Wetenschappelijk Onderzoek- en Documentatiecentrum

Cahier 2022-8

# De hackbevoegdheid in de praktijk

*Een empirisch onderzoek naar de uitvoering van de hackbevoegdheid (artikelen 126nba, 126uba, 126zpa Sv)*

Wetenschappelijk onderzoek- en kennisinstituut voor het ministerie van Justitie en Veiligheid

Cahier 2022-8

# De hackbevoegdheid in de praktijk

*Een empirisch onderzoek naar de uitvoering van de hackbevoegdheid (artikelen 126nba, 126uba, 126zpa Sv)*

A. van Uden
C.A.J. van den Eeden

Met medewerking van:
J.J. van Berkel

**Cahier**
De reeks Cahier omvat de rapporten van onderzoek dat door en in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum is verricht. Opname in de reeks betekent niet dat de inhoud van de rapporten het standpunt van de Minister van Justitie en Veiligheid weergeeft.

# Inhoud

# Begrippenlijst

In deze lijst staat een opsomming gegeven van de belangrijkste begrippen inclusief een uitleg wat deze begrippen inhouden. Daarbij is niet altijd de juridische definitie gevolgd.

| | |
|---|---|
| Digit | Bij de inzet van de hackbevoegdheid heeft Digit (*Digital Intrusion Team*) een centrale rol. Digit zelf kent twee onderdelen: Digit-politie en Digit-OM. |
| Digit-Politie | De uitvoering van de hackbevoegdheid is in handen van Digit-politie, een deel van hen is het technisch team waarnaar in het wettelijk kader wordt verwezen. Digit-politie is een specialistisch team, ondergebracht bij de landelijke eenheid van de Nationale Politie. |
| Digit-OM | Digit-politie wordt aangestuurd door Digit-OM, ondergebracht bij het Landelijk Parket van het Openbaar Ministerie. Digit-OM bestaat uit twee personen: een officier van justitie en een parketsecretaris. Naast de aansturing door Digit-politie is Digit-OM voor alle betrokken factoren aanspreekpunt en vraagbaak. |
| Inzet | Digit zet de hackbevoegdheid in binnen een tactisch opsporingsonderzoek. |
| Tactisch team | Het tactisch team van de politie, bijvoorbeeld een team van de districtsrecherche of Team High Tech Crime, voert het opsporingsonderzoek uit waarin de inzet van Digit plaatsvindt. |
| Zaaksofficier | Het tactisch team werkt onder gezag van een tactisch zaaksofficier van justitie. |
| Centrale Toetsingscommissie (CTC) | De CTC is een intern adviesorgaan binnen het Openbaar Ministerie dat advies geeft aan het College van Procureurs-Generaal over onder andere de voorgenomen inzet van enkele bijzondere opsporingsbevoegdheden. |
| Geautomatiseerd werk | 'Een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken' (artikel 80sexies Sr). Voorbeelden van geautomatiseerde werken zijn servers, computers, routers, tablets en smartphones. |
| Technisch hulpmiddel | Een middel, doorgaans software, waarmee Digit data die relevant zijn voor een tactisch onderzoek (denk aan chatberichten, e-mails, |

| | |
|---|---|
| | geluidsbestanden), ophaalt bij de verdachte en opslaat in de digitale omgeving van Digit |
| Handmatige inzet | Indien geen technisch hulpmiddel wordt gebruikt door Digit, is sprake van een handmatige inzet. |
| Technische infrastructuur | Een technische voorziening van een technisch team bedoeld voor de vastlegging van gegevens ter uitvoering van een bevel. |
| Keuring en keuringsdienst | Technische hulpmiddelen moeten (voorafgaand aan de inzet ervan) worden gekeurd. Tijdens de keuring wordt gekeken of een technisch hulpmiddel voldoet aan de in het Besluit gestelde eisen met betrekking tot de betrouwbaarheid, integriteit en herleidbaarheid van gegevens. De Keuringsdienst, onderdeel van de Landelijke eenheid van de Nationale politie, neemt de keuring van technische hulpmiddelen voor haar rekening. |
| Kwetsbaarheid | Kwetsbaarheden zijn zwakke plekken in hard- of software waardoor het voor derden mogelijk kan worden om op een geautomatiseerd werk binnen te komen. Kwetsbaarheden moeten dan wel eerst gebruiksklaar gemaakt zijn. Drie soorten kwetsbaarheden kunnen worden onderscheiden: bekende, bekende onbekende en onbekende onbekende kwetsbaarheden. |
| Bekende kwetsbaarheid | Een bekende kwetsbaarheid is een kwetsbaarheid die bij een fabrikant van een product (bijvoorbeeld een telefoon) reeds bekend is. Dit soort kwetsbaarheden worden op diverse plekken op het internet gepubliceerd. Fabrikanten van deze producten ontwikkelen regelmatig updates om de bij hun bekende kwetsbaarheden te verhelpen. Zolang de fabrikant geen update beschikbaar stelt of de klant deze niet installeert, kan de politie de kwetsbaarheid gebruiken om een geautomatiseerd werk binnen te dringen. |
| Onbekende kwetsbaarheid | Een kwetsbaarheid die nog niet wordt verspreid en dus niet bij het grote publiek bekend kan zijn. Ook is er nog geen update voor de kwetsbaarheid beschikbaar, omdat de fabrikant nog niet de tijd heeft gehad (nul dagen) om die te ontwikkelen (NCTV, 2020). Tot het moment van verspreiden is sprake van een zero *day*. Ook zo'n kwetsbaarheid kan gebruikt worden om een geautomatiseerd werk binnen te dringen. |

| | |
|---|---|
| Bekende onbekende kwetsbaarheid | Bij een bekende onbekende kwetsbaarheid gaat het om een onbekende kwetsbaarheid die wel bekend is bij opsporingsinstanties, maar waarvan de fabrikant van een product nog niet op de hoogte is van het bestaan ervan. Daardoor is er een kleinere kans dat de fabrikant de kwetsbaarheid verhelpt en kan de politie er gebruik van maken (hoogstwaarschijnlijk langer dan dat dat het geval is bij een bekende kwetsbaarheid). |
| Onbekende onbekende kwetsbaarheid | Bij een onbekende onbekende kwetsbaarheid gaat het om een kwetsbaarheid die onbekend is, niet alleen bij de fabrikant van een product, maar ook bij opsporingsinstanties. Zo'n soort kwetsbaarheid kan zich bevinden in producten die opsporingsinstanties bij commerciële leveranciers aanschaffen om een geautomatiseerd werk binnen te komen. |

# Samenvatting

Op 1 maart 2019 is de Wet computercriminaliteit III (hierna Wet CCIII) in werking getreden. Met deze wet heeft de hackbevoegdheid een grondslag gekregen in het Wetboek van Strafvordering (artt. 126nba, 126uba en 126zpa Sv). De nieuwe bevoegdheid maakt het mogelijk dat opsporingsambtenaren, 'onder voorwaarden een geautomatiseerd werk, dat bij een verdachte in gebruik is, op afstand heimelijk [kunnen] binnendringen met het oog op bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten'. Na het binnendringen van een geautomatiseerd werk (bijvoorbeeld een telefoon of een server) mag de politie een beperkt aantal onderzoekshandelingen verrichten, namelijk A) de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan; B) de uitvoering van een bevel tot het opnemen van vertrouwelijke communicatie of het aftappen en opnemen van communicatie; C) de uitvoering van een bevel tot stelselmatige observatie; D) de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen; en E) de ontoegankelijkmaking van gegevens. Deze handelingen mogen alleen worden verricht door speciaal daartoe aangewezen opsporingsambtenaren die onderdeel uitmaken van een specialistisch team van de Landelijke Eenheid van de Nationale Politie. De Wet CCIII kent verder een aantal grondslagen om bij of krachtens Algemene Maatregel van Bestuur regels te stellen met betrekking tot de uitvoering van de hackbevoegdheid. Dat is bijvoorbeeld gebeurd in het Besluit onderzoek in een geautomatiseerd werk (hierna Besluit).
In dit rapport is het proces geëvalueerd rondom de uitvoering van de hackbevoegdheid in de eerste twee jaar na inwerkingtreding van de Wet CCIII. Aan het einde van 2024 volgt een rapport over het tweede deel van de evaluatie waarin de uitvoering van de volledige Wet CCIII centraal zal staan. De hoofdvraag in het huidige onderzoek was:

*Op welke wijze wordt in de praktijk uitvoering gegeven aan de hackbevoegdheid en welke eventuele knelpunten doen zich daarbij voor in de opsporingspraktijk?*

Om de onderzoeksvraag te beantwoorden is een combinatie van onderzoeksmethoden gebruikt: documentanalyse, interviewen en dossieranalyse. In deze samenvatting wordt een beschrijving gegeven van de belangrijkste bevindingen en conclusies. Eerst wordt stilgestaan bij het proces rondom de uitvoering van de hackbevoegdheid. Daarna wordt een aantal thema's uitgelicht waarbinnen zich knelpunten voordoen. Voorafgaand hieraan is het belangrijk om op te merken dat bij de (uitvoering van de) bevoegdheid zowel technische als tactische actoren betrokken zijn. Vanuit de technische kant is dat Digit (*Digital Intrusion Team*). Digit zelf kent twee onderdelen: Digit-politie en Digit-OM. De uitvoering van de hackbevoegdheid is in handen van Digit-politie, onderdeel van de Landelijke Eenheid van de Nationale Politie. Digit-politie wordt aangestuurd door Digit-OM dat ondergebracht is bij het Landelijk Parket van het Openbaar Ministerie. Een inzet van de hackbevoegdheid door Digit (hierna 'inzet') vindt plaats binnen een al lopend opsporingsonderzoek. Dat opsporingsonderzoek wordt uitgevoerd door een tactisch team van de politie (bijvoorbeeld een team van de districtsrecherche of Team High Tech Crime) onder gezag van een zaaksofficier van justitie. Deze zaaksofficier is eindverantwoordelijk voor het opsporingsonderzoek waarbinnen Digit een inzet doet en hij/zij dient verantwoording af te leggen in de rechtbank als een zittingsrechter de zaak behandelt.

## Proces inzet van de hackbevoegdheid

*Intake en toetsing*

De versleuteling van gegevens(dragers) is in dit onderzoek naar voren gekomen als een belangrijke reden voor tactische onderzoeksteams om de hackbevoegdheid in te willen zetten. Vaak zijn al veel andere (bijzondere) opsporingsbevoegdheden ingezet die niet hebben geleid tot het gewenste resultaat. Indien een tactisch team een inzet overweegt, wendt het team zich tot Digit. Niet elk verzoek leidt tot een inzet van de hackbevoegdheid. In de afgelopen twee jaar is aan het grootste deel van de verzoeken aan Digit (ruim twee derde) geen uitvoering gegeven. Hierbij speelden zowel technische als tactische argumenten een rol.
Indien een tactisch team zich meldt, volgt een uitgebreid intakeproces dat bestaat uit twee processen die deels op elkaar aansluiten en deels simultaan plaatsvinden: een operationeel proces en een procedure rondom de toetsing van de inzet. Binnen het operationele proces bekijkt Digit of een inzet technisch en tactisch haalbaar is. Indien dat geval is, gaat het tactisch team aan de slag met een (concept) aanvraagproces-verbaal voor de inzet van de bevoegdheid. Digit-OM leest hierbij mee. Digit-politie richt zich op het maken van een inschatting van de technische haalbaarheid van een inzet en de mogelijke afbreukrisico's.
Naast het operationele proces wordt voorafgaand aan de daadwerkelijke inzet van de hackbevoegdheid een uitgebreide, arbeidsintensieve toetsingsprocedure doorlopen. De voorgenomen inzet wordt onder andere besproken binnen de Centrale ToetsingsCommissie (CTC), een intern adviesorgaan binnen het Openbaar Ministerie. Tijdens de CTC-bijeenkomst wordt zowel aandacht besteed aan het tactische belang van de inzet van de bevoegdheid voor het opsporingsonderzoek (door de zaaksofficier) als aan de technische kant (indien nodig toegelicht door Digit-OM). Bij het overgrote deel van de verzoeken adviseert de CTC positief. Uiteindelijk moet er een machtiging van de rechter-commissaris komen op basis waarvan de zaaksofficier een bevel afgeeft aan Digit-politie. Gedurende het zojuist beschreven toetsingsproces speelt Digit-OM in overleg en samenspraak met Digit-politie voor alle betrokken actoren een belangrijke rol, als vraagbaak en adviseur. Dat geldt vooral voor de technische aspecten van een inzet. De rest van de betrokken actoren vaart op die deskundigheid. Dat deze verantwoordelijkheid op de schouders van één of twee personen rust, maakt de positie van Digit-OM kwetsbaar.

