekoperatoren (zoals AND en OR) kan gebruiken om gericht informatie te zoeken.	53,5	16,2	30,3
4.	Ik weet wat iRN (internet Recherche Netwerk) is.	32,3	14,4	53,2

Bij de derde en vierde stelling zijn significante verschillen gevonden tussen de functiegroepen. De **effecten** zijn respectievelijk middelmatig tot groot, en zeer groot. Voor de derde stelling geldt dat regionale recherche (M = 3,10) en districtsrecherche (M = 2,97) hoger scoren dan intake en service (M = 2,06) en basisteamrecherche (M = 2,33). Voor de vierde stelling geldt dat regionale recherche (M = 3,87) en districtsrecherche (M = 3,74) hoger scoren dan intake en service (M = 2,33), blauw (M = 2,59) en basisteamrecherche (M = 3,02). Daarnaast scoort basisteamrecherche hoger dan intake en service.

Op de eerste stelling scoren vrouwen (M = 3,78) significant hoger dan mannen (M = 3,50) en de jongere politiemensen (M = 3,83) significant hoger dan vijftigplussers (M = 3,42). Bij de derde stelling scoren mannen (M = 2,81) significant hoger dan vrouwen (M = 2,42). Op de tweede, derde en vierde stelling scoren politiemensen die een opleiding of cursus hebben gevolgd op het gebied van digitale criminaliteit (M = 3,68; M = 3,04; M = 3,65) significant hoger dan politiemensen die dit niet hebben (M = 3,37; M = 2,51; M = 3,07).

Vervolgens is aan de respondenten die weten wat iRN is (53,2%) een viertal aanvullende stellingen voorgelegd in relatie tot het gebruik ervan, zie Tabel 5.18. Hier wordt duidelijk dat kennis over gebruik en mogelijke risico's niet optimaal is.

Tabel 5.18: Kennis van gebruik iRN (in procenten, N = 214)

		(helemaal) mee oneens		(helemaal) mee eens
1.	Het gebruiken van een iRN computer minimaliseert het afbreukrisico van onderzoek doen op internet.	6,1	11,2	82,7
2.	iRN is een geschikte tool om onlineprivézaken mee te regelen.	93,0	4,2	2,8
3.	Ik weet voldoende om met iRN te werken.	19,2	34,1	46,7
4.	Ik weet wat de risico's zijn van het gebruik van iRN.	18,2	34,1	47,7

Op de derde stelling scoort de groep jonger dan vijftig (M = 3,51) significant hoger dan de groep vijftigplussers (M = 3,18).

De volgende vier stellingen gaan over kennis van bronnen voor het zoeken naar informatie op internet, zie Tabel 5.19. Wederom zit veel spreiding in de antwoorden van de respondenten.

Tabel 5.19: Kennis van bronnen voor het zoeken naar informatie op internet (in procenten, N = 402)

		(helemaal) mee oneens		(helemaal) mee eens
1.	Ik weet welk type informatie je kunt vinden op welk type internetbron.	43,5	34,3	22,1
2.	Ik weet waar ik op internet moet zoeken om persoonsgegevens te achterhalen.	30,6	37,1	32,3
3.	Ik weet waar ik op internet moet zoeken om bedrijfsgegevens te achterhalen.	26,9	35,6	37,6
4.	Ik weet hoe ik als politiemedewerker zo weinig mogelijk sporen kan achterlaten bij het zoeken op internet.	49,3	29,9	20,9

Bij de eerste en vierde stelling zijn significante verschillen gevonden tussen de functiegroepen. Het **effect** van de vierde stelling is middelmatig tot groot. Voor de eerste stelling geldt dat regionale recherche (M = 2,98) hoger scoort dan intake en service (M = 2,44) en basisteamrecherche (M = 2,41). Daarnaast scoort districtsrecherche (M = 2,90) hoger dan basisteamrecherche. Voor de vierde geldt dat districtsrecherche (M = 2,94) en regionale recherche (M = 2,84) hoger scoren dan intake en service (M = 2,14) en blauw (M = 2,13).

We vonden voor leeftijd significante verschillen bij stelling één, twee en drie. In alle gevallen scoren politiemensen jonger dan vijftig (M = 2,90; M = 3,15; M = 3,29) hoger dan de vijftigplussers (M = 2,52; M = 2,85; M = 2,90). Voor politiemensen die een opleiding of cursus hebben gevolgd op het gebied van digitale criminaliteit (M = 2,91; M = 3,27; M = 3,29; M = 2,95) geldt dat zij significant hoger scoren dan politiemensen die dit niet hebben voor alle vier stellingen (M = 2,62; M = 2,89; M = 3,01; M = 2,46).

5.2.5 Onlinecommunicatie met burgers

De volgende twee stellingen zijn alleen voorgelegd aan blauw en gaan over hun kennis over het via internet kunnen communiceren met burgers, zie tabel 5.20. Voor beide stellingen geldt dat ongeveer een derde het er (helemaal) mee eens is, een derde een neutrale mening is toegedaan en een derde het er (helemaal) mee oneens is.

Tabel 5.20: Onlinecommunicatie met burgers (in procenten, N = 54)

		(helemaal) mee oneens		(helemaal) mee eens
1.	Ik weet van welke internettoepassingen burgers gebruik maken.	27,8	40,7	31,5
2.	Ik weet van welke internettoepassingen ik gebruik kan maken om met verschillende doelgroepen online in contact te treden.	35,2	31,5	33,3

Politiemensen die een opleiding of cursus hebben gevolgd op het gebied van digitale criminaliteit scoren significant hoger op de tweede stelling (M = 4,00) dan politiemensen die dit niet hebben (M = 2,82). Het **effect** is zeer groot.

5.2.6 Aangiften cyberdelicten

Hoewel deze kennisnorm geldt voor medewerkers intake en service, zijn de stellingen ook aan de functiegroep blauw voorgelegd, omdat deze groep soms ook aangiften opneemt (N = 118). De volgende stellingen gaan over de kennis van politiemensen over aangiften van cyberdelicten, zie Tabel 5.21. Met uitzondering van de stelling over welke digitale sporen geïnventariseerd kunnen worden, scoren beide functiegroepen hoog op deze stellingen.

Tabel 5.21: Kennis betreffende aangiften van cyberdelicten (in procenten, N = 118)

		(helemaal) mee oneens		(helemaal) mee eens
1.	Bij het opnemen van een aangifte is het essentieel om de modus operandi (MO) zo uitgebreid mogelijk te registreren.	4,2	5,1	90,7
2.	Hacken is een basisdelict dat vaak verband houdt met andere delicten.	3,4	19,5	77,1
3.	Doorvragen bij een aangifte van een delict kan ertoe leiden dat meerdere delicten aan het licht komen.	2,5	0,8	96,6
4.	Ik weet welke digitale sporen geïnventariseerd kunnen worden voor het aanvullen van een aangifte.	33,1	35,6	31,4

Bij stelling drie en vier zijn significante verschillen gevonden. Politiemensen die veel tot uitsluitend ervaring hebben met zaken op het gebied van digitale criminaliteit (M = 4,45; M = 3,29) scoren in beide gevallen hoger dan politiemensen die geen tot weinig ervaring hebben met dergelijke zaken (M = 3,98; M = 2,60). Bij beide stellingen is sprake van een middelmatig tot groot **effect**.

Vervolgens is gevraagd naar een aantal specifieke digitale sporen die geïnventariseerd kunnen worden voor het aanvullen van een aangifte, zie Tabel 5.22. Kennis van nieuwere sporen – Bitcoinadressen en Moneygram registratienummers – blijft enigszins achter bij kennis van de overige sporen die al langere tijd de ronde doen.

Tabel 5.22: Kennis van digitale sporen die geïnventariseerd kunnen worden voor het aanvullen van een aangifte (in procenten, N = 118)

Ik weet wat bedoeld wordt met:		(helemaal) mee oneens		(helemaal) mee eens
1.	IP-adres verdachte	5,9	5,1	89,0
2.	E-mailadres	0	0	100
3.	Advertentienummer(s)	4,2	4,2	91,5
4.	Bitcoinadressen (wallets)	38,1	17,8	44,1
5.	Moneygram registratienummers	57,6	19,5	22,9

Voor de eerste en derde stelling werd een significant verschil gevonden tussen de functiegroepen. Intake en service (M = 4,31; M = 4,41) scoort in beide gevallen hoger dan blauw (M = 3,94; M = 3,96). Politiemensen die veel tot uitsluitend ervaring hebben met zaken op het gebied van digitale criminaliteit weten gemiddeld beter

wat bitcoinadressen (de vierde stelling) zijn (M = 3,60) dan politiemensen die geen tot weinig ervaring hebben met dergelijke zaken (M = 2,71). In dit laatste geval is het **effect** middelmatig tot groot.

De volgende drie stellingen gaan over de kennis van het inventariseren van opsporingsrelevante digitale sporen, zie Tabel 5.23. De optie om een expert te raadplegen wordt veelal ingevuld. Het toepassen van de zeven W's lukt in ongeveer de helft van de gevallen. Minder kennis hebben de respondenten van wat vluchtige gegevens zijn.

Tabel 5.23: Kennis van het inventariseren van opsporingsrelevante digitale sporen (in procenten, N = 118)

		(helemaal) mee oneens		(helemaal) mee eens
1.	Ik weet hoe ik de 7 W's (wie, wat, waar, waarmee, welke wijze, wanneer, waarom) moet toepassen om de relevantie van digitale sporen te bepalen.	17,8	29,7	52,5
2.	Bij twijfel over de relevantie van digitale sporen moet een expert worden geraadpleegd.	2,5	2,5	94,9
3.	Ik weet wat 'vluchtige gegevens' zijn.	41,5	38,1	20,3

Alleen voor de eerste stelling werd een significant verschil gevonden voor de functiegroepen. Intake en service (M = 3,69) scoort hoger dan blauw (M = 3,15). Ook scoren politiemensen die een opleiding of cursus hebben gevolgd op het gebied van digitale criminaliteit (M = 3,92) significant hoger dan politiemensen die dit niet hebben (M = 3,32). Het **effect** is in dit geval middelmatig. Ook politiemensen die veel tot uitsluitend ervaring hebben met zaken op het gebied van digitale criminaliteit (M = 3,83) scoren hoger dan politiemensen die geen tot weinig ervaring hebben met dergelijke zaken (M = 3,12). Hier gaat het ook om een middelmatig **effect**.

De groep die aangaf te weten wat vluchtige gegevens zijn (n = 24), is de volgende stelling voorgelegd: Wanneer er sprake is van 'vluchtige gegevens' moet een expert worden ingeschakeld. Vier op de vijf (79,2%) is het hier (helemaal) mee eens. De overige respondenten waren het niet eens, maar ook niet oneens (16,7%) of helemaal oneens (4,2%) met deze stelling.

De volgende twee stellingen gaan over kennis van het adviseren over het veiligstellen van digitale sporen, zie Tabel 5.24. Wederom wordt de optie om een expert te raadplegen veel ingevuld. Op de stelling hoe veelvoorkomende digitale sporen veilig te stellen geeft meer dan de helft aan hiervan geen kennis te hebben.

Tabel 5.24: Kennis van het adviseren over het veiligstellen van digitale sporen (in procenten, N = 118)

		(helemaal) mee oneens		(helemaal) mee eens
1.	Ik weet hoe veelvoorkomende digitale sporen veiliggesteld kunnen worden.	51,7	29,7	18,6
2.	Bij twijfel over hoe veelvoorkomende digitale sporen veiliggesteld kunnen worden moet een expert worden ingeschakeld.	1,7	5,1	93,2

Tot slot zijn vijf stellingen voorgelegd over het aanleveren van digitale sporen met de vraag of zij juist of onjuist zijn, zie Tabel 5.25. Hoewel alle mogelijkheden correct zijn, worden de onderste drie opties door ongeveer een derde van de respondenten bestempeld als incorrect.

Tabel 5.25: Kennis van aanleveren digitale sporen (in procenten, N = 118)

		Onjuist	Juist
1.	Aanleveren van digitale sporen kan digitaal, op een cd/dvd.	11,9	88,1
2.	Aanleveren van digitale sporen kan digitaal, op een usb-stick.	5,9	94,1
3.	Aanleveren van digitale sporen kan digitaal, met print screens.	28,0	72,0
4.	Aanleveren van digitale sporen kan fysiek, met prints op papier.	32,2	67,8
5.	Aanleveren van digitale sporen kan fysiek, met foto's.	32,2	67,8

5.3 Suggesties over het verhogen van het kennisniveau

Om suggesties te kunnen doen met betrekking tot het verhogen van het kennisniveau zijn vier interviews afgenomen, met in totaal zes experts (zie ook sectie 3.2.3). Twee interviews vonden plaats binnen de politieorganisatie, met twee onderwijskundigen en met een staffunctionaris van de Politieacademie. De andere twee interviews vonden buiten de politie plaats, waarvan één met twee experts van een vergelijkbare organisatie als de politie en één met een associate lector van het lectoraat Wendbaar Vakmanschap.

De interviews zijn verwerkt in twee onderdelen. In het algemene deel (sectie 5.3.1.) is aandacht voor belangrijke punten bij het 'uitleren van kennis', het trainen van grote groepen medewerkers, en mogelijkheden om kennis aan te bieden. Het specifieke deel (sectie 5.3.2) gaat in op de vragenlijstresultaten. Hieruit bleek met name aandacht noodzakelijk te zijn voor de verdeling van kennis tussen generalisten en specialisten, internetrechercheren, herkenning digitale sporen, zicht op diepgaandere digitale sporen bij aangifte, en digitaal contact met burgers in het werkgebied. Daarnaast was van belang om na te gaan wat de basisnorm zou moeten zijn waar politiemensen aan gehouden dienen te worden. Aan het einde van een van de interviews gaf een expert aan dat de aangekaarte problematieken niet beperkt worden onder de noemer digitaal. Alle vakgebieden binnen de politieorganisatie hebben hiermee te maken.

5.3.1 Algemeen

Voor de politieorganisatie is het van belang om te weten welke methoden denkbaar zijn om digitale kennis structureel te verbeteren. Veel van de bekende leermethoden worden door de geïnterviewden genoemd, zoals: cursussen, klassikaal leren, e-learning, Massive Online Courses (MOC), training-on-the-job, ervaringsleren, train-de-trainer, profchecks, reflectief leren, briefings, presentaties, en zelfstudie. Het is eveneens mogelijk om de betreffende digitale kennis op te nemen in de standaarden die jaarlijks getoetst worden. Eén van de experts geeft aan dat dit wel andere problematiek met zich meebrengt, omdat mogelijk te veel van dit soort zaken op de standaard komen. Hierdoor kan een dergelijke standaard verwateren. Twee experts geven tevens aan dat kennis niet altijd op dezelfde wijze beklijft. De een leert van tekst, de ander van gesproken woord, de volgende visueel en anderen wellicht van ervaren.

De vraag die het belangrijkst wordt geacht bij leermethoden is de effectiviteit van het lesprogramma. Een aantal experts spreekt een bepaalde mate van weerstand uit bij het gebruik van sommige methoden. In dat verband noemen geïnterviewden onder andere de volgende voorbeelden: wasstraten waar iedereen doorheen moet, verplichte opleidingen, een platform creëren zonder goede communicatie, visuele presentatie boven inhoud zetten, en beperkt gebruik maken van zelf aangedragen opleidingen/behoeften. Eén van de experts wijst er nadrukkelijk op dat het sturen van personeel naar een opleiding door de component ‘moeten’ niet altijd effectief is. Bovendien geeft een andere expert aan dat het ‘jullie kunnen dit niet, en moeten dat leren’ niet werkt, omdat wanneer het geleerd is, de wereld alweer vijf stappen verder is.

Twee experts geven aan dat een combinatie van methoden en middelen, aansluitend op de diverse leerstijlen, het meeste effect kunnen opleveren. Het gedegen communiceren over deze ‘leermix’ zou een essentieel onderdeel moeten zijn van een dergelijk opleidingsprogramma.

Een gemene deler die door alle geïnterviewde experts wel als effectief wordt bestempeld is ervaringsleren. Dit kan door het uitoefenen van (gesimuleerde) praktijkcasussen, maar ook door training-on-the-job, praktijkleren, et cetera. Een voordeel van werken met een echte casus is dat de urgentie sneller duidelijk is dan wanneer je een cursusboek openslaat. Een expert illustreert dit door aan te geven wanneer politiemensen dingen echt gaan doen, het leren, terwijl ze aan het werk zijn, ‘on the fly’ gebeurt. Ook in een interview uit ronde twee werd hierop gereflecteerd. *“Niet het onderwijs, maar per eenheid verschillende praktijkroutines bepalen voor het overgrote deel hoe politiemensen handelen. Politiemensen zijn doeners, geen lezers. Zij leren dus liever van hun naaste collegae dan in de schoolbanken. De norm, en dus de betreffende cultuur, is bepalend.”*

Het belangrijkste aspect dat benoemd wordt met ervaringsleren is het – zowel individueel als samen met collega’s – reflecteren op het handelen, zodat de (aan)geleerde kennis beter beklijft. Wel is het belangrijk dat daar begeleiding omheen wordt georganiseerd, eventueel op afstand. Andere

positieve ervaringen van experts over leren omvatten: korte en cyclische herhalingen van kleine brokjes informatie, de benoemde herhalingen via verschillende manieren aan de man brengen en die liefst precies op tijd en passend zijn bij wat mensen niet weten. Daarnaast worden kennisvergroting 'framen' buiten het kader van leren, kwaliteit van inhoud boven visuele aspecten stellen, gebruik maken van specialisten die in het werkveld rondlopen, de train-de-trainer methode toepassen, en de wijze van leren op de behoefte laten aansluiten genoemd als *'good practices'*.

Een belangrijk onderscheid dat gemaakt moet worden, is of de kennis uit het hoofd gekend moet worden (parate kennis) of niet. Het gaat volgens de experts vooral om dat mensen worden geleerd om de informatie te kunnen vinden c.q. om te weten hoe een vraagstuk is op te lossen in plaats van het zelf hebben van specifieke kennis. Immers, niet iedereen hoeft alle kennis te hebben. Men moet onderkennen dat sprake is van een leerprobleem en zich de vraag stellen: "Hoe kan ik dit leerprobleem oplossen?". Bij die vraag kunnen politiemensen in het netwerk de betreffende kennis mogelijk vinden. Zodoende kan het versterken en onderhouden van netwerken tevens een belangrijke factor zijn. Voordat politiemensen hun eigen leerprobleem kunnen inschatten is wel een bepaalde basiskennis noodzakelijk om deze inschatting te kunnen maken. Deze mening wordt door een andere expert gedeeld; men moet echter wel onderkennen dat sprake is van een leerprobleem en niet zomaar een protocol afwerken.

Door één van de experts wordt aangegeven dat medewerkers ook door systemen ondersteund kunnen worden in de uitvoering van hun werkzaamheden. Zo wordt bij de regionale servicecentra gebruik gemaakt van een vraag-en-antwoord-systeem, waarin kennis over allerlei onderwerpen zit opgeslagen. Het nadeel van dergelijke systemen is volgens deze expert dat deze kennis vaak in een script zit. Wanneer iemand bijvoorbeeld meer kennis heeft dan in het script is opgeslagen, kan het spaak lopen ('dat weet ik al'). Een andere expert vertelt hierover dat dit soort ondersteuning het liefst 'just-in-time' en op niveau gedaan wordt. Iemand telkens hetzelfde aanbieden werkt niet volgens deze geïnterviewde; men gaat zich dan aan een dergelijke functie irriteren.

Voor een organisatie is het (tijdig) aanbieden van kennis van belang. Dat informatie en/of de relevante mensen in het netwerk goed vindbaar moeten zijn lijkt evident, maar is in de praktijk niet altijd het geval. Zo zijn binnen de politie bijvoorbeeld drie verschillende platformen waar kennis te vinden is. Kennis buiten de opleidingen van de Politieacademie (zie ook bijlage I) wordt bij de politieorganisatie aangeboden via het intranet, Agora, en Kompol. Op het intranet hebben de organisatieonderdelen, personeelszaken en dergelijke informatieve pagina's. Ook kent het intranet een deel met de nieuwsitems van elke afdeling. Agora is een deel van het intranet waarop teams en individuen hun eigen pagina kunnen creëren en bijhouden. Dit kan informatief zijn, maar kan ook worden gebruikt om kennis te delen. Hier staat echter informatie die niet gevalideerd is. Kompol is

een kennisbank voor de politie waar gevalideerde kennis gedeeld wordt. Ook is het belangrijk om te weten hoe 'houdbaar' de gevonden informatie is. Het goed onderhouden van kennis is dus volgens de geïnterviewden van groot belang.

De experts dragen diverse methoden aan voor goed kennismanagement. De een geeft aan dat dit belegd moet worden bij de experts, terwijl een andere aangeeft dat dit bij eenieder ligt door continu te reflecteren op het onderwerp. Daarnaast geeft een expert aan dat eigenaarschap belangrijk is in dit verband. Tegelijkertijd moeten die eigenaren van een dergelijk probleem wel de ruimte krijgen om hierop te acteren. In een interview kwam naar voren dat kennismanagement momenteel niet goed is georganiseerd binnen de politieorganisatie door gebrek aan geld en capaciteit. Eén van de geïnterviewden gebruikte de volgende metafoor om dit probleem te illustreren. "Een houthakker is druk bezig bomen om te hakken. Een jongetje loopt langs en merkt op dat de bijl van de houthakker bot is. De houthakker reageert: 'Daar heb ik toch geen tijd voor? Ik moet dit hele bos nog omhakken!'" De moraal hierbij is dat wanneer de houthakker de tijd neemt om de bijl te slijpen hij veel meer bomen in minder tijd kan omhakken en de investering van het slijpen snel terug zal verdienen.

Hoewel bovenstaande aspecten vooral betrekking hebben op het individuele leerproces, is het aanleren van kennis aan grote groepen lastig. Er komen veel zaken bij kijken waarbij vraagstukken over kosten en capaciteit belangrijke zijn. De training Contra-Terrorisme, Extremisme en Radicalisme is hier een voorbeeld van. Dit was de eerste landelijk uitgerolde opleiding van twee of drie dagen voor alle executieve politiemensen. De training verliep via de train-de-trainer-methodiek en kostte een kwart miljoen aan operationele uren. Door de gehanteerde methodiek waren de financiële kosten overigens relatief laag. Volgens één expert is de grootte van de 'pijn' die de organisatie lijdt bij een dergelijke opgave te verlichten door bijvoorbeeld te spreiden of de opleidingen beter op de functiegroepen af te stemmen.

Andere zaken die spelen op groepsniveau betreffen bijvoorbeeld een verschil in (begin)niveau. Het liefst wordt de aangeboden kennis op het voor de ontvanger juiste niveau aangeboden. Hierop kan natuurlijk wel worden geanticipeerd. Bij de ene groep moet worden ingezet op het verhogen van parate kennis, terwijl bij een andere het belangrijker om handreikingen te doen hoe die informatie is op te zoeken.

Het laatste aspect van kennis dat we hier benoemen is het verspreiden van het kennis- en leeraanbod. Diverse methoden worden door de geïnterviewde experts geopperd, zoals via intranet, interne zoekmachines, productcatalogi op onderdeelsniveau, en in diverse (vak)bladen. Een radicaler voorbeeld van één van de experts is het verspreiden van kennis door het op een 'Netflix-achtige' manier aan te bieden. Het belang van communicatie speelt volgens een andere expert tevens een belangrijke rol.

5.3.2 Specifiek

In deze sectie volgen de belangrijkste bevindingen uit de interviews die direct samenhangen met de resultaten van de vragenlijst (par. 5.2). Het gaat om bevindingen over internetrechercheren, digitale sporen, en contact met burgers. Tevens staat het concept 'basiskennis' centraal.

Eén van de belangrijkste bevindingen gaat over basiskennis. Op de vraag hoeveel van de tien politiemensen van de basiskennis op de hoogte dienen te zijn, ontstonden levendige discussies. Hoe basis is basis? In situaties, aldus de experts, waarin de politie snel moet handelen, is het zaak dat de betreffende politiemensen de voor dat optreden vereiste kennis, paraat hebben – anders kunnen ze immers niet snel handelen. Hebben politiemensen de tijd om het handelen uit te stellen, dan hoeft de voor dat optreden vereiste kennis bij minder of geen van de politiemensen paraat aanwezig te zijn. Dan is er immers de mogelijkheid om het op te zoeken of anderen te raadplegen. Indien snel kunnen handelen is vereist, zou de norm volgens experts kunnen liggen tussen zeven à tien politiemensen van een groep van tien (70-100%). Bij handelingen die uitgesteld kunnen worden veronderstellen experts dat een team van tien zich moet kunnen redden wanneer drie leden de betreffende kennis hebben (30-%). Wel geldt dan natuurlijk als voorwaarde dat minstens één van de kennisdragers bereikbaar is.

Eén van de experts merkt op dat binnen het uitoefenen van het beroep sprake is van kennis die aansluit bij het werk. Deze expert geeft aan: "Ik denk niet dat er zoiets bestaat als basiskennis. Ik denk wel dat er zoiets bestaat als dat je kennis, houding, vaardigheden hebt om je aan te sluiten bij een bepaalde community. Die community heeft per definitie een opdracht. En in het geval van de politie is die opdracht vrij duidelijk. Deze community ontwikkelt zelf kennis. Die moet je geen bak met kennis geven, want daar hebben ze eigenlijk niks aan. Tegen de tijd dat ze die bak hebben, is de bak alweer veranderd. Dus moet je ze de ruimte en mogelijkheden geven om kennis op te doen." Al werkend en reflecterend leert men, waardoor kennis ontstaat. In groepen mensen is het normaal dat de een meer van bepaalde onderwerpen afweet dan de ander. De communities van die mensen kunnen kennisontwikkeling dragen door ze in aanraking te laten komen met politiemensen die minder kennis hebben. Van belang is elkaar op de hoogte houden om een goede kennisbasis te houden.

De geïnterviewden laten een eenduidig beeld zien in het antwoorden op de vragen over waar basiskennis van digitaal belegd moet worden. De basiskennis (of kennisbasis zoals een andere expert het verwoord) moet overal aanwezig zijn – dus bij zowel specialisten als generalisten – en dat heeft verschillende redenen. Zo wordt specialistische kennis steeds generalistischer, zeker bij digitaal, en zal een generalist met de specialist moeten kunnen overleggen en de juiste vragen kunnen stellen. Eén van de experts merkt op dat dit wel goed georganiseerd moet worden. De generalisten moeten de mogelijkheid krijgen om te leren. Ter illustratie: wanneer alle phishingmails gefilterd worden, dan

zal de medewerker nooit kunnen leren over hoe deze te herkennen. En dat 'herkennen' is een gevoeligheid die ontwikkeld moet worden.