*Inzet van de bevoegdheid*

Zodra er een bevel is, gaat Digit aan de slag met de inzet. In de periode maart 2019 tot en met maart 2021 zijn in 26 opsporingsonderzoeken bevelen afgegeven. Dat betekent dat aan de minderheid van verzoeken vanuit tactische teams gehoor is gegeven. In tegenstelling tot wat de naam computercriminaliteit suggereert, is de afgelopen twee jaar de hackbevoegdheid vooral ingezet in opsporingsonderzoeken naar zwaardere vormen van traditionele criminaliteit zoals (poging tot) moord, zaken rondom verdovende middelen, valsheid in geschrifte, witwassen, zeden, terrorisme en lidmaatschap van een criminele organisatie. Slechts bij één inzet was sprake van een misdrijf in de categorie cybercriminaliteit in enge zin.
Inzetten van Digit kunnen ook worden verlengd. Dat is bij het grootste deel van de inzetten gebeurd. Vaak heeft het tactisch team aanvullende gegevens nodig naar aanleiding van de gegevens die al verzameld zijn. Inmiddels is binnen Digit de afspraak gemaakt dat inzetten niet voor langere tijd verlengd kunnen worden (in principe maximaal twee keer vier weken). Een inzet wordt niet altijd verlengd,

bijvoorbeeld als een verdachte aangehouden wordt of als het onderzoek te weinig informatie oplevert. Bij de beslissing of een inzet verlengd wordt, zijn dezelfde actoren betrokken die zich bezighouden met de vraag of een inzet überhaupt binnen een opsporingsonderzoek mag plaatsvinden, inclusief het daarbij behorende tijdpad.

Digit heeft een poging tot binnendringen gedaan en/of is binnengedrongen op zes typen geautomatiseerde werken (telefoon, telefoon in combinatie met een ander geautomatiseerd werk, server, router, laptop en *wireless access point*). Gedurende de onderzoeksperiode zijn vooral telefoons onderwerp van onderzoek geweest. Voor die inzetten (hierna 'standaardinzetten') is inmiddels een min of meer standaardwerkwijze ontwikkeld waarbij gebruik wordt gemaakt van een commercieel middel. Bij de overige inzetten (hierna 'maatwerkinzetten') bedenkt Digit per geval hoe zij het beste kan binnendringen en onderzoekshandelingen kan verrichten. Dat soort inzetten zijn voor Digit arbeidsintensiever. Meestal beperkt een geautomatiseerd werk waarop wordt binnengedrongen zich tot één of twee apparaten.
Nadat is binnengedrongen, verricht Digit een aantal onderzoekshandelingen, vastgelegd in subA t/m E (zie eerder). Bij de standaardinzetten wordt vaak gekozen voor een combinatie van onderzoekshandelingen: vaststellen van kenmerken (subA), opnemen vertrouwelijke communicatie en/of tappen (subB), stelselmatige observatie (subC) en het vastleggen van gegevens (subD). Deze combinatie wordt gezien als logische keuze, omdat in de telefoon veel informatie te vinden is over het doen en laten van een verdachte, zowel in het verleden als in het heden. Bij de maatwerkinzetten liggen de uit te voeren onderzoekshandelingen minder voor de hand. Bij deze inzetten lijkt vooral gekozen te worden voor het vaststellen van kenmerken (subA) en het vastleggen van gegevens (subD), met soms (daarna) de ontoegankelijkmaking van gegevens (subE).

Digit verricht onderzoekshandelingen zowel met een technisch hulpmiddel als handmatig. Een technisch hulpmiddel zorgt er kort gezegd voor dat data die relevant zijn in het kader van een tactisch opsporingsonderzoek (denk aan chatberichten, e-mails, geluidsbestanden) opgehaald worden bij de verdachte en worden opgeslagen in de digitale omgeving van Digit. Indien geen technisch hulpmiddel wordt gebruikt, is sprake van een handmatige inzet. Door Digit ontwikkelde technische hulpmiddelen worden, in lijn met het wettelijk kader, gekeurd door de Keuringsdienst, onderdeel van de Landelijke Eenheid van de Nationale Politie. De Keuringsdienst beoordeelt aan de hand van een keuringsprotocol deze technische hulpmiddelen. Dit protocol is gebaseerd op een aantal artikelen in het Besluit dat tot doel heeft ervoor te zorgen dat een technisch hulpmiddel in staat is om op een betrouwbare, integere en herleidbare manier gegevens te verzamelen. Op die manier kan bijvoorbeeld met meer zekerheid worden gesteld dat de verzamelde gegevens daadwerkelijk op het geautomatiseerde werk van een verdachte hebben gestaan. Goedkeuring van een technisch hulpmiddel betekent dat, mocht een zittingsrechter de zaak inhoudelijk behandelen, geen uitleg hoeft te worden gegeven over de precieze werking van het hulpmiddel. Zo kunnen de gehanteerde onderzoeksmethoden worden afgeschermd. Bij een handmatige inzet dient wel uitleg te worden gegeven over de werkwijze die gehanteerd is.

De keuring van een technisch hulpmiddel is een belangrijke waarborg voor de controle op de inzet van de bevoegdheid. Dat geldt ook voor het toezicht door de Inspectie Justitie en Veiligheid (hierna Inspectie). Sinds de inwerkingtreding van de wet houdt de Inspectie toezicht op de uitvoering van de hackbevoegdheid. Het is de bedoeling dat dit systeemtoezicht betreft wat betekent dat de Inspectie toezicht houdt op het functioneren van het wettelijk systeem. Deze vorm van toezicht is er gekomen, omdat

er gedurende het wetgevingstraject zorgen waren over het feit dat niet alle zaken waarin een inzet heeft plaatsgevonden, voorgelegd zullen worden aan een zittingsrechter. Bovendien bestonden er vragen over de technische deskundigheid van de zittingsrechter.

*Afronding inzet en opbrengst*

Een inzet wordt beëindigd als een bevel is uitgevoerd, of anders uiterlijk op de laatste dag van de looptijd van het bevel. Na beëindiging van een inzet wordt het technisch hulpmiddel doorgaans (zo goed als) volledig verwijderd. Daarna worden de verzamelde gegevens overgedragen aan het tactisch team. Bij de overdracht van gegevens kijkt Digit in principe niet of er geheimhoudersgegevens aanwezig zijn. Het is aan het tactisch team om dat te controleren. Geheimhoudersgegevens zijn gegevens die bijvoorbeeld betrekking hebben op de communicatie van de verdachte met zijn of haar advocaat. Op grond van artikel 126aa Sv moeten dit soort gegevens worden vernietigd. Vanuit Digit wordt echter aangegeven dat op dit moment tegenstrijdige regelgeving bestaat. De vernietiging op basis van artikel 126aa Sv zou in strijd zijn met artikel 28 van het Besluit waarin onder andere staat genoemd dat de inhoud van de op de technische infrastructuur vastgelegde gegevens in principe niet mag worden gewijzigd. Wanneer een deel van de gegevens uit een bestand wordt verwijderd, zou dat invloed hebben op de integriteit van een bestand. Op basis van de toelichting op het Besluit moet dat worden uitgesloten. Digit-OM heeft daarom tot nu toe besloten dat geheimhoudersgegevens niet definitief verwijderd worden.
Van elke inzet stelt Digit een aantal processen-verbaal op. De afgelopen tijd is Digit bezig geweest met het op orde brengen hiervan. Vanuit Digit-OM is wat betreft het verbaliseren het kader meegegeven om minimaal te verbaliseren in verband met de afscherming van opsporingsmethoden. Een 'slimme lezer' van een proces-verbaal zou, op basis van de informatie in het proces-verbaal, niet in staat moeten zijn zich te verdedigen tegen de technische hulpmiddelen die Digit inzet. Verder dient Digit in haar eigen interne systemen gedetailleerd bij te houden wat zij gedaan heeft ('maximaal journaliseren').

Voor dit onderzoek is een beperkt aantal inzetten meer diepgaand bestudeerd. Daaruit blijkt dat de bevoegdheid in die zaken tot nu toe vooral sturingsinformatie oplevert. De verzamelde gegevens leveren, in tegenstelling tot sommige verwachtingen, tot nog toe niet *het* bewijs op binnen een opsporingsonderzoek. Verder heeft een zittingsrechter, voor zover bekend, nog geen enkele inzet inhoudelijk behandelt. Bij een deel ervan zal dat ook nooit gebeuren, bijvoorbeeld omdat er in een zaak geen verdachte is of omdat de bevoegdheid (en ook andere bevoegdheden) onvoldoende belastende informatie heeft opgeleverd. Daardoor kunnen op dit moment (nog) geen uitspraken worden gedaan over de waardering van de nieuwe bevoegdheid als bewijsmiddel: dragen de middels de hackbevoegdheid verzamelde gegevens bij aan de bewijsvoering in een strafzaak?

In het voorgaande is het proces beschreven rondom de uitvoering van de hackbevoegdheid. Hierbij is al een aantal knelpunten naar voren gekomen dat zich voordoet in de opsporingspraktijk. In de komende paragrafen wordt een aantal thema's meer gedetailleerd toegelicht, omdat zich daarbinnen (ook) knelpunten voordoen/zich hebben voorgedaan.

## Binnendringen

Het is de bedoeling dat de bevoegdheid heimelijk en op afstand wordt ingezet. In de praktijk is het voor het binnendringen soms nodig om op locatie, in de buurt van het geautomatiseerde werk, aanwezig te zijn. De wetgever lijkt met deze optie geen rekening te hebben gehouden. Om toch in de buurt van een geautomatiseerd werk te kunnen zijn, moet Digit soms gebruikmaken van een (bijzondere) opsporingsbevoegdheid. Van zo'n opsporingsbevoegdheid kan alleen gebruik worden gemaakt als die toevallig al door een tactisch team in het opsporingsonderzoek wordt ingezet. Deze afhankelijkheid van een tactisch team vormt voor Digit een knelpunt, omdat een tactisch team niet altijd van plan is zo'n bevoegdheid in te zetten. Daarom heeft Digit behoefte aan een steunbevoegdheid, vergelijkbaar met de wijze waarop dit geregeld is rondom het opnemen van vertrouwelijke communicatie (artikel 126l Sv). Daarnaast bestaat de wens vanuit Digit-OM om de inzet van deze steunbevoegdheid buiten het procesdossier te kunnen houden vanwege de afscherming van de gehanteerde methodes. De vraag is dan wel in hoeverre met die heimelijkheid nog voldoende beoordeeld kan worden of een inzet proportioneel is, bijvoorbeeld in verband met eventuele ongewenste gevolgen van een binnendringactie. Indien op geen enkele plek hierover verantwoording wordt afgelegd (de methode wordt immers afgeschermd) en feitelijk maar een beperkt aantal mensen een beslissing neemt over de wijze van binnendringen, kan de vraag worden gesteld of die beoordeling over de proportionaliteit op voldoende plekken wordt gemaakt.

*Kwetsbaarheden en meldplicht*

Om te kunnen binnendringen maakt Digit gebruik van kwetsbaarheden in geautomatiseerde werken. Kwetsbaarheden zijn zwakke plekken in hard- of software waardoor het voor derden mogelijk kan worden om op een geautomatiseerd werk binnen te komen. Om te kunnen binnendringen moeten kwetsbaarheden wel eerst gebruiksklaar gemaakt zijn. Drie soorten kwetsbaarheden kunnen worden onderscheiden: bekende, bekende onbekende kwetsbaarheden en onbekende onbekende kwetsbaarheden. Een bekende kwetsbaarheid is een kwetsbaarheid die bij een fabrikant van een product (bijvoorbeeld een telefoon) reeds bekend is. Dit soort kwetsbaarheden worden op diverse plekken op het internet gepubliceerd. Fabrikanten van deze producten ontwikkelen regelmatig updates om de bij hun bekende kwetsbaarheden te verhelpen. Zolang de fabrikant geen update beschikbaar stelt of de klant deze niet installeert, kan de politie de kwetsbaarheid gebruiken. Een onbekende kwetsbaarheid (zowel 'bekend onbekend' als 'onbekend onbekend') is een kwetsbaarheid die nog niet via het internet wordt verspreid en dus niet bij het grote publiek bekend kan zijn. Ook is er nog geen update beschikbaar. Tot het moment van verspreiden is sprake van een zero *day*. Ook zo'n kwetsbaarheid kan gebruikt worden om een geautomatiseerd werk binnen te dringen. Bij een bekende onbekende kwetsbaarheid gaat het om een kwetsbaarheid die wel bekend is bij opsporingsinstanties, maar waarvan de fabrikant van een product nog niet op de hoogte is van het bestaan ervan. Daardoor is er een kleinere kans dat de fabrikant de kwetsbaarheid verhelpt en kan de politie er gebruik van maken (hoogstwaarschijnlijk langer dan dat dat het geval is bij een bekende kwetsbaarheid). Bij een onbekende onbekende kwetsbaarheid gaat het om een kwetsbaarheid die ook niet bekend is bij opsporingsinstanties. Zo'n soort kwetsbaarheid kan zich bevinden in producten die opsporingsinstanties bij commerciële leveranciers aanschaffen om een geautomatiseerd werk binnen te komen.

Rondom het gebruik van kwetsbaarheden zijn door verschillende partijen zorgen geuit, vooral omdat het bestaan en gebruik van deze kwetsbaarheden computersystemen onveiliger zouden maken. Vanuit het kabinet is de verwachting uitgesproken dat de politie vooral bekende kwetsbaarheden benut, maar dat het gebruik van een onbekende kwetsbaarheid wordt gezien als 'een uiterste maar onmisbare optie voor de bestrijding van ernstige vormen van criminaliteit'. In verband met zorgen over veiligheidsaspecten is (op indirecte wijze) een meldplicht ten aanzien van onbekende kwetsbaarheden afgesproken (voortkomend uit artikel 126ffa Sv waarin geregeld is dat het melden van een onbekende kwetsbaarheid uitgesteld mag worden, na een schriftelijke machtiging van een rechter-commissaris). Door een kwetsbaarheid te melden zou de (online) veiligheid verhoogd worden, omdat deze kwetsbaarheid niet langer misbruikt kan worden (ervan uitgaande dat de fabrikant de kwetsbaarheid verholpen heeft). Op producten aangeschaft bij een commerciële leverancier is de meldplicht niet van toepassing. Een leverancier van dit soort producten geeft doorgaans niets prijs over de samenstelling van zijn product, waardoor voor degene die het product aanschaft onbekend is van welke (soort) kwetsbaarheid gebruik is gemaakt. Als gevolg daarvan kan dan geen melding worden gedaan. De meldplicht geldt dus alleen voor bekende onbekende kwetsbaarheden.

De zojuist beschreven meldplicht vormt voor Digit een belangrijk knelpunt. In de eerste plaats omdat de meldplicht ook geldt voor kwetsbaarheden in systemen die specifiek gemaakt zijn voor en door personen met criminele intenties. Dat betekent dat deze personen uiteindelijk op de hoogte moeten worden gesteld dat in hun systeem, vrijwel alleen gebruikt voor criminele doeleinden, zich een kwetsbaarheid bevindt. Dit roept de vraag op in hoeverre het melden van dit soort kwetsbaarheden zorgt voor meer veiligheid. Het lijkt er eerder op dat personen met criminele intenties in dit soort gevallen juist de gelegenheid krijgen om hun afscherming beter op orde te brengen. Ten tweede kan de meldplicht samenwerking met nationale, maar ook internationale partijen bemoeilijken. In sommige landen is het gebruik van een kwetsbaarheid staatsgeheim. Als Nederland met dat soort landen zou willen samenwerken, is dat problematisch omdat Nederland de verplichting heeft om hetgeen staatsgeheim is in het buitenland, in Nederland te melden. Het risico hiervan is dat die kwetsbaarheid niet langer bruikbaar is en samenwerking voor die landen erg onaantrekkelijk wordt.

*Commerciële producten*

Hoewel het gebruik van een onbekende kwetsbaarheid werd gezien als 'uiterste optie', heeft Digit bij het overgrote deel van haar inzetten gebruikgemaakt van een commercieel product (en dus onbekende onbekende kwetsbaarheden). Dat product wordt gebruikt voor de standaardinzetten en met het product kan de politie zowel binnendringen als onderzoekshandelingen verrichten. Voor Digit is het gebruik van dit product onmisbaar, omdat zij anders een groot deel van de inzetten niet zou kunnen doen. Hiervoor is een aantal redenen genoemd. Eén van de redenen is dat het zelf vinden van een onbekende kwetsbaarheid in een geautomatiseerd werk, dat door nagenoeg alle Nederlanders wordt gebruikt, heel erg lastig is. Een andere reden is de meldplicht. Mocht het al lukken om zelf een onbekende kwetsbaarheid te vinden en gebruiksklaar te maken, dan moet deze gemeld worden. Dat betekent dat die kwetsbaarheid, waarin veel tijd is gaan zitten om hem gebruiksklaar te maken, slechts een heel beperkt aantal keren kan worden gebruikt.
Uit het Regeerakkoord 2017-2021 volgt dat het gebruik van een commercieel product dient te worden beperkt om de markt van onbekende kwetsbaarheden niet te

stimuleren. Daarom is afgesproken dat per zaak een licentie moet worden aangeschaft, in plaats van dat één keer het product wordt aangeschaft dat vervolgens voor meerdere inzetten kan worden benut. Omdat dit product in de praktijk juist bij veel inzetten is gebruikt, wordt geschat dat deze afspraak ertoe heeft geleid dat inmiddels ruim twee keer de aanschafprijs voor het product betaald is. Ingeschat wordt dat het gaat om 'enkele miljoenen'. Gezien het relatief grote aantal inzetten waarin dit hulpmiddel wordt ingezet, is het onwaarschijnlijk dat het afgesproken licentiemodel ervoor zorgt dat de markt van onbekende kwetsbaarheden minder gestimuleerd wordt.

## Technische hulpmiddelen

Digit gebruikt twee soorten technische hulpmiddelen: commerciële producten (zojuist besproken) en eigen door Digit-politie ontwikkelde hulpmiddelen. Daarnaast kan zoals gezegd handmatig gewerkt worden. Over de reikwijdte van het begrip technisch hulpmiddel (en de handmatige inzet) bestaat discussie, vooral tussen Digit en de Inspectie. De vraag of iets wel of geen technisch hulpmiddel is, is relevant omdat alleen een technisch hulpmiddel gekeurd dient te worden en Digit ziet de keuring als een groot knelpunt in de uitvoering (zie over de keuring zelf de volgende paragraaf). Slechts bij een klein aantal inzetten heeft Digit gebruik kunnen maken van een eigen ontwikkeld technisch hulpmiddel. Een belangrijke reden hiervoor is dat het veel tijd kost om een hulpmiddel te ontwikkelen èn uiteindelijk goedgekeurd te krijgen. Die lange doorlooptijd zorgt ervoor dat Digit slechts een klein aantal eigen ontwikkelde hulpmiddelen heeft kunnen gebruiken.
Tot nu toe is voor elke inzet een 'nieuw' technisch hulpmiddel gebruikt, omdat een nieuwe inzet vaak vraagt om een aantal aanpassingen aan het technisch hulpmiddel. Bij Digit bestaat de wens om een aantal standaardcomponenten te ontwikkelen die reeds (goed)gekeurd zijn. Deze kunnen dan in vrij korte tijd worden aangevuld, afhankelijk van de onderzoekwensen bij een specifieke inzet. Er ontstaat dan een technisch hulpmiddel met deels al (goed)gekeurde componenten, dat in een concrete zaak kan worden ingezet. Deze opzet is vooralsnog lastig gebleken, omdat bij de keuringen dit onderscheid niet wordt gemaakt en elk hulpmiddel wordt gezien als een nieuw middel dat volledig gekeurd moet worden, inclusief de daarbij behorende keuringstermijnen.
In de opsporingspraktijk wordt momenteel vaker dan in de begintijd overwogen een handmatige inzet te doen. Bij een handmatige inzet dient Digit haar werkwijze uitgebreider te verantwoorden, zodat op die manier met meer zekerheid kan worden gezegd dat met de werkwijze betrouwbare, integere en herleidbare gegevens zijn verzameld. Dat betekent wel dat de werkwijze niet volledig afgeschermd kan blijven. Niet in alle gevallen wordt dat door Digit als problematisch gezien.

## Keuring technische hulpmiddelen

De keuring van technische hulpmiddelen vormt voor Digit een groot knelpunt. Dat heeft te maken met het feit dat de twee betrokken actoren (Keuringsdienst en Digit) vanuit verschillende perspectieven naar het keuringsproces kijken. Deze perspectieven botsen in de uitvoeringspraktijk soms met elkaar. Vanuit het perspectief van de Keuringsdienst staan vooral de regels uit het Besluit centraal en de daaruit voortvloeiende keuringseisen. Dat betekent onder andere dat een hulpmiddel, in lijn met het Besluit, alleen kan worden goedgekeurd als aan alle eisen wordt voldaan, al

dan niet aangevuld met een aantal (extra) vervangende waarborgen. Op die manier kan met zekerheid worden gesteld dat de gegevens die verzameld zullen worden met het technisch hulpmiddel betrouwbaar, integer en herleidbaar zijn. Dit perspectief botst soms met het perspectief van waaruit Digit het keuringsproces benadert. Binnen dit perspectief staan vooral de uitvoerbaarheid en de noodzakelijkheid van de regels uit het Besluit centraal en de daaruit voortvloeiende keuringseisen in het keuringsprotocol. Digit is kritisch ten opzichte van de keuring door de Keuringsdienst, omdat deze niet goed zou passen bij de hulpmiddelen die Digit ontwikkelt. Inherent aan software, en dus aan de middelen die Digit gebruikt, is bijvoorbeeld dat met enige regelmaat een update plaatsvindt. Dat is anders dan bij fysieke hulpmiddelen, zoals bakens, en het is de vraag in hoeverre de Keuringsdienst daar rekening mee moet en kan houden, zeker wanneer een hulpmiddel vooraf goedgekeurd dient te worden. Dat laatste vloeit voort uit de toelichting op het Besluit. Naast de uitvoerbaarheid wordt ook de noodzakelijkheid van de regels en eisen kritisch bekeken door Digit. In tegenstelling tot hoe de Keuringsdienst het keuringsproces bekijkt is het volgens Digit niet nodig dat een technisch hulpmiddel aan alle keuringseisen voldoet. Daarom zou er, geredeneerd vanuit het perspectief van Digit, (meer) ruimte moeten zijn om rekening te kunnen houden met bewijswaardes en risicoanalyses. Rekening houden met bewijswaardes betekent dat het niet per se problematisch hoeft te zijn als een hulpmiddel niet volledig is goedgekeurd. In de rechtszaal zou hier verantwoording over kunnen worden afgelegd. De consequentie hiervan is wel dat een opsporingsmethode niet meer volledig afgeschermd zal blijven. Vervolgens is het aan de rechter, eventueel na raadpleging van deskundigen, om het verzamelde bewijs op waarde te schatten. Dat vraagt wel dat een zaak waarin een inzet plaatsvond voor de rechter komt en dat een rechtbank over voldoende technische deskundigheid beschikt om deze inschatting te kunnen maken. Hoogstwaarschijnlijk zullen niet alle zaken inhoudelijk behandeld worden door een zittingsrechter. Daarnaast is het de vraag of de benodigde technische deskundigheid op dit moment voldoende aanwezig is. Verder betekent het centraal stellen van risicoanalyses dat veel meer uitgegaan zou moeten worden van de vraag wat het risico is als niet aan een bepaalde eis uit het keuringsprotocol wordt voldaan, in plaats van dat het hulpmiddel voor goedkeuring aan die eis moet voldoen.

*Moment van keuren en waarborgen*

In de afgelopen jaren is het Digit nauwelijks gelukt om een vooraf goedgekeurd technisch hulpmiddel in te zetten, vooral in verband met de (lange) ontwikkeltijd die hiermee gepaard gaat. In de nota van toelichting op het Besluit staat zoals gezegd beschreven dat dat in principe wel zou moeten. Die ontwikkeltijd staat op gespannen voet met het dringende opsporingsbelang waarvan sprake moet zijn om de bevoegdheid überhaupt in te mogen zetten. Het is dan ook de vraag of het altijd realistisch is om te eisen dat een vooraf goedgekeurd hulpmiddel dient te worden ingezet. In het Besluit is ook de mogelijkheid opengehouden om een hulpmiddel achteraf ter keuring aan te bieden of een keuring volledig achterwege te laten. Dat laatste zou een uitzondering moeten zijn. In de praktijk is dat niet het geval. De Digit-officier van justitie heeft geoordeeld dat de aard van een veelvuldig gebruikt commercieel hulpmiddel zich tot nu toe verzet tegen een keuring. Dat betekent dat aan één van de waarborgen, namelijk de keuring, bij een groot deel van de inzetten niet wordt voldaan. Wel is er in die gevallen aandacht voor het nemen van aanvullende technische en tactische waarborgen (zie volgende alinea). In de praktijk is overigens gebleken dat dat middel hoogstwaarschijnlijk ook niet goedgekeurd kan worden. Het middel maakt namelijk gebruik van een server waartoe de leverancier toegang heeft. Weliswaar worden de verzamelde gegevens, zoals chatberichten van de verdachte,

uiteindelijk op de server van Digit opgeslagen, maar dat neemt niet weg dat ook de leverancier gedurende het binnendringen en uitvoeren van onderzoekshandelingen (in theorie) toegang heeft tot de gegevens van een verdachte. Hoewel contractuele afspraken zijn gemaakt dat de leverancier deze gegevens niet mag inzien en alleen toegang mag hebben tot de server voor het onderhoud van zijn product, kan niet worden uitgesloten dat de leverancier ook op andere momenten zichzelf toegang verschaft tot de server. Alleen om die reden al kan het middel niet goedgekeurd worden. Vanuit Digit wordt beredeneerd dat een leverancier zich nooit op eigen initiatief toegang zal verschaffen tot de server om gegevens in te zien, omdat er afspraken over zijn gemaakt. Het schenden daarvan maakt de kans op reputatieschade te groot en de financiële risico's die dat met zich meebrengt te hoog. Toch betekent dit dat de betrouwbaarheid en de integriteit van de verzamelde gegevens in het gedrang kunnen komen.
Indien de Digit-officier besluit dat de aard van een technisch hulpmiddel zich verzet tegen een keuring, dan dienen waarborgen aanwezig te zijn om ervoor te zorgen dat de verzamelde gegevens betrouwbaar, herleidbaar en integer zijn. In de toelichting op het Besluit blijkt dat het daarbij vooral kan gaan om technische waarborgen. Deze aanvullende waarborgen dient de officier van justitie te verantwoorden in het procesdossier. In de opsporingspraktijk wordt niet alleen gezorgd voor aanvullende technische waarborgen, maar ook voor aanvullende tactische waarborgen. Bij die laatste soort waarborgen gaat het om maatregelen die het tactisch team neemt om gegevens verkregen met het niet gekeurde technisch hulpmiddel te kunnen verifiëren. In het Besluit wordt er geen rekening mee gehouden dat dat soort maatregelen genomen kan worden en in de praktijk ook genomen wordt. Dit roept de vraag op of het niet mogelijk is – voordat een zittingsrechter dat kan doen – met dit soort waarborgen rekening te houden bij een beoordeling van de betrouwbaarheid, herleidbaarheid en integriteit van de verzamelde gegevens.