Om de kennis over internetrechercheren te verhogen is volgens één expert van belang om eerst de noodzaak te erkennen en daarna een specifiek opleidings-/leerplan te maken. Een andere expert geeft aan dat e-learning via casuïstiek heel geschikt zou kunnen zijn voor dit thema, het liefst zo interactief mogelijk. De e-learning moet echter wel up-to-date gehouden worden en moet aansluiten bij *'use-cases'*. Een derde expert geeft aan dat enthousiasme over dit onderwerp enorm van belang is, dan willen medewerkers zelf leren en studeren.

Voor het borgen van kennis over digitale sporen wordt door één expert aangegeven dat 100% dekking waarschijnlijk nooit haalbaar is. De vraag tussen kennis die gemist wordt versus de investering die nodig is om dit aan te pakken is belangrijk. Een oplossing zonder opleiden is het borgen van kennis over digitale sporen bij een specialist en deze specialist *'just-in-time'* op de juist plaats krijgen. Vervolgens wordt aangegeven dat conceptuele kennis van digitaal erg belangrijk is, want dan weet men wat ongeveer kan en waar meer informatie te vinden is. Specialisten kunnen hierbij ondersteund worden door *'performance support by design'*, ofwel kennis in systemen. Daarbij is het belangrijk om een vaste plek te creëren waar die kennis te vinden is. Een andere expert vult hierop aan dat het leren over digitale sporen op een plaats delict prima via een *'virtual reality'*-omgeving plaats zou kunnen vinden. Een derde manier is *'training-on-the-job'*, waarbij politiemensen door experts meegenomen worden in het herkennen, de omgang, en het gebruik van digitale sporen. Eén van de experts geeft in dit verband aan dat het goed is om politiemensen samen te laten werken die meer en minder kennis hebben van zaken (zogenoemde 'perifere participatie').

In drie interviews is ingegaan op het verbeteren van aandacht voor diepgaandere digitale sporen bij een aangifte. Hierbij zien de geïnterviewden duidelijke kansen voor een systeem dat voorziet in het eerdergenoemde *performance support by design*. Dat houdt in dat bijvoorbeeld bij het opnemen van een aangifte tips gegeven worden door een systeem. Door het volgen van een script, ontstaat een soort checklist, waardoor belangrijke punten niet vergeten worden. Een potentieel risico is dat door het gebruik van scripts geen afwijkingen mogelijk zijn wat mogelijk zorgt voor frustratie. Een 'slim' systeem zou dan uitkomst kunnen bieden. Eén van de experts geeft tot slot aan dat het weten te vinden van specialisten op het onderwerp eveneens van belang is. De politiemensen weten dan wie ze waarvoor kunnen bellen als hun kennis ontoereikend blijkt te zijn.

Een laatste specifieke vraag die in de interviews werd gesteld ging over het borgen van kennis die benodigd is om in contact te treden met burgers in het werkgebied. Politiemensen zouden moeten weten van welke kanalen en/of applicaties burgers gebruikmaken en hoe ze deze zelf kunnen gebruiken. Een van de opmerkingen is dat kennis hierover in de opleiding voor wijkagenten moet komen. Een andere expert gaf aan dat dit via e-learning uitgeleerd kan worden. Tevens wordt

door experts aangegeven dat dit onderwerp zich goed leent voor oudere politiemensen om bij hun jongere collega's kennis op te halen. Dit zit echter niet in de politiecultuur. Tot slot is het van belang dat politiemensen goed op de hoogte zijn van verschillen tussen privé- en zakelijk gebruik van dergelijke applicaties.

6. Conclusie, discussie, beperkingen

In dit hoofdstuk staan we ten eerste stil bij de conclusies en bediscussiëren we de belangrijkste resultaten (par. 6.1). Ten tweede bespreken we de beperkingen van het onderzoek (par. 6.2).

6.1 Conclusies en discussie

In deze paragraaf beantwoorde we de onderzoeksvragen. Als eerste hebben we aandacht voor hoe de intake en afhandeling van digitale criminaliteit en van criminaliteit met een digitale component is georganiseerd. Daarna gaan we in op de kennisnormen voor digitale aspecten van politiewerk. We staan stil bij zowel de theorie (wat politiemensen zouden moeten weten op basis van literatuur en interviews met experts) als de praktijk (uitkomsten vragenlijst). Vervolgens bespreken we waar eventuele kennistekorten zich voordoen en hoe die kunnen worden bestreden.

6.1.1 Hoe is de intake en afhandeling van digitale criminaliteit en van criminaliteit met een digitale component georganiseerd?

Om de vraag 'Hoe is de intake en afhandeling van digitale criminaliteit en van criminaliteit met een digitale component georganiseerd?' te beantwoorden bestudeerden we eerst de literatuur. Vervolgens hebben we de bevindingen uit de theorie via interviews vergeleken met de praktijk. De interviews bevestigen grotendeels de bevindingen uit de literatuur.

Volgens de literatuur doorloopt het opsporingsproces de volgende fasen: (1) kennis nemen van een misdrijf (via melding, aangifte of politiestraatwerk), (2) initieel onderzoek (informatie veiligstellen), (3) evaluatie opsporingsonderzoek (beslissen om wel of niet over te gaan tot opsporingsonderzoek), (4) waarheidsvinding (identificeren van verdachten en vergaren van zowel belastend als ontlastend materiaal), (5) evaluatie bewijs (beslissen om opsporingsonderzoek [vroegtijdig] te beëindigen of aanvullend onderzoek te verrichten), en (6) afronding onderzoek (strafrechtelijk dossier opmaken en overdragen aan het Openbaar Ministerie). Vanuit de praktijk wordt een soortgelijke beschrijving gegeven: (1) intake (input), (2) casescreening (beoordelen input), (3) voorbereiden, (4) uitvoering (verrichten van opsporingsonderzoek), en (5) afronding.

Voorgaande is een abstracte beschrijving van het opsporingsproces. Hoe concreet invulling wordt gegeven aan het proces van intake en afhandeling en wie daarbij betrokken zijn, is afhankelijk van het type criminaliteit en het soort aanpak. De politie onderscheidt drie typen criminaliteit: (1) veel voorkomende criminaliteit (VVC), (2) high impact crime (HIC), en (3) ondermijning. Ook kent zij drie aanpakken: (1) incidentgerichte aanpak, (2) probleemgerichte aanpak, en (3) programmatische aanpak. In het te doorlopen proces wordt geen expliciet onderscheid gemaakt tussen klassieke criminaliteit en digitale criminaliteit: zowel klassieke als digitale criminaliteit kunnen worden

geschaard onder VVC, HIC of ondermijning en ook alle politiële bestrijdingsstrategieën kunnen van toepassing zijn.

In het 'toewijzingskader' voor de opsporing staat hoe de onderscheiden criminaliteitssoorten en aanpakken zich tot elkaar verhouden en welk organisatieonderdeel (basisteamniveau, districtsniveau, regionaal niveau, landelijk niveau) bij de aanpak daarvan betrokken is. Campman e.a. (2012) hebben gepoogd om het toewijzingskader te vertalen naar digitale criminaliteit. Daaruit blijkt op hoofdlijnen (1) dat basisteams zich voornamelijk toespitsen op de incidentgerichte aanpak van VVC binnen geografische grenzen, (2) dat districtsrecherche verantwoordelijk is voor de incidentgerichte aanpak van cybercrimes met een grote impact en de probleemgerichte aanpak van VVC (voornamelijk locatiegebonden), en (3) dat de regionale recherche zowel kan worden belast met de incidentgerichte als de probleemgerichte aanpak van digitale criminaliteitsvormen met een hoge impact en ondermijning alsook met de thematische aanpak van alle onderscheiden criminaliteitssoorten. Hoewel de landelijke recherche niet centraal staat in dit onderzoek werd duidelijk dat opgeschaald wordt tot een landelijke aanpak als sprake is van locatie-onafhankelijke uitingsvormen van digitale criminaliteit met een grote impact of als sprake is van digitale uitingsvormen van ondermijning. Daarbij kan zowel sprake zijn van de incidentgerichte, probleemgerichte als programmatische benadering.

Het toewijzingskader voor de opsporing laat op hoofdlijnen zien dat met name de omvang (geografisch, capaciteit) en complexiteit van een zaak bepalen welk rechercheniveau wordt belast met het opsporingsonderzoek. Algemeen geldt – voor zowel klassieke delicten als cybercrime – hoe omvangrijker en complexer de criminaliteit en het soort aanpak, hoe hoger het rechercheniveau. Overigens is het op alle rechercheniveaus mogelijk om, waar nodig, digitale expertise in te schakelen. Dit laatste geldt ook bij het opnemen van aangiften, bijvoorbeeld bij complexe cybercrimezaken.

Doorgaans is intake het vertrekpunt voor het opsporingsproces. In de praktijk wordt dus vooral gewerkt volgens de incidentgerichte en in mindere mate volgens de probleemgerichte of programmatische benadering. Bij de incidentgerichte benadering wordt kennisgenomen van strafbaar gedrag via een melding/aangifte van een burger. De wijze waarop de intake is georganiseerd kan verschillen per eenheid, maar het overgrote deel van de intakewerkzaamheden wordt verricht door speciaal daarvoor aangestelde medewerkers intake en service. In sommige eenheden worden ook executieve medewerkers in de gebiedsgebonden politiezorg (blauw) belast met het opnemen van meldingen en aangiften op het bureau. Als een aangifte daartoe voldoende aanknopingspunten biedt, wordt de zaak overgedragen aan de recherche. Afgeronde zaken worden vervolgens doorgestuurd naar het OM.

Tot slot merkten we vanuit de praktijk op dat cybercrimezaken al gauw als complex worden gezien en dat in de praktijk daarom sneller wordt opgeschaald naar een hoger rechercheniveau dan

bij klassieke zaken. In alle eenheden is inmiddels een specifiek cybercrimeteam actief. Opschalen naar het cybercrimeteam is volgens de beleidsuitgangspunten meestal niet nodig, maar gebeurt in de praktijk wel vaak. Volgens geïnterviewde experts ontbreekt het tactisch rechercheurs aan kennis om opsporingsonderzoek naar cybercrime te verrichten. Door enkele geïnterviewden wordt betwist of die opvatting van rechercheurs terecht is, omdat cyberopsporing grotendeels gelijk is aan klassieke opsporing. Bijvoorbeeld, vroeger werden NAW-gegevens (naam, adres, woonplaats) gevorderd bij een kenteken, nu bij een IP-adres. De digitale terminologie ('IP-adres') leidt mogelijk tot onnodige koudwatervrees, aldus een van de geïnterviewden.

6.1.2 Welke kennis inzake digitale aspecten van politiewerk moeten de eerder onderscheiden vijf groepen politiemensen hebben (de norm)?

In paragraaf 5.1 hebben we op basis van literatuur en interviews per functiegroep kennisnormen ontwikkeld. Daarnaast is een kennisnorm onderscheiden voor alle functiegroepen, namelijk voor informatiegaring op internet.

In Tabel 6.1 zijn de normen samengevat voor medewerkers intake en service. In Tabel 6.2 zijn de normen voor blauw en de drie recherchegroepen uiteengezet. In Tabel 6.3 staan de normen voor informatiegaring op internet centraal.

Tabel 6.1: Kennisnormen voor intake en service

Code	Competentie
I.1	Het kennen van de standaardprocedure voor het opnemen van aangifte
I.2	Verschijningsvormen van digitale criminaliteit kennen en weten te herkennen op basis van praktijksignalen
I.3	De strafbaarstelling van cyberdelicten weten vast te stellen
I.4	Weten dat verbanden bestaan tussen cyberdelicten en weten hoe die verbanden te toetsen tijdens het opnemen van de aangifte
I.5	Kennis hebben van het inventariseren van opsporingsrelevante digitale sporen
I.6	Weten hoe te adviseren over het veiligstellen van digitale sporen
I.7	Kennis hebben van voor 'cyber'intake ontwikkelde handreikingen en op basis daarvan weten hoe de aangever

*Tabel 6.2: Kennisnormen voor blauw en recherchegroepen**

Code	Competentie	Blauw	Basisteam-recherche	Districts-recherche	Regionale recherche
B.1, R.2	Het kennen van de fasen in het optreden op de PD	X	X	X	X
B.2, R.1	Het kennen van het juridisch kader voor het optreden op de PD	X	X	X	X
B.3, R.1	Het kennen en weten uit te voeren van de eerste maatregelen	X	X	X	X

**Notitie. Competenties R.1 en R.2 van de recherchegroepen zijn samengevoegde competenties die onder blauw als losstaande competenties zijn beschreven.*

Tabel 6.2 (vervolg): Kennisnormen voor blauw en recherchegroepen

Code	Competentie	Blauw	Basisteam-recherche	Districts-recherche	Regionale recherche
B.4, R.2	Weten hoe onderzoek op de PD te verrichten	X*	X	X	X
B.5, R.2	Het kennen van de specifieke basisstappen in het geval van een PD (met digitale sporen)	X	X	X	X
B.6, R.2	Weten hoe relevante digitale gegevensdragers te herkennen op een digitaal PD	X	X	X	X
B.7, R.2	Weten hoe op forensisch technisch verantwoorde wijze relevante digitale gegevensdragers kunnen worden veiliggesteld	X	X	X	X
B.8, R.2	Weten hoe onderzoek op de PD te verrichten	X	X	X	X
B.9	Kennis van communicatie met burgers via internet	X			
R.3	Weten hoe met het oog op opsporing de waarde van de aangedragen informatie te beoordelen		X	X	X
R.4	Weten hoe planmatig/systematisch aan een opsporingsonderzoek gewerkt kan worden		X	X	X
R.5	Weten hoe opsporingsonderzoek te verrichten		X	X	X
R.6	Kennis van specifieke opsporingskennis en -vaardigheden in een gedigitaliseerde samenleving			X	X
R.7	Weten hoe onderzoeksbevindingen te analyseren en duiden		X	X	X
R.8	Weten hoe de waarde van bewijs te beoordelen		X	X	X
R.9	Weten hoe eigen onderzoekshandelingen vast te leggen		X	X	X

**Notitie. Alleen geldend voor het voorbereiden van eenvoudige PD's.*

Tabel 6.3: Kennisnormen voor informatiegaring op internet

Competentie
Informatiegaring op internet: Kennis van internet en sporen
Informatiegaring op internet: Kennis van het juridisch kader
Informatiegaring op internet: Kennis van monitoren en identificeren
Informatiegaring op internet: Kennis van tools
Informatiegaring op internet: Kennis van bronnen
Informatiegaring op internet: Kennis van taal / jargon / thema's

Deze normen gelden ten tijde van dit onderzoek. Omdat de technologische ontwikkeling snel gaat en de voor goed politiewerk vereiste 'digitale kennis' mee verandert, zijn deze normen tijdsgebonden (zie ook par. 7.1).

6.1.3 Welke kennis inzake digitale aspecten van politiewerk hebben politiemensen (de realiteit)?

Een antwoord op de vraag over welke kennis politiemensen beschikken inzake digitale aspecten van politiewerk, geven we aan de hand van zes thema's: (1) kennis omtrent digitale criminaliteit, (2) kennis omtrent optreden op een plaats delict, (3) kennis omtrent digitale sporen, (4) kennis omtrent informatiegaring op internet, (5) kennis omtrent onlinecommunicatie met burgers, en (6) kennis omtrent het doen van aangifte van cybercrime.

1. Digitale criminaliteit. Wat opvalt is dat zowel het kennen als het herkennen van strafbare gedragingen aan de lage kant is. Voor het herkennen werden vier casussen voorgelegd. Voor elke casus geldt dat een tot twee op de vijf politiemensen dit niet goed kon beantwoorden. Dit betekent dat in het opleidingen- en/of cursusaanbod aandacht besteed moeten worden aan kennis over hoe strafbare gedragingen te herkennen.

2. Optreden plaats delict (PD). Aspecten die hier opvielen waren (a) een gebrek aan kennis van risico's met betrekking tot het vernietigen of besmetten van digitale sporen en (b) een gebrek aan kennis van basisprocedures voor het veiligstellen van digitale gegevensdragers. Ook werd laag gescoord op kennis omtrent het toekennen van prioriteit voor het veiligstellen van gegevensdragers. Dit zijn aspecten waarbij de politieorganisatie op kennisvergroting moet inzetten. Daarentegen werd over het algemeen hoog gescoord op aspecten die te maken hebben met handelingen op een PD en bewijsvoering.

Gegevensdragers die mogelijk op een PD aanwezig zijn, worden herkend wanneer het algemene, veelvoorkomende gegevensdragers betreft. Nieuwe, of zelf geknutselde, gegevensdragers worden minder herkend. Bij het aantreffen van onbekende gegevensdragers gaf bijna iedereen aan een specialist in te schakelen, wat door geïnterviewde experts wordt gezien als een zeer belangrijke handeling.

3. Digitale sporen. Over het algemeen lagen de gemiddelde scores bij de kennisvragen over dit thema boven het gemiddelde. Voor de politieorganisatie valt echter nog wel wat te winnen door hierop in te zetten. Zaken die bijzonder de aandacht verdienen zijn: welke digitale sporen van belang zijn voor opsporingsonderzoek (o.a. toepassing van de zeven W's en herkennen digitale sporen); welke digitale sporen kunnen worden uitgelezen; het opstellen van uitleesvragen en de eisen die daaraan zijn verbonden; en het gebruik van softwarepakketten voor, en het vastleggen van bevindingen over, de analyse van digitale sporen.

Op algemene termen scoren politiemensen globaal genomen hoog, alleen specifieke termen als clearweb en deepweb worden minder goed herkend. De kennis van interceptie is over het algemeen ook hoog. Wat betreft het gebruik van hulpmiddelen is de kennis aan de lage kant; slechts twee op de vijf politiemensen zijn bekend met de webapps van de Politieacademie.

4. Informatiegaring op internet. Aspecten die binnen het subthema 'vorderen van gegevens' aandacht verdienen zijn bekendheid met: OSINT, Intel, verantwoordelijkheden voor informatiegaring op internet, IPv4- en IPv6-adressen. Het tweede subthema 'juridische implicaties voor het zoeken naar informatie op internet' moet in zijn geheel worden versterkt binnen de politieorganisatie. De scores op kennisvragen hieromtrent zijn over het algemeen laag. Daarnaast scoren respondenten laag op kennis van zoektermen en van zoekoperatoren. Ook scoren politiemensen laag op hoe met iRN gewerkt moet worden en welke internetbronnen voor welke informatie geraadpleegd kunnen

worden. Wel scoren respondenten over het algemeen hoger op 'tools' voor het zoeken van informatie op internet.

5. Onlinecommunicatie met burgers. Op dit thema wordt laag gescoord. Respondenten weten over het algemeen niet van welke internettoepassingen burgers gebruik maken en ook niet van welke toepassingen zij kunnen gebruik om in contact te treden met burgers.

6. Aangiften van cybercrime. Over het algemeen zijn de scores hoog. Op enkele voor de opsporing belangrijke onderdelen kan worden geïnvesteerd om dit thema te versterken. Specifiek gaat het daarbij om kennis van welke sporen geïnventariseerd kunnen worden en hoe veelvoorkomende digitale sporen veiliggesteld kunnen worden. Daarnaast geldt dat medewerkers intake en service laag scoren op kennis van de zeven W's om de relevantie van digitale sporen te bepalen alsook van wat vluchtige gegevens zijn. Tevens zijn zij in drie op de tien gevallen onvoldoende op de hoogte van hoe digitale sporen aangeleverd kunnen worden.

6.1.4 In hoeverre is er een kennistekort bij de onderscheiden vijf groepen politiemensen en waar doet dit tekort zich eventueel voor?

Naast het in kaart brengen van kennis aangaande digitale aspecten van politiewerk over de volle breedte van de politieorganisatie (sectie 6.1.3), hebben we gekeken of we preciezer konden aanwijzen waar binnen de organisatie een eventueel tekort zich voordoet. In eerste instantie hebben we dit gedaan door naar functiegroepen te kijken (intake, blauw, drie recherchegroepen). Aanvullend hebben we gekeken in hoeverre achtergrondkenmerken van politiemensen een verklarende rol spelen. Daarbij gaat het om analyses naar geslacht, leeftijd, wel of geen opleiding/cursus op cybergebied en mate van ervaring met cyberzaken.

Significante verschillen tussen groepen doen zich vooral voor op functieniveau. Over het algemeen geldt dat de recherchegroepen hoger scoren dan blauw en intake en service. Binnen de recherchegroepen scoren respondenten van de regionale recherche vaak hoger dan respondenten van de districts- en basisteamrecherche. Wel moet hierbij worden opgemerkt dat de effecten veelal klein of klein tot middelmatig zijn.

In een aantal gevallen waren de effecten sterker. Eén van de aanbevelingen in de vorige sectie is om de basisprocedures voor het veiligstellen van digitale gegevensdragers onder de aandacht te brengen. Hoewel alle functiegroepen hiervan kunnen profiteren laat nadere analyse zien dat dit het noodzakelijkst is voor blauw.

Kennis versterken van wat vluchtige gegevens zijn, werd al geopperd in voorgaande sectie voor intake en service en blauw. Een analyse op de recherchegroepen laat echter zien dat dit ook noodzakelijk is voor medewerkers van de basisteamrecherche. Deze drie groepen zijn ook gebaat bij meer kennis over OSINT, Intel, en juridische regels van zoeken naar informatie op internet. Analyses

op functiegroepen lieten zien dat deze kennis over het algemeen gemiddeld tot hoog werd gescoord door politiemensen die werkzaam zijn voor de districts- of regionale recherche. Voor twee juridische regels scoorden echter ook respondenten van de districts- of regionale recherche – hoewel hoger dan de andere functiegroepen – beneden het gemiddelde. Het gaat hierbij om kennis van de beslisboom waarmee kan worden bepaald of een onderzoek uitgevoerd mag worden binnen de kaders van de taakstelling van de politie en de wetsartikelen die regels stellen voor informatiegaring op internet.

In voorgaande paragraaf werd de suggestie gedaan voor meer opleiding op het gebied van iRN. Functiegroepanalyse laat zien dat deze kennis reeds aanwezig is bij de districts- en regionale recherche. Een kennisimpuls is dus vooral nodig bij medewerkers intake en service, blauw en basisteamrecherche.

Tussen mensen met en zonder opleiding op digitaal gebied zijn bij 51 vragen/stellingen ook significante verschillen gevonden. In alle gevallen scoorden respondenten die een cursus of opleiding hebben gevolgd gemiddeld hoger. In één geval werd een middelmatig effect (toepassing zeven W's) geconstateerd en in één geval was het effect groot (uitwerking doorvragen bij aangifte). In de overige gevallen was het effect klein tot middelmatig of zwak. Overigens is daarmee niet gezegd dat de opleiding de oorzaak is van het beter scoren. Het kan immers zijn dat politiemensen met een bovengemiddelde interesse in en kennis van digitaal, om die reden een opleiding hebben gevolgd. Het is dus nog maar de vraag of het zou helpen om degenen die nu laag scoren een opleiding te laten volgen. Tegelijk kan het wel zo zijn dat mensen die een opleiding hebben gevolgd om die reden hoger scoren. Als dat het verband is, loont het dus kennelijk om mensen een opleiding te laten volgen. De richting van het verband tussen 'opleiding omtrent digitaal gevolgd' en 'kennis van digitaal' moet dus nader worden onderzocht (zie ook par. 7.2).

De analyses voor geslacht deden er weinig toe om het kennisniveau te duiden. Bij tien vragen/stellingen werden significante verschillen gevonden tussen mannen en vrouwen. Tweemaal scoorden vrouwen hoger en achtmaal deden mannen dat. In alle gevallen waren de effecten klein tot middelmatig.

Voor leeftijd waren ook niet veel verschillen te ontdekken. Bij negen vragen/stellingen zijn significante verschillen gevonden tussen de twee onderscheiden leeftijdsgroepen. In alle gevallen scoorden respondenten tot 50 jaar gemiddeld hoger dan politiemensen van 50 jaar en ouder. Echter, de effecten waren in alle gevallen klein tot middelmatig of zwak. Hoewel onderzoek laat zien dat op individueel niveau bijvoorbeeld jongeren meer dan ouderen geneigd zijn nieuwe technologie te omarmen en meer interesse tonen in het uitvoeren van cognitief complexe taken (Edison & Geissler, 2003), willen wij hier benadrukken dat ons onderzoek geen grond geeft voor de conclusie dat de kennistekorten op digitaal gebied generatiegebonden zijn. Deze bevinding komt overeen met

bevindingen uit een recent onderzoek naar het benutten van digitale sporen (Marskamp-Zuurveen & Stol, in druk). Dit betekent dat het kennistekort niet vanzelf wordt opgelost wanneer door vergrijzing veel politiemensen uitstromen en nieuwe, jongere politiemensen instromen. Wel kan hierop worden geanticipeerd in de vooropleiding.

Hoewel bij slechts zeven vragen/stellingen significante verschillen zijn gevonden betreffende ervaring met cyberzaken, hadden vier hiervan een middelmatig tot groot effect. Deze hadden betrekking op intake en service-normen (I.4, I.5 en I.6) die ook zijn bevraagd bij blauw. Net als bij opleiding ging het hier onder andere ook om de toepassing van de zeven W's en de uitwerking van doorvragen bij aangifte. Daarnaast ging het om kennis van welke digitale sporen geïnventariseerd kunnen worden voor het aanvullen van een aangifte en kennis van wat bitcoinadressen zijn. Hierbij geldt dat hoe meer ervaren, hoe hoger de scores.

6.1.5 Indien een tekort is vastgesteld, hoe kan dat worden bestreden?

Het bestrijden van het kennistekort is geen eenvoudige opgave en leidde in de interviews met experts tot een discussie over wat basiskennis inhoudt en welk aandeel van de politiemensen deze kennis dient te bezitten. Bepaalde kennis moet bij ieder politiemens paraat zijn. Heeft men langer de tijd om te handelen, dan is parate kennis minder van belang, omdat politiemensen deze kunnen halen uit groepen, netwerken of systemen.