## Toezicht door de Inspectie

De Inspectie houdt zoals gezegd toezicht op de uitvoering van de hackbevoegdheid. In de uitvoeringspraktijk doet zich een aantal knelpunten voor waardoor het toezicht door de Inspectie in de praktijk niet zonder discussie verloopt. Naar aanleiding van de Verslagen van de Inspectie is Digit begonnen een aantal elementen binnen haar werkwijze te verbeteren. Toch heeft Digit besloten een aantal door de Inspectie gesignaleerde punten, bijvoorbeeld het registratieproces rondom de uitgifte van technische hulpmiddelen, naast zich neer te leggen. Dat heeft te maken met het feit dat Digit deze punten binnen het Besluit niet goed uitvoerbaar vindt. De Inspectie richt zich echter op de wijze waarop Digit volgens het wettelijk kader zou moeten handelen, omdat het aan de wetgever is een oordeel te vellen over de uitvoerbaarheid van dat wettelijk kader (en of aanpassing nodig is). Geen oog voor de uitvoerbaarheid betekent dat de eisen uit het Besluit waarvan Digit besloten heeft dat zij daaraan niet zal (kunnen) voldoen, punten zullen zijn die de Inspectie zal blijven constateren en waarmee Digit op haar beurt niets zal doen. Een dergelijke patstelling roept de vraag op of de beoogde effecten van het toezicht behaald kunnen worden en wat de consequenties zijn als de Inspectie iets constateert en Digit besluit om daar verder niets mee te doen.

Het tweede knelpunt betreft de reikwijdte van het toezicht. De Inspectie houdt toezicht op het handelen van de politie en niet op dat van het Openbaar Ministerie. Het handelen van de Digit-officier en van Digit-politie is in de praktijk echter onlosmakelijk

met elkaar verbonden en beide zijn daardoor lastig uit elkaar te trekken. Digit-OM stelt zich op het standpunt dat nagenoeg alle handelingen die Digit verricht onder het gezag van de officier van justitie plaatsvinden en dat om die reden de Inspectie niets over die handelingen te zeggen heeft. De Inspectie vindt dat zij daar wel degelijk toezicht op kan houden, omdat Digit-politie deze handelingen uitvoert en soms Digit-OM hierover adviseert. Bovendien zou de beperkte invulling van het toezicht, zoals Digit-OM het ziet, ervoor zorgen dat de Inspectie bijna nergens meer uitspraken over kan doen. Om die reden is het wenselijk dat er meer duidelijkheid komt wie nu toezicht houdt en op welke onderwerpen de Inspectie toezicht houdt. Met deze gesprekken is reeds een begin gemaakt.

Een derde knelpunt gaat over de vraag wat nodig is om goed systeemtoezicht uit te kunnen voeren. In de wetsgeschiedenis wordt niet veel gezegd over *hoe* dat systeemtoezicht zou moeten plaatsvinden, behalve dat de Inspectie naar individuele zaken kan kijken. Juist de *hoe*-vraag levert in de uitvoeringspraktijk problemen op. De Inspectie wil zich bij haar toezicht kunnen baseren op interne kwaliteitssystemen van Digit. Dit is in lijn met de wijze waarop systeemtoezicht door de Inspectieraad gedefinieerd wordt. Op het moment van schrijven van dit rapport is zo'n kwaliteitssysteem niet (volledig) aanwezig. Bovendien blijkt er onduidelijkheid te bestaan over de vraag wat een kwaliteitssysteem precies inhoudt. In de nabije toekomst zou het daarom goed zijn om te kijken naar wat in de praktijk georganiseerd moet worden om het systeemtoezicht van de grond te krijgen.

### Inzetten met een internationale component

In een OM-aanwijzing (Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex. artikel 126 nba Sv) wordt geregeld hoe gehandeld dient te worden als gegevens zich op buitenlands grondgebied bevinden. Digit is in de onderzochte periode betrokken geweest bij een beperkt aantal inzetten met een internationale component. Het gaat hierbij om inzetten vanuit Nederland in het buitenland en om inzetten vanuit het buitenland in Nederland.
Wat betreft standaardinzetten is in principe de afspraak dat niet op een telefoon wordt binnengedrongen die zich in het buitenland bevindt. Voor de maatwerkinzetten is het wel of niet inzetten van de bevoegdheid afhankelijk van de relatie met het betreffende land.
De OM-aanwijzing richt zich op inzetten in het buitenland, maar is niet altijd toereikend. Dat geldt bijvoorbeeld indien veel verschillende geautomatiseerde werken in het spel zijn zoals bij een botnet. In het geval van de OM-aanwijzing wordt afgeweken, wordt de Minister van Justitie en Veiligheid geïnformeerd. Inzetten met een internationale component kunnen vooral politiek ingewikkeld zijn.
Inzetten door het buitenland in Nederland zijn op dit moment niet geregeld, ook niet in de OM-aanwijzing. Voor de uitvoeringspraktijk is dat ingewikkeld, omdat in die gevallen complexe juridische constructies moeten worden bedacht waarbinnen verschillende rechtshulpverzoeken over en weer worden ingediend. Een ander meer praktisch punt is dat voor inzetten door het buitenland geen verlofprocedure is afgesproken, terwijl die voor andere bijzondere opsporingsbevoegdheden wel bestaat. Zo'n verlofprocedure houdt in dat, indien het buitenland een bijzondere opsporingsbevoegdheid in Nederland wil inzetten en daar toestemming voor is, de rechter-commissaris toestemming moet geven voor de daadwerkelijke overdracht van gegevens die met de bijzondere opsporingsbevoegdheid verzameld zijn. Dit is ter controle van een rechtmatige toepassing van de bevoegdheid.

## Functiescheiding

Uit de wetsgeschiedenis blijkt dat sprake dient te zijn van strikte functiescheiding. Die functiescheiding moet onder andere voorkomen dat het tactisch team Digit beïnvloedt als zij afwegingen maakt ten aanzien van de haalbaarheid van een inzet en de uitvoering ervan. In de praktijk vindt tussen het technisch en het tactisch team regelmatig overleg en informatie-uitwisseling plaats, zowel voordat de bevoegdheid wordt ingezet als gedurende de inzet. Juist voor een goede uitvoering, zo laat dit onderzoek zien, is Digit afhankelijk van de informatie van het tactisch team. Een inzet van Digit is minder goed uit te voeren zonder dat overleg. Daarom is functiescheiding in het licht van de hackbevoegdheid een problematisch concept.

## Tot besluit

Dit eerste evaluatieonderzoek heeft zich vooral gericht op het proces rondom de uitvoering van de hackbevoegdheid door Digit. In tegenstelling tot de meer technische kant van een inzet is minder aandacht besteed aan wat de inzet van deze nieuwe bevoegdheid praktisch betekent voor de aanvragende tactische teams en welke meerwaarde de inzet kan hebben voor een opsporingsonderzoek. Dat onderwerp zal uitgewerkt worden in het tweede deel van de evaluatie. In deel 2 van de evaluatie wordt verder beoogd meer aandacht te hebben voor zaken die een zittingsrechter inhoudelijk behandeld heeft en waarin gegevens inhoudelijk zijn gewogen. Indien voorhanden wordt in deze rechterlijke uitspraken wellicht meer duidelijk over de vragen en dilemma's die op basis van dit eerste onderzoek naar voren zijn gekomen. Daarnaast zal in het tweede deel van de evaluatie nader worden ingegaan op de andere onderdelen van de Wet CCIII.
Op basis van deze eerste evaluatie is echter wel al een aantal knelpunten naar voren gekomen waarvan duidelijk is dat die de uitvoering van de bevoegdheid bemoeilijken en waaraan nu al iets gedaan zou kunnen worden: 1) de manier waarop kan worden binnengedrongen, 2) de inzet van commerciële middelen, 3) de meldplicht, 4) het toezicht door de Inspectie en 5) de keuring van technische hulpmiddelen.
Ten eerste het binnendringen. Binnendringen dient heimelijk en op afstand plaats te vinden. De praktijk laat zien dat bij de uitvoering van de hackbevoegdheid de politie niet altijd volledig op afstand kan blijven. In dat soort situaties zou een steunbevoegdheid kunnen helpen bij de uitvoering van de bevoegdheid.
Ten tweede de inzet van commerciële middelen. Wanneer Digit gebruik maakt van een commercieel middel, dient voor elke inzet een aparte licentie aangeschaft te worden. Omdat een middel veelvuldig is ingezet, leidt deze afspraak tot hoge kosten. Vanuit de opsporingspraktijk wordt aangegeven dat men niet zonder dit product kan. Als op eenzelfde manier met dit product gewerkt blijft worden, dan zou het goed zijn om de afspraak aparte licenties aan te schaffen tegen het licht te houden. Daarnaast is het nodig aandacht te hebben voor de wijze waarop met dit product herleidbare, betrouwbare en integere gegevensverzameling gewaarborgd kan worden, bijvoorbeeld middels technische en tactische waarborgen. Dat is van belang, omdat dit product onder het huidige keuringsregime niet goedgekeurd zal worden.
Ten derde de meldplicht. Vanuit veiligheidsoogpunt is (op indirecte wijze) een meldplicht ten aanzien van onbekende kwetsbaarheden in het leven geroepen. Deze meldplicht geldt voor alle onbekende kwetsbaarheden en dus ook voor kwetsbaarheden in geautomatiseerde werken die voor en door personen met criminele intenties zijn ontwikkeld. Bovendien kan de meldplicht samenwerking bemoeilijken

met zowel binnen- als buitenlandse partijen. Het is dan ook de vraag of de meldplicht zoals die nu geldt in alle gevallen veiligheidsbevorderend kan werken.
Ten vierde het toezicht door de Inspectie. Op dit moment is het voor de Inspectie niet goed mogelijk om, vanwege het ontbreken van een kwaliteitssysteem bij Digit, het door de wetgever gewenste systeemtoezicht te houden. Om die reden zou het goed zijn om te kijken naar wat in de praktijk georganiseerd zou moeten worden om het systeemtoezicht van de grond te krijgen. Daarnaast is het nodig meer duidelijkheid te krijgen over de wijze waarop het toezicht door de Inspectie tot haar recht kan komen en daarbij ook oog te hebben voor de uitvoerbaarheid van de bevoegdheid.
Tot slot de keuring. De keuring vormt voor Digit een groot knelpunt. Bovendien blijkt het lastig om een vooraf goedgekeurd hulpmiddel in te zetten. Daarom zou het goed zijn om met alle betrokken actoren *gezamenlijk* te kijken op welke manieren het beste een oordeel kan worden gegeven of gegevens op een betrouwbare, integere en herleidbare manier verzameld kunnen worden, ook wanneer gebruik wordt gemaakt van commerciële middelen. Het verzamelen van betrouwbare gegevens is per slot van rekening een belang dat *alle* actoren met elkaar delen.

# 1 Inleiding

De samenleving digitaliseert en dat heeft invloed op de ontwikkeling en opsporing van criminaliteit. Opsporingsinstanties kunnen problemen ervaren bij de aanpak van nieuwere vormen van criminaliteit (Custers, 2018, p. 100), maar ook bij de oudere vormen (Odinot & De Jong, 2012). In de afgelopen jaren zijn om die reden verschillende wetten aangenomen die opsporingsinstanties meer handvatten bieden hun opsporingstaak te vervullen. Bij al deze wetten ging het om aanpassingswetgeving. Dat betekent dat verschillende extra bepalingen zijn toegevoegd en dat bestaande bepalingen zijn aangepast (Custers, 2018, p. 101). Eén van die wetten waarin bepalingen zijn toegevoegd is de Wet computercriminaliteit III. Daarin is onder andere een hackbevoegdheid opgenomen. In het Regeerakkoord 2017-2021 'Vertrouwen in de toekomst' is vastgelegd dat een eerste evaluatie van de wet plaatsvindt twee jaar na inwerkingtreding.[1] Op 1 maart 2019 is de Wet computercriminaliteit III in werking getreden. In dit rapport wordt daarom ingezoomd op de uitvoering van de hackbevoegdheid gedurende de eerste twee jaar.

## 1.1 Wet computercriminaliteit I & II

De Wet computercriminaliteit uit 1993 die 'opsporing van digitale netwerken en computernetwerken reguleert' (Custers, 2018, p. 101) wordt gezien als de eerste computerwetgeving. In deze wet worden onder andere computervredebreuk (artikel 138ab Sr) en het wissen en wijzigen van digitale gegevens (artikel 350a Sr) strafbaar gesteld. Verder is in de wetstekst 'niet voor het publiek bestemd gegevensverkeer via de telecommunicatie-infrastructuur' het alternatief geworden voor 'telefoongesprekken'. Op die manier kunnen ook andere wijzen van communiceren, zoals e-mail en Skype, worden meegenomen (Custers, 2018, p. 102).
In 1999 dient het kabinet bij de Tweede Kamer de Wet computercriminaliteit II (hierna Wet CCII) in. Het belangrijkste doel is het actualiseren van de eerste wet uit 1993. De behandeling van de Wet CCII loopt parallel met het opstellen van een internationaal Cybercrimeverdrag[2] en de wens van het kabinet om Nederlandse wetgeving hierop aan te laten sluiten. Dat is een belangrijke reden dat de wet uiteindelijk pas in 2006 in werking treedt. De Wet CCII betekent onder andere een uitbreiding van de definitie van hacken (er is ook sprake van computervredebreuk wanneer géén beveiliging wordt doorbroken) en de strafbaarstelling van *grooming* (artikel 248e Sr). *Grooming* betekent het via internet regelen van een seksuele ontmoeting met een minderjarige of van seksuele afbeeldingen van die minderjarige. Ook worden in de nieuwe wet de strafmaxima voor een aantal delicten verhoogd waardoor verdachten in voorlopige hechtenis kunnen worden genomen. Omdat het (internationale) Cybercrimeverdrag geratificeerd is, is het grootste deel van de computercriminaliteit ook strafbaar in Nederland als een Nederlander zich in het buitenland er schuldig aan maakt. De Wet CCII zorgt tot slot voor een aantal wijzigingen binnen het formele strafrecht. Zo mag, naast open, besloten communicatie worden afgetapt, bijvoorbeeld e-mailverkeer op interne netwerken (Koops & Oerlemans, 2019, p. 159). Daarnaast wordt het vorderen van gegevens (artt. 126nc-126ni Sv) aangescherpt (Custers, 2018, 104-105).