Het is volgens de geïnterviewden niet zo dat kennis alleen bij specialisten belegd moet worden om het kennistekort op te lossen. Specialistische kennis op digitaal gebied wordt steeds vaker generalistisch. Daarnaast moet een generalist met een specialist kunnen communiceren over de te nemen stappen. Daarvoor is ook een bepaalde mate van basiskennis nodig. Een kennisgebrek kan er bijvoorbeeld toe leiden dat politiemensen niet de goede vragen stellen in opsporingsonderzoek en digitale sporen niet kunnen duiden (Marskamp-Zuurveen & Stol, in druk).

Een diversiteit aan leermethoden wordt aangeraden om het kennistekort aan te pakken, best passend bij functiegroep en kennisthema. Een belangrijk onderdeel hiervan is praktijkleren (zie ook Van Diepen, e.a., 2009), waarbij eveneens – individueel en met collega's – gereflecteerd wordt op het handelen. Dit kan met kerninstructeurs, casuïstiek, training-on-the-job, et cetera. Met andere woorden, leren gebeurt effectiever wanneer dit contextrijk gebeurt, met een authentiek/actueel vraagstuk, en wanneer dit aansluit bij waar de 'lerende' staat. Ook wordt actief leren in een sociale setting, via interactie met anderen, als effectief beschouwd.

Ervaring met cyberzaken – alsook een positieve inschatting van eigen kennis en vaardigheden en het hebben gevolgd van een cursus op cybergebied – hebben een positieve invloed op de bereidheid om aan cyberzaken te werken (Bossler, e.a., 2019). Tevens moet kennis goed te vinden zijn; op het juiste moment en op de juiste plaats, en met de voorwaarde dat het up-to-date is. Ook

het aanbod van bijvoorbeeld opleidingen en cursussen moet goed vindbaar zijn (Flory, 2016; Marskamp-Zuurveen & Stol, in druk). Een ander genoemde methode om kennis te verbeteren, dan wel te borgen, is door *performance support by design*. Hierbij worden politiemensen geholpen door systemen die politiemensen de informatie aanbieden die zij op dat moment nodig hebben. In vervolgonderzoek kan middels experimenten met verschillende en/of gecombineerde leermethoden worden gekeken welke methoden wanneer het geschiktst zijn c.q. het meeste effect sorteren. In hoofdstuk 7 gaan we nader in op strategieën om het kennisterkort aan te pakken.

Daarnaast is bij het uitleren van kennis bij grote groepen de balans tussen de effectiviteit van de methode versus de hiermee gemoeide kosten van wezenlijk belang. Dit is overigens geen nieuwe constatering en geldt voor veel gebieden binnen de politie. Zo wordt bijvoorbeeld in het rapport van Ernst, ter Veen, Lam, en Kop (2019) aangegeven dat de factor 'gebrek aan capaciteit', c.q. aantal en kwaliteit van medewerkers, het technologisch innoveren binnen de Nationale Politie belemmert. Een ander voorbeeld betreft onlinefraudebestrijding door de politie waarbij onder meer een gebrek aan middelen en expertise worden aangemerkt als belemmerde factoren (Bossler, e.a., 2019).

6.2 Beperkingen

Ons onderzoek kent een aantal beperkingen. Er is beperkt inzicht verkregen in opleidings-documentatie van de Politieacademie. De bereidwilligheid om documentatie te delen was laag, doordat – zo werd aangegeven – de betreffende documentatie op moment van onderzoek werd herzien. Deze beperking hebben we kunnen ondervangen door gebruik te maken van literatuur en interviews.

In de interviews die tot doel hadden om te duiden hoe de intake en afhandeling van digitale criminaliteit en van criminaliteit met een digitale component verloopt binnen de politieorganisatie, kwam naar voren dat er veelal een zogenoemde incidentgerichte benadering wordt gehanteerd (zie par. 4.2). Dit betekent dat in de interviews weinig aandacht was voor de twee overige benaderingen, namelijk de probleemgerichte en programmatische aanpak. Hoewel deze benaderingen onderbelicht zijn gebleven in de interviews, hebben we informatie kunnen putten uit relevante documentatie.

Een andere beperking ligt in de methode voor het meten van kennis. Voor dit onderzoek is dat gedaan aan de hand van een online vragenlijst. Voor het doel van de studie was dit een geëigende methode. Om het kennisniveau op individueel niveau vast te stellen, zou echter een meer kwalitatieve benadering, zoals observatie, de voorkeur hebben. Desalniettemin kunnen we stellen dat de resultaten voor een groot deel te generaliseren zijn. Zo werden amper significante verschillen gevonden tussen de meewerkende eenheden (zie ook par. 3.5). Daarnaast kan het geven van sociaalwenselijke antwoorden een negatieve rol spelen in vragenlijstonderzoek. Dit hebben we zo goed mogelijk proberen te ondervangen door in de introductie duidelijk te maken dat de

vragenlijstdata anoniem worden verwerkt. Ook werden de respondenten geïnstrueerd dat er geen goede of foute antwoorden zijn, maar dat het belangrijk is om hun mening te delen.

Ten slotte, om de vijfde deelvraag – over het bestrijden van kennistekort – te beantwoorden, zijn vier interviews afgenomen. Hoewel dit een eerste overzicht biedt van mogelijkheden om het kennistekort aan te pakken, verdient het aanbeveling om hier in vervolgonderzoek dieper op in te gaan. Met dit onderzoek is gekeken naar kennis over digitale aspecten op operationeel gebied. In vervolgonderzoek kan tevens worden gekeken naar hoe veilig politiemensen omgaan met het gebruik van digitale middelen (cyberveilig-gedrag); eveneens een belangrijke thema aangaande digitalisering. Daarnaast is het interessant om te inventariseren welke lokale initiatieven er zijn binnen de politie op het gebied van kennisvergroting en te evalueren in hoeverre deze werken. Hierbij is het wel van belang om goed te kijken naar de doorwerking ervan in nationaal perspectief.

7. Slotbeschouwing en aanbevelingen

In dit hoofdstuk wordt teruggeblikt op het onderzoek en formuleren we onze centrale boodschap. Daarnaast worden een aantal gerichte aanbevelingen gedaan voor vervolgstappen om de geconstateerde kennislacunes het hoofd te bieden.

7.1 Slotbeschouwing

Dit onderzoek ging onder andere over het bepalen van een kennisnorm aangaande digitale aspecten van politiewerk en is een eerste stap in die richting. Het onderzoek wijst uit dat (a) het bepalen van een norm niet alleen erg belangrijk is, maar (b) ook zeer lastig is vast te stellen.

Alles overziend kan worden geconcludeerd dat het beantwoorden van de vraag wat het kennisniveau van politiemensen inzake digitale aspecten van politiewerk is, aan de ene kant nieuwe vragen oproept. Aan de andere kant moet worden geconstateerd dat verbetering in de breedte en diepte noodzakelijk is. Welbeschouwd werd op veel digitale aspecten van politiewerk niet hoog gescoord. Dat kan een risico vormen. Denk bijvoorbeeld aan de gevolgen voor een opsporingsonderzoek wanneer een aangifte onvolledig of onjuist wordt opgenomen, op een PD de aanwezige digitale sporen worden vernietigd of besmet, of vluchtige gegevens verloren gaan.

De kennisnormen – een belangrijke uitkomst van dit onderzoek – kunnen helpen om hier verbetering in aan te brengen. We weten nu immers beter dan voorheen waar de deficits zich voordoen en bij welke groep(en). De grootste deficits liggen bij de functiegroepen intake en service, en blauw. In mindere mate liggen deze bij de basisteamrecherche. Ook de andere groepen zijn niet uitgeleerd zolang de digitalisering voortgaat. Het verdient nogmaals de aandacht dat de kennisnormen – in deze snel veranderende, gedigitaliseerde samenleving – tijdelijk van aard zijn. De uitkomsten van dit onderzoek kunnen dan ook worden gezien als een tussenstand. Welke digitale kennis politiewerk vereist, verandert continu en vergt meebewegen. De vraag die dat oproept is hoe dat ‘meebewegen’ in kennis het beste gaat. Ons onderzoek laat enkele mogelijkheden zien.

Daarnaast heeft dit onderzoek gepoogd inzichtelijk te maken hoe het kennistekort kan worden bestreden. Wanneer we kijken naar recente ontwikkelingen binnen de politieorganisatie (buiten het onderzoek om) zien we dat er volop initiatieven worden genomen en stappen worden gezet om aansluiting te zoeken bij allerlei technologische ontwikkelingen. Gezien het belang van de benodigde – maar nu nog niet volledig toereikende – kennis, dient een duidelijke, veelomvattende actie tot kennisvermeerdering ingezet te worden.

Opleiden lijkt het meest voor de hand liggend om het kennistekort aan te pakken. Dit onderzoek laat een verband zien tussen het gevolgd hebben van een opleiding/cursus over digitaal en de mate van kennis. Mensen met een opleiding scoren veelal hoger dan mensen zonder. De vraag hierbij is echter wel of politiemensen die naar een opleiding zijn gegaan, bij voorbaat al meer dan

gemiddeld kennis omtrent digitaal hadden, of dat zij door het volgen van een opleiding een hoger digitaal kennisniveau hebben gekregen. In het laatste geval is te concluderen dat opleiden helpt en dat daarop dus kan worden geïnvesteerd (zie ook par. 7.2).

Opleiden kan op diverse wijzen ingevuld worden (zie par. 6.1). Wij presenteren hier een van de mogelijkheden die ons het kansrijkst lijkt. Geïnterviewde experts wezen op *learning on the job* (ervaringsleren). Die route sluit aan bij de praktijk van alledag en bij hoe politiemensen vaak al leren. In dat licht is aan te raden om een werksituatie te creëren waarin politiemensen op basis van echte zaken in aanraking komen met 'digitaal' en daaraan werken met collega's met diverse (digitale) expertise. Door het met elkaar te doen ontstaat het leren bijna vanzelf. Belangrijk is wel om dit te faciliteren. Enerzijds door medewerkers de ruimte te geven om ook te reflecteren op het handelen (als individu en als groep), alsook door ondersteuning te bieden bij het vergaren van kennis.

Volgens experts hoeven politiemensen niet altijd alle benodigde kennis paraat te hebben, zolang zij maar op het juiste moment over die kennis kunnen beschikken. Hier zijn reeds diverse oplossingen voor aanwezig, zoals een *Real Time Intelligence Center* (RTIC), het beschikbaar hebben van apps, het bevragen van collega's, aandachtvestigingen in de briefing, et cetera. Tegelijk blijkt uit dit onderzoek dat deze oplossingen niet altijd goed werken, bijvoorbeeld omdat ze simpelweg niet bekend zijn bij politiemensen. De bekendheid met de webapps van de Politieacademie is hier een voorbeeld van. Dit lijkt binnen de Nationale Politie overigens niet een op zichzelf staand probleem. Het recentste RTIC-onderzoek bijvoorbeeld leidt tot de conclusie dat de informatievoorziening 'nog niet effectief georganiseerd is' (Scholtens e.a. 2016, p. 157). Ook communicatie kan een rol spelen. Een voorbeeld hiervan zijn de briefings: 'Briefings bevatten doorgaans te veel informatie, waardoor deze aan slag- en zeggingskracht verliest.' (Den Hengst & In 't Veld 2014, p.129). Naast communicatie over bijvoorbeeld het wie, wat en waar, is het van belang dat specialisten en generalisten elkaars 'taal' leren spreken.

Kennis op het juiste moment en tijdig bij politiemensen krijgen kan ook met het concept *performance support by design* (ondersteuning via tips vanuit een computerprogramma). Op dit gebied is bij ons weten nog weinig ervaring opgedaan. We kennen althans geen evaluatiestudies. Duidelijk is wel dat de strategie om politiemensen te voorzien van informatie op of vlak voor het moment dat zij die nodig hebben, niet zomaar effectief is. Investeren in het beschikbaar krijgen van kennis, bijvoorbeeld door een goed portaal, *performance support by* design, en menselijke ondersteuning, is essentieel voor politiemensen om hun weg te vinden in de snel veranderende wereld.

Hiermee hebben we twee strategieën aangeduid voor het vergroten van digitale kennis bij politiemedewerkers. De twee strategieën zijn: (een combinatie van) opleiden en kennismanagement. Bij opleiden lijkt *learning on the job* goed te passen bij politiemensen. Bij kennismanagement gaat

het over kennissystemen, *performance by design* en kennisnetwerken. Elk apart of gecombineerd initiatief verdient het om te worden geëvalueerd, want een bewezen effectieve praktijk (dé oplossing) staat niet zomaar klaar.

Bij deze strategieën gaat het niet alleen om implementatie. De borging ervan is minstens zo belangrijk. Veel afzonderlijke initiatieven zullen falen wanneer niet wordt gekeken naar de overkoepelende organisatie. Persoonlijke ontwikkeling en *learning on the job* kunnen bijvoorbeeld niet plaatsvinden wanneer dit niet gefaciliteerd wordt (denk aan betrokkenheid van leidinggevenden en praktijkbegeleiding). Een kennisportaal – hoe goed ook – zal niet gevonden worden zonder hierover te communiceren. En kennisnormen zullen niet worden behaald zolang deze niet expliciet vastgelegd worden en iemand zich er hard voor maakt. Vervolgonderzoek moet uitwijzen bij wie of welk (eventueel nog op te richten) organisatieonderdeel deze verantwoordelijkheid moet komen te liggen. Het voordeel om de verantwoordelijkheid te beleggen is dat er niet vrijblijvend mee kan worden omgegaan.

Tot slot willen wij benadrukken dat de problematiek die we in dit onderzoek hebben behandeld alsook de mogelijke oplossingen, niet alleen gelden voor het digitale vakgebied, maar dat ze – gezien de digitale transformatie van de samenleving – voor alle vakgebieden binnen de politieorganisatie relevant kunnen zijn.

7.2 Aanbevelingen

Dit onderzoek laat zien dat op diverse punten vervolgonderzoek noodzakelijk is. Suggesties voor vervolgonderzoek zijn hierna uiteengezet. Daarnaast presenteren wij diverse aanbevelingen die gericht zijn op de politieorganisatie, opleiden en kennismanagement, met als doel het kennisniveau aangaande digitale aspecten van politiewerk te verbeteren.

7.2.1 Vervolgonderzoek

Nu volgen de aanbevelingen voor vervolgonderzoek. Ten eerste bevelen we aan om nader onderzoek te doen naar de kennisnormen voor de verschillende takenprofielen. Door een dergelijk onderzoek wordt steeds duidelijker wie welke kennis dient te bezitten (het gaat hier om *parate* kennis). Dit onderzoek heeft zich beperkt tot kennisnormen die kunnen dienen voor een basisprofiel voor de vijf onderscheidden functiegroepen. Door te kijken naar takenprofielen worden de kennisnormen verder gespecificeerd en kunnen gerichte programma's worden ontworpen om die normen te halen. Wellicht kunnen de takenprofielen ook worden uitgebreid.

Ten tweede is het raadzaam te investeren in onderzoek naar de verschillen tussen noodzakelijke *parate* kennis en kennis die in groepen, netwerken of systemen weggezet kan worden.

Uit dit onderzoek komt namelijk naar voren dat wanneer men langer de tijd heeft om te handelen, de noodzaak kennis *paraat* te hebben kleiner wordt.

Ten derde is vervolgonderzoek naar de effectiviteit van opleiden en opleidingsstrategie(ën) noodzakelijk. Bestaat inderdaad een positief causaal verband tussen opleiden en mate van kennis over politiewerk in een gedigitaliseerde samenleving? Dit onderzoek doet dat vermoeden, maar zekerheid is van wezenlijk belang. Wanneer blijkt dat het huidige opleiden geen remedie is, dan kan dit aan de manier van opleiden liggen, maar wellicht ook aan het type politiemensen dat wordt geselecteerd voor die opleiding.

Ten vierde is onderzoek gewenst naar randvoorwaarden – of kritische succesfactoren – die een leerproces effectief maken. Gezien de (negatieve) invloed die opleiden heeft op de inzetbare capaciteit, is het evident dat het rendement van opleiden zo groot mogelijk moet zijn. Een goed startpunt is bijvoorbeeld om de rol van leidinggevenden (denk aan procesbewaking) en praktijkbegeleiders te evalueren. Daarnaast moet ook gekeken worden naar de rol van de betreffende politiemens zelf, zoals het nemen van eigen verantwoordelijkheid voor resultaten.

Tot slot vonden we *geen* onderbouwing voor het idee dat het digitaal kennistekort bij de politie generatiegebonden is. Dat vergt nader onderzoek want dat stelt de politie namelijk voor de vraag op wie zij zich kan verlaten als het aankomt op het versterken van haar digitale kennis. Onze bevindingen wijzen erop dat de oplossing niet als vanzelf komt met een nieuwe generatie politiemensen. De vraag is dus wie dan wel de dragers zullen zijn van de digitale kennis die de politie steeds meer nodig heeft.

7.2.2 Kennisontwikkeling: politieorganisatie, opleiden en kennismanagement

In deze sectie zijn aanbevelingen opgenomen die tot doel hebben het kennistekort van politiemensen aangaande digitale aspecten van politiewerk te bestrijden. De aanbevelingen met betrekking tot de politieorganisatie, opleiden en kennismanagement raken elkaar zodanig dat deze niet los van elkaar te zien zijn en worden dus gezamenlijk gepresenteerd.

Voor de politieorganisatie is de belangrijkste aanbeveling dat de kennisnormen gesteld wordt voor alle functies binnen de Nationale Politie. In de vastgestelde beroepsprofielen 2020-2030 (Nationale Politie, 2020) is reeds abstract beschreven dat deze kennis noodzakelijk is. Door een norm te stellen dient men in de breedte aan deze norm te (gaan) voldoen. Dat geldt dan dus ook voor nieuwe medewerkers. Door het personeelsbeleid van deze normen te laten doordringen wordt de kraan dus afgesloten en kan het dweilen echt beginnen. Wel moeten de normen periodiek geëvalueerd en geactualiseerd worden. Op het gebied van digitalisering bevelen wij aan dit maximaal elke twee jaar, maar liever elk jaar, te laten plaatsvinden. Mogelijk kan dit samenlopen met het

vaststellen van de jaarlijkse beleidsdoelen aangaande cybercrime voor de Gezamenlijke Veiligheidsagenda van het Ministerie van Justitie en Veiligheid.

Ten tweede bevelen wij met betrekking tot kennismanagement aan om een raamwerk op te stellen dat voor eenieder duidelijk maakt welke kennis (over digitale aspecten) waar te vinden is. Hierbij zou het niet uit moeten maken waar de kennis zich bevindt – mensen, middelen of systemen – zolang deze maar vindbaar is. Het bestaan van het raamwerk en de vindplaats ervan, dient onderdeel te zijn van de basiskennis.

Ten derde verwachten wij dat goede communicatie met betrekking tot de genomen stappen essentieel is. Het moet voor politiemensen duidelijk zijn waar welke kennis te vinden is, welke opleidingen passen bij het huidige en toekomstige functioneren en op welke wijze experts uit de diverse kennisnetwerken te vinden zijn. Een eerste stap kan zijn om politiemensen in leidinggevende posities van de onderscheidden functiegroepen hierin mee te nemen, zodat zij dit kunnen overbrengen richting de werkvloer. Een andere mogelijkheid is om hiervoor cyberambassadeurs aan te stellen die nieuwe ontwikkelingen bij collega's onder de aandacht brengen.

Tot slot denken wij dat de Nationale Politie gebaat zou zijn bij het ontwikkelen van een *roadmap* met betrekking tot het opleiden van politiemensen. Vanwege de snelle ontwikkelingen van gedigitaliseerde samenleving is het van belang duidelijk te maken waar men nu staat en welke stappen men gaat zetten om klaar te zijn voor zowel de nabije als verdergelegen toekomst. Wij adviseren daarnaast om alle leerwijzen tegen het licht te houden en deze – waar nodig – aan te vullen met de digitale aspecten van het dagelijkse (politie)werk. Het is belangrijk om 'digitaal' niet te zien als iets dat plaatsvindt naast regulier politiewerk, maar als een geïntegreerd onderdeel van de dagelijkse praktijk. Immers, de scheidslijn tussen online en offline is veelal niet scherp, maar vloeit in elkaar over. Een andere reden is dat cybercrime, gedigitaliseerde criminaliteit en criminaliteit met een digitale component nu zoveel voorkomen dat het niet aan specialisten kan worden overgelaten. In combinatie met het aanbevolen vervolgonderzoek wordt een duidelijk beeld verschaft van hetgeen wel en niet werkt op het gebied van opleiden en welke randvoorwaarden hieraan verbonden zijn.

Referenties

ACPO (Association of Chief Police Officers) (2005). *Practice advice on core investigative doctrine.* Cambridgeshire: ACPO.

Amelsvoort, A. van, & Groenendal, H. (2017). *Handleiding Optreden plaats delict.* Den Haag: SDU uitgevers.

Bossler, A.M., Holt, T.J., Cross, C., & Burruss, G.W. (2019). Policing fraud in England and Wales: Examining constables' and sergeants' online fraud preparedness. *Security Journal*, doi: https://doi.org/10.1057/s41284-019-00187-5.

Bryant, R., & Kennedy, I. (2014). Investigating digital crime. In: R. Bryant, & S. Bryant (red.), *Policing digital crime* (pp. 123-146). Farnham: Ashgate.

Campman, I., Dedert, P., Hesseling, R., Huijskes, P. J., Kegel, D., Tijsmans, N., Vulpen, S., van & Witteveen, Z. (2012). *Criminaliteit in een gedigitaliseerde samenleving.* Politie (Amsterdam-Amstelland, Haaglanden, Rotterdam-Rijnmond, Utrecht, KLPD).

Derickx, J.W.H., Hoogendam, L., & Spijkerman-van Zon, F.M. (1994). *Statistische gegevensverwerking met SPSS/PC+.* Houten: Stenfert Kroese.

Diepen, N.M. van, Stefanova, E., & Miranowicz, M. (2009). Mastering skills using ICT: An active learning approach. In: A. Méndez-Vilas, A. Solano Martin, J. Mesa González, & J.A. Mesa Gonzalez (Eds.), *Research, reflections and innovations in integrating ICT in education*. Badajoz, Spanje: Formatex.

Edison, S.W. & Geisler, G.L. (2012). Measuring attitudes towards general technology: Antecedents, hypotheses, and scale development. *Journal of Targeting, Measurement and Analysis for Marketing, 12*(2), 137-156.

Ernst, S., Veen, H. ter, Lam, J., & Kop, N. (2019). *Leren van technologisch innoveren: De techniek is niet zo spannend.* Apeldoorn: Politieacademie.

Field, A. (2009). *Discovering statistiscs using SPSS (3e editie).* London, Verenigd Koninkrijk: SAGE.

Flory, T.A.C. (2016). Digital forensics in law enforcement: A needs based analysis of Indiana agencies. *Journal of Digital Forensics, 11*(1), 7-38.

Hengst, M. den & Veld, M. in 't (2014). *Briefen voor en door basisteams: Een onderzoek naar verbeteringen in de overdracht van briefingsinformatie*. Apeldoorn: Politieacademie.

Huisman, A., Princen, M., Klerks, P., & Kop, N. (2016). *Handelen naar waarheid. Sterkte- en zwakteanalyse van de opsporing.* Verkregen via: https://www.politie.nl/binaries/content/assets/politie/nieuws/2016/00-km/handelen-naar-waarheid.pdf

Jansen, J. & Van Valkengoed (2019). *Level-Up! Addendum: Statistische output; vergelijkingen van groepen*. Leeuwarden: Cybersafety Research Group.

Jong, L., de (2015a). *Werking Digitaal Platform.* Politie (interne rapportage).

Jong, L., de (2015b). *Werking Team Digitale Opsporing.* Politie (interne rapportage).

Korps Nationale Politie (2012). *Inrichtingsplan Nationale Politie*. Den Haag: Nationale Politie.

Kruger, J., & Dunning, D. (1999). Unskilled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of Personality and Social Psychology, 77*(6), 1121-1134.

Leukfeldt, E.R., Veenstra, S., Domenie, M.M.L., & Stol, W.Ph. (2012). *De strafrechtketen in een gedigitaliseerde samenleving: Een onderzoek naar de strafrechtelijke afhandeling van cybercrime.* Leeuwarden: lectoraat Cybersafety.

Leukfeldt, R., Kentgens, A., Frans, B., Toutenhoofd, M., Stol, W., & Stamhuis, E. (2012). *Alledaags politiewerk in een gedigitaliseerde wereld: Handreiking voor delicten met een digitale component.* Den Haag: Boom Lemma Uitgevers.

Leukfeldt, R., Kentgens, A., Prins, E. & Stol, W. (2015). *Alledaags politiewerk in een gedigitaliseerde wereld: Handreiking voor de intake van delicten met een digitale component.* Leeuwarden: Lectoraat Cybersafety.

Marskamp-Zuurveen, R. & Stol, W. (in druk). *Benutten van digitale sporen*. Den Haag: Politie & Wetenschap.

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

Ministerie van Veiligheid en Justitie (2012). *Inrichtingsplan Nationale Politie*. Den Haag: Ministerie van Veiligheid en Justitie.

Ministerie van Veiligheid en Justitie (2015). *Herijkingsnota: Herijking realisatie van de nationale politie.* Den Haag: Ministerie van Veiligheid en Justitie.

Nationale Politie (2020). *Beroepsprofielen Politie 2020-2030.* Den Haag: Nationale Politie.

Hess Orthman, C., & Matison Hess, K. (2013). *Criminal investigation (tenth edition)*. New York: Delmar Cengage Learning.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. Journal of Applied Psychology, 88(5), 879–903.

Scholtens, A., Hengst, M den & Waterreus, R. (2016). *Het real-time informeren van noodhulpeenheden: Een onderzoek naar de RTI-functie om frontlijnpolitiefunctionarissen snel te voorzien van relevante informatie.* Reeks Politiekunde, nr. 77. Amsterdam: Reed Business.

Stelfox, P. (2009). *Criminal investigation. An introduction to principles and practice.* Cullomton: Willan Publishing.

Stol, W.Ph. (1996). *Politieoptreden en informatietechnologie. Over sociale controle van politiemensen.* Lelystad: Koninklijke Vermande.

Stol, W.Ph., Treeck, R.J. van & Ven, A.E.B.M. van der (1999). *Criminaliteit in cyberspace: Een praktijkonderzoek naar aard, ernst en aanpak in Nederland.* Den Haag: Elsevier.