[1] Zie ook: *Kamerstukken I*, Handelingen 19 juni 2018, nr. 34, p. 16.
[2] Dit verdrag wordt ook wel het Verdrag van Boedapest genoemd en is het eerste internationale verdrag voor criminaliteit dat via het internet wordt gepleegd (Custers, 2018, p. 101).

Ondanks de hiervoor geschetste wetgeving is er, onder andere door nieuwe technologische ontwikkelingen zoals versleuteling, behoefte aan andere bevoegdheden waarvoor nog geen wettelijke regeling bestaat (Oerlemans, 2011, p. 888). Eén daarvan is de mogelijkheid van de politie om een geautomatiseerd werk, zoals een computer, te kunnen hacken. Deze behoefte blijkt onder andere uit het feit dat de politie een aantal keer gehackt zou hebben (dan wel vergelijkbare activiteiten zou hebben uitgevoerd) zonder dat daar een wettelijke grondslag voor was (Oerlemans, 2011, p. 903). Een wettelijke regeling voor een dergelijke bevoegdheid is echter wel nodig, omdat met het hacken een ernstige inbreuk wordt gemaakt op de persoonlijke levenssfeer van degene waarvan een geautomatiseerd werk binnengedrongen wordt (Oerlemans, 2011). Met de Wet computercriminaliteit III heeft de hackbevoegdheid een grondslag gekregen in het Wetboek van Strafvordering.

## 1.2 Wet computercriminaliteit III

De Wet computercriminaliteit III (hierna Wet CCIII) moet het 'juridisch instrumentarium voor de opsporing en vervolging van computercriminaliteit'[3] versterken (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 7) en de nota naar aanleiding van het verslag wordt duidelijk dat het gaat om meer vormen van criminaliteit dan de naam computercriminaliteit suggereert. De volgende tweedeling wordt genoemd: strafbare feiten die volledig in de digitale wereld plaatsvinden en andere vormen van criminaliteit. Bij de eerste categorie gaat het om botnets, computervredebreuk en sabotage. Bij de tweede categorie kan gedacht worden aan 'voorbereidingshandelingen voor liquidaties, afpersingen, hoogwaardige computercriminaliteit, grootschalige fraude, oplichting en de verspreiding van kinderpornografisch materiaal' (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 18). In het wetsvoorstel voor de Wet CCIII staan zowel wijzigingen van het Wetboek van Strafrecht als wijzigingen van het Wetboek van Strafvordering. Wat betreft het Wetboek van Strafrecht wordt ten eerste voorgesteld 'het wederrechtelijk overnemen van gegevens en het voor handen hebben of bekend maken van door misdrijf verkregen gegevens strafbaar te stellen'. De tweede voorgestelde wijziging is het verruimen van de 'strafbaarstelling van het verleiden van minderjarigen tot ontucht en *grooming* (artt. 248a en 248e Sr). Opsporingsambtenaren zouden voortaan zogenoemde lokpubers mogen inzetten die zich als minderjarigen voordoen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 4). De derde wijziging betreft het strafbaar stellen van online handelsfraude. Daarbij gaat het om 'het via het internet aanbieden van goederen of diensten, zonder de intentie die goederen of diensten te leveren, zodat de kopers worden gedupeerd' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 4).

Naast de drie genoemde wijzigingen worden twee bevoegdheden aan het Wetboek van Strafvordering toegevoegd. De eerste bevoegdheid is het aanpassen van een reeds bestaande bevoegdheid van de officier van justitie om te bevelen gegevens op het internet ontoegankelijk te maken. Dit is een bevoegdheid die op het moment dat het wetsvoorstel werd ingediend, opgenomen was in het Wetboek van Strafrecht (artikel 54 Sr). Het doel van de aanpassing is dat de regeling in de toekomst beter kan worden toegepast. In de memorie van toelichting staat expliciet vermeld dat met de aanpassing niet beoogd wordt om het toepassingsbereik van de bestaande bevoegdheid tot ontoegankelijkmaking van gegevens te verruimen (*Kamerstukken II*

[3] Computercriminaliteit wordt gedefinieerd als 'het plegen van strafbare feiten met behulp van, dan wel gericht op een geautomatiseerd werk' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 7).

2015/16, 34 372, nr. 3, p. 3). De tweede bevoegdheid betreft de 'hackbevoegdheid' (Koops & Oerlemans, 2019, p. 157).

### *1.2.1 Hackbevoegdheid*

De hackbevoegdheid (artt. 126nba, 126uba, 126zpa Sv) regelt dat opsporingsambtenaren die daarvoor aangewezen zijn, 'onder voorwaarden een geautomatiseerd werk, dat bij een verdachte in gebruik is, op afstand heimelijk [kunnen] binnendringen met het oog op bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 3). Een geautomatiseerd werk is 'een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken' (artikel 80sexies Sr).[4]
De nieuwe bevoegdheid is een zogenoemde 'paraplubevoegdheid', in de zin dat na het binnendringen verschillende andere opsporingsbevoegdheden kunnen worden benut (Oerlemans, 2017, p. 355). De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) beschikken al over een dergelijke bevoegdheid en ook in enkele Europese landen (Frankrijk, België, Duitsland) bestaat een wettelijke regeling om in het kader van de opsporing van strafbare feiten informatiesystemen heimelijk te doorzoeken (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 7). e hackbevoegdheid zou moeten voorzien in een 'leemte in de bestaande bevoegdheden' en wordt nodig geacht, omdat de bestaande opsporingsbevoegdheden in toenemende mate tekortschieten om 'aan de wezenlijke problemen en gebleken knelpunten op het gebied van de bestrijding van computercriminaliteit tegemoet te komen' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 7).

## 1.3 Centrale vraagstelling

De Wet CCIII moet vijf jaar na inwerkingtreding geëvalueerd worden. Naar aanleiding van een toezegging in het Regeerakkoord is deze evaluatie opgesplitst in twee delen. In het eerste deel, beschreven in dit rapport, is het proces geëvalueerd rondom de uitvoering van de hackbevoegdheid gedurende de eerste twee jaar na inwerkingtreding van de Wet. Eind 2024 volgt een rapport over het tweede deel van de evaluatie waarin de uitvoering van de volledige Wet CCIII centraal zal staan. De hoofdvraag van dit eerste deel van de evaluatie luidt:

*Op welke wijze wordt uitvoering gegeven aan de hackbevoegdheid en welke eventuele knelpunten doen zich daarbij voor in de opsporingspraktijk?*

Om een antwoord te kunnen geven op bovenstaande hoofdvragen zijn vijf deelvragen geformuleerd:

1 Hoe ziet het wettelijk kader van de hackbevoegdheid eruit?
2 Hoe verloopt het intake- en toetsingstraject in aanloop naar de inzet van de bevoegdheid?
3 Hoe verloopt de daadwerkelijke inzet van de bevoegdheid?
4 Hoe verloopt de controle op de bevoegdheid gedurende de uitvoering ervan?
5 Hoe verloopt de afronding van de inzet van de bevoegdheid?

[4] Zie in dit verband ook de opmerkingen van de Nederlandse Vereniging voor de Rechtspraak in de eerste consultatieronde (bijlage bij *Kamerstukken II* 2015/16, 34 372, nr. 3).

Het doel van de eerste deelvraag is om zicht te krijgen op de verschillende aspecten van het wettelijk kader. Daarbij gaat het om wetsteksten en toelichtende teksten zoals de memorie van toelichting. Ook wordt kort stilgestaan bij de aanleiding voor de hackbevoegdheid zoals geschetst in de Kamerstukken. In het tweede deel van de evaluatie zal hier uitgebreider aandacht aan worden besteed middels een uiteenzetting van de beleidstheorie en een reflectie daarop. Deelvragen 2 tot en met 5 hebben tot doel om inzicht te krijgen in de wijze waarop de bevoegdheid wordt uitgevoerd, inclusief knelpunten die zich voordoen in de opsporingspraktijk. Met knelpunten worden punten bedoeld die de uitvoering van de bevoegdheid in de praktijk belemmeren.
De opbrengst van de bevoegdheid in opsporingsonderzoeken komt tijdens de eerste evaluatie beperkt aan bod, omdat deze evaluatie betrekking heeft op de eerste twee jaar na inwerkingtreding van de wet. Om die reden is het lastiger om over concrete opbrengsten in tactische opsporingsonderzoeken al uitspraken te doen. Bovendien is het tactisch perspectief in deze eerste evaluatie slechts beperkt meegenomen waardoor nog geen volledig zicht kan worden verkregen op de wijze waarop gegevens worden gebruikt die middels de hackbevoegdheid verkregen zijn.

## 1.4 Methoden van onderzoek

In dit evaluatieonderzoek is een combinatie van onderzoeksmethoden gebruikt. Deze methodentriangulatie komt de validiteit van het onderzoek ten goede (Maseschalck, 2010; Braster, 2000). Triangulatie stelt onderzoekers in de gelegenheid om vanuit meerdere kanten een verschijnsel te begrijpen. Op die manier wordt een completer beeld van de werkelijkheid verkregen. In dit onderzoek is gebruikgemaakt van documentanalyse (paragraaf 1.4.1), interviews (paragraaf 1.4.2) en dossieranalyse (paragraaf 1.4.3). Het eerste deel van de evaluatie heeft zoals gezegd betrekking op de eerste twee jaar nadat de bevoegdheid in werking is getreden. Dat betekent dat in de interviews de nadruk heeft gelegen op de ervaringen in de eerste twee jaar. Omdat een groot deel van de dataverzameling in de periode na maart 2021 plaatsvond (tot en met november 2021), zijn soms ook ervaringen besproken van na die periode. Verder is het goed om op te merken dat de werkwijze van de betrokken actoren in ontwikkeling is. Dat betekent dat sommige beschrijvingen in deze evaluatie inmiddels (iets) verouderd zijn en niet meer een exacte weergave zijn van de wijze waarop er *op dit moment* gewerkt wordt. Op enkele plekken zal dit worden aangegeven, indien bij de onderzoekers bekend. Wat betreft de Verslagen van de Inspectie Justitie en Veiligheid moet hier nog worden opgemerkt dat het derde Verslag van de Inspectie (2022) verscheen op het moment dat onderhavig rapport werd afgerond. Daarom wordt er in dit rapport beperkt naar verwezen, vooral als het onderwerpen betreft waarbij veranderingen zijn geconstateerd ten opzichte van eerdere verslagjaren.

### *1.4.1 Documentanalyse*

Om een goed beeld te krijgen van de inhoud van het wettelijk kader (deelvraag 1) zijn diverse documenten bestudeerd. Daarbij lag de nadruk op de analyse van de parlementaire stukken zoals de wetstekst zelf, de memorie van toelichting, het Besluit onderzoek in een geautomatiseerd werk, de inbreng van deskundigen gedurende de verschillende consultatierondes en de (schriftelijke en mondelinge) debatten die zijn gevoerd in de Tweede en Eerste Kamer. Op die manier kon inzicht worden gekregen in de vraag waarom de wet op een bepaalde manier vorm heeft gekregen inclusief

eventueel aangebrachte wijzigingen als gevolg van de debatten in het parlement. Dat betekent dat analyses in de wetenschappelijke literatuur niet zijn meegenomen.
Veel van deze documenten zijn gevonden in het dossier Computercriminaliteit III (nr. 34 372) op de website overheid.nl.[5] In eerste instantie werden 64 documenten gevonden. Vervolgens zijn op basis van de sneeuwbalmethode nog enkele aanvullende documenten geraadpleegd. Enkele voorbeelden van documenten die gedurende het zoekproces naar boven kwamen zijn de Kamerbrief uit 2016 waarin het kabinet schrijft hoe zij met kwetsbaarheden (in software) zal omgaan (*Kamerstukken II* 2016/17, 26 643, nr. 428). De 'Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex. artikel 126 nba Sv' (Staatscourant, 2019) en evaluaties van andere actoren zoals Verslagen van de Inspectie Justitie en Veiligheid.
Ook in het kader van de tweede tot en met de vijfde deelvraag, waarin de daadwerkelijke uitvoering van de bevoegdheid centraal staat, heeft een documentanalyse plaatsgevonden. Het betreft hier interne documenten van het Openbaar Ministerie en de politie waarin bijvoorbeeld werkprocessen worden beschreven of afwegingen worden gemaakt hoe bepaalde begrippen uit het wettelijk kader geïnterpreteerd dienen te worden. Omdat deze documenten intern zijn, wordt in het rapport niet naar de titel verwezen, maar in plaats daarvan naar 'intern document' inclusief een toegekend nummer.

### *1.4.2 Interviews*

**Interviews - Wie?**
De tweede onderzoeksmethode die gedurende dit onderzoek gebruikt is, is het *topic* gestuurde interview (Hutjes & Van Buuren, 1992). Dit soort interviews was vooral bedoeld om inzichtelijk te krijgen hoe de daadwerkelijke uitvoering van de hackbevoegdheid in de praktijk verliep (deelvragen 2 t/m 5). Ook waren de interviews bruikbaar om zicht te krijgen op de inhoud van het wettelijk kader inclusief de belangrijke thema's die gedurende de totstandkoming van de wet voor discussie hebben gezorgd (deelvraag 1). Er is met diverse personen gesproken in de periode december 2020 tot november 2021. Wat betreft de interviews met betrekking tot de uitvoering is het belangrijk om vooraf op te merken dat de uitvoering van de bevoegdheid in handen ligt van een beperkt aantal personen. Deze kleine kring voorziet de andere actoren, die betrokken zijn bij de inzet van de bevoegdheid en de toetsing ervan, van informatie.

*Beleidsmakers & wetgevingsjuristen*
In het kader van het eerste deel van de evaluatie zijn tien personen geïnterviewd die nauw betrokken waren bij het wetgevingsproces, denk daarbij aan beleidsmakers en wetgevingsjuristen van het ministerie van Justitie en Veiligheid en vertegenwoordigers van het Openbaar Ministerie en de politie. Soms werden geïnterviewden individueel gesproken en in andere gevallen vond een groepsinterview plaats (twee of meer personen tegelijkertijd). In totaal zijn vijf gesprekken gevoerd. Doel van deze gesprekken was om verder zicht te krijgen op het wettelijk kader en eventuele wijzigingen die hebben plaatsgevonden als gevolg van discussies gedurende het wetgevingstraject.

*Uitvoerders wet*
Ten tweede is gesproken met de 'uitvoerders' van de wet. Bij een opsporingsonderzoek zijn vanuit de politie twee teams betrokken: een tactisch team

[5] Zie: https://www.eerstekamer.nl/wetsvoorstel/34372_computercriminaliteit_iii%22www.eerstekamer.nl/wetsvoorstel/34%20372_computercriminaliteit_iii (laatst geraadpleegd op 9 november 2020).

en Digit-politie. Het tactisch team houdt zich bezig met het tactisch opsporingsonderzoek waarbinnen de hackbevoegdheid één van de opsporingsbevoegdheden is die wordt ingezet. Digit-politie houdt zich bezig met de inzet van de hackbevoegdheid (hierna 'inzet'). Het eerste deel van de evaluatie computercriminaliteit III heeft zich vooral gericht op Digit-politie. Daarom heeft een groot deel van de interviews daar plaatsgevonden.
Twee soorten interviews zijn in het kader van het eerste deel van de evaluatie gehouden: zaaksinterviews en overkoepelende interviews. Zaaksinterviews hadden betrekking op één zaak/inzet en boden de onderzoekers meer zicht op de (achtergronden van de) verschillende keuzes die gedurende een inzet werden gemaakt. Naast zaaksinterviews hebben interviews plaatsgevonden over de keuring van een specifiek hulpmiddel. Deze interviews waren in eerste instantie niet gepland. Gedurende het onderzoek bleek dat het doorgronden van het keuringsproces complex was. Daarom is ervoor gekozen twee aanvullende interviews te doen.
Tijdens overkoepelende interviews is op een algemener niveau gesproken over de (inzet van de) bevoegdheid. Binnen de overkoepelde interviews hebben twee thematische groepsinterviews plaatsgevonden: over de keuring van technische hulpmiddelen en over (de aanschaf van) commerciële middelen. De keuring van technische hulpmiddelen was een onderwerp dat door Digit aangedragen werd als belangrijk. Om die reden werd door de onderzoekers een aparte sessie over dat onderwerp georganiseerd. Commerciële producten bleek een thema waarover niet iedereen vrijuit wilde praten. Binnen Digit houdt een klein aantal personen zich hiermee bezig. Daarom is met hen een aparte sessie georganiseerd, zodat de onderzoekers wel de benodigde informatie konden krijgen over dit thema.

*Waarborgen voor controle*
Er zijn ook personen geïnterviewd die betrokken zijn bij de controle rondom de (inzet van de) bevoegdheid. Binnen het Openbaar Ministerie zijn een officier van justitie en een parketsecretaris volledig vrij gemaakt om toe te zien op de uitvoering van de bevoegdheid. Met hen (Digit-OM) zijn overkoepelende interviews gehouden. Ten tweede is gesproken met tactisch-officieren van justitie, die de leiding hadden over een opsporingsonderzoek waarin de hackbevoegdheid werd ingezet (zaaksinterviews). Hoewel de nadruk tijdens het eerste deel van de evaluatie lag op de werkwijze van Digit, werd gedurende het onderzoek duidelijk dat niet helemaal voorbij kon worden gegaan aan het tactisch perspectief. Daarom is met een beperkt aantal tactisch zaaksofficieren gesproken. Het tactisch perspectief zal in deel 2 van de evaluatie veel uitgebreider aan bod komen. Ten derde is gesproken met secretarissen van de Centrale Toetsingscommissie (overkoepelende interviews). De CTC speelt door haar adviesrol een belangrijke rol bij het vooraf toetsen van de inzet van de bevoegdheid. Ten vierde is gesproken met twee gespecialiseerde rechters-commissarissen (overkoepelde interviews). De rechter-commissaris wordt in de wetsgeschiedenis een belangrijke rol toebedeeld in het kader van de verschillende waarborgen die gekoppeld zijn aan de wet. Verder heeft hij/zij een belangrijke rol in het kader van de 'vervanging' voor de toetsing achteraf als een zaak niet voor de rechter komt (*Kamerstukken I* 2017/18, 34 372, G, p. 19). De rol van de CTC en de rechter-commissaris is, onder andere vanwege tijdtechnische redenen, beperkt onderzocht. Ook dat onderwerp zal in het tweede deel van de evaluatie meer nadruk krijgen. Dat geldt ook voor de rol van de zittingsrechter. Gedurende de looptijd van de eerste evaluatie is, voor zover bekend, géén opsporingsonderzoek waarin de bevoegdheid succesvol is ingezet, inhoudelijk behandeld. Daarvoor zijn verschillende redenen. Zo was er in één zaak geen verdachte en kwam het voor dat het opsporingsdossier nog moest worden afgerond. Hopelijk worden gedurende de looptijd van het tweede deel

van de evaluatie wel zaken inhoudelijk behandeld waardoor ook dat aspect aan bod kan komen.
Ten vijfde hebben overkoepelende interviews plaatsgevonden met de Inspectie Justitie en Veiligheid. Haar is, met het oog op haar toezichthoudende taak op de politie, een belangrijke rol toegekend aangaande het toezicht op de inzet van de bevoegdheid. Omdat de rapportages van de Inspectie openbaar zijn, hadden de interviews vooral een aanvullend karakter. Tot slot zijn meer overkoepelende interviews gehouden met personen die zich bezighouden met de keuring van technische hulpmiddelen die Digit gebruikt om gegevens te verzamelen.

*Benadering respondenten*
Voor dit onderzoek is, naast een begeleidingscommissie, een expertgroep ingesteld. Deze groep bestaat uit vijf leden afkomstig vanuit het Landelijk Parket en Digit-politie. De leden van deze groep zijn geïnterviewd in het kader van dit onderzoek. Daarnaast voorzag deze groep de onderzoekers van (technische) achtergrondinformatie, zodat de werking van de bevoegdheid in de praktijk goed begrepen kon worden. Het raadplegen van de expertgroep was daarnaast één van de manieren om andere mogelijk te interviewen personen voor het onderzoek te werven. Dit soort personen werden ook benaderd vanuit het netwerk van de onderzoekers zelf (het ministerie van Justitie en Veiligheid, het Openbaar Ministerie, de politie en de Inspectie Justitie en Veiligheid). Daarnaast zijn via de sneeuwbalmethode (Baarda et al., 2013) geïnterviewden benaderd. De expertgroep heeft tot slot meegelezen met de empirische hoofdstukken van het eindrapport. Het was haar taak om de onderzoekers te wijzen op passages waarin opsporingsbelangen geschaad werden en/of op feitelijke onjuistheden. Ook de Keuringsdienst is, vanwege de technische complexiteit van het onderwerp, gevraagd om het hoofdstuk over het keuringsproces op feitelijke onjuistheden mee te lezen. Daarnaast is de Inspectie, op haar verzoek, in de gelegenheid gesteld om te reageren op het hoofdstuk over de Inspectie. Verder is de paragraaf over de rol van de rechter-commissaris aan de betrokken geïnterviewden voorgelegd. Ook is aan één zaaksofficier een aantal passages voorgelegd in verband met het afschermen van opsporingsmethoden. Op basis van de reacties zijn enkele wijzigingen aangebracht in het rapport. Deze wijzigingen betroffen aanvullingen en het verwijderen van informatie waarmee te veel opsporingsinformatie werd prijsgegeven. Tot slot zijn citaten voorgelegd aan geïnterviewden die mogelijk herleidbaar zouden zijn. Dit in verband met de vooraf toegezegde anonimiteit.

In tabel 1.1 is te zien dat in het totaal 22 overkoepelde interviews zijn gehouden met 26 verschillende personen.

**Tabel 1.1 Aantal overkoepelende interviews**

| Wie | Aantal interviews | Aantal personen |
|---|---|---|
| Politie (inclusief twee themasessies) | 12 | 14 |
| OM | 3 | 2 |
| CTC | 1 | 2 |
| RC | 2 | 2 |
| Inspectie Justitie en Veiligheid | 2 | 4 |
| Keuringsdienst/TNO | 2 | 2 |
| **Totaal** | **22** | **26** |

Naast overkoepelende interviews vonden zoals gezegd zaaksinterviews plaats en twee interviews over de keuring van één specifiek technisch hulpmiddel. In het totaal zijn veertien zaaksinterviews[6] gehouden en twee keuringsinterviews met in het totaal achttien personen. Zie voor meer details tabel 1.2.

**Tabel 1.2 Aantal zaaksinterviews**

| Wie | Aantal interviews | Aantal personen |
|---|---|---|
| Digit-politie | 7 | 5 |
| Zaaks-OM | 7 | 10 |
| Interviews m.b.t. keuring technisch hulpmiddel | | |
| Digit-politie | 1 | 2 |
| Keuringsdienst | 1 | 1 |
| **Totaal** | **16** | **18** |

In bijlage 2 wordt nader uiteengezet op welke wijze de interviews hebben plaatsgevonden.

### 1.4.3 *Dossieranalyse: algeheel overzicht en selectie van zeven dossiers*

Naast de analyse van documenten en het houden van interviews, zijn zeven dossiers geanalyseerd. Het doel van deze analyse was om zicht te krijgen op het soort zaken waarvoor de bevoegdheid wordt ingezet en de wijze waarop dat gebeurt (deelvragen 2 t/m 5). Hoe zien bijvoorbeeld de verschillende fases eruit als Digit uitvoering geeft aan de inzet van de hackbevoegdheid? Oorspronkelijk was het idee om zowel dossiers van tactische opsporingsteams te analyseren als dossiers die bij Digit bijgehouden worden. Vanwege de keuze om het eerste deel van de evaluatie vooral te richten op de werkwijze van Digit en vanwege de beperkte doorlooptijd van het onderzoek, is besloten om alleen de Digit-dossiers te raadplegen. Een Digit-dossier bestaat doorgaans uit een map waarin officiële stukken zijn opgenomen, zoals aanvraagprocessen-verbaal, de vordering tot machtiging aan de rechter-commissaris, de machtiging van de rechter-commissaris en het bevel van de officier van justitie.[7] Indien sprake was van een verlenging van een inzet dan waren ook die stukken aanwezig. Daarnaast zijn in een dossier processen-verbaal opgenomen, en, indien van toepassing, Europese onderzoeksbevelen (EOB's) en/of rechtshulpverzoeken. Ook was doorgaans het haalbaarheidsonderzoek toegevoegd aan het dossier. Daarin maakt Digit een inschatting van de technische haalbaarheid van een inzet. Verder beschikt Digit over een digitaal systeem waarin het journaal (een soort logboek) wordt bijgehouden en waarin ook een deel van de zojuist genoemde stukken staat. De onderzoekers hadden geen toegang tot de plannen van aanpak die Digit opstelt. Ook is niet gekeken naar de loggingsystemen. Naar beide heeft de Inspectie van Justitie en Veiligheid al gekeken en over gerapporteerd (Inspectie JenV, 2020, 2021, 2022). Voor dit onderzoek zijn zoals gezegd uiteindelijk zeven Digit-dossiers uitgebreid bestudeerd. In bijlage 2 staat beschreven hoe de selectie hiervan heeft plaatsgevonden.

[6] Bijna alle geïnterviewden vanuit Digit die in het kader van een specifieke zaak zijn geïnterviewd, waren ook al één of meerdere keren geïnterviewd in het kader van de overkoepelde interviews.

[7] Deze mappen waren niet altijd helemaal compleet. Gedurende de looptijd van dit onderzoek werd gewerkt aan het op orde brengen van de dossiers.