Stol, W.Ph., Velt, C.J.E. in 't & Treeck, R.J. van (2000). *Praktijkboek politieonderzoek: Handleiding voor het opzetten van verbetergericht onderzoek bij de politie.* Den Haag: Elsevier.

Tilley, N., Robinson, A., & Burrows, J. (2007). The investigation of high volume crime. In: T. Newburn, T. Williamson & A. Wright (red.), *Handbook of criminal investigation* (pp. 226-254). Abingdon: Willan Publishing.

Toutenhoofd, M.H., Veenstra, S., Domenie, M.M.L., Leukfeldt, E.R., & Stol, W.Ph. (2009). *Politie en Cybercrime: Intake en eerste opvolging.* Leeuwarden: Noordelijke Hogeschool Leeuwarden.

TRIO opsporing (2014). *Landelijk Werkingsdocument Opsporing.* Politie (interne rapportage).

Valkengoed, T. van (2017). *Competentieonderzoek cybercrimeopsporing.* Amsterdam: Team Digitale Opsporing – politie-eenheid Amsterdam (afstudeerscriptie).

Veenstra, S., Zuurveen, R., Kerstens, J., & Stol, W. (2016). *Opsporing in een gedigitaliseerde samenleving. Een handreiking voor het herkennen, vinden en benutten van digitale sporen.* Leeuwarden: Lectoraat Cybersafety.

Zuurveen, R., Doodeman, M., Veenstra, S., & Stol, W. (2015). *Herkennen en veiligstellen van digitale apparatuur.* Leeuwarden: Lectoraat Cybersafety.

Bijlage I: Overzicht onderwijsaanbod

In deze bijlage is het relevante opleidingsaanbod van de Politieacademie opgenomen, gerubriceerd naar aard van het onderwijs en doelgroep. Deze inventarisatie is ontleend aan (dd. 24 januari 2018): https://www.politieacademie.nl/onderwijs/onderwijsaanbod/.[27] Ten tijde van het onderzoek werd duidelijk dat het onderwijs sterk in ontwikkeling is. Dit betekent dat het huidige aanbod hoogstwaarschijnlijk is gewijzigd op een aantal onderdelen. De klankbordgroep verwoorde dit als volgt: waar de Politieacademie voorheen onderwijs aanbood waar politiemensen gebruik van konden maken, bepaalt de vraag vanuit de politiepraktijk tegenwoordig welk onderwijs er wordt aangeboden.

Algemeen onderwijs

Tabel I.1: Intake en service

Module Intake en Service medewerker	Dienstverlening, afhandelen melding, afhandelen aangifte, informatieverzoek, kwaliteit van aangiften
Module Intake en Service assistent (B)	-

Tabel I.2: Blauw

Opleiding: Master of Science in Policing	Gemeenschappelijke veiligheidszorg, criminaliteitsanalyse, gebiedsgebonden werk, positie van politie in samenleving / legitimiteitsvragen, recherchewetenschap, criminaliteitsstrategieën, politiesamenwerking in Europa
Opleiding: HBO-Bachelor of policing	Noodhulp, opsporing en handhaving, Er is een specialisatie 'recherchekunde'
Opleiding: allround Politiemedewerker 2.0	Opgeleid voor de politiekerntaken Intake, Handhaven, Noodhulp, Opsporen en Signaleren en Adviseren
Module: optreden op plaats delict bij ernstige delicten	Waarnemen, eerste hulp aan SLO, afzetten PD, Sporen beveiligen, contact met instanties, verdachte onderzoeken/aanhouden, voorgeleiden, rapporteren

Tabel I.3: Recherche

Opleiding: Recherchekundig master / tactisch	Structureren rechercheonderzoek, afwegingen en keuzes maken, hypothesen/scenario's, uitvoeren onderzoek + methoden en technieken toepassen, bewijs vergaren, kennisontwikkeling, gesprekspartner
Opleiding: Recherchekundig master / criminaliteitsanalyse en recherchekunde	Idem, andere accent

[27] Achterliggende opleidingsdocumentatie was niet inzichtelijk voor de onderzoekers.

Tabel I.3 (vervolg): Recherche

Opleiding: Politiekundige bachelor, specialisatie recherchekunde	Noodhulp, opsporing en handhaving, Er is een specialisatie 'recherchekunde', als wordt gekozen voor de minor Recherche
Opleiding: leergang recherchemedewerker: tactisch rechercheur (niveau 4)	Algemene recherchevaardigheden: rechercheren in een meer omvattende zaak en TGO, tactisch data onderzoek, dossiervorming basis, aangevuld met een afstudeerrichting (zeden, drugs en wapens, FinEc, milieu) en keuzemodules (geen digi).
Training: Kerntaak opsporing (opvolger van de Basisopleiding Recherche – BOR)	Rechercheren / tactische methoden, verdachte en verdachtenverhoor, getuige(n)verhoor, materiaal strafrecht, bevoegdheden, aangifte, aanhouding en zoeking, FinEc, drugs en wapens, digitaal rechercheren, BOB, Internet en sociale media, bestuursrecht, confrontatie
Module: Minor recherche	Recht, BOB, PD management en forensics, informatieorganisatie, privacy, digitale opsporing, financieel rechercheren, vormverzuim, actualiteitenopsporing, internationale aspecten, georganiseerde criminaliteit en verhoor.
Module: Professioneel Verhoor	Leidt op tot professioneel verhoorder in complexe zaken. Er zijn ook nog verdiepende / specialiserende trainingen / cursussen.
Module: Dossiervorming basis	Opleiding voor de functie dossiervormer in meer omvattende rechercheonderzoeken. Er zijn verdiepende trainingen mogelijk, bijvoorbeeld over werken met politiesystemen.

Cyberonderwijs

De Politieacademie lijkt geen cyberonderwijs aan te bieden dat specifiek is gericht op medewerkers intake en service. Wellicht dat zij wel baat kunnen hebben en/of gebruik maken van 'algemene' cybermodules. Intake en service, blauw, en recherche zijn geen elkaar uitsluitende functiegroepen. 'Blauwe' politiemedewerkers, kunnen ook zijn belast met intake- en/of recherchewerk. Een aantal van de cyber-gerelateerde opleidingen/modules/trainingen die in dit overzicht zijn toebedeeld aan 'recherche' zijn dus ook voor blauw relevant. Voor deze rubricering is gekozen, omdat het opleidingsaanbod op de Politieacademie onder de categorie 'opsporing' valt.

Tabel I.4: Recherche

Opleiding: MSc Forensic Computing & Cybercrime Investigation	Externe master
Opleiding: Recherchekundig master / digitaal	Beschrijving op website is gelijk aan die van de reguliere recherchekundige master/tactisch. Betreft een specialisatie.
Opleiding: Recherchekundig master / forensisch digitaal	Idem.
Module: Internet en opsporing (fase 1)	Aanpak, analyse, interpretatie, afbreukrisico en werkwijze met betrekking tot het forensisch veiligstellen van data uit openbare (inter)netwerken en verslaglegging in PV

Tabel I.4 (vervolg): Recherche

Module: Tactisch Data Onderzoek	Leren gebruik te maken van (forensische) opsporingsmogelijkheden in digitale omgevingen
Module: Vaststellen en beoordelen van de bewijswaarde van digitale sporen	Wetenschappelijke bronnen en research, digitale wetenschappen en opsporingscriminalistiek, juridische bewijswaarde
Module: Volledig forensisch technisch onderzoek bij VVC	Leren een forensisch sporenonderzoek uit te voeren bij VVC en maken bijbehorend PV
Module: Hacking Investigation	Forensische verantwoord veiligstellen van relevante data uit gehackte systemen
Module: Forensisch digitaal opsporen in eenvoudige situaties	Juridische, technische en tactische aspecten van forensisch digitaal opsporen
Module: Forensisch digitaal opsporen in complexe situaties	Vervolgopleiding, met aandacht voor werken met EnCase
Training: Digitalisering in de opsporingspraktijk	'Maakt je bewust van de mogelijkheden die de digitalisering van de samenleving biedt voor de opsporing'. Herkennen en benutten digi sporen (voor tactisch rechercheurs).
Training: Basis Internet Training (BIT)	Basisprincipes van internet en gebruik iRN
Training: Basistraining internetonderzoek met IRN (blauw)	Idem
E-learning: GOBI online	Veilig gebruik van openbare internetbronnen
Training internet/jeugd/sociale media	Effectief zoeken in sociale media
Training: Uitlezen Communicatiemiddelen	Basisvaardigheden over het veiligstellen en uitlezen van communicatiemiddelen.
Training: Internet Evidence Finder	Leren werken met IEF

Bijlage II: Interviewprotocol intake en afhandeling

INTRODUCTIE
Onderzoek naar digitalisering van samenleving en de gevolgen daarvan voor veiligheid en rechtshandhaving.

Toelichting Level-Up!
Inzicht bieden in het kennisniveau van politiemedewerkers 'inzake digitale aspecten van politiewerk'. Daarmee worden cybercrime, gedigitaliseerde criminaliteit en criminaliteit met een digitale component (het gebruik van digitale sporen) bedoeld. 3 stappen:

- Vaststellen over welke kennis en vaardigheden politiemensen moeten beschikken om effectief uitvoering te geven aan politiewerk in een gedigitaliseerde samenleving
- Vaststellen over welke kennis en vaardigheden politiemensen daadwerkelijk beschikken
- Meten waar een eventueel kennistekort zich voordoet en wat dat kennistekort inhoudt

Het onderzoek leidt uiteindelijk tot een advies over het reduceren van het kennistekort inzake digitale aspecten van politiewerk. PIAC is opdrachtgever.

Het interview
Doel is het kennisniveau te meten onder vijf functiegroepen: intake en service, blauw en de drie rechercheniveaus (basis, regio, eenheid). Het is daarom essentieel eerst inzicht te bieden in de wijze waarop de intake en afhandeling (door blauw/recherche) van 'digitale criminaliteit' zijn georganiseerd en wie daarin welke rol vervult. Daarover gaat het interview.

Opmerkingen vooraf
Alle input wordt anoniem verwerkt in het onderzoeksrapport
Verslag wordt ter verificatie voorgelegd
Toestemming tot opname?

VRAGEN

Mogelijkheden voor politiecontact
Welke mogelijkheden zijn er om melding te doen binnen de eenheid?
Welke mogelijkheden bestaan er om aangifte te doen binnen de eenheid?
In hoeverre verschillen de contactmogelijkheden voor traditionele criminaliteit (met een digitale component), gedigitaliseerde criminaliteit en cybercrime?

Bekende mogelijkheden - Politiebureau (3d aangifteloket) - Telefonisch - Internet: mijnpolitie, meldpunten - Locatie (bij mensen thuis/bedrijf)

Proces van melding/aangifte
Wat gebeurt er met meldingen?
-Verschil tussen traditionele criminaliteit, gedigitaliseerde criminaliteit/cybercrime?
Wat gebeurt er met aangiften? Toelichting aangifteproces

Uit eerder onderzoek en beleidsdocumentatie weten we dat idealiter de volgende stappen (kunnen) worden doorlopen - opnemen aangifte, - casescreening, - toewijzen aan blauw/recherche, - opnieuw wegen (door dossiermanager van betreffende organisatieonderdeel), - opsporingsonderzoek Over een aantal van deze processtappen volgen hierna verdiepingsvragen.

Opnemen aangifte

Hoe verloopt het opnemen van aangifte?

- Verschil tussen traditioneel / gedigitaliseerde criminaliteit / cybercrime?

Wie neemt aangifte op?

- Verschil tussen traditioneel / gedigitaliseerde criminaliteit / cybercrime?
- In hoeverre worden bij gedigitaliseerde criminaliteit / cybercrime-experts geraadpleegd? Waarom?

Over welke kennis en vaardigheden moet een medewerker die aangifte opneemt beschikken 'inzake digitale aspecten van politiewerk'? Wat zijn de basisvereisten, wat is gewenst?

- Welke kennis of vaardigheden van reguliere medewerkers intake en service schieten te kort?

Casescreening

Hoe verloopt het proces van casescreening?

Welke factoren spelen een rol bij de afweging of een aangifte behandeld wordt?

- Kwaliteit van de aangifte
- Kennis en vaardigheden (Geschikte capaciteit) blauw/recherche
- Verschil tussen traditioneel / gedigitaliseerde criminaliteit / cybercrime?

Wie krijgt welke zaken en waarom? (blauw, recherche basisteam, recherche regio/district, recherche eenheid, cybercrimeteam?)

Onderzoek door blauw

- In hoeverre wordt 'blauw' belast met het afhandelen van aangiften? Welk type aangiften? (VVC, HIC, cyber, 9-uurs zaken et cetera)?
- In hoeverre is er een dossiermanager en wat is diens taak? (volgens documentenanalyse: beheerder van alle onderzoeksdossiers, prioriteert zaken en zet ze uit, bewaakt voortgang)
- In hoeverre wordt bij de toedeling van zaken aan blauw onderscheid rekening gehouden met type zaak (traditioneel / gedigitaliseerde criminaliteit / cybercrime)?
- Welke afdoeningsmogelijkheden zijn er binnen blauw (vroegtijdig beëindigen, afronden)?
    - Wat zijn redenen voor vroegtijdige beëindiging?
- In hoeverre is bij digitale criminaliteit sprake van een kennistekort? Waarin schiet men tekort?
- Over welke kennis en vaardigheden moet blauw beschikken 'inzake digitale aspecten van politiewerk'? Wat zijn de basisvereisten, wat is gewenst?

Onderzoek door recherche

- Welke rechercheafdelingen kunnen worden onderscheiden?
    - Basis, regio, eenheidsniveau
    - Zeden, cyber, FinEc?
- In hoeverre is er een dossier manager? Per afdeling, of recherche-breed? En wat is diens taak? (volgens documentenanalyse: beheerder van alle onderzoeksdossiers, prioriteert zaken en zet ze uit, bewaakt voortgang)
- Welke afdeling behandelt welk type zaken? In hoeverre wordt rekening gehouden met type zaken (traditioneel, gedigitaliseerd, cyber) per afdeling?
- Welke afdoeningsmogelijkheden zijn er binnen de recherche (vroegtijdig beëindigen, afronden)?
    - Wat zijn redenen voor vroegtijdige beëindiging?
- In hoeverre is bij digitale criminaliteit sprake van een kennistekort binnen de rechercheafdelingen? Bestaat verschil naar afdeling? En waarin schiet men tekort?
- Over welke (basis)kennis en vaardigheden moet de recherche beschikken 'inzake digitale aspecten van politiewerk'? Wat zijn de basisvereisten, wat is gewenst?

Bijlage III-a: Interviewprotocol intake en service

INTRODUCTIE
Onderzoeker bij onderzoeksgroep Cybersafety. Onderzoek naar digitalisering van samenleving en de gevolgen daarvan voor veiligheid en rechtshandhaving.

Toelichting Level-Up!
Inzicht bieden in het kennisniveau van politiemedewerkers 'inzake digitale aspecten van politiewerk'. Daarmee worden cybercrime, gedigitaliseerde criminaliteit en criminaliteit met een digitale component (het gebruik van digitale sporen) bedoeld. 3 stappen:

- Vaststellen over welke kennis en vaardigheden politiemensen moeten beschikken om effectief uitvoering te geven aan politiewerk in een gedigitaliseerde samenleving
- Vaststellen over welke kennis en vaardigheden politiemensen daadwerkelijk beschikken
- Meten waar een eventueel kennistekort zich voordoet en wat dat kennistekort inhoudt

Het onderzoek leidt uiteindelijk tot een advies over het reduceren van het kennistekort inzake digitale aspecten van politiewerk. PIAC is opdrachtgever.

Het interview
Doel is het kennisniveau te meten onder vijf functiegroepen: intake en service, blauw en de drie rechercheniveaus (basis, regio, eenheid). Het is daarom essentieel om vast te stellen over welke kennis en vaardigheden politiemensen moeten beschikken om effectief uitvoering te geven aan politiewerk in een gedigitaliseerde samenleving. Daarover gaat het interview.

Opmerkingen vooraf
Gedurende het interview worden vragen gesteld over digitale criminaliteit. Daaronder worden cybercrime, gedigitaliseerde criminaliteit en criminaliteit met een digitale component verstaan.
-Alle input wordt anoniem verwerkt in het onderzoeksrapport
-Verslag wordt ter verificatie voorgelegd
-Toestemming tot opname?

VRAGEN

Klassiek versus digitaal politiewerk

- In hoeverre zijn voor het behandelen van 'digitale criminaliteit' dezelfde kennis en vaardigheden nodig als voor het behandelen van klassieke delicten voor intake medewerkers? (procentuele inschatting)

Algemeen
Op basis van literatuuronderzoek is beschreven over welke kennis en vaardigheden medewerkers in het intakeproces moeten beschikken.

- In hoeverre is de toegezonden kennisnorm voor intake volledig? Welke kennis en vaardigheden ontbreken in de concept-kennisnorm? Dadelijk lopen we de individuele competenties nog even langs.

Digitale kennis en vaardigheden
<u>Indien bij vorige vragen niet wordt ingegaan op digitaal</u>

Gezien de focus van ons onderzoek, zijn we met name geïnteresseerd in kennis en vaardigheden die noodzakelijk zijn voor intake bij digitale criminaliteit.

- In hoeverre ontbreken kennis en vaardigheden die noodzakelijk zijn voor het behandelen van digitale criminaliteit in de concept-kennisnorm?

KENNIS EN VAARDIGHEDEN VOOR MEDEWERKERS IN HET INTAKEPROCES
De concept-kennisnorm voor medewerkers in het intakeproces is grotendeels gebaseerd op:

- Leukfeldt, Kentgens, Prins en Stol (2015) *Alledaags politiewerk in een gedigitaliseerde wereld. Handreiking voor de intake van delicten met een digitale component.* Leeuwarden: Lectoraat Cybersafety.
- De webapp cybercrime van de politieacademie (https://webapps.politieacademie.nl/cybercrime).

Competentie	Indicatoren
Kennisnemen van informatie tijdens eerste politiecontact en het op basis daarvan bepalen van een vervolgactie	Kennisnemen van (potentieel) werkaanbod
	Bepalen van vervolgactie. Volgens de webapp cybercrime zijn daarvoor de volgende mogelijkheden 1. Grote impact en hoog (potentieel) afbreukrisico = direct inschakelen relevant rechercheonderdeel. In geval van cybercrime: cybercrimeteam 2. Geringe impact + heterdaadmogelijkheid = direct inschakelen relevant rechercheonderdeel. In geval van cybercrime: cybercrimeteam. Er wordt dan door de recherche een besluite genomen over het al dan niet overgaan tot 'first response' 3. Geringe impact + geen heterdaad = opnemen aangifte, melding en/of adviseer de burger
Volledig:	- **Ja / Nee**
Verdiepingsvragen:	- **Geen**

Kennen en kunnen toepassen van de standaardprocedure voor het opnemen van aangifte	De standaardprocedure kent volgens de handreiking voor de intake van delicten met een digitale component de volgende stappen: 2. Geef de aangever de ruimte te vertellen wat er is gebeurd 3. Bepaal of je een aangifte opneemt 4. Bepaal of het nodig is een expert in te schakelen om de aangifte op te nemen 5. Beschrijf de situatie 6. Noteer de gegevens van de aangever en het delict (gespecificeerd in verschillende bullets, zoals, datum en tijd, persoonsgegevens, plaats waar het feit is gepleegd, en zo voort) 7. Bepaal om welk delict het gaat 8. Bepaal welke wetsartikelen van toepassing zijn 9. Beschrijf de werkwijze van de verdachte(n) 10. Laat de aangever zo veel mogelijk bewijsmiddelen vastleggen. Specifiek digitaal bewijsmateriaal om naar te vragen: 11. Analyseer de informatie 12. Formaliseer de aangifte
Volledig:	- **Ja / Nee**
Verdiepingsvragen:	- **In hoeverre bestaat er verschil tussen de standaardprocedure voor intake en de intakeprocedure bij digitale criminaliteit?**

Weten wat (cyber)criminaliteit is (vigerende definities)	Onderscheid kennen tussen cybercrime, gedigitaliseerde criminaliteit en criminaliteit met een digitale component o Cybercrime: ICT is zowel doel als middel o Gedigitaliseerde criminaliteit: ICT is middel o Criminaliteit met een digitale component
Volledig:	- **Ja / Nee**
Verdiepingsvragen:	- **In hoeverre is het voor medewerkers intake en service noodzakelijk om vigerende definities van criminaliteit met een digitale component / gedigitaliseerde criminaliteit / cybercrime te kennen?**

Verschijningsvormen van cybercriminaliteit kennen en kunnen herkennen op basis van praktijksignalen	Er wordt onderscheid gemaakt naar 4 hoofdcategorieën • Hacken en andere criminaliteit gericht op computers • Internetfraude en andere criminaliteit met een financieel oogmerk • Bedreiging en andere vormen van persoonsgerichte criminaliteit • Kinderpornografie en andere zedendelicten
Volledig:	- **Ja / Nee**
Verdiepingsvragen:	- **Medewerkers intake en service moeten volgens de kennisnorm in staat zijn om digitale criminaliteit te herkennen op basis van 'praktijksignalen'. In het onderzoek moeten we uiteindelijk**

	toetsen in hoeverre zij daartoe in staat zijn. Het voert echter te ver om alle praktijksignalen uit te vragen. Welke praktijksignalen voor cyberdelicten moeten medewerkers intake en service in ieder geval herkennen? (bijv.: inloggegevens opgestuurd via e-mail, kan niet inloggen, valse e-mail ontvangen, gegevens zijn verwijderd, bedreigd via e-mail). Noem maximaal 5.

De strafbaarstelling van cyberdelicten kennen en/of kunnen vaststellen	Hacken en andere criminaliteit gericht op computers o Hacken (138ab Sr) o Gegevensdiefstal (data, foto's, e-mail, enz.) (138ab en 139c Sr) o Stoornis veroorzaken (138b, 161sexies en 161septies Sr) o Gegevens vernielen (350a en 350b Sr) o Defacing (350a en 350b Sr) o Malware (139d en 161sexies Sr)
	Internetfraude en andere criminaliteit met een financieel oogmerk o Identiteitsmisbruik (231b,326, 225 en 232 Sr) o Phishing (326 en 225 Sr) o Skimming (232 Sr) o Fraude via veiling- en verkoopsites (326 en 225 Sr o Voorschotfraude (326 Sr) o Diefstal (310 Sr) o Heling van computergegevens (139e Sr) o Afpersing of chantage (317, 318 en 285 Sr) o Spam (11.7 Tw)
	Bedreiging en andere vormen van persoonsgerichte criminaliteit o Stalking of belaging (285b Sr) o Smaad of laster (261, 262 en 268 Sr) o Belediging (266 en 271 Sr) o Discriminatie (137c-137g en 429quater Sr) o Bedreiging (285 Sr) o Cyberpesten (in eerste aanleg niet strafbaar) o Zonder toestemming verspreiden van teksten via internet (Aw) o Zonder toestemming verspreiden van foto's via internet (19-21 en 35 Aw)
	Kinderpornografie en andere zedendelicten o Kinderpornografie (240b Sr en 246 Sr) o Grooming (248e Sr)
Volledig:	- **Ja / Nee**
Verdiepingsvragen:	- **In hoeverre moeten medewerkers intake en service de strafbaarstelling van cyberdelicten kennen? Volstaat het als medewerkers intake en service met behulp van bijvoorbeeld handreikingen kunnen bepalen om welk delict of om welke delicten het gaat? Waar ligt de grens: van welke delicten moeten zij de strafbaarstelling in ieder geval uit hun hoofd kennen?**

Weten dat er verbanden bestaan tussen cyberdelicten en die verbanden toetsen tijdens het opnemen van de aangifte	Het voert te ver om alle mogelijke verbanden uit te werken. Het is ook niet van belang alle verbanden te kennen. Wel is van belang om te toetsen of het delict waarvan aangifte wordt gedaan mogelijk verband houdt met andere delicten. Hacken is een basisdelict dat bijvoorbeeld verband kan houden met gegevensdiefstal of afpersing.
Verdiepingsvragen:	- **Medewerkers intake en service moeten volgens de kennisnorm in staat zijn om verbanden tussen digitale criminaliteitsvormen te toetsen. In het onderzoek moeten we uiteindelijk toetsen in hoeverre zij daartoe in staat zijn. Het voert echter te ver om alle verbanden uit te vragen. Welke verbanden tussen cyberdelicten moeten medewerkers intake en service in ieder geval kennen en kunnen toetsen? (bijv. hacken en gegevensdiefstal, afpersing). Noem maximaal 5.**

Kennen van opsporingsrelevante digitale sporen	Relevante digitale sporen (volgens handreiking en webapp): o IP-adres verdachte o E-mailadres, e-mailbericht en e-mailheader o Gebruikersnaam verdachte o Internetadres (domeinnaam) o Telefoonnummer o Advertentienummer(s) o Afbeeldingen o (Chat)logfiles o Unieke gegevens van goederen (serienummer) o Betaalgegevens (rekeningnummers, afschriften, kwitanties, creditcard-, contactgegevens) o Gebruikte valuta, betaalmiddel/-wijze; o Cryptovaluta; bijv. bitcoinadressen (wallets) o Moneygram / Western Union registratienummers
Volledig:	- **Ja / Nee**
Verdiepingsvragen:	- **Geen**

Kunnen adviseren over het veiligstellen van digitale sporen	De medewerker intake en service hoeft zelf niet exact te weten hoe digitale sporen moeten worden veiliggesteld, maar hij moet de aangever kunnen verwijzen naar hulpmiddelen om dat zelf te doen: o Kennen van de webapp cybercrime van de PA o Kennen van internetsporen.nl
	Aanleveren van digitale sporen kan digitaal, (bijv. cd/usb), met print screens, prints op papier of foto's
Verdiepingsvragen:	- **In hoeverre moeten medewerkers intake en service zelf, met het oog op advisering aan burgers, weten hoe digitale sporen kunnen worden veiliggesteld? Volstaat het als zij daarover kunnen adviseren op basis van hulpmiddelen? Waar ligt de grens: van welke digitale sporen moeten medewerkers intake en service in ieder geval weten hoe ze veilig kunnen worden gesteld?**

Het kunnen adviseren van de aangever over preventie en/of vervolgstappen	Delict-specifiek en dus voert het te ver om alle adviezen hieruit te werken. In algemene zin worden in de webapp cybercrime van de politieacademie preventietips beschreven. In de handreiking voor de intake van delicten met een digitale component zijn delict-specifieke adviezen beschreven o Kennen van de webapp cybercrime van de PA o Kennen van de handreiking voor de intake van delicten met een digitale component
Verdiepingsvragen:	- **In hoeverre moeten medewerkers intake en service zelf, met het oog op advisering aan burgers, weten hoe aangevers te adviseren over preventie? Volstaat het als zij daarover kunnen adviseren op basis van hulpmiddelen? Waar ligt de grens: wat moeten medewerkers intake en service in ieder geval weten?**

Kennen en gebruikmaken van voor 'cyber' intake ontwikkelde handreikingen	o Kennen en gebruiken van de webapp cybercrime van de PA o Kennen en gebruiken van de handreiking voor de intake van delicten met een digitale component
Verdiepingsvragen:	- **Geen**

Hoewel niet opgenomen in het overzicht; in hoeverre vindt u dat medewerkers intake en service ook in staat moeten zijn tot informatievergaring op internet (bijv. om de aangifte te verrijken)? Over welke kennis en vaardigheden moeten zij daartoe beschikken?

Hebt u tot slot nog een opmerking of gedachte in relatie tot de kennisnorm die u met ons wilt delen?
Bedankt voor uw tijd. Wij zijn aan het einde gekomen van het interview.

Bijlage III-b: Interviewprotocol politiemensen in uniformdienst (blauw)

INTRODUCTIE
Zie bijlage III-a.

VRAGEN

Klassiek versus digitaal politiewerk

- In hoeverre zijn voor het behandelen van 'digitale criminaliteit' dezelfde kennis en vaardigheden nodig als voor het behandelen van klassieke delicten voor intake medewerkers? (procentuele inschatting)

Algemeen
Wie kunnen er worden belast met het optreden op de plaats delict? Zijn dat, naast de FO, zowel blauw als recherchemedewerkers van basis-/districts-/eenheidsniveau?
Op basis van literatuuronderzoek is beschreven over welke kennis en vaardigheden medewerkers die belast zijn met het optreden op de plaats delict moeten beschikken.

- In hoeverre is de toegezonden kennisnorm voor PD volledig? / Welke kennis en vaardigheden ontbreken in de concept-kennisnorm? Dadelijk lopen we de individuele competenties nog even langs.

Digitale kennis en vaardigheden
<u>Indien bij vorige vragen niet wordt ingegaan op digitaal</u>

Gezien de focus van ons onderzoek, zijn we met name geïnteresseerd in kennis en vaardigheden die noodzakelijk zijn voor optreden 'digitale' PD.

- In hoeverre ontbreken kennis en vaardigheden die noodzakelijk zijn voor het optreden op een digitale PD?

KENNIS EN VAARDIGHEDEN VOOR HET OPTREDEN OP DE PLAATS DELICT
De concept-kennisnorm voor het optreden op de PD is grotendeels gebaseerd op:

- Van Amelsvoort en Groenendaal (2017) *Handleiding optreden plaats delict.* Sdu Uitgevers
- Zuurveen, Doodeman, Veenstra & Stol (2015) Herkennen en veiligstellen van digitale apparatuur. Leeuwarden: Lectoraat Cybersafety

Graag loop ik de kennisnorm per competentie met u na. Wil u het aangeven als:

- De uitwerking van een competentie (indicatoren) onvolledig is;
- Er volgens u verschil bestaat tussen de kennis en vaardigheden die per functieniveau (basis, district, eenheid) noodzakelijk zijn.

Competentie	**Indicatoren**
Kennen van de fasen in het optreden op de PD	Volgens de handleiding optreden plaats delict ○ Fase 1: voorafgaand aan het bezoek aan de PD zoveel mogelijk informatie vergaren over de PD ○ Fase 2: het nemen van de eerste maatregelen, gericht op het beschermen van sporen op de PD ○ Fase 3: het eventueel verrichten van onderzoek op en rondom de PD
Volledig	Ja / Nee
Verdiepingsvragen	Nee

Kennen van het juridisch kader voor het optreden op de PD	Het verrichten van onderzoek op de PD valt onder artikel 3, algemene politietaak
	Hoewel het optreden op de PD mag op basis van artikel 3 Pw, kan het tijdens het optreden op de PD nodig zijn om kennis te hebben van verschillende mogelijk inzetbare bevoegdheden: • Hulpverlening (art. 3 & 7 Pw) • 'Bevriezen' PD (art. 96, lid 2 Sv • Inbeslagname (art. 96, lid 1 Sv bij heterdaad voor misdrijf als omschreven in art. 67 Sv). Geldt alleen voor wat 'met het blote

	oog' zichtbaar is. 'Zoeken' naar in beslag te nemen sporendragers mag niet, daarvoor is toestemming OvJ nodig. • Bij PD van 'geheimhouder' (art. 110 Sv), toestemming Rechter-Commissaris (RC) noodzakelijk • Schouwen (art. 151 Sv – met toestemming (H)OvJ - / 192 Sv – met toestemming RC): 'het in ogenschouw nemen van de plaatselijke toestand of enig voorwerp. Het zoeken naar sporen en sporendragers met het doel deze in beslag te nemen valt niet onder de schouw' (p.31) • Aanhouden: 'Wanneer een verdachte (art. 27 Sv) zich op de PD bevindt of zich nog kan bevinden, dan mag je die plaats betreden om hem aan te houden (art. 55 Sv) • Bij PD in woning is ook de Algemene Wet op het Binnentreden (art. 2) van toepassing • Bevoegdheden voor 'onderzoeken van verdachte' en 'inbeslagname van voorwerpen van verdachte' zijn opgenomen in art. 56 en 95 Sv. • In beslag te nemen voorwerpen zijn bij niet verdachten te vorderen op basis van art 96a Sv. (bij heterdaad of misdrijf als omschreven in 67 Sv) Niet voldoen aan de vordering is strafbaar. • Ordemaatregelen (art. 124 en 125 Sv)
Volledig	Ja / Nee
Verdiepingsvragen	In hoeverre moeten politiemedewerkers de bevoegdheden die relevant (kunnen) zijn voor optreden op de plaats delict uit hun hoofd kennen? - Bestaat daarin verschil per functie (basispolitiezorg, basisteamrecherche, districtsrecherche, eenheidsrecherche)? Wat is het verschil?

Het kennen en kunnen uitvoeren van de eerste maatregelen	Ter plaatse gaan • Goed geïnformeerd zijn over wat op de PD kan worden aangetroffen • Aanrijden naar de PD met rechercheogen en -oren: letten op verdachte personen en/of voertuigen en vastleggen / doorgeven relevante informatie • Schakel eigen wifi en bluetoothverbindingen uit • 'Stil' benaderen van de PD, om vluchtgedrag te voorkomen
	Oriënteren op de PD-situatie • Oriënteer ter plaatse de PD van enige afstand. Voorkom 'besmetting' van het gehele gebied waar het feit is gepleegd en/of sporen zijn achtergelaten (kleiner maken PD is makkelijker dan groter maken, zonder dat sporen verloren gaan) • Herkennen van sporen(dragers)
	Primaire taken op de PD (beschermen) • Informeren OC (zodat juiste inzet van mensen en middelen kan volgen) • Bevriezen situatie (zorg dat de toestand op de PD blijft zoals hij is). • Noodgedwongen handelingen verrichten In principe wordt de PD niet betreden door de first responder, in verband met risico op het vernietigen, beschadigen of besmetten van sporen. Echter, de PD kan worden betreden als maatregelen moeten worden getroffen 'die absoluut geen uitstel dulden' (p.46): o Hulpverlening slachtoffer o Beëindigen gevaarlijke situatie o Aanhouden van nog aanwezige verdachte o Verwijderen van publiek o Beschermen van belangrijke fysieke en digitale sporen die anders verloren gaan

	Stelregels bij noodgedwongen eerste handelingen: o Gebruik onderzoekshandschoenen o Baken het 'voorlopige looppad' af o Verplaats geen voorwerpen
Volledig	Ja / Nee
Verdiepingsvragen	In hoeverre bestaat per functie verschil tussen de noodzakelijke kennis en vaardigheden bij het treffen van de eerste maatregelen (ter plaatse gaan en beschermen PD)?

Het verrichten van onderzoek op de PD	Werkproces voor onderzoek op de PD: • Oriënteren en opstellen van hypotheses en scenario's • Voorbereiden van het onderzoek op de PD o Prioriteit bepalen o Volgordelijkheid van werkzaamheden bepalen o Onderzoeksmethodologie bepalen o Externe hulp overwegen / inschakelen Uitvoeren PD-onderzoek: toetsen en waar nodig bijstellen hypotheses o Verdeel de PD in segmenten en werk van buiten naar binnen en van beneden naar boven o Gebruik een goede lichtbron (scheer- en frontaal licht) o Stel een sporenbeeld vast (wat is er gebeurd en hoe): o Gebruik situatiesporen (sporen die duiden op activiteiten, zoals MO); o Vergaar informatie over het gebruik van middelen (wapen, muts et cetera) o Vergaar informatie over 'daderkenmerken' (snoepen, eten, drinken, urine) o Vergaar informatie over motieven
	Afronden PD-onderzoek • Vastleggen resultaten in proces-verbaal. Daarin staat beschreven: o Bevindingen over de toedracht van het delict o De onderzoekshandelingen die zijn verricht o De aangetroffen en veiliggestelde sporen
Volledig	Ja / Nee
Verdiepingsvragen	Op een PD waar de FO vanwege beleidskeuzes of capaciteitsgebrek geen onderzoek verricht, is het onderzoek op de PD de taak en verantwoordelijkheid van de opsporingsambtenaar die het onderzoek uitvoert. In hoeverre bestaat per functie verschil tussen de noodzakelijke kennis en vaardigheden bij het verrichten van onderzoek op de PD? En rondom de PD?

Ken specifieke basisstappen in het geval van een PD met digitale sporen	• Ga zelf bij elke handeling na of je daartoe bevoegd bent. Bij twijfel: raadpleeg een deskundige. • Zet de wifi en bluetooth op de gegevensdragers die je zelf bij je draagt (zoals een smartphone) uit. Wanneer je een wifi-hotspot hebt ingeschakeld, schakel deze uit. • Maak, voordat je iets aanraakt, enkele overzichtsfoto's van de situatie waarin je de gegevensdrager(s) aantreft. • Houd rekening mee dat alles wat je zegt en doet via de aanwezige digitale apparatuur kan worden opgenomen en afgeluisterd. Zijn er gegevensdragers met daarin een cameralens of is er een webcam? Plak voor je eigen veiligheid en die van je collega's de lens af (je kan uiteraard nog steeds worden afgeluisterd). • Wanneer anderen dan politie-specialisten willen helpen met het veiligstellen van gegevensdragers of anderszins technische bijstand willen verlenen: weiger dit.

	• Noteer wie zich op welke plaats bevond toen je op de PD arriveerde. Zorg ervoor dat personen op de PD geen digitale gegevensdragers gebruiken en dat ze niets aanraken. Houd hen uit de buurt van elektriciteit leverende apparatuur (zoals generatoren en accu's), meterkasten en (elektriciteits)kabels. Vraag naar hun identiteitsbewijs. • Als je statisch geladen bent kan dat de gegevensdragers die je aanraakt beschadigen. Raak daarom eerst met je blote handen een geaard voorwerp aan (bijv. een kraan, een kale water- of cv-leiding). • Digitale gegevensdragers kunnen onzichtbare fysieke sporen bevatten (vingerafdrukken, DNA). Doe daarom de handschoenen aan die speciaal voor dit doel in je uitrusting zitten.
Volledig	Ja / Nee
Verdiepingsvragen	In hoeverre moeten politiemedewerkers *de basisstappen voor het optreden op een PD met digitale sporen* uit hun hoofd kennen (check bevoegdheid, zet wifi en bluetooth uit, wees alert op afluisteren, maak foto's et cetera)? - Volstaat het als zij de app 'digitale PD' kennen en kunnen gebruiken? - In hoeverre bestaat per functie verschil in de benodigde kennis van de basisstappen?

Het kunnen herkennen van relevante digitale gegevensdragers op een digitaal PD	Computers o Desktop o Laptop o Server o Mediabox en hd/dvd-recorder o Gameconsole o Tablet en E-reader Mobiele telefoons o Gsm-telefoon o Smartphone Opslagapparatuur/datadragers o Externe harde schijf/NAS o Tapedrive o Diskette, cd-rom of dvd o Geheugenkaart o USB-stick LAN-verbindingsapparatuur o Modem en router o LAN, Switch en PowerPlug o GSM-Alarm Overige gegevensdragers o Digitale foto- en videocamera o Digitale fotolijst o Muziekspeler o Draagbare navigatieapparatuur o Automotive systems o Printer, scanner, kopieer- en faxapparaten Nieuwe gegevensdragers o Smartwatch o NFC-ringen o Chromecast Dongel o Google Glass o Mouse Jiggler Randapparatuur o Muist, toetsenbord, webcam en beeldscherm/monitor o Docking station o Externe diskette-, cd- of dvd-speler Kunnen omgaan met onbekende gegevensdragers (specialist inschakelen)

Volledig	Ja / Nee
Verdiepingsvragen	In hoeverre is het overzicht van (meest voorkomende) gegevensdragers die politiemedewerkers moeten kunnen herkennen actueel?

Het op forensisch technisch verantwoorde wijze kunnen veiligstellen van relevante digitale gegevensdragers	Kennen van de basisprocedure voor het veiligstellen van digitale gegevensdragers o Stel vast welk(e) device(s) op de PD aanwezig zijn. o Stel de volgorde van veiligstellen vast (in verband met op afstand wissen / belang van sporen) o Stel de status van de gegevensdrager vast (aan / uit, wel of niet beveiligd et cetera) o Stel de gegevensdragers - op volgorde van prioriteit en afhankelijk van status – veilig o Schakel waar nodig hulp van een digitaal expert in
	De wijze waarop gegevensdragers moeten worden vastgesteld is gegevensdrager specifiek. Het voert daarom te ver voor niet specialisten om te weten hoe iedere gegevensdrager dient te worden veiliggesteld. Om die reden is de webapp digitale PD beschikbaar voor politiemensen. Politiemensen moeten dus: o Weten van het bestaan van de webapp o De webapp kunnen gebruiken te vragen
Volledig	Ja / Nee
Verdiepingsvragen	De procedure voor het veiligstellen van gegevensdragers verschilt per gegevensdrager. In hoeverre moeten politiemedewerkers uit hun hoofd weten hoe verschillende gegevensdragers op forensisch technische wijze kunnen worden veiliggesteld? - Volstaat het als zij de app ‘digitale PD’ kennen en kunnen gebruiken? - In hoeverre bestaat per functie verschil in de benodigde kennis over het veiligstellen van gegevensdragers?

Het verrichten van onderzoek rondom de PD	Omgevingsonderzoek kent verschillende mogelijkheden: • Omgevingsonderzoek naar verdachte • Omgevingsonderzoek naar voorwerpen • Omgevingsonderzoek naar camerabeelden • Omgevingsonderzoek naar financiële sporen • Omgevingsonderzoek naar ontvangstapparatuur van wifi- en bluetoothapparaten • Verhoor getuigen • Verhoor aangever/melder • Buurtonderzoek • Vraag verkeersgegevens telecommunicatie op • Registreer gegevens van personen en voortuigen die zich in de onmiddellijke omgeving van de PD bevinden.
Volledig	Ja / Nee
Verdiepingsvragen	Een van de competenties voor het optreden plaats delict is het kunnen verrichten van omgevingsonderzoek. Welke kennis en vaardigheden zijn essentieel voor omgevingsonderzoek bij ‘digitale criminaliteit’?

Hebt u tot slot nog een opmerking of gedachte in relatie tot de kennisnorm die u met ons wilt delen?
Bedankt voor uw tijd. Wij zijn aan het einde gekomen van het interview.

Bijlage III-c: Interviewprotocol rechercheurs

INTRODUCTIE
Zie bijlage III-a.

VRAGEN

Klassiek versus digitaal politiewerk

- In hoeverre zijn voor het behandelen van 'digitale criminaliteit' dezelfde kennis en vaardigheden nodig als voor het behandelen van klassieke delicten voor intake medewerkers? (procentuele inschatting)

Algemeen
Op basis van literatuuronderzoek is beschreven over welke kennis en vaardigheden medewerkers in het opsporingsproces moeten beschikken.

- In hoeverre is de toegezonden kennisnorm voor opsporing volledig? / Welke kennis en vaardigheden ontbreken in de concept-kennisnorm? Dadelijk lopen we de individuele competenties nog even langs.

Digitale kennis en vaardigheden
Indien bij vorige vragen niet wordt ingegaan op digitaal

Gezien de focus van ons onderzoek, zijn we met name geïnteresseerd in kennis en vaardigheden die noodzakelijk zijn voor intake bij digitale criminaliteit.

- In hoeverre ontbreken kennis en vaardigheden die noodzakelijk zijn voor het behandelen van digitale criminaliteit in de concept-kennisnorm?

KENNIS EN VAARDIGHEDEN VOOR OPSPORING IN EEN GEDIGITALISEERDE SAMENLEVING
De concept-kennisnorm is gebaseerd op algemene (inter)nationale literatuur over het verrichten van opsporingsonderzoek. Voor de beschrijving van specifieke 'digitale' kennis en vaardigheden is geput uit:

- Van Valkengoed (2017). *Competentieonderzoek Cybercrimeopsporing.* Amsterdam: TDO
- Veenstra, Zuurveen, Kerstens & Stol (2016) *Opsporing in een gedigitaliseerde samenleving: Een handreiking voor het herkennen, vinden en benutten van digitale sporen.* Leeuwarden: Lectoraat Cybersafety
- Kennis- en Expertisecentrum Cybercrime (2014). Vademecum Interceptie: Voor de opsporing en de rechterlijke macht. Rotterdam: Landelijk Parket Openbaar Ministerie (vertrouwelijk).

Graag loop ik de kennisnorm per competentie met u na. Wil u het aangeven als:

- De uitwerking van een competentie (indicatoren) onvolledig is;
- Er volgens u verschil bestaat tussen de kennis en vaardigheden die per functieniveau (basis, district, eenheid) noodzakelijk zijn.

COMPETENTIE	**INDICATOREN**
Weten wat (cyber)criminaliteit is (vigerende definities)	Onderscheid kennen tussen cybercrime, gedigitaliseerde criminaliteit en criminaliteit met een digitale component o Cybercrime: ICT is zowel doel als middel o Gedigitaliseerde criminaliteit: ICT is middel o Criminaliteit met een digitale component
Volledig	Ja / Nee
Verdiepingsvragen	In hoeverre is het voor rechercheurs noodzakelijk om vigerende definities van criminaliteit met een digitale component / gedigitaliseerde criminaliteit / cybercrime te kennen?

Kennis van het strafrecht **Kunnen vaststellen of sprake is van een misdrijf**	Specifiek op het gebied van cybercrime en gedigitaliseerde criminaliteit gaat het over: Hacken en andere criminaliteit gericht op computers o Hacken (138ab Sr) o Gegevensdiefstal (data, foto's, e-mail, enz.) (138ab en 139c Sr)

	○ Stoornis veroorzaken (138b, 161sexies en 161septies Sr) ○ Gegevens vernielen (350a en 350b Sr) ○ Defacing (350a en 350b Sr) ○ Malware (139d en 161sexies Sr) Internetfraude en andere criminaliteit met een financieel oogmerk ○ Identiteitsmisbruik (231b,326, 225 en 232 Sr) ○ Phishing (326 en 225 Sr) ○ Skimming (232 Sr) ○ Fraude via veiling- en verkoopsites (326 en 225 Sr ○ Voorschotfraude (326 Sr) ○ Diefstal (310 Sr) ○ Heling van computergegevens (139e Sr) ○ Afpersing of chantage (317, 318 en 285 Sr) ○ Spam (11.7 Tw) Bedreiging en andere vormen van persoonsgerichte criminaliteit ○ Stalking of belaging (285b Sr) ○ Smaad of laster (261, 262 en 268 Sr) ○ Belediging (266 en 271 Sr) ○ Discriminatie (137c-137g en 429quater Sr) ○ Bedreiging (285 Sr) ○ Cyberpesten (in eerste aanleg niet strafbaar) ○ Zonder toestemming verspreiden van teksten via internet (Aw) ○ Zonder toestemming verspreiden van foto's via internet (19-21 en 35 Aw) Kinderpornografie en andere zedendelicten ○ Kinderpornografie (240b Sr en 246 Sr) ○ Grooming (248e Sr)
Volledig	Ja / Nee
Verdiepingsvragen	In hoeverre moeten rechercheurs de strafbaarstelling van cyberdelicten kennen? - Volstaat het als rechercheurs met behulp van bijvoorbeeld handreikingen kunnen bepalen om welk delict of om welke delicten het gaat? - Waar ligt de grens: van welke delicten moeten zij de strafbaarstelling in ieder geval uit hun hoofd kennen? - In hoeverre bestaat per functie (basis / district / eenheid) verschil in de noodzakelijke kennis over de strafbaarstelling van cyberdelicten?

Kunnen optreden op en rondom een (digitaal) Plaats Delict	Zie kennisnorm PD – niet relevant in opsporingsinterviews

Het kunnen beoordelen van informatie uit het intakeproces op bruikbaarheid	○ Aanwijzingen voor de opsporing kunnen filteren uit de informatie die tijdens het opnemen van de aangifte, op de plaats delict of op basis van intelligence is aangedragen aan het opsporingsteam ○ De waarde van de aanwijzingen voor de opsporing kunnen beoordelen ○ Het nemen van een besluit: wel óf geen opsporingsonderzoek starten
Volledig	Ja / Nee
Verdiepingsvragen	NVT.

Het maken van een Plan Van Aanpak (PVA) voor het te	Het systematisch plannen / inrichten van onderzoek (volgen van empirische cyclus)

verrichten onderzoek	o Stap 1: inventariseer startinformatie o Stap 2: formuleer opsporingsvragen (zeven gouden W's) o Stap 3: bepaal de onderzoeksmethoden o Stap 4: maak een planning
	Met het oog op het bepalen van de onderzoeksmethodologie is van belang verschillende typen zaken te kennen / te kunnen onderscheiden o Klip en klaar, waarbij iemand op heterdaad is aangehouden o Verificatie, waarbij het verhaal en de verdachte bekend is en moet worden geverifieerd o Opsporing, waarbij het verhaal bekend is, maar de verdachte moet worden opgespoord o Zoekzaken, waarbij onduidelijk is wat is voorgevallen en wie betrokken is Het type zaak bepaalt (mede) de methodologie
	Met het oog op het bepalen van de onderzoeksmethodologie is van belang om verschillende opsporingsstrategieën te kennen, zoals o Korteklapstrategie (heterdaad + bewijsvoering) o Domino- of ijsschotsstrategie (bestaande informatie als uitgangspunt, nieuwe informatie leidt tot nieuwe stappen in opsporing) o Schil- of pelstrategie (het van buiten naar binnen pellen van een CSV, om zodoende bij de leider uit te komen) o Facilitator- of bruggenbouwstrategie (gericht in kaart brengen en onderuithalen van facilitators) o Slachtofferstrategie (leven van slachtoffer in kaart brengen met het oog op opsporingsaanwijzingen) o Misdrijfgeleide strategie (het gepleegde misdrijf als uitgangspunt voor de opsporingshandelingen?) o Verdachtengeleide strategie (bewijsmateriaal verzamelen tegen verdachte(n) Het type zaak bepaalt (mede) de strategie
	Met het oog op het bepalen van de onderzoeksmethodologie is van belang om relevante opsporingsbevoegdheden (wet BOB) te kennen o observatie, infiltratie, pseudokoop, pseudodienst-verlening, stelselmatige informatie-inwinning, betreden van een besloten plaats en opnemen van vertrouwelijke communicatie met een technisch hulpmiddel; o verscheidene vormen van bijstand aan opsporing door burgers, zoals de informant, de burgerinfiltrant en de burgerpseudokoop- of dienstverlening; o de bevoegdheid van het opnemen van telecommunicatie en het vorderen van inlichtingen; o kennen van de (nieuwe) grondslag voor de toepassing van opsporingsbevoegdheden, namelijk het vermoeden dat in georganiseerd verband ernstige misdrijven worden beraamd of gepleegd; o een regeling van het verkennend onderzoek. Afhankelijk van de zaak wordt de inzet van opsporingsbevoegdheden overwogen
Volledig	Ja / Nee
Verdiepingsvragen	- Welke bevoegdheden zijn van belang voor digitale opsporing? - In hoeverre bestaat per niveau verschil in de mate waarin rechercheurs die bevoegdheden moeten kennen?

Het verrichten van opsporingsonderzoek	Neem altijd de eigen veiligheid, de veiligheid van slachtoffers, getuigen en verdachten in acht
	Vergaar informatie door gebruik te maken van verschillende bronnen.

	Volgens Stelfox (2009) kan informatie aanwezig zijn in mensen of als data/sporen in systemen (zie ook Hess Orthman en Matison Hess [2013]) Informatiebronnen in systemen o Gebruik van (reacties op) berichtgeving in de media o Gebruik van intelligence (aangiften, dossiers en databases binnen politie) o Informatievergaring op internet o Vorderen van gegevens o Interceptie telecomgegevens o Doorzoeking en inbeslagname bewijsmateriaal Informatie van mensen o Horen van slachtoffers, getuigen, melders o Buurtonderzoek o Betreden/doorzoeken van (besloten) plaats o Gebruik van (geheime) informanten / inlichtingen o Observatie (menselijk / technisch – bijv. CCTV) o Stelselmatige informatie-inwinning o Infiltratie o Gebruik van compositietekeningen, uitvoeren van confrontaties o Inzet publiek bij identificatie o Onderzoek aan lichaam en kleding van verdachte(n) o Verhoren/ondervragen van verdachte(n)
	Indien nodig, vraag hulp van experts
	Het waar mogelijk lokaliseren en aanhouden van verdachte(n). Indien geen verdachte is geïdentificeerd, wordt bepaald of aanvullend onderzoek tot de mogelijkheden behoort (op basis van nieuwe inzichten.
Volledig	Ja / Nee
Verdiepingsvragen	Literatuurstudie en eerdere expertdiscussies wijzen uit dat: - Informatievergaring op internet - Benutten van sporen uit digitale gegevensdragers - Vorderen van gegevens - Interceptie Voor digitaal onderzoek het meest van belang zijn. Klopt dat?