### *1.4.4 Analyse*

De hoofdanalyse is onder te verdelen in twee delen. Voorafgaand aan een groot deel van de dataverzameling zijn de meeste documenten, gerelateerd aan het wettelijk kader en de wetsgeschiedenis, gecodeerd in analyseprogramma Maxqda. Een klein deel is handmatig geanalyseerd. Daarmee kon deelvraag 1 grotendeels al beantwoord worden. Ook vormde deze eerste analyse een belangrijke basis voor de dataverzameling met betrekking tot het in kaart brengen van de daadwerkelijke uitvoering van de bevoegdheid en knelpunten die zich daarbij voordeden (deelvragen 2 t/m 5).
Nadat alle interviews waren afgerond en van alle geselecteerde inzetten een topiclijst was ingevuld, is gestart met deel 2 van de hoofdanalyse. Tussentijds vonden (handmatig) ook al eerste analyses plaats, zodat bijvoorbeeld bepaald kon worden of het nodig was om tijdens interviews aanvullende topics aan te snijden.
Voorafgaand aan deel 2 van deze analyse is op basis van de deelvragen 2 t/m 5 een eerste indeling gemaakt van onderwerpen die aan de orde zouden komen in het rapport. Vervolgens is de analyse verdeeld tussen twee onderzoekers. Eén onderzoeker nam de analyse voorafgaand aan de inzet en na afloop van de inzet voor haar rekening (deelvraag 2 en 5) en de andere onderzoeker de daadwerkelijk inzet (deelvraag 3 en 4). Vervolgens zijn alle interviewverslagen ingevoerd in Maxqda (versie 18.2.5). Algemene documenten vanuit de verschillende organisaties en topiclijsten van de geselecteerde inzetten zijn handmatig geanalyseerd. In Maxqda hebben de twee onderzoekers codes aangemaakt, beiden in een apart bestand. De eerder besproken onderwerpen binnen de deelvragen vormden hiervoor de basis. Vervolgens zijn aan de hand van de verzamelde data nieuwe, open codes toegevoegd. Een voorbeeld van een reeds bestaande code was ‘onderzoekshandelingen’. Latere toegevoegde codes met betrekking tot dit thema waren bijvoorbeeld ‘maatwerk’ en ‘brede inzet’. Nadat alle documenten gecodeerd waren heeft (handmatig) een volgende analyseslag plaatsgevonden waarin codes werden samengenomen die betrekking hadden op een groter thema dat tevens in het onderzoeksrapport is verwerkt. Voorbeelden hiervan zijn ‘juiste sub bepalen’ en ‘meerdere onderzoekshandelingen’. Gedurende het codeer- en analyseproces hadden beide onderzoekers ten minste één keer per week contact, bijvoorbeeld over nieuw aangemaakte codes, of hoe bepaalde codes en eventuele overkoepelde thema’s geduid zouden kunnen worden. Ook hielden beiden een lijstje bij van codes die mogelijk ook relevant waren voor de ander, inclusief een toelichting wat die betreffende code inhield.

## 1.5 Opbouw rapport

Dit rapport is als volgt opgebouwd (zie ook tabel 1.3). Hoofdstuk 2 richt de aandacht op een gedetailleerde beschrijving van het wettelijk kader (deelvraag 1). Na een inleiding op de empirische hoofdstukken staat in de hoofstukken 3 t/m 6 de uitvoering centraal. In hoofdstuk 3 wordt het traject voorafgaand aan de daadwerkelijke inzet van de bevoegdheid behandeld (deelvraag 2). Ingegaan wordt onder andere op de wijze waarop de inzet van de bevoegdheid wordt getoetst door de daartoe aangewezen actoren. In de hoofdstukken 4 en 5 richt de aandacht zich op wat er gebeurt tijdens de uitvoering van de bevoegdheid. Hoofdstuk 4 gaat over het binnendringen, het uitvoeren van onderzoekshandelingen en de uitvoering van inzetten met een internationale component (deelvraag 3). Hoofdstuk 5 richt zich op de controle die gedurende de uitvoering van de bevoegdheid plaatsvindt (deelvraag 4). In dat

hoofdstuk is onder andere aandacht voor de Keuringsdienst en de Inspectie Justitie en Veiligheid. In hoofdstuk 6 staat de afronding van de inzet centraal en hetgeen er daarna gebeurt (deelvraag 5). In hoofdstuk 7 tot slot volgt de conclusie met daarin het antwoord op de in dit hoofdstuk geformuleerde hoofdvraag. Dat gebeurt aan de hand van zeven kernonderwerpen.

### Tabel 1.3 Opbouw rapport

| Hoofdstuk | Onderzoeksvraag | Onderwerp(en) die behandeld worden |
|---|---|---|
| H2 | Hoe ziet het wettelijk kader van de hackbevoegdheid eruit? | Uiteenzetting wettelijk kader. |
| H3 | Hoe verloopt het intake- en toetsingstraject in aanloop naar de inzet van de bevoegdheid? | Aanleiding inzet bevoegdheid, selectie van inzetten die in behandeling worden genomen en toetsingstraject. |
| H4 | Hoe verloopt de daadwerkelijke inzet van de bevoegdheid? | Binnendringen, gebruik van kwetsbaarheden, onderzoekshandelingen inclusief technische hulpmiddelen en inzetten met een internationale component. |
| H5 | Hoe verloopt de controle op de bevoegdheid gedurende de uitvoering ervan? | Controle gedurende de inzet, onder andere: keuring van technische hulpmiddelen, toezicht door de Inspectie Justitie en Veiligheid en verlenging van de inzet. |
| H6 | Hoe verloopt de afronding van de inzet van de bevoegdheid? | Overdracht van gegevens aan het tactisch team, dossiervorming, opbrengsten tactisch onderzoek, notificatieplicht en zittingsrechter. |
| H7 | Op welke wijze wordt uitvoering gegeven aan de hackbevoegdheid en welke eventuele knelpunten doen zich daarbij voor in de opsporingspraktijk? | Antwoord op de onderzoeksvraag. Uiteenzetting van de zeven belangrijkste thema's waarbinnen zich knelpunten voordoen. |

# 2 Wettelijk kader van de hackbevoegdheid

## 2.1 Inleiding

In dit hoofdstuk staat het wettelijk kader van de hackbevoegdheid beschreven, gebaseerd op een analyse van wetsteksten en daarbij behorende Kamerstukken (deelvraag 1). Hoe de hackbevoegdheid in de praktijk wordt uitgevoerd komt aan de orde in de hoofdstukken 3 tot en met 6. Om de hackbevoegdheid een wettelijke grondslag te geven zijn drie artikelen toegevoegd aan het Wetboek van Strafvordering (arikel 126nba, 126uba, 126zpa Sv)[8] (hierna wordt gemakshalve gesproken van 126nba Sv, tenzij anders vermeld). Dat er een nieuw wetsartikel is gekomen past bij het feit dat met de nieuwe bevoegdheid een ernstige inbreuk wordt gemaakt op de persoonlijke levenssfeer van degene waarvan een geautomatiseerd werk wordt binnengedrongen. Op basis van het Europees Verdrag voor de Rechten van de Mens (EVRM) dient er daarom een wettelijke grondslag te zijn. Deze grondslag hoeft geen formele wet te zijn, maar de rechtsgrond dient wel 'voldoende toegankelijk en voorzienbaar' te zijn (Oerlemans, 2011, p. 900). Ook vanwege het strafvorderlijk legaliteitsbeginsel is een wettelijke grondslag nodig op basis waarvan opsporingsinstanties 'bewijsvergaringsactiviteiten' kunnen uitvoeren. Op het moment dat sprake is van nieuwe opsporingsmethoden, of wanneer bestaande methoden in een nieuwe context worden toegepast, dan moet het Wetboek van Strafvordering worden aangepast, ten minste als sprake is van meer dan geringe inmenging en/of een risico voor de integriteit voor de opsporing. Het is niet aan de rechter of aan opsporingsinstanties om een juridische basis te doen laten ontstaan voor nieuwe methoden die worden toegepast (Koops & Oerlemans, 2019, p. 121-122). Toch is het in de praktijk zo dat bestaande bevoegdheden in het Wetboek van Strafvordering soms een nieuwe invulling krijgen wanneer ze in het digitale domein worden ingezet en waarbij de rechter zorgt voor aanvullende normering, bijvoorbeeld het smartphone-arrest.[9] Sinds enkele jaren wordt gewerkt aan de modernisering van het Wetboek van Strafvordering. Deze modernisering moet er onder andere toe leiden dat beter ingespeeld wordt op de huidige en toekomstige technologische ontwikkelingen (Commissie modernisering opsporingsonderzoek in het digitale tijdperk, 2018, p. 6).

De hackbevoegdheid wordt heimelijk toegepast, zonder dat de verdachte daarvan op de hoogte is. Daarom is de bevoegdheid, op advies van de afdeling Advisering van de Raad van State, opgenomen in titel IV van het Eerste Boek. Ook vertoont de nieuwe bevoegdheid inhoudelijke overeenkomsten met de bijzondere opsporingsbevoegdheden van Titel IVA van het eerste boek. Het feit dat het artikel op deze plek in het wetboek is geplaatst, betekent dat diverse rechtswaarborgen (denk daarbij onder andere aan een uitgebreidere notificatieplicht, het voegen van processen-verbaal bij de processtukken en de vernietiging van processen-verbaal of andere voorwerpen met betrekking tot verschoningsgerechtigden) ook van toepassing zijn op het verrichten van onderzoekshandelingen in een geautomatiseerd werk (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 16). De Wet CCIII kent verder een aantal grondslagen om bij of krachtens Algemene Maatregel van Bestuur regels te stellen met betrekking tot de uitvoering van de bevoegdheid. In het Besluit onderzoek in een

[8] Dat de hackbevoegdheid in drie artikelen is vastgelegd heeft te maken met de reikwijdte (het soort zaken) waarvoor de bevoegdheid kan worden ingezet (zie paragraaf 2.3.1).

[9] In februari 2021 heeft de Hoge Raad een uitspraak gedaan waarin aangegeven is dat het rechtmatig is geweest om een verdachte te dwingen zijn smartphone te ontgrendelen middels zijn eigen vingerafdruk (Hoge Raad, 2021).

geautomatiseerd werk (hierna Besluit) bijvoorbeeld zijn op basis van artikel 126ee Sv regels geformuleerd aangaande de onderzoekshandelingen die worden verricht met een technisch hulpmiddel. Dit Besluit is deels gebaseerd op het Besluit technische hulpmiddelen strafvordering.[10]
Na een korte uiteenzetting over de aanleiding voor de nieuwe bevoegdheid richt de aandacht zich in dit hoofdstuk op wat er in wet- en regelgeving over de bevoegdheid is vastgelegd. Allereerst wordt stilgestaan bij het soort misdrijven waarvoor de bevoegdheid mag worden ingezet. Vervolgens wordt de uitvoering, uitgesplitst in vier fases, nader belicht. Daarna komt de wijze waarop toezicht en toetsing plaatsvinden aan de orde. Vervolgens richt de aandacht zich op de waarborgen die belangrijk zijn in het kader van de nieuwe bevoegdheid. Deze zijn slechts schematisch weergegeven, omdat ze eerder al in de tekst aan de orde zijn geweest. Het hoofdstuk sluit af met hoe deze bevoegdheid in een internationale context zou moeten worden toegepast.

## 2.2 Aanleiding nieuwe bevoegdheid

Op basis van de memorie van toelichting wordt duidelijk dat de nieuwe bevoegdheid een oplossing moet bieden voor het feit dat opsporingsinstanties niet goed meer in staat zijn om computercriminaliteit en andere vormen van ernstige criminaliteit aan te pakken (*Kamerstukken II* 2015/16, 34 372, nr. 3).[11] Een belangrijke reden hiervoor is dat de bestaande (bijzondere) opsporingsbevoegdheden niet altijd meer bruikbaar zijn om de in een opsporingsonderzoek benodigde gegevens te verzamelen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 7-13).[12] Hieraan ligt een aantal oorzaken ten grondslag waarvan de opkomst van nieuwe technologische ontwikkelingen de meeste aandacht krijgt in de wetsteksten. Drie technologische ontwikkelingen worden genoemd: versleuteling, draadloze netwerken en *cloud computing* (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 7-13). Versleuteling van gegevens, ook wel encryptie, betekent dat met behulp van een wiskundig algoritme leesbare data zodanig worden omgevormd dat ze niet meer leesbaar zijn (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 7). Zowel individuele gegevensbestanden als bijvoorbeeld een gehele harde schijf kunnen op eenvoudige wijze worden versleuteld. Versleuteling is mogelijk, zo blijkt uit de memorie van toelichting, van vastgelegde gegevens (een harde schijf) én van stromende gegevens[13] (communicatie via WhatsApp; *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 8). De tweede ontwikkeling is het toenemende gebruik van draadloze netwerken om toegang te krijgen tot het internet (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 10). In de memorie van toelichting wordt uitgelegd dat draadloze netwerken, ook wel wifi-netwerken, op veel plaatsen aanwezig zijn, bijvoorbeeld in huis, hotspots op straat, in het openbaar vervoer en in horecagelegenheden. Een individuele internetgebruiker benut doorgaans in een week tijd, of zelfs op één dag, meerdere

[10] Dat geldt bijvoorbeeld voor artikel 9, lid 2 Besluit onderzoek in een geautomatiseerd werk (Bogw). Dat artikel is gebaseerd op artikel 11 van het Besluit technische hulpmiddelen strafvordering. Omdat steeds minder 'gewoon' getelefoneerd wordt, is, op advies van de Nationale Politie, de Raad voor de Rechtspraak en de Nederlandse Vereniging voor de Rechtspraak, een 'techniek onafhankelijke formulering' gebruikt in plaats van het ouderwetse 'nummer'. Gekozen is voor de formulering dat een technisch hulpmiddel 'uitsluitend de communicatie die plaatsvindt met gebruikmaking van één of meer identificerende kenmerken van het geautomatiseerde werk van de individuele gebruiker of gebruikers op wie het bevel betrekking heeft registreren' (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 38).

[11] Hoeveel misdrijven niet worden opgelost, omdat deze nieuwe bevoegdheid er niet is, wordt niet duidelijk (zie bijlage 3).

[12] Er wordt nog een andere reden genoemd, maar deze reden komt veel beperkter aan bod, namelijk dat de bestaande bevoegdheden niet altijd proportioneel zijn (oa. *Kamerstukken II* 2015/16 34 372, nr 3, p. 10).

[13] Opgeslagen gegevens zijn gegevens die staan opgeslagen in een computer. Stromende gegevens zijn gegevens 'die in een proces zijn van verwerking of overdracht tussen computers' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 18). Koops en Oerlemans (2019, p. 118) maken onderscheid tussen 'reeds bestaande (opgeslagen) gegevens' en 'niet reeds ergens vastgelegde gegevens'.

netwerken en daarvoor gebruikt hij of zij meerdere toegangspunten (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 10). Beide ontwikkelingen zorgen ervoor dat bijvoorbeeld de bevoegdheid om te kunnen tappen niet meer goed bruikbaar is.
Middels het plaatsen van een telefoon-, e-mail- of internettap (artt. 126m, 126t en 126zg Sv) kan communicatie afgetapt en opgenomen worden. Indien communicatie wordt versleuteld, dan zijn deze (bijzondere) opsporingsbevoegdheden[14] niet bruikbaar. Opsporingsinstanties kunnen zien dat communicatie plaatsvindt, maar zij zijn niet in staat om de inhoud ervan te achterhalen, zo blijkt uit de memorie van toelichting (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 9). Met de nieuwe bevoegdheid wordt het mogelijk om inzicht te krijgen in communicatie voordat deze wordt versleuteld of nadat deze is ontsleuteld (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 10).
Ook het gebruik van draadloze netwerken zorgt ervoor dat het bestaande tappen (de internettap) niet meer goed bruikbaar is (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 10). Eén van de redenen is dat een tapbevel per toegangspunt tot het internet wordt afgegeven. Op het moment dat meerdere toegangspunten in het spel zijn, betekent dit dat meerdere taps moeten worden geplaatst (bij elke netwerk- en dienstenaanbieder een tap). Dat is praktisch niet werkbaar vanwege de grote hoeveelheid data die verzameld wordt. Hierdoor wordt het moeilijker om volledig zicht te krijgen op de communicatie van een verdachte (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 10).
De derde ontwikkeling is *cloud computing*. In de memorie van toelichting wordt uitgelegd dat veel bedrijven en burgers tegenwoordig gebruikmaken van '*webbased* toepassingen om hun gegevens op te slaan', bijvoorbeeld een al dan niet verspreide opslag van gegevens in de *cloud.* Een gebruiker bewaart zijn of haar gegevens in dat geval niet (alleen) op zijn of haar harde schijf, maar de opslag van gegevens vindt plaats op servers die zich elders in Nederland, of zelfs in het buitenland bevinden. Op verschillende servers slaan deze diensten, langs geautomatiseerde weg, de gegevens op. Waar en op welke servers dat gebeurt, daar heeft de gebruiker geen invloed op en in sommige gevallen is dat ook voor de aanbieder onbekend. Meestal worden bestanden in gedeelten opgeslagen, verspreid over meerdere servers die zich deels op buitenlands grondgebied bevinden (*Kamerstukken II*, 2015/16, 34 372, nr. 3, p. 11). *Cloud computing* is voor opsporingsinstanties problematisch, omdat voor sommige bevoegdheden de opsporing afhankelijk is van de medewerking van een aanbieder (artt. 126n, 126na, 126ng, 126u, 126 ua, 126ug, 126zi en 126zl Sv). Bij *cloud computing* is het echter niet altijd duidelijk of een aanbieder kan worden gezien als aanbieder in de zin van de wet, waardoor geen bevel tot medewerking kan worden gegeven. Mocht dit wel kunnen, dan kan het zijn dat een aanbieder niet onder de Nederlandse rechtsmacht valt. In zo'n geval is het indienen van een rechtshulpverzoek nodig. Dat is lastig als Nederland met dat land geen rechtshulprelatie onderhoudt (*Kamerstukken II*, 2015/16, 34 372, nr. 3, p. 11-12). De hackbevoegdheid moet een oplossing bieden aan de problemen die verbonden zijn met de zojuist genoemde drie technologische ontwikkelingen.

[14] De telefoontap wordt in de memorie van toelichting genoemd, maar de problemen die worden geschetst hebben betrekking op de internet- en de e-mailtap. Er is wel een ander probleem met betrekking tot de telefoontap, namelijk dat de inzet hiervan steeds minder effectief is, omdat gebruik wordt gemaakt van alternatieve communicatiemiddelen (Odinot & De Jong, 2012, p. 10). Dit wordt overigens niet expliciet genoemd in de memorie van toelichting.

## 2.3 Reikwijdte bevoegdheid

### *2.3.1 Misdrijven – gedifferentieerde opbouw*

In de wetstekst zelf (Staatsblad, 322, 2018, p. 5-7), de memorie van toelichting (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 15-19) en het Besluit (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 2, 11-12) wordt aangegeven voor welke misdrijven de bevoegdheid kan worden ingezet. Ten eerste mag de bevoegdheid pas gebruikt worden voor de opsporing van misdrijven als bedoeld in artikel 67 eerste lid Sv., zogenoemde voorlopige hechtenis-feiten ('VH-feiten') en voor misdrijven die een ernstige inbreuk op de rechtsorde opleveren (art 126nba Sv). Ten tweede is de bevoegdheid bedoeld voor een onderzoek naar personen ten aanzien van wie een redelijk vermoeden bestaat dat zij zich bezighouden met het beramen en/of plegen van misdrijven in georganiseerd verband (artikel 126uba Sv). Ten derde kan de bevoegdheid worden ingezet wanneer er aanwijzingen zijn voor een terroristisch misdrijf (artikel 126zpa Sv). Afhankelijk van het opsporingsdoel dat opsporingsinstanties voor ogen hebben, is, op advies van de Raad van State (zie ook bijlage 3), een aanvullend vierde en vijfde criterium opgenomen. Wanneer opsporingsinstanties gegevens veilig willen stellen en/of ontoegankelijk willen maken, moet sprake zijn van een misdrijf waarvoor volgens de wettelijke omschrijving een gevangenisstraf van acht jaar of meer kan worden opgelegd. Ook zijn deze opsporingshandelingen toegestaan in opsporingsonderzoeken naar misdrijven die bij Algemene Maatregel van Bestuur zijn aangewezen. Het gaat dan om misdrijven waarvoor geen gevangenisstraf van acht jaar of meer geldt, maar die met een geautomatiseerd werk worden gepleegd en die een geautomatiseerd werk als doel hebben (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 2). Ook betreft het, aldus het Besluit, ernstige commune misdrijven die steeds vaker met behulp van een geautomatiseerd werk worden gepleegd. Voor al deze misdrijven zou gelden dat er vaak geen ander aanknopingspunt is voor de opsporing dan het geautomatiseerde werk waarmee het misdrijf wordt gepleegd (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 11). Bovendien is er een duidelijk maatschappelijk belang bij de beëindiging van de strafbare situatie en de vervolging van de daders (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 11).

### *2.3.2 Geautomatiseerde werken*

Met de nieuwe bevoegdheid kunnen geautomatiseerde werken worden binnengedrongen. In de wet CCIII is een nieuwe definitie opgenomen van een geautomatiseerd werk. Een geautomatiseerd werk is 'een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken' (artikel 80sexies Sr).[15] Voorbeelden van geautomatiseerde werken zijn servers, computers, routers, tablets en smartphones (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 86). Met deze definitie van een geautomatiseerd werk wordt het Cybercrimeverdrag van Europa gevolgd (grotendeels want computergegevens zijn uitgezonderd; *Kamerstukken II* 2015/16, 34 372, nr. 6, p. 13; *Kamerstukken I* 2016/17, 34 372, D).[16] Dat betekent

[15] Zie in dit verband ook de opmerkingen van de Nederlandse Vereniging voor de Rechtspraak in de eerste consultatieronde (bijlage bij *Kamerstukken II* 2015/16, 34 372, nr. 3).

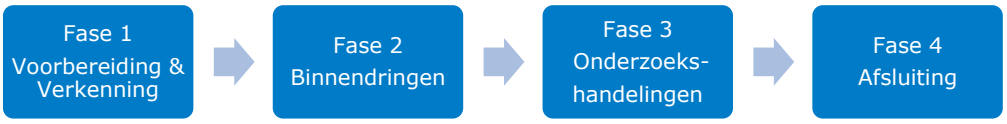
[16] Het uitzonderen van computergegevens is gebeurd op verzoek van het advies van de Raad van State (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 85-86). In eerste instantie was deze passage nog toegevoegd aan de definitie: 'Onder geautomatiseerd werk wordt verstaan (…) alsmede de computergegevens die met dat apparaat of groep van apparaten worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud daarvan' (Concept wetstekst zoals voorgelegd aan de Raad van State, p. 1).

dat gekozen is voor een ruime definitie die betrekking heeft op veel verschillende apparaten.[17] Ook een 'groep van onderling verbonden apparaten' wordt beschouwd als een geautomatiseerd werk. Een bevel kan betrekking hebben op meerdere geautomatiseerde werken, mits de verdachte het geautomatiseerde werk gebruikt en dat het binnendringen noodzakelijk wordt geacht voor de opsporing van strafbare feiten (*Kamerstukken II* 2015/16, 34 372, nr. 6, p. 13).

### 2.3.3 *Uitvoering – vier fases inclusief schema*

Op basis van de documentanalyse kunnen vier fases[18] worden onderscheiden met betrekking tot de inzet van de bevoegdheid, zie figuur 2.1.

**Figuur 2.1 Uitvoering in vier fases**




In de komende paragrafen wordt per fase nader toegelicht welke handelingen daarbinnen moeten plaatsvinden, hoe deze precies moeten worden uitgevoerd en welke actoren hierbij betrokken zijn. Wat betreft dat laatste kan op deze plek al worden genoemd dat bij een opsporingsonderzoek vanuit de politie twee soorten teams betrokken zijn: een tactisch en het technisch team. Het tactisch team houdt zich bezig met het tactisch opsporingsonderzoek en het technisch team dient zich te richten op de voorbereiding en uitvoering van het onderzoek in een geautomatiseerd werk (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 14). De organisatie van het technisch team is ondergebracht bij de Landelijke Eenheid van de Nationale Politie (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 14), team Digit-politie. De 'strikte taakverdeling en functiescheiding' (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 14) wat betreft tactiek en techniek is één van de waarborgen die ervoor moet zorgen dat het opsporingsonderzoek zorgvuldig verloopt (*Kamerstukken I* 2016/17, 34 372, D, p. 41). De wetgever verwacht niet dat deze scheiding de samenwerking tussen het tactisch en het technische team zal belemmeren, omdat de officier van justitie die het onderzoek leidt, een 'schakelfunctie' zal vervullen (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 17).

### 2.3.4 *Fase 1 – Voorbereiding & Verkenning*

Het is de bedoeling dat het tactisch team van de politie eerst een voorstel doet waarom het de bevoegdheid in wil zetten (*Kamerstukken I*, Handelingen 19 juni 2018, p. 19).[19] Zo'n projectvoorstel kan afkomstig zijn van tactische rechercheteams van de politie, van de Kmar of van een bijzondere opsporingsdienst. In het projectplan wordt onder andere aandacht besteed aan de volgende aspecten: een beschrijving van de verdachte, de verdenking, de noodzaak om de onderzoeksbevoegdheid toe te passen en de gewenste resultaten van de toepassing van de bevoegdheid (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 14). Daarna vraagt de officier van justitie een

17 Dit was een belangrijk discussiepunt gedurende het wetgevingstraject, zie bijlage 3.
18 Deze indeling is deels gebaseerd op de PIA (Politie, 2014, p. 8). In de memorie van toelichting worden drie fases onderscheiden. De voorbereidende fase wordt niet expliciet genoemd en de fase 'binnendringen' en 'onderzoek' zijn samengenomen (*Kamerstukken II* 2015/16, 34 372, nr. 3).
19 Er worden verschillende termen gebruikt die raken aan het voorstel dat ingediend moet worden, namelijk projectvoorstel en projectplan (Besluit onderzoek in een geautomatiseerd werk).

technisch team om de haalbaarheid van het onderzoek in te schatten (Besluit onderzoek in een geautomatiseerd werk, 2018. p. 14). Het technisch team stelt op basis van de beschikbare gegevens een rapport haalbaarheidsonderzoek op voor de officier van justitie. Dat rapport bevat een plan van aanpak met betrekking tot de uitvoering van het onderzoek in het geautomatiseerde werk. Verder komen onder andere de volgende onderwerpen naar voren: de benodigde bevelen, of en welke software van derden moet worden aangeschaft en welk technisch hulpmiddel moet worden gebruikt voor het uitvoeren van onderzoekshandelingen (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 16, 44). De officier van justitie gebruikt het haalbaarheidsonderzoek om van het College van Procureurs-generaal toestemming te krijgen voor de inzet van de bevoegdheid en voor de voorafgaande machtiging van de rechter-commissaris (zie ook paragraaf 2.4; Besluit onderzoek in een geautomatiseerd werk, 2018, p. 16). Een onderzoek in een geautomatiseerd werk kan worden uitgevoerd