Beschikken over specifieke opsporingskennis en –vaardigheden in een gedigitaliseerde samenleving	**Benutten van sporen uit gegevensdragers** o Weten dat het daadwerkelijk uitlezen van gegevensdragers het werk is voor experts (TDO). Hulp van experts kunnen inschakelen. o Kennen van bevoegdheden tot inbeslagname en onderzoek aan gegevensdragers o 95Sv bepaalt dat alle voorwerpen die kunnen dienen om de waarheid aan het licht te brengen vatbaar zijn voor inbeslagneming o 96 / 97 Sv regelen de bevoegdheid tot inbeslagname / doorzoeking o Houd altijd rekening met het proportionaliteits- en subsidiariteitsbeginsel o Weten hoe je digitale sporen uit gegevensdragers kunt benutten in opsporingsonderzoek - Stap 1: vaststellen welke digitale gegevensdragers beschikbaar zijn voor uitlezen; - Stap 2: inventariseer uitleesmogelijkheden: bepaal welke mogelijk relevante sporen kunnen worden uitgelezen. o Veel voorkomende gegevens die met behulp van computers, smartphones of tablets – de meest frequent veiliggestelde gegevensdragers – kunnen worden

	achterhaald: ▪ Persoonsgegevens (gebruikersgegevens, contactenlijst, gesprekkenlijst, telefoonnummer) ▪ Berichten ▪ Bestanden ▪ Beeldmateriaal ▪ Locatiegegevens ▪ Informatie voor het maken van een tijdlijn ▪ Browsergeschiedenis ▪ Overige (telefoon)gegevens (serienummers, IP-/MAC-adressen, aangestraalde verbindingen) - Stap 3: overweeg nut en noodzaak van uitlezen - Stap 4: overweeg of uitgelezen gegevens tijdig kunnen worden aangeleverd - Stap 5: stel gerichte vragen - Stap 6: ken de eisen die worden gesteld aan de uitleesaanvraag en conformeer de aanvraag daaraan o Gebruik kunnen maken van Hansken voor de analyse van digitale sporen o Kunnen analyseren/waarderen van de bevindingen o Verslag kunnen leggen van de bevindingen (zie dossiervorming) o Rapporteer zowel belastend als ontlastend materiaal
Volledig	Ja / Nee
Verdiepingsvragen	Niveauverschillen? In hoeverre moeten tactisch rechercheurs op zowel basisteam, als districts- en eenheidsniveau dit weten/kunnen?

	Informatievergaring op internet - Maak gebruik van een anonimiseringstool (iRN) - Weet welke informatie mogelijk via internet kan worden achterhaald en stel vast naar welke informatie wordt gezocht - Ken relevante gegevensbronnen en bevoegdheden o Overweeg proportionaliteit en subsidiariteit o Artikel 3 Pw volstaat als geen sprake is van een meer dan geringe privacyinbreuk o Meer dan geringe inbreuk op de privacy => stelselmatige observatie (126g Sv) o Meer dan geringe inbreuk op de privacy en actief interfereren in leven van verdachte / betrokkene => stelselmatige informatie-inwinning (126j Sv) - Ken de zoekregimes voor verschillende onlineomgevingen o Zoeken in een grote hoeveelheid ongerichte data o Zoeken in een specifieke omgeving ▪ Zonder deurbeleid ▪ Niet gehandhaafd deurbeleid • Werk uitsluitend via een nepaccount dat nooit gekoppeld is aan privé en/of werkgerelateerde contactgegevens • Houd het account zo anoniem en weinig aangekleed mogelijk • Controleer of het nepaccount niet in verband kan worden gebracht met een bestaand persoon ▪ Strikt deurbeleid => voorbehouden aan WOD - Werk gestructureerd, hanteer een zoekplan: - Stap 1: bepaal input voor de zoekslag op internet - Stap 2: bepaal bevoegdheid - Stap 3: voer de zoekslag uit en registreer hoe is gezocht en leg

	relevante resultaten vast - Analyseer en waardeer de gevonden informatie - Optimaliseer, waar nodig, de zoekstrategie - Informatie kunnen zoeken over een IP-adres - Informatie kunnen zoeken over een telefoonnummer
Volledig	Ja / Nee
Verdiepingsvragen	Niveauverschillen? In hoeverre moeten tactisch rechercheurs op zowel basisteam, als districts- en eenheidsniveau dit weten/kunnen?

	Het vorderen van gegevens - Ken mogelijk vorderbare sporen. Vorderbare sporen zijn (niet limitatief): o Persoonsgegevens o Beeldmateriaal o Gegevens over internet of telefonie ▪ Identificerende gegevens ▪ Verkeersgegevens ▪ Gegevens over de inhoud van communicatie o Financiële gegevens o Reisgegevens o Administratieve kenmerken - Werk gestructureerd: o Stap 1: maak op basis van de startinformatie in het onderzoek een overzicht van mogelijk vorderbare sporen o Stap 2: overweeg of vorderen mogelijk is (bevoegdheid) o Stap 3: overweeg nut en noodzaak van vorderen ▪ Overweeg proportionaliteit en subsidiariteit ▪ Overweeg bruikbaarheid van de te vorderen gegevens ▪ Overweeg noodzaak van vorderen voor het opsporen van de verdachte en/of bewijsvoering tegen de verdachte ▪ Overweeg tijdigheid van de te vorderen gegevens ▪ Overweeg mogelijk afbreukrisico van vorderen o Stap 4: overweeg het bevriezen van vluchtige gegevens (art. 126ni Sv) o Stap 5: ken het vorderingsregime ▪ Voor vorderen bij aanbieders van een telecommunicatienetwerk of –dienst (art. 126la, 126n, 126na en 126nb Sv) ▪ Voor vorderen bij 'eenieder' (art. 126nc, 126nd, 126ne, 126nf, 126ng en 126nh Sv) o Ken de eisen die aan een vordering worden gesteld en conformeer de vordering daaraan. ▪ Ken / gebruik de standaardformulieren in Summ-IT o Ken de afspraken die met buitenlandse aanbieders van telecommunicatienetwerken of –diensten zijn gemaakt (vrijwillige verstrekking, zonder rechtshulpverzoek) o Indien nodig, de hulp van de gemeenschappelijke BOB-kamer of de interceptiecoördinator van de eenheid in kunnen schakelen o Stap 6: Analyseer en waardeer de gevonden informatie
Volledig	Ja / Nee
Verdiepingsvragen	Niveauverschillen? In hoeverre moeten tactisch rechercheurs op zowel basisteam, als districts- en eenheidsniveau dit weten/kunnen?

	Interceptie (gebaseerd op vademecum interceptie) - Ken de bevoegdheden voor het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel o Inzet IMSI Catcher (gericht op achterhalen IMSI- & IMEI-nummer van mobiele telefoon) ter verkrijgen van tapkenmerken (art. 126m/t en of 126n/u) o Bestandsanalyse van basisstationverkeersgegevens, (gericht op het achterhalen van telefoonnummer) ter verkrijging van tapkenmerken (126na/ua lid 2 Sv) o Verkeersgegevenstap: een tap zonder de call-content (126n/u Sv). Niet bij alle aanbieders mogelijk, omdat verkeersgegevens en inhoud niet altijd zijn los te koppelen. o Locatiegegevens vorderen (art. 126ng/ug lid 1 jo art. 126nd/ud Sv) o Stille sms voor plaatsbepaling in het kader van opsporing (art. 3 Pw, mits in combinatie met een tap) o IMSI-catcher ter plaatsbepaling (art. 3 Pw, mits in combinatie met een tap) o Interceptie telefonie: actuele en toekomstige inhoud (art. 126m/t in combinatie met 126n/u Sv.) o Interceptie van overige communicatie, SMS/EMS/MMS/FAX (art. 126m/t Sv) o Interceptie IP: actuele en toekomstige inhoud (art. 126 m/t Sv jo art. 126n/u Sv) o Interceptie e-mail: actuele en toekomstige inhoud (126 m/t Sv jo art. 126n/u Sv) - Kunnen toepassen van bevoegdheden voor het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel o Kennen en kunnen toepassen van interceptiedoel specifieke aanvraagprocedures - Indien nodig, de hulp van de gemeenschappelijke BOB kamer of de interceptiecoördinator van de eenheid in kunnen schakelen
Volledig	Ja / Nee
Verdiepingsvragen	Niveauverschillen? In hoeverre moeten tactisch rechercheurs op zowel basisteam, als districts- en eenheidsniveau dit weten/kunnen?

Analyseren en duiden van onderzoeksbevindingen	Nadat (digitale) sporen zijn verzameld, is het belangrijk om de onderzoeksbevindingen te analyseren en te duiden. Het identificeren / uitsluiten van verdachte(n) staat centraal.
	Het kennen van tegenmaatregelen van internetcriminelen is van belang bij de interpretatie van de onderzoeksresultaten (niet alles is wat het lijkt, bijv. door gebruik van anonimiseringstool gespoofde IP-adressen).
	Het waar mogelijk lokaliseren en aanhouden van verdachte(n). Indien geen verdachte is geïdentificeerd, wordt bepaald of aanvullend onderzoek tot de mogelijkheden behoort (op basis van nieuwe inzichten.
Volledig	Ja / Nee
Verdiepingsvragen	NVT.

Kunnen beoordelen van waarde van bewijs: 'evidential evaluation'	Het is van belang te kunnen beoordelen of er voldoende bewijs is om over te gaan tot vervolging Bij onvoldoende bewijs wordt aanvullend onderzoek overwogen o Bij voldoende bewijs wordt het onderzoek afgerond en overgedragen aan het OM.
Volledig	Ja / Nee
Verdiepingsvragen	NVT.

Dossiervorming	• Het systematisch vastleggen van onderzoekshandelingen tijdens het

	opsporingsonderzoek • Het uiteindelijk verslagleggen en verantwoorden van de uitkomsten van het opsporingsonderzoek
Volledig	Ja / Nee
Verdiepingsvragen	NVT

Persoonlijke eigenschappen die van belang zijn voor de rechercheur	Het valt buiten het bestek van dit onderzoek om alle in de literatuur benoemde persoonlijke eigenschappen (empathisch, integer, nieuwsgierig) hierop te noemen. Wat zijn, met het oog op digitaal onderzoek, de belangrijkste eigenschappen?
Antwoord	

Overige digitale kennis en vaardigheden	- De rechercheur moet geen ´technofobia´ hebben: kennis van computers, de wil om technologie te omarmen, en algemene ICT-vaardigheden zijn belangrijk - Kennis van 'emerging digital trends' en 'digital threats' - Om kunnen gaan met grote hoeveelheden data - Kennis van internationaal recht / jurisdictie problematiek - Basiskennis over het op forensisch deugdelijke wijze veiligstellen van sporen - Dat een generalist de hulp van een digitaal expert in moet roepen om digitaal bewijs veilig te stellen en te interpreteren. Belangrijk, omdat In 'computer crime cases' de verdediging vaak de toelaatbaarheid van digitaal bewijs aanvalt. - Kennis van Engelse taal met het oog op de veelal Engelstalige computer terminologie
Volledig	Ja / Nee
Verdiepingsvragen	- Over welke overige (niet in de norm genoemde) specifieke digitale kennis en vaardigheden moeten rechercheurs beschikken?

Hebt u tot slot nog een opmerking of gedachte in relatie tot de kennisnorm die u met ons wilt delen?
Bedankt voor uw tijd. Wij zijn aan het einde gekomen van het interview.

Bijlage III-d: Interviewprotocol onlinegegevensgaring

INTRODUCTIE
Zie bijlage III-a.

Rollen bij informatievergaring op internet
- In hoeverre heeft *intake* een rol bij informatievergaring op internet? Wat is die rol?
- In hoeverre heeft *blauw* een rol bij informatievergaring bij internet? Wat is die rol?
- In de voorlopige kennisnorm alleen aandacht voor opsporing. Heeft blauw ook een rol bij online signalering en handhaving?
    - Over welke kennis en vaardigheden op het gebied van informatievergaring op internet moet een medewerker GGP in het kader van handhaving beschikken?

Kennisnorm informatievergaring op internet
Doornemen van de op basis van literatuur en documenten opgestelde concept-kennisnorm

Kennis en vaardigheden - informatievergaring op internet
- Maak gebruik van een anonimiseringstool (iRN)
- Weet welke informatie mogelijk via internet kan worden achterhaald en stel vast naar welke informatie wordt gezocht
- Ken relevante gegevensbronnen en bevoegdheden
    - Overweeg proportionaliteit en subsidiariteit
    - Artikel 3 Pw volstaat als geen sprake is van een meer dan geringe privacyinbreuk
    - Meer dan geringe inbreuk op de privacy => stelselmatige observatie (126g Sv)
    - Meer dan geringe inbreuk op de privacy en actief interfereren in leven van verdachte / betrokkene => stelselmatige informatie-inwinning (126j Sv)
- Ken de zoekregimes voor verschillende onlineomgevingen
    - Zoeken in een grote hoeveelheid ongerichte data
    - Zoeken in een specifieke omgeving
        - Zonder deurbeleid
        - Niet gehandhaafd deurbeleid
            - Werk uitsluitend via een nepaccount dat nooit gekoppeld is aan privé- en/of werkgerelateerde contactgegevens
            - Houd het account zo anoniem en weinig aangekleed mogelijk
            - Controleer of het nepaccount niet in verband kan worden gebracht met een bestaand persoon
        - Strikt deurbeleid => voorbehouden aan WOD (werken onder dekmantel)
- Werk gestructureerd, hanteer een zoekplan:
    - Stap 1: bepaal input voor de zoekslag op internet
    - Stap 2: bepaal bevoegdheid
    - Stap 3: voer de zoekslag uit en registreer hoe is gezocht en leg relevante resultaten vast
- Analyseer en waardeer de gevonden informatie
- Optimaliseer, waar nodig, de zoekstrategie
- Informatie kunnen zoeken over een IP-adres
- Informatie kunnen zoeken over een telefoonnummer

Ik heb de norm naast de opleidingsniveaus voor onlinegegevensgaring gelegd en zie veel overeenkomsten, maar ook enkele verschillen. Daar wil ik graag eerst op ingaan:

Uit de OGG blijkt dat verschil bestaat tussen eenvoudige en complexe/meervoudige zoekvragen.
- Wat is het verschil?
- Wie (basisteam-/district-/eenheidsrecherche) moet wat kunnen?

Uit de OGG blijkt dat politiemedewerkers ook moeten kunnen zoeken op deepweb
- Geldt dit voor generalisten in de tactische opsporing (basis/district/eenheid)?
- Welke kennis en vaardigheden zijn daarvoor vereist?

Uit de OGG blijkt dat politiemedewerkers gebruik moeten kunnen maken van tooling.

- Geldt dit voor generalisten in de tactische opsporing (basis/district/eenheid)?
- Welke tools en wat houdt die tooling in?
- Wie (basisteam-/district-/eenheidsrecherche) moet wat kunnen?

Uit de OGG (niveau 3) blijkt dat medewerkers dashboards moeten kunnen bouwen.

- Geldt dit voor generalisten in de tactische opsporing (basis/district/eenheid)?
- Zo ja, wat houdt dat in?

In hoeverre is de kennisnorm, met inachtneming van zojuist besproken toevoegingen, volledig?
Welke kennis en vaardigheden ontbreken?

Graag zou ik per competentie inzichtelijk maken in hoeverre verschil bestaat tussen de kennis en vaardigheden waarover politiemedewerkers van verschillende niveaus moeten beschikken. Ik zou daarvoor de volgende tabel gezamenlijk willen doorlopen:

Kennis en vaardigheden	**Blauw**	**Basisteam-recherche**	**District**	**Eenheid**
Maak gebruik van een anonimiseringstool (iRN)				
Weet welke informatie mogelijk via internet kan worden achterhaald en stel vast naar welke informatie wordt gezocht				
Ken relevante gegevensbronnen en bevoegdheden - Overweeg proportionaliteit en subsidiariteit - Artikel 3 Pw volstaat als geen sprake is van een meer dan geringe privacyinbreuk - Meer dan geringe inbreuk op de privacy => stelselmatige observatie (126g Sv) - Meer dan geringe inbreuk op de privacy en actief interfereren in leven van verdachte / betrokkene => stelselmatige informatie-inwinning (126j Sv)				
Ken de zoekregimes voor verschillende onlineomgevingen o Gebruik kunnen maken van eenvoudige zoekvragen o Gebruik kunnen maken van complexe zoekvragen o Gebruik kunnen maken van tooling o Zoeken in een grote hoeveelheid ongerichte data o Zoeken in een specifieke omgeving ▪ Zonder deurbeleid ▪ Niet gehandhaafd deurbeleid • Werk uitsluitend via een nepaccount dat nooit gekoppeld is aan privé- en/of werkgerelateerde contactgegevens • Houd het account zo anoniem en weinig aangekleed mogelijk • Controleer of het nepaccount niet in verband kan worden gebracht met een bestaand persoon ▪ Strikt deurbeleid => voorbehouden aan WOD o Informatievergaring via darkweb				

Werk gestructureerd, hanteer een zoekplan: - Stap 1: bepaal input voor de zoekslag op internet - Stap 2: bepaal bevoegdheid - Stap 3: voer de zoekslag uit en registreer hoe is gezocht en leg relevante resultaten vast				
Analyseer en waardeer de gevonden informatie - Het kunnen maken van dashboards				
Optimaliseer, waar nodig, de zoekstrategie				
Informatie kunnen zoeken over een IP-adres				
Informatie kunnen zoeken over een telefoonnummer				

Bijlage IV: Interviewprotocol verbetering kennisniveau

INTRODUCTIE
Onderzoek naar digitalisering van samenleving en de gevolgen daarvan voor veiligheid en rechtshandhaving.

Toelichting Level-Up!
Inzicht bieden in het kennisniveau van politiemedewerkers 'inzake digitale aspecten van politiewerk'. Daarmee worden cybercrime, gedigitaliseerde criminaliteit en criminaliteit met een digitale component (het gebruik van digitale sporen) bedoeld. 3 stappen:

- Vaststellen over welke kennis en vaardigheden politiemensen moeten beschikken om effectief uitvoering te geven aan politiewerk in een gedigitaliseerde samenleving
- Vaststellen over welke kennis en vaardigheden politiemensen daadwerkelijk beschikken
- Meten waar een eventueel kennistekort zich voordoet en wat dat kennistekort inhoudt

Het onderzoek leidt uiteindelijk tot een advies over het reduceren van het kennistekort inzake digitale aspecten van politiewerk. PIAC is opdrachtgever.

Het interview
Doel van dit interview is inzicht verkrijgen in hoe kennis over digitale aspecten van politiewerk bij politiemensen structureel kan worden verbeterd.

Opmerkingen vooraf
-Mag uw naam en/of de naam van uw organisatie worden gebruikt in het openbaar te verschijnen onderzoeksrapport? Zo niet, dan wordt alle input anoniem verwerkt in het onderzoeksrapport.
-De uitwerking van het interview wordt – indien gewenst – ter verificatie voorgelegd. Reageertermijn is twee weken na aanlevering. *Behalve wanneer anders wordt overeengekomen gezien aanstaande vakantieperiode. Ook kan dit moment gebruikt worden om eventuele anonimiteit te heroverwegen.
-Toestemming tot opname? De opname wordt alleen gebruikt voor uitwerkingsdoeleinden. Daarna wordt de opname vernietigd.

VRAGEN

Algemeen

1. Kunt u meer vertellen over uw functie en welke rol u hebt in relatie tot opleidingen en/of het opleiden van politiemensen (of grote groepen [vergelijkbare] professionals)?

2. Op welke wijze kan digitale kennis structureel worden verbeterd binnen de politieorganisatie (of grote groepen [vergelijkbare] professionals)? (Wellicht zijn er meer methoden denkbaar naast traditionele onderwijsvormen)

3. Op welke wijze kunnen grote groepen binnen een organisatie het beste worden opgeleid (geschoold [kennis] en getraind [vaardigheden])? (algemeen, en specifiek voor digitale aspecten; zitten daar verschillen tussen?)
    a. Welke methoden worden effectief geacht en waarom? (Beklijft de opgedane kennis? Waarvan afhankelijk? Is dat onderzocht; effectstudie?)
        i. In hoeverre kan maatwerk worden geleverd; voor verschillende groepen, niveaus, et cetera?
        ii. De politieorganisatie kan worden getypeerd als 'ervaringsorganisatie'. In hoeverre kan daarop worden ingespeeld in het aanbieden van opleidingen en/of cursussen?
    b. Op welke wijze kan voor een gezonde balans worden gezorgd tussen opleiden enerzijds en werkdruk/capaciteit in de dagelijkse (politie)praktijk anderzijds?

4. Hoe kan ervoor worden gezorgd dat de kennis (tijdig) op de juiste plekken in de organisatie wordt aangeboden?
    a. Op welke wijze zou in de organisatie kennis beschikbaar moeten zijn?
    b. Hoe kan duidelijk worden gemaakt waar en/of hoe politiemensen de juiste informatie kunnen vinden, en er überhaupt vanaf weten dat het er is? (leven lang leren; snelle ontwikkelingen op digitaal gebied)

c. In hoeverre is het wenselijk dat politiemensen worden ondersteund in de beschikbaarheid/vindbaarheid van kennis? Bijvoorbeeld middels digitale hulpmiddelen? (De telefoonmedewerkers van de politie worden bijvoorbeeld ondersteund door een computersysteem waarin voor diverse onderwerpen handelingskaders worden gegeven. Hierin is veel kennis geborgd).
d. Hoe kan ervoor worden gezorgd dat politiemensen op de hoogte zijn van het actuele opleidingen- en cursusaanbod?

5. Hebt u algemene aanbevelingen / good practices / do's en don'ts voor wat betreft het opleiden van grote groepen (politiemensen) in digitale aspecten (van politiewerk)?

Specifiek
We willen u nu graag enkele vragen stellen op basis van onze bevindingen van de resultaten van een vragenlijst die we hebben uitgezet onder ongeveer 400 politiemensen over hun kennis van digitale aspecten van politiewerk. Deze vragen zijn gebaseerd op door ons ontwikkelde kennisnormen.

Een van de bevindingen is dat de respondenten niet over alle kennis beschikken die idealiter nodig wordt geacht. Dit is echter ook geen realistische verwachting en ook niet noodzakelijk. Dit brengt ons tot de volgende vraag.

6. Hoeveel van de tien medewerkers moeten aan de (basis/minimum) kennisnorm voldoen? Is het bijvoorbeeld voldoende dat zeven van de tien medewerkers goed scoren op kennisvragen? Waar moet de politie naar streven, en waarom?
7. In hoeverre is het volgens u belangrijk/wenselijk dat kennis (van digitale aspecten van politiewerk) aanwezig is in de volle breedte van de organisatie? Moet iedereen beschikken over dezelfde (basis)kennis?
    a. In hoeverre volstaat het dat alleen specialisten binnen de politie over deze kennis beschikken?
        i. In hoeverre houdt dit effectief gebruik maken van digitale mogelijkheden (denk aan digitale sporen) tegen?
        ii. Hoe kunnen politiemensen zonder kennis (en ervaring) aan specialisten de juiste vragen stellen?

Notitie de volgende vragen zijn alleen relevant voor interviewkandidaten van de politie.

8. Kennis over internetrechercheren is beduidend laag bij politiemensen; zowel om te kunnen internetrechercheren als over de wetgeving omtrent internetrechercheren. Op welke wijze kunnen medewerkers hier het beste in worden opgeleid?

9. De opsporing lijkt kansen te missen doordat digitale sporen niet worden herkend, de gevaren van besmetting niet worden onderkent en de basishandelingen hierbij niet worden gebruikt. Op welke wijze zou u deze kennis borgen?

10. Bij het opnemen van een aangifte is te weinig zicht op diepgaandere digitale sporen. Op welke wijze kan men ervoor zorgen dat dit wel het geval is?

11. De politie moet in staat zijn om in contact te kunnen treden met de bewoners in hun gebied. De agenten in de wijk weten echter niet welke internettoepassingen door burgers worden gebruikt en hoe zijn deze zelf kunnen gebruiken om in contact te treden met burgers. Op welke wijze is deze kennis in de organisatie te borgen?

AFSLUITING
12. Is er een onderwerp onbelicht gebleven die u graag wilt bespreken of hebt u nog een gedachte over dit thema die u graag wilt delen?

Interviewkandidaat bedanken voor deelname.

Bijlage V: Gespreksprotocol focusgroep

Introductie
Onderzoekers bij onderzoeksgroep Cybersafety. Onderzoek naar digitalisering van samenleving en de gevolgen daarvan voor veiligheid en rechtshandhaving.

- Voorstelrondje deelnemers: naam, functie, eenheid.

Toelichting Level-Up!
Inzicht bieden in het kennisniveau van politiemedewerkers 'inzake digitale aspecten van politiewerk'. Daarmee worden cybercrime, gedigitaliseerde criminaliteit en criminaliteit met een digitale component (het gebruik van digitale sporen) bedoeld. 3 stappen:

- Vaststellen over welke kennis en vaardigheden politiemensen moeten beschikken om effectief uitvoering te geven aan politiewerk in een gedigitaliseerde samenleving
- Vaststellen over welke kennis en vaardigheden politiemensen daadwerkelijk beschikken
- Meten waar een eventueel kennistekort zich voordoet en wat dat kennistekort inhoudt

Het onderzoek leidt uiteindelijk tot een advies over het reduceren van het kennistekort inzake digitale aspecten van politiewerk. PIAC is opdrachtgever.

Het groepsinterview
Doel is het kennisniveau te meten onder vijf functiegroepen: intake en service, blauw en de drie rechercheniveaus (basis, regio, eenheid). Met rechercheurs worden tactisch generalisten bedoeld (geen experts).
Het is essentieel om vast te stellen over welke kennis en vaardigheden politiemensen moeten beschikken om effectief uitvoering te geven aan politiewerk in een gedigitaliseerde samenleving. Dit groepsinterview gaat alleen over blauw en de drie rechercheniveaus.

Er is al documentenanalyse (bestaande handreikingen) en literatuuronderzoek verricht en er zijn ruim 10 interviews afgenomen. Het groepsinterview heeft tot doel om de tot dusver opgedane inzichten te verifiëren en, waar nodig, aan te scherpen. Op basis daarvan wordt een meetinstrument ontwikkeld om het kennisniveau hierover te toetsen bij collega-politiemedewerkers. Deelnemende eenheden zijn: Noord-Holland, Midden Nederland, Oost Nederland, Zeeland-West-Brabant.

Opmerkingen vooraf

- Alle meningen / zienswijzen zijn welkom; wel proberen we door middel van discussie te komen tot overeenstemming
- Alle input wordt anoniem verwerkt in het onderzoek
- Toestemming tot opname?

VRAGEN

1. Kennis van de normen
Voorafgaand aan het groepsinterview zijn de normen aan de respondenten toegestuurd en is uitgelegd dat het van belang is dat zij de norm(en) die betrekking hebben op hun expertisegebied vooraf doornemen.
Controlevraag:

- Wie heeft welke kennisnorm(en) doorgenomen?
    - Als de norm(en) niet zijn doorgenomen, moet dat per norm op competentieniveau worden gedaan. Het tijdens het interview doornemen van alle indicatoren is ondoenlijk. Het doel is om te verifiëren of de opgenomen competenties (linker kolom) volledig zijn. Respondenten die daartoe bereid zijn worden uitgenodigd om verbetersuggesties na te zenden.

Notitie. We beginnen bij de normen voor opsporing. Daarna gaan we over naar blauw, omdat daar meer verdiepingsvragen zijn opgenomen.

2. Kennisnorm opsporing

A. Competenties
In hoeverre zijn de in de norm opgenomen (hoofd)competenties volledig (linker kolom)?
- Indien onvolledig, welke competentie(s) ontbreekt (ontbreken) en waarom?
- Competenties aanscherpen? Waarom?
- Indien overcompleet, welke competentie(s) kan (kunnen) worden weggelaten en waarom?

B. Uitwerking van competenties
Zijn er op- en/of aanmerkingen op de uitwerking van de competenties in de kennisnorm (middelste kolom)?
- Zo ja, wat kan er beter en hoe?
    - Indicatoren toevoegen? Waarom?
    - Indicatoren aanscherpen? Waarom?
    - Indicatoren weglaten? Waarom?

C. Verdiepingsvragen

<u>Competentie 6: deel; vorderen van gegevens.</u>
1. Klopt het aangebrachte niveauverschil op het gebied van vorderen?

    Vorderingen op basisteamniveau blijven beperkt tot het vorderen van identificerende gegevens (126na lid 1 Sv, 126ng lid 1 jo. 126 nc SV, 126nc Sv). Alles daarboven (verkeersgegevens, gegevens over de inhoud van communicatie, gevoelige gegevens, et cetera - zie handreiking opsporing in een gedigitaliseerde samenleving) is voorbehouden aan de districts- en regionale recherche.

<u>Competentie 6: deel; interceptie.</u>
2. Klopt het aangebrachte niveauverschil op het gebied van interceptie?

    Basisteamrecherche hoeft geen interceptiemogelijkheden te kennen en toe te passen

3. Kennisnorm blauw

A. Competenties
In hoeverre zijn de in de norm opgenomen (hoofd)competenties volledig (linker kolom)?
- Indien onvolledig, welke competentie(s) ontbreekt (ontbreken) en waarom?
- Competenties aanscherpen? Waarom?
- Indien overcompleet, welke competentie(s) kan(kunnen) worden weggelaten en waarom?

B. Uitwerking van competenties
Zijn er op- en/of aanmerkingen op de uitwerking van de competenties in de kennisnorm (rechter kolom)?
- Zo ja, wat kan er beter en hoe?
    - Indicatoren toevoegen? Waarom?
    - Indicatoren aanscherpen? Waarom?
    - Indicatoren weglaten? Waarom?

C. Verdiepingsvragen

<u>Competentie 2: juridisch kader.</u>
1. Zijn de 'bevoegdheden' die staan beschreven onder deze competentie volledig?

    *Houd tijdens de discussie de 80/20 regel (hoofd- en bijzaken onderscheiden) en de doelgroep (politiemensen in uniformdienst) in het achterhoofd.

2. In de eerste sub-norm wordt gesproken over vrijwilligheid. Hoe vrijwillig is het dat als de politie op je stoep staat? Met andere woorden kunnen we dit dus wel zo stellen?

3. Volgens een juridisch expert bij OM zouden onderstaande 4 artikelen kunnen of moeten worden toegevoegd aan de norm. Hoe denken jullie daarover?

- Art. 96b Sv
    - Geeft de opsporingsambtenaar in het geval van heterdaad of buiten heterdaad bij feiten waarvoor een voorlopige hechtenis kan worden opgelegd, de mogelijkheid een voertuig te doorzoeken.
- Art. 49 Wet Wapens en Munitie (WWM).
    - Geeft aanvullende bevoegdheden voor een doorzoeking (ook in een woning) bij WWM-overtredingen.)
- Art. 9 van de Opiumwet (Ow)
    - Geeft diverse mogelijkheden voor binnentreden ter inbeslagname bij Opiumwetdelicten.
- Art. 125i SV e.v.
    - Geeft bevoegdheden voor in beslagname van gegevens die zijn vastgelegd op een gegevensdrager.

<u>Competentie 3: kennen en kunnen uitvoeren van de eerste maatregelen, deel primaire taken op PD</u>
4. Onder deze competentie is beschreven:

> 'In principe wordt de PD niet betreden door de first responder, in verband met risico op het vernietigen, beschadigen of besmetten van sporen. Echter, de PD kan worden betreden als maatregelen moeten worden getroffen 'die absoluut geen uitstel dulden' (p.46):
>
> - Hulpverlening slachtoffer
> - Beëindigen gevaarlijke situatie
> - Aanhouden van nog aanwezige verdachte
> - Verwijderen van publiek
> - **Beschermen van belangrijke fysieke en digitale sporen die anders verloren gaan**

a) Kun je, zonder de PD te betreden, als first responder weten of er digitale sporen zijn? Zo niet, kunnen we dan stellen dat de first responder de PD altijd moet betreden om na te gaan of er digitale sporen zijn?

Vervolgens wordt in deze competentie het volgende gesteld: Een first responder verricht geen noodgedwongen eerste handelingen als, gezien de aard van de zaak, de FO ter plaatse komt.

b) Klopt deze bewering? De onderliggende vraag is of de FO zo snel ter plaatse komt dat de first responder ook geen digitale sporen hoeft veilig te stellen. Is dat juist?

<u>Competentie 5: basisstappen</u>
5. De benaming van competentie 5 luidt: Ken specifieke basisstappen in het geval van **een PD met digitale sporen**. In hoeverre klopt deze benaming? Zou het uitgangspunt niet moeten zijn dat iedere PD digitale sporen heeft totdat uit onderzoek het tegendeel blijkt? Met andere woorden: zijn er ook PD's zonder digitale sporen?

Afsluiting
Zijn er nog andere op- en/of aanmerkingen op de kennisnormen of eventuele opmerkingen en/of suggesties ten aanzien van dit onderzoek?

Bijlage VI: Online vragenlijst

In deze bijlage is de online vragenlijst opgenomen. Bij een verschillende vragen is een aantal antwoordcategorieën vetgedrukt. Dat betekent is die gevallen dat het om het juiste antwoord of om een correctie handeling gaat.

Achtergrondkenmerken

Notitie. Alle vragen betreffende 'achtergrondkenmerken' zijn aan alle functiegroepen gesteld.

1. In welke eenheid bent u werkzaam?

O	Midden-Nederland
O	Noord-Holland
O	Oost-Nederland
O	Zeeland-West-Brabant
O	Andere eenheid (einde vragenlijst)

2. Wat typeert uw huidige werkzaamheden het best?

O	Ik verzorg als politiemedewerker de intake
O	Ik ben politiemedewerker in uniformdienst (Blauw)
O	Ik ben tactisch rechercheur bij de basisteamrecherche (VVC teams, et cetera)
O	Ik ben tactisch rechercheur bij de districtsrecherche
O	Ik ben tactisch rechercheur bij de regionale recherche
O	Ik ben tactisch rechercheur bij de landelijke recherche (einde vragenlijst)
O	Geen van dezen (einde vragenlijst)

3. Wat is uw functie?

O	Assistent A
O	Assistent B
O	Medewerker
O	Generalist
O	Senior
O	Operationeel expert
O	Operationeel specialist
O	Anders

4. Wat is uw geboortejaar?

   [scrol-down menu jaartallen]

5. Wat is uw geslacht?

O	Man
O	Vrouw

6. Hebt u een opleiding of cursus gevolgd op het gebied van digitale criminaliteit? (meerdere antwoorden mogelijk)

□	Ja, zowel op het gebied van cybercrime als gedigitaliseerde criminaliteit
□	Ja, alleen op het gebied van cybercrime
□	Ja, alleen op het gebied van gedigitaliseerde criminaliteit
□	Ja, maar onbekend of het ging over cybercrime of gedigitaliseerde criminaliteit
□	Ja, ik heb een aparte opleiding gevolgd op het gebied van IT
□	Nee

7. In hoeverre hebt u in de afgelopen vijf jaar te maken gehad met zaken op het gebied van digitale criminaliteit?

O	Uitsluitend met dergelijke zaken te maken gehad
O	Veel mee te maken gehad
O	Niet veel, maar ook niet weinig mee te maken gehad
O	Weinig mee te maken gehad
O	Nooit mee te maken gehad

Digitale criminaliteit

Notitie. Alle vragen betreffende 'digitale criminaliteit' zijn aan alle functiegroepen gesteld.

8. Geef aan in hoeverre u het eens bent met onderstaande stelling.

	Helemaal mee oneens				Helemaal mee eens
Ik weet wat voor strafbare gedragingen vallen onder de term digitale criminaliteit.	O	O	O	O	O

Nu volgen vier korte casussen die betrekking hebben op digitale criminaliteit.

Casus 1:
Nadat persoon X een paar maanden geen gebruik heeft gemaakt van zijn Twitteraccount, blijkt dat een onbekend persoon zijn account heeft gebruikt. Die persoon heeft belastende informatie over persoon X op Twitter gezet.

9. a. Van welk strafbaar feit is hier (mogelijk) sprake? (meerdere antwoorden mogelijk)

□	Er is geen sprake van strafbaar gedrag
□	**Computervredebreuk / hacken**
□	Gegevensdiefstal
□	**Smaad / laster**
□	Cyberpesten
□	DDoS-aanval
□	Malware verspreiden

Casus 2: Kort nadat persoon X via een buitenlandse webshop een product heeft gekocht, worden met de creditcardgegevens van persoon X, zonder medeweten en zonder toestemming, goederen gekocht en ontvangt persoon X rekeningen van deze goederen.

9. b. Van welk strafbaar feit is hier (mogelijk) sprake? (meerdere antwoorden mogelijk)

□	Er is geen sprake van strafbaar gedrag
□	**Identiteitsmisbruik**
□	Skimming
□	**Oplichting / phishing**
□	Voorschotfraude
□	Witwassen
□	Stoornis veroorzaken

Casus 3: In het computerspel Habbo Hotel heeft speler X een paarse koelkast gekocht. Dit product is enkel voor deze speler bedoeld en de speler kan dit product gebruiken of verkopen aan een andere speler. Speler Y weet door een truc het product over te zetten naar zijn account, waardoor speler X het niet meer kan gebruiken of verkopen.

9. c. Van welk strafbaar feit is hier (mogelijk) sprake? (meerdere antwoorden mogelijk)

□	Er is geen sprake van strafbaar gedrag
□	**Computervredebreuk / hacken**
□	Afpersing / chantage
□	**Diefstal**
□	Heling van computergegevens
□	Fraude via veiling- en/of verkoopsites
□	Zonder toestemming verspreiden van goederen via internet

Casus 4: Een 15-jarig meisje zat op internet en nu blijkt dat via de webcam opnames van haar zijn gemaakt terwijl ze een ontbloot bovenlichaam had. Ze had de webcam niet zelf aangezet en wist niet dat de webcam aanstond. Er circuleren nu foto's van haar op internet.

9. d. Van welk strafbaar feit is hier (mogelijk) sprake? (meerdere antwoorden mogelijk)

□	Er is geen sprake van strafbaar gedrag
□	**Kinderpornografie**
□	**Computervredebreuk / hacken**
□	Bedreiging
□	Stalking / belaging
□	Smaad
□	Grooming

Optreden op en rondom een plaats delict

Notitie. Alle vragen betreffende 'digitale criminaliteit' zijn aan alle functiegroepen gesteld.

Nu volgen enkele vragen over het optreden op en rondom een plaats delict (PD). Het optreden kent verschillende basisstappen, maar die vallen buiten het bestek van dit onderzoek. De volgende stellingen hebben uitsluitend betrekking op digitale aspecten van het politiewerk op en rondom een PD.

10. Geef aan in hoeverre u het eens bent met onderstaande stellingen.

	Helemaal mee oneens				Helemaal mee eens
Ik weet welke risico's er zijn met betrekking tot het besmetten/vernietigen van digitale sporen.	O	O	O	O	O
Bij twijfel over bevoegdheden om handelingen te verrichten op een PD met digitale sporen moet een expert worden ingeschakeld.	O	O	O	O	O
Ik ken de basisprocedure voor het veiligstellen van digitale gegevensdragers.	O	O	O	O	O
Tijdens een buurtonderzoek moet ook aandacht zijn voor het inventariseren van digitale sporen.	O	O	O	O	O

11. Geef van onderstaande acties aan of zij juist of onjuist zijn bij het optreden op een PD met digitale sporen.

Als ik een PD met digitale sporen betreed dan moet ik:	Onjuist	Juist
Met blote handen een geaard voorwerp aanraken in verband met mogelijk statisch geladen zijn.	O	O
Zo spoedig mogelijk alle elektronische apparatuur uitschakelen.	O	O
Handelingen verrichten om te voorkomen dat sporen op afstand worden gewist.	O	O
Erop toezien dat digitale sporen niet worden besmet.	O	O
Hulp vragen aan de eigenaren van de ICT.	O	O
Hulp vragen aan omstanders.	O	O
Van tevoren op de eigen gegevensdrager(s) wifi en bluetooth uitzetten.	O	O

12. Geef van onderstaande uitspraken aan of zij juist of onjuist zijn.

	Onjuist	Juist
Er moet worden vastgesteld welke gegevensdragers aanwezig zijn op de PD.	O	O
Gegevensdragers moeten worden veiliggesteld van groot naar klein.	O	O
Het is niet belangrijk om de status van gegevensdragers vast te stellen (bijv. of ze aan of uit staan).	O	O
Digitaal experts kunnen worden ingeschakeld bij het veiligstellen van digitale gegevensdragers.	O	O
Gegevensdragers die snel kunnen worden uitgelezen moeten als eerste worden veiliggesteld.	O	O
Digitale gegevensdragers mogen alleen worden veiliggesteld door collega's die een forensische opleiding hebben afgerond.	O	O

13. Geef van onderstaande uitspraken over bewijsvoering aan of zij juist of onjuist zijn.

	Onjuist	Juist
Uitsluitend klassieke of uitsluitend digitale sporen meenemen van een PD is voldoende om een sporenbeeld te maken.	O	O
Voor het vaststellen van het sporenbeeld op de PD is het belangrijk om zowel klassieke als digitale sporen veilig te stellen.	O	O
Op een PD weegt het veiligstellen van klassieke sporen altijd zwaarder dan het veiligstellen van digitale sporen.	O	O

14. Indien u een voor u onbekende gegevensdrager aantreft op een PD, welke stap(pen) zet u dan meest waarschijnlijk? (meerdere antwoorden mogelijk)

□	Ik stel deze veilig zoals ik dat gewend ben te doen met andere, voor mij bekende, gegevensdragers.
□	**Ik schakel een specialist in.**
□	Ik laat de gegevensdrager achter op de PD.
□	**Ik maak gebruik van de webapp 'Digitale PD'.**
□	Ik zoek het serienummer op van de gegevensdrager.
□	Ik schakel de gegevensdrager direct uit.
□	Ik neem zo snel mogelijk kennis van de inhoud van de gegevensdrager.

Nu volgt een aantal voorbeelden van gegevensdragers die u kunt tegenkomen op een PD. We vragen u om aan te geven om wat voor gegevensdrager het gaat.

15. a. Wat voor gegevensdrager is dit?

O	Gameconsole
O	Externe hardeschijf
O	**Nas / server**

15. b. Wat voor gegevensdrager is dit?

O	Zipdrive
O	**Tapedrive**
O	Netwerkdrive

15. c. Wat voor gegevensdrager is dit?

O	Tablet
O	**Smartphone**
O	E-reader

15. d. Wat voor gegevensdrager is dit?

O	**Switch**
O	PowerPlug
O	LAN

15. e. Wat voor gegevensdrager is dit?

**Afbeelding vervaagt in verband met rechten.*

O	**Desktop computer**
O	Mediabox
O	Hifi Entertainment system

15. f. Wat voor gegevensdrager is dit?

O	Dongel
O	NFC Ring
O	**Activity tracker**

Digitale sporen

16. Geef aan in hoeverre u het eens bent met onderstaande stellingen.

	Helemaal mee oneens				Helemaal mee eens
Ik weet welke digitale sporen van belang zijn voor opsporingsonderzoek.	O	O	O	O	O
Ik weet hoe de 7 W's (wie, wat, waar, waarmee, welke wijze, wanneer, waarom) kunnen worden toegepast om de relevantie van digitale sporen te bepalen.	O	O	O	O	O
Alternatieven dan het strafrecht kunnen effectiever zijn bij de bestrijding van digitale criminaliteit.	O	O	O	O	O
Ik ken mijn eigen beperkingen bij het verrichten van een opsporingsonderzoek naar digitale criminaliteit.	O	O	O	O	O
Ik weet hoe ik moet handelen wanneer ik bij het verrichten van opsporingsonderzoek naar digitale criminaliteit onvoldoende kennis heb.	O	O	O	O	O
Ik weet wat 'vluchtige gegevens' zijn.	O	O	O	O	O

Routing. Indien 'ik weet wat vluchtige gegevens zijn' met (helemaal) eens wordt beantwoord, dan de volgende vraag tonen, zo niet dan vraag 17 overslaan.

17. Geef aan in hoeverre u het eens bent met onderstaande stelling.

	Helemaal mee oneens				Helemaal mee eens
Ik weet hoe te handelen wanneer er sprake is van digitale 'vluchtige gegevens'.	O	O	O	O	O

De volgende stellingen gaan over uw kennis over het benutten van sporen uit gegevensdragers.

18. Geef aan in hoeverre u het eens bent met onderstaande stellingen.

	Helemaal mee oneens				Helemaal mee eens
Ik ken de bevoegdheden tot inbeslagname van gegevensdragers.	O	O	O	O	O
Ik weet welke gegevensdragers op een PD relevant zijn voor inbeslagname.	O	O	O	O	O
Ik weet welke gegevensdragers kunnen worden uitgelezen.	O	O	O	O	O
Ik weet welke digitale sporen kunnen worden uitgelezen.	O	O	O	O	O
Ik weet tijdens een onderzoek wanneer het nuttig/noodzakelijk is om gegevensdragers uit te lezen.	O	O	O	O	O
Ik weet hoeveel tijd het kost om een gegevensdrager uit te laten lezen.	O	O	O	O	O
Ik weet hoe lang het duurt om het resultaat van een uitleesaanvraag te ontvangen.	O	O	O	O	O
Ik weet hoe gerichte uitleesvragen opgesteld moeten worden waarmee de digitaal expert aan de slag kan.	O	O	O	O	O
Ik weet welke eisen zijn verbonden aan uitleesvragen.	O	O	O	O	O
Ik weet hoe ik softwarepakketten moet gebruiken om digitale sporen te analyseren.	O	O	O	O	O
Klik voor deze 'stelling' het middelste antwoord aan.	O	O	O	O	O
Ik weet hoe ik de bevindingen van digitaal sporenonderzoek moet vastleggen (dossiervorming).	O	O	O	O	O
Ik weet dat het maken van een forensische kopie van de sporen op een gegevensdrager is voorbehouden aan daarvoor opgeleide politiemensen.	O	O	O	O	O
Bij twijfel over de interpretatie van de analyseresultaten moet een digitaal expert worden ingeschakeld.	O	O	O	O	O

De volgende stellingen gaan over uw kennis over het vorderen van gegevens.

19. Geef aan in hoeverre u het eens bent met onderstaande stellingen.

	Helemaal mee oneens				Helemaal mee eens
Ik weet hoe ik uit moet zoeken welke digitale sporen gevorderd kunnen worden.	O	O	O	O	O
Ik weet hoe ik vorderbare digitale sporen kan herkennen.	O	O	O	O	O
Bij twijfel over de (on)mogelijkheden om digitale sporen te vorderen moet een expert worden ingeschakeld.	O	O	O	O	O
Bij twijfel over het geven van prioriteit aan het vorderen van digitale sporen moet een expert worden ingeschakeld.	O	O	O	O	O

De volgende stelling(en) gaan over uw kennis over interceptie.

20. a. Geef aan in hoeverre u het eens bent met onderstaande stelling.

	Helemaal mee oneens				Helemaal mee eens
Ik weet wat interceptie is	O	O	O	O	O

Routing. De volgende vraag over interceptie niet voorleggen aan respondenten 'basis'. Basis routen naar vraag 21. Indien deze vraag wordt beantwoord met 4 of 5 ([helemaal] mee eens) dan routen naar volgende vraag, zo niet dan naar vraag 21.

20. b. Geef aan in hoeverre u het eens bent met onderstaande stellingen.

	Helemaal mee oneens				Helemaal mee eens
Ik ken de mogelijkheden van interceptie	O	O	O	O	O
Ik weet hoe interceptiemogelijkheden toegepast moeten worden	O	O	O	O	O
Bij twijfel over de (on)mogelijkheden van interceptie moet een expert worden ingeschakeld	O	O	O	O	O

20. c. In hoeverre bent u bekend met interceptiemogelijkheden om **tapkenmerken** te verkrijgen (met als doel om een tap te plaatsen)?

O	Ik ben hier niet mee bekend
O	Ik ben hiermee bekend, maar heb hier nog nooit gebruik van gemaakt
O	Ik ben hiermee bekend, en heb hier wel eens gebruik van gemaakt
O	Ik ben hiermee bekend, en heb hier vaak gebruik van gemaakt

20. d. In hoeverre bent u bekend met interceptiemogelijkheden om gegevens over **plaatsbepaling** te verkrijgen (bijv. met als doel om een verdachte te lokaliseren)

O	Ik ben hier niet mee bekend
O	Ik ben hiermee bekend, maar heb hier nog nooit gebruik van gemaakt
O	Ik ben hiermee bekend, en heb hier wel eens gebruik van gemaakt
O	Ik ben hiermee bekend, en heb hier vaak gebruik van gemaakt

20. e. In hoeverre bent u bekend met interceptiemogelijkheden om **verkeersgegevens** te verkrijgen (bijv. wanneer er gebeld is, naar welk nummer en hoe lang)

O	Ik ben hier niet mee bekend
O	Ik ben hiermee bekend, maar heb hier nog nooit gebruik van gemaakt
O	Ik ben hiermee bekend, en heb hier wel eens gebruik van gemaakt
O	Ik ben hiermee bekend, en heb hier vaak gebruik van gemaakt

20. f. In hoeverre bent u bekend met interceptiemogelijkheden om actuele en toekomstige inhoud van **telefonie** te **tappen**?

O	Ik ben hier niet mee bekend
O	Ik ben hiermee bekend, maar heb hier nog nooit gebruik van gemaakt
O	Ik ben hiermee bekend, en heb hier wel eens gebruik van gemaakt
O	Ik ben hiermee bekend, en heb hier vaak gebruik van gemaakt

20. g. In hoeverre bent u bekend met interceptiemogelijkheden om actuele en toekomstige inhoud van **internetcommunicatie** te **tappen**?

O	Ik ben hier niet mee bekend
O	Ik ben hiermee bekend, maar heb hier nog nooit gebruik van gemaakt
O	Ik ben hiermee bekend, en heb hier wel eens gebruik van gemaakt
O	Ik ben hiermee bekend, en heb hier vaak gebruik van gemaakt

Omdat in uw geval de eerstvolgende vragen niet van toepassing zijn, gaat u verder met vraag 21.

De volgende vragen hebben betrekking op hulpmiddelen.

21. In hoeverre bent u bekend met de website 'Internetsporen.nl'?

O	Ik had nog nooit van deze website gehoord
O	Ik kende de website al, maar heb deze nog nooit geraadpleegd
O	Ik kende de website al, en heb deze wel eens geraadpleegd
O	Ik kende de website al, en heb deze vaak geraadpleegd

22. a. Bent u bekend met de webapps van de Politieacademie?

O	Ja
O	Nee

Routing. Indien deze vraag met 'nee' wordt geantwoord dan doorgaan naar vraag 23.

22. b. In hoeverre bent u bekend met de webapp 'Cybercrime'?

O	Ik had nog nooit van deze app gehoord
O	Ik kende de app al, maar heb deze nog nooit gebruikt
O	Ik kende de app al, en heb deze wel eens gebruikt
O	Ik kende de app al, en heb deze vaak gebruikt

22. c. In hoeverre bent u bekend met de webapp 'Digitale PD'?

O	Ik had nog nooit van deze app gehoord
O	Ik kende de app al, maar heb deze nog nooit gebruikt
O	Ik kende de app al, en heb deze wel eens gebruikt
O	Ik kende de app al, en heb deze vaak gebruikt

22. d. In hoeverre bent u bekend met de webapp ‘H.U.I.B (internetbevraging)’?

O	Ik had nog nooit van deze app gehoord
O	Ik kende de app al, maar heb deze nog nooit gebruikt
O	Ik kende de app al, en heb deze wel eens gebruikt
O	Ik kende de app al, en heb deze vaak gebruikt

De volgende stellingen gaan over uw kennis over internet en sporen.

23. Geef aan in hoeverre u het eens bent met onderstaande stellingen.

Ik weet wat bedoeld wordt met:	Helemaal mee oneens				Helemaal mee eens
internetrechercheren	O	O	O	O	O
‘clearweb’	O	O	O	O	O
‘deepweb’	O	O	O	O	O
‘darkweb’	O	O	O	O	O
IP-adres	O	O	O	O	O
domeinnaam	O	O	O	O	O

Informatiegaring op internet

Notitie. Alle vragen betreffende ‘informatiegaring’ zijn aan alle functiegroepen gesteld.

24. Geef aan in hoeverre u het eens bent met onderstaande stellingen.

	Helemaal mee oneens				Helemaal mee eens
Ik weet hoe ik informatie moet vergaren op internet, bijvoorbeeld via zoekmachines en open bronnen.	O	O	O	O	O
Ik weet wat OSINT (open source intelligence) inhoudt.	O	O	O	O	O
Ik weet wat Intel (intelligence) inhoudt.	O	O	O	O	O
Ik weet waar in de politieorganisatie de verantwoordelijkheid ligt voor informatievergaring op internet.	O	O	O	O	O
Van een politiemedewerker wordt verwacht dat hij/zij zich actief op de hoogte stelt over ontwikkelingen in het omgaan met internetbronnen.	O	O	O	O	O
Onderzoek op internet kent in potentie een groot afbreukrisico voor politieonderzoek.	O	O	O	O	O
Bij het zoeken naar online-informatie laat je sporen achter.	O	O	O	O	O
Ik weet welke sporen worden achtergelaten bij het zoeken naar online-informatie.	O	O	O	O	O
Sporen die tijdens het zoeken naar informatie op verschillende plekken op internet worden achtergelaten kunnen met elkaar in verband worden gebracht.	O	O	O	O	O
Bij het gebruik van internet moeten werk en privé van elkaar worden gescheiden.	O	O	O	O	O

Ik weet wat het verschil is tussen interne en externe IP-adressen.	O	O	O	O	O
Ik weet wat een IPv4-adres is.	O	O	O	O	O
Ik weet wat een IPv6-adres is.	O	O	O	O	O
Het is mogelijk om op het internet gevonden sporen veilig te stellen.	O	O	O	O	O

De volgende stellingen gaan over uw kennis over juridische implicaties van zoeken naar informatie op internet.

25. Geef aan in hoeverre u het eens bent met onderstaande stellingen.

	Helemaal mee oneens				Helemaal mee eens
Ik ken de algemene juridische regels van zoeken naar informatie op internet.	O	O	O	O	O
Ik ken de beslisboom waarmee kan worden bepaald of een onderzoek uitgevoerd mag worden binnen de kaders van de taakstelling van de politie (artikel 3 Politiewet 2012).	O	O	O	O	O
Ik weet dat er mogelijk verschil is in kwaliteit van gevonden informatie op internet.	O	O	O	O	O
Ik ken de wetsartikelen die regels stellen voor informatievergaring op internet.	O	O	O	O	O
Ik weet dat er bij een zoektocht op internet snel sprake kan zijn van stelselmatige observatie.	O	O	O	O	O
Ik ken de privacywetgeving in relatie tot het zoeken en vastleggen van informatie van internet.	O	O	O	O	O
Ik weet dat contacten leggen tijdens zoeken in internetbronnen altijd moet worden vermeden.	O	O	O	O	O
Ik weet bij informatieverzoeken (vordering) of ik die zelf mag uitvoeren of dat die bevoegdheid bij een ander ligt.	O	O	O	O	O

De volgende stellingen gaan over uw kennis over monitoren en identificeren.

26. Geef aan in hoeverre u het eens bent met onderstaande stellingen.

	Helemaal mee oneens				Helemaal mee eens
Ik weet wat bruikbare zoektermen zijn om informatie op internet te vinden.	O	O	O	O	O
Ik weet wat zinvolle zoektermen zijn om een identificatie-/traceeractie te laten starten.	O	O	O	O	O

De volgende stellingen gaan over uw kennis over tools voor het zoeken naar informatie op internet.

27. Geef aan in hoeverre u het eens bent met onderstaande stellingen.

	Helemaal mee oneens				Helemaal mee eens
Ik weet voldoende om met zoekmachines zoals Google te werken.	O	O	O	O	O
Ik weet wat de risico's zijn van het gebruik van zoekmachines, zoals Google.	O	O	O	O	O
Ik weet dat ik zoekoperatoren (zoals AND en OR) kan gebruiken om gericht informatie te zoeken.	O	O	O	O	O

28. a. Geef aan in hoeverre u het eens bent met onderstaande stellingen.

	Helemaal mee oneens				Helemaal mee eens
Ik weet wat iRN (internet Recherche Netwerk) is.	O	O	O	O	O

Routing: wanneer respondenten op deze stelling aangeven (helemaal) mee eens te zijn dan het volgende blok met stellingen tonen; zo niet dan doorgaan met vraag 29.

28. b. Geef aan in hoeverre u het eens bent met onderstaande stellingen.

	Helemaal mee oneens				Helemaal mee eens
Het gebruiken van een iRN computer minimaliseert het afbreukrisico van onderzoek doen op internet.	O	O	O	O	O
iRN is een geschikte tool om onlineprivézaken mee te regelen.	O	O	O	O	O
Ik weet voldoende om met iRN te werken.	O	O	O	O	O
Ik weet wat de risico's zijn van het gebruik van iRN.	O	O	O	O	O

De volgende stellingen gaan over uw kennis over bronnen voor het zoeken naar informatie op internet.

29. Geef aan in hoeverre u het eens bent met onderstaande stellingen.

	Helemaal mee oneens				Helemaal mee eens
Ik weet welk type informatie je kunt vinden op welk type internetbron.	O	O	O	O	O
Ik weet waar ik op internet moet zoeken om persoonsgegevens te achterhalen.	O	O	O	O	O
Ik weet waar ik op internet moet zoeken om bedrijfsgegevens te achterhalen.	O	O	O	O	O
Ik weet hoe ik als politiemedewerker zo weinig mogelijk sporen kan achterlaten bij het zoeken op internet.	O	O	O	O	O

Communiceren met burgers

De volgende vragen zijn alleen gesteld aan de doelgroep blauw.

De volgende stellingen gaan over uw kennis over bronnen voor het via internet kunnen communiceren met burgers.

30. Geef aan in hoeverre u het eens bent met onderstaande stellingen.

	Helemaal mee oneens				Helemaal mee eens
Ik weet van welke internettoepassingen burgers gebruik maken.	O	O	O	O	O
Ik weet van welke internettoepassingen ik gebruik kan maken om met verschillende doelgroepen online in contact te treden.	O	O	O	O	O

Aangifte van cybercrime

De volgende vragen zijn alleen gesteld aan de functiegroepen intake en service en blauw.

De volgende stellingen gaan over uw kennis over aangiften van cyberdelicten.

31. Geef aan in hoeverre u het eens bent met onderstaande stellingen.

	Helemaal mee oneens				Helemaal mee eens
Bij het opnemen van een aangifte is het essentieel om de modus operandi (MO) zo uitgebreid mogelijk te registreren.	O	O	O	O	O
Hacken is een basisdelict dat vaak verband houdt met andere delicten.	O	O	O	O	O
Doorvragen bij een aangifte van een delict kan ertoe leiden dat meerdere delicten aan het licht komen.	O	O	O	O	O
Ik weet welke digitale sporen geïnventariseerd kunnen worden voor het aanvullen van een aangifte.	O	O	O	O	O

32. Ik weet wat bedoeld wordt wanneer wordt gesproken over:

	Helemaal mee oneens				Helemaal mee eens
IP-adres verdachte	O	O	O	O	O
E-mailadres	O	O	O	O	O
Advertentienummer(s)	O	O	O	O	O
Bitcoinadressen (wallets)	O	O	O	O	O
Moneygram registratienummers	O	O	O	O	O

De volgende stellingen gaan over uw kennis over het inventariseren van opsporingsrelevante digitale sporen.

33. Geef aan in hoeverre u het eens bent met onderstaande stellingen.

	Helemaal mee oneens				Helemaal mee eens
Ik weet hoe ik de 7 W's (wie, wat, waar, waarmee, welke wijze, wanneer, waarom) moet toepassen om de relevantie van digitale sporen te bepalen.	O	O	O	O	O
Bij twijfel over de relevantie van digitale sporen moet een expert worden geraadpleegd.	O	O	O	O	O

34. a Geef aan in hoeverre u het eens bent met onderstaande stellingen.

	Helemaal mee oneens				Helemaal mee eens
Ik weet wat 'vluchtige gegevens' zijn.	O	O	O	O	O

Routing. Indien ik weet wat vluchtige gegevens zijn met (helemaal) eens wordt beantwoord, dan doorgaan naar volgende vraag, zo niet dan naar 35.

34. b Geef aan in hoeverre u het eens bent met onderstaande stelling.

	Helemaal mee oneens				Helemaal mee eens
Wanneer er sprake is van 'vluchtige gegevens' moet een expert worden ingeschakeld.	O	O	O	O	O

De volgende stellingen gaan over uw kennis over het adviseren over het veiligstellen van digitale sporen.

35. Geef aan in hoeverre u het eens bent met onderstaande stellingen.

	Helemaal mee oneens				Helemaal mee eens
Ik weet hoe veelvoorkomende digitale sporen veiliggesteld kunnen worden.	O	O	O	O	O
Bij twijfel over hoe veelvoorkomende digitale sporen veiliggesteld kunnen worden moet een expert worden ingeschakeld.	O	O	O	O	O

36. Geef van onderstaande stellingen over het aanleveren van digitale sporen aan of zij juist of onjuist zijn.

	Onjuist	Juist
Aanleveren van digitale sporen kan digitaal, op een cd/dvd.	O	O
Aanleveren van digitale sporen kan digitaal, op een usb-stick.	O	O
Aanleveren van digitale sporen kan digitaal, met print screens.	O	O
Aanleveren van digitale sporen kan fysiek, met prints op papier.	O	O
Aanleveren van digitale sporen kan fysiek, met foto's.	O	O

Afsluiting

Dit is het einde van de vragenlijst. Hartelijk dank voor uw deelname.

Bijlage VII: Intranetbericht deelname onderzoek

Level-Up! Onderzoek naar kennis van digitale aspecten van politiewerk

De komende weken worden veel collega's uit de operatie benaderd voor een onderzoek naar digitale kennis die nodig is voor het politiewerk.

Tegenwoordig heeft veel politiewerk te maken met de digitale wereld. Bijvoorbeeld bij het opnemen van aangiften en het behandelen van zaken. Het is echter onduidelijk hoe het kennisniveau van digitale aspecten er op dit moment voorstaat binnen de politieorganisatie. Daarom wordt binnenkort een groot onderzoek uitgevoerd naar digitale aspecten van politiewerk. Met dit onderzoek krijgen we inzicht in welke kennis nodig is voor effectief digitaal politiewerk en welke kennis politiemensen daarvan hebben. Met de resultaten kan de politie toewerken naar een norm.

In de komende weken worden diverse collega's van Intake & Service, GGP en drie rechercheniveaus (basisteam, district en regionaal) uitgenodigd om een online vragenlijst in te vullen. Behalve in onze eenheid gebeurt dit ook in de eenheden Midden-Nederland, Noord-Holland en Oost-Nederland. Het is van belang dat zoveel mogelijk van deze collega's de vragenlijst invullen. De verwachting is dat de resultaten eind dit jaar bekend zijn. Hierover volgt te zijner tijd bericht via intranet.

Het onderzoek wordt uitgevoerd door de Onderzoeksgroep Cybersafety van NHL Stenden Hogeschool en de Politieacademie in opdracht van het Nationale Programma Digitalisering & Cybercrime.

Bijlage VIII: Gemiddelde scores op vragenlijstitems

In deze bijlage zijn de gemiddelde scores op de vragenlijstitems opgenomen. De scores zijn gepresenteerd in dezelfde volgorde zoals ze in de vragenlijst naar voren komen en zijn gecategoriseerd aan de hand van de competenties.

Tabel VII.1: Gemiddelde scores voor kennisnorm R.1, I.2, I.3

Vraag	**Item**	**N**	**M**
8	Ik weet wat voor strafbare gedragingen vallen onder de term digitale criminaliteit.	402	3,00

Tabel VII.2: Gemiddelde scores voor kennisnorm R.2, B.5, B.6, B.7, B.8

Vraag	**Item**	**N**	**M**
10a	Ik weet welke risico's er zijn met betrekking tot het besmetten / vernietigen van digitale sporen.	338	3,01
10b	Bij twijfel over bevoegdheden om handelingen te verrichten op een PD met digitale sporen moet een expert worden ingeschakeld.	338	4,45
10c	Ik ken de basisprocedure voor het veiligstellen van digitale gegevensdragers.	338	2,89
10d	Tijdens een buurtonderzoek moet ook aandacht zijn voor het inventariseren van digitale sporen.	338	4,14
11a	Met blote handen een geaard voorwerp aanraken in verband met mogelijk statisch geladen zijn.	338	1,12
11b	Zo spoedig mogelijk alle elektronische apparatuur uitschakelen.	338	1,09
11c	Handelingen verrichten om te voorkomen dat sporen op afstand worden gewist.	338	1,96
11d	Erop toezien dat digitale sporen niet worden besmet.	338	1,98
11e	Hulp vragen aan de eigenaren van de ICT.	338	1,44
11f	Hulp vragen aan omstanders.	338	1,03
11g	Van tevoren op de eigen gegevensdrager(s) wifi en bluetooth uitzetten.	338	1,87
12a	Er moet worden vastgesteld welke gegevensdragers aanwezig zijn op de PD.	338	1,99
12b	Gegevensdragers moeten worden veiliggesteld van groot naar klein.	338	1,29
12c	Het is niet belangrijk om de status van de gegevensdragers vast te stellen (bijv. of ze aan of uit staan).	338	1,07
12d	Digitaal experts kunnen worden ingeschakeld bij het veiligstellen van digitale gegevensdragers.	338	1,99
12e	Gegevensdragers die snel kunnen worden uitgelezen moeten als eerste worden veiliggesteld.	338	1,39
12f	Digitale gegevensdragers mogen alleen worden veiliggesteld door collega's die een forensische opleiding hebben afgerond.	338	1,28
13a	Uitsluitend klassieke of uitsluitend digitale sporen meenemen van een PD is voldoende om een sporenbeeld te maken.	338	1,02
13b	Voor het vaststellen van het sporenbeeld op de PD is het belangrijk om zowel klassieke als digitale sporen veilig te stellen.	338	2,00
13c	Op een PD weegt het veiligstellen van klassieke sporen altijd zwaarder dan het veiligstellen van digitale sporen.	338	1,07

Tabel VII.2 (vervolg): Gemiddelde scores voor kennisnorm R.2, B.5, B.6, B.7, B.8

Vraag	Item	N	M
14a	Ik stel deze veilig zoals ik dat gewend ben te doen met andere, voor mij bekende, gegevensdragers	338	0,33
14b	Ik schakel een specialist in	338	0,96
14c	Ik laat de gegevensdrager achter op de PD	338	0,01
14d	Ik maak gebruik van de webapp 'Digitale PD'	338	0,22
14e	Ik zoek het serienummer op van de gegevensdrager	338	0,14
14f	Ik schakel de gegevensdrager direct uit	338	0,03
14g	Ik neem zo snel mogelijk kennis van de inhoud van de gegevensdrager	338	0,06

Tabel VII.3: Gemiddelde scores voor kennisnorm R.3, R.5

Vraag	Item	N	M
16a	Ik weet welke digitale sporen van belang zijn voor opsporingsonderzoek.	284	3,06
16b	Ik weet hoe de 7 W's (wie, wat, waar, waarmee, welke wijze, wanneer en waarom) kunnen worden toegepast om de relevantie van digitale sporen te bepalen.	284	3,06
16c	Alternatieven dan het strafrecht kunnen effectiever zijn bij de bestrijding van digitale criminaliteit.	284	3,44
16d	Ik ken mijn eigen beperkingen bij het verrichten van een opsporingsonderzoek naar digitale criminaliteit.	284	4,14
16e	Ik weet hoe ik moet handelen wanneer ik bij het verrichten van opsporingsonderzoek naar digitale criminaliteit onvoldoende kennis heb.	284	3,69
16f	Ik weet wat 'vluchtige gegevens' zijn.	284	3,66
17	Ik weet hoe te handelen wanneer er sprake is van digitale 'vluchtige gegevens'.	199	3,21

Tabel VII.4: Gemiddelde scores voor kennisnorm R.6

Vraag	Item	N	M
18a	Ik ken de bevoegdheden tot inbeslagname van gegevensdragers.	284	3,53
18b	Ik weet welke gegevensdragers op een PD relevant zijn voor inbeslagname.	284	3,34
18c	Ik weet welke gegevensdragers kunnen worden uitgelezen.	284	3,26
18d	Ik weet welke digitale sporen kunnen worden uitgelezen.	284	3,06
18e	Ik weet tijdens een onderzoek wanneer het nuttig / noodzakelijk is om gegevensdragers uit te lezen.	284	3,38
18f	Ik weet hoeveel tijd het kost om een gegevensdrager uit te laten lezen.	284	3,25
18g	Ik weet hoe lang het duurt om het resultaat van een uitleesaanvraag te ontvangen.	284	3,19
18h	Ik weet hoe gerichte uitleesvragen opgesteld moeten worden waarmee de digitaal expert aan de slag kan.	284	3,02
18i	Ik weet welke eisen zijn verbonden aan uitleesvragen.	284	2,65
18j	Ik weet hoe ik softwarepakketten moet gebruiken om digitale sporen te analyseren.	284	2,20
18k	Ik weet hoe ik de bevindingen van digitaal sporenonderzoek moet vastleggen (dossiervorming).	284	2,99

Tabel VII.4 (vervolg): Gemiddelde scores voor kennisnorm R.6

18l	Ik weet dat het maken van een forensische kopie van de sporen op een gegevensdrager is voorbehouden aan daarvoor opgeleide politiemensen.	284	3,79
18m	Bij twijfel over de interpretatie van de analyseresultaten moet een digitaal expert worden ingeschakeld.	284	4,15
19a	Ik weet hoe ik uit moet zoeken welke digitale sporen gevorderd kunnen worden.	284	3,20
19b	Ik weet hoe ik vorderbare digitale sporen kan herkennen.	284	2,77
19c	Bij twijfel over de (on) mogelijkheden om digitale sporen te vorderen moet een expert worden ingeschakeld.	284	4,20
19d	Bij twijfel over het geven van prioriteit aan het vorderen van digitale sporen moet een expert worden ingeschakeld.	284	4,13
20a	Ik weet wat interceptie is.	284	3,74
20b-1	Ik ken de mogelijkheden van interceptie.	165	3,68
20b-2	Ik weet hoe interceptiemogelijkheden toegepast moeten worden.	106	3,92
20b-3	Bij twijfel over de (on) mogelijkheden van interceptie, moet een expert worden ingeschakeld.	106	4,36
20c	In hoeverre bent u bekend met interceptiemogelijkheden om tapkenmerken te verkrijgen (met als doel om een tap te plaatsen)?	106	3,23
20d	In hoeverre bent u bekend met interceptiemogelijkheden om gegevens over plaatsbepaling te verkrijgen (bijv. met als doel om een verdachte te lokaliseren)?	106	3,44
20e	In hoeverre bent u bekend met interceptiemogelijkheden om verkeersgegevens te verkrijgen (bijv. wanneer er gebeld is, naar welk nummer en hoe lang)?	106	3,60
20f	In hoeverre bent u bekend met interceptiemogelijkheden om actuele en toekomstige inhoud van telefonie te tappen?	106	3,44
20g	In hoeverre bent u bekend met interceptiemogelijkheden om actuele en toekomstige inhoud van internetcommunicatie te tappen?	106	2,94

Tabel VII.5: Gemiddelde scores voor kennisnorm R.5, B niet-geclassificeerd, I.6

Vraag	**Item**	**N**	**M**
21	In hoeverre bent u bekend met de website ‘internetsporen.nl’?	402	1,46
22a	Bent u bekend met de webapps van de Politieacademie?	402	1,58
22b	In hoeverre bent u bekend met de webapp ‘Cybercrime’?	169	1,83
22c	In hoeverre bent u bekend met de webapp ‘Digitale PD’?	169	1,44
22d	In hoeverre bent u bekend met de webapp ‘H.U.I.B. (internetbevraging)’?	169	1,34

Tabel VII.6: Gemiddelde scores voor kennisnorm R.7, B.9, I.8

Vraag	**Item**	**N**	**M**
23a	Internetrechercheren.	402	3,81
23b	Clearweb.	402	2,16
23	Deepweb.	402	2,62
23d	Darkweb.	402	3,74
23e	IP-adres.	402	4,22
23f	Domeinnaam.	402	4,02

Tabel VII.6 (vervolg): Gemiddelde scores voor kennisnorm R.7, B.9, I.8

Vraag	Item	N	M
24a	Ik weet hoe ik informatie moet vergaren op internet, bijvoorbeeld via zoekmachines en open bronnen.	402	3,73
24b	Ik weet wat OSINT (open source intelligence) inhoudt.	402	3,04
24c	Ik weet wat Intel (intelligence) inhoudt.	402	2,96
24d	Ik weet waar in de politieorganisatie de verantwoordelijkheid ligt voor informatievergaring op internet.	402	2,97
24e	Van een politiemedewerker wordt verwacht dat hij/zij zich actief op de hoogte stelt over ontwikkelingen in het omgaan met internetbronnen.	402	3,33
24f	Onderzoek op internet kent in potentie een groot afbreukrisico voor politieonderzoek.	402	3,51
24g	Bij het zoeken naar online-informatie laat je sporen achter.	402	4,21
24h	Ik weet welke sporen worden achtergelaten bij het zoeken naar online-informatie.	402	3,09
24i	Sporen die tijdens het zoeken naar informatie op verschillende plekken op internet worden achtergelaten, kunnen met elkaar in verband worden gebracht.	402	3,88
24j	Bij het gebruik van internet moeten werk en privé van elkaar worden gescheiden.	402	4,19
24k	Ik weet wat het verschil is tussen interne en externe IP-adressen.	402	3,31
24l	Ik weet wat een IPv4-adres is.	402	2,44
24m	Ik weet wat een IPv6-adres is.	402	2,42
24n	Het is mogelijk om op internet gevonden sporen veilig te stellen.	402	3,83
25a	Ik ken de algemene juridische regels van zoeken naar informatie op internet.	402	2,80
25b	Ik ken de beslisboom waarmee kan worden bepaald of een onderzoek uitgevoerd mag worden binnen de kaders van de taakstelling van de politie (artikel 3 Politiewet 2012).	402	2,53
25c	Ik weet dat er mogelijk verschil is in kwaliteit van gevonden informatie op internet.	402	3,34
25d	Ik ken de wetsartikelen die regels stellen voor informatievergaring op internet.	402	2,53
25e	Ik weet dat er bij een zoektocht op internet snel sprake kan zijn van stelselmatige observatie.	402	3,18
25f	Ik ken de privacywetgeving in relatie tot het zoeken en vastleggen van informatie van internet.	402	2,73
25g	Ik weet dat contacten leggen tijdens zoeken in internetbronnen altijd moet worden vermeden.	402	3,26
25h	Ik weet bij informatieverzoeken (vordering) of ik die zelf mag uitvoeren of dat die bevoegdheid bij een ander ligt.	402	3,19
26a	Ik weet wat bruikbare zoektermen zijn om informatie op internet te vinden.	402	3,01
26b	Ik weet wat zinvolle zoektermen zijn om een identificatie- / traceeractie te laten starten.	402	2,48
27a	Ik weet voldoende om met zoekmachines zoals Google te werken.	402	3,61
27b	Ik weet wat de risico's zijn van het gebruik van zoekmachines, zoals Google.	402	3,46
27c	Ik weet dat ik zoekoperatoren (zoals AND en OR) kan gebruiken om gericht informatie te zoeken.	402	2,65
28a	Ik weet wat iRN (internet Recherche Netwerk) is.	402	3,23
28b-1	Het gebruiken van een iRN computer minimaliseert het afbreukrisico van onderzoek doen op internet.	214	3,92
28b-2	iRN is een geschikte tool om online privézaken mee te regelen.	214	1,68
28b-3	Ik weet voldoende om met iRN te werken.	214	3,35
28b-4	Ik weet wat de risico's zijn van het gebruik van iRN.	214	3,35

Tabel VII.6 (vervolg): Gemiddelde scores voor kennisnorm R.7, B.9, I.8

Vraag	Item	N	M
29a	Ik weet welk type informatie je kunt vinden op welk type internetbron.	402	2,70
29b	Ik weet waar ik op internet moet zoeken om persoonsgegevens te achterhalen.	402	2,99
29c	Ik weet waar ik op internet moet zoeken om bedrijfsgegevens te achterhalen.	402	3,08
29d	Ik weet hoe ik als politiemedewerker zo weinig mogelijk sporen kan achterlaten bij het zoeken op internet.	402	2,60

Tabel VII.7: Gemiddelde scores voor kennisnorm B.10

Vraag	Item	N	M
30a	Ik weet van welke internettoepassingen burgers gebruik maken.	54	2,98
30b	Ik weet van welke internettoepassingen ik gebruik kan maken om met verschillende doelgroepen online in contact te treden.	54	2,89

Tabel VII.8: Gemiddelde scores voor kennisnorm I.4, I.5, I.6

Vraag	Item	N	M
31a	Bij het opnemen van een aangifte is het essentieel om de modus operandi (MO) zo uitgebreid mogelijk te registreren.	118	4,15
31b	Hacken is een basisdelict dat vaak verband houdt met andere delicten.	118	3,87
31c	Doorvragen bij een aangifte van een delict kan ertoe leiden dat meerdere delicten aan het licht komen.	118	4,19
31d	Ik weet welke digitale sporen geïnventariseerd kunnen worden voor het aanvullen van een aangifte.	118	2,94
32a	IP-adres verdachte.	118	4,14
32b	E-mailadres.	118	4,42
32c	Advertentienummer(s).	118	4,20
32d	Bitcoinadressen (wallets).	118	3,12
32e	Moneygram registratienummers.	118	2,56
33a	Ik weet hoe ik de 7 W's (wie, wat, waar, waarmee, welke wijze, wanneer, waarom) moet toepassen om de relevantie van digitale sporen te bepalen.	118	3,44
33b	Bij twijfel over de relevantie van digitale sporen moet een expert worden geraadpleegd.	118	4,37
34a	Ik weet wat 'vluchtige gegevens' zijn.	118	2,68
34b	Wanneer er sprake is van 'vluchtige gegevens', moet een expert worden ingeschakeld.	24	4,04
35a	Ik weet hoe veelvoorkomende digitale sporen veiliggesteld kunnen worden.	118	2,56
35b	Bij twijfel over hoe veelvoorkomende digitale sporen veiliggesteld kunnen worden, moet een expert worden ingeschakeld.	118	4,30
36a	Aanleveren van digitale sporen kan digitaal, op een cd/dvd.	118	1,88
36b	Aanleveren van digitale sporen kan digitaal, op een usb-stick.	118	1,94
36c	Aanleveren van digitale sporen kan digitaal, met print screens.	118	1,72
36d	Aanleveren van digitale sporen kan fysiek, met prints op papier.	118	1,68
36e	Aanleveren van digitale sporen kan fysiek, met foto's.	118	1,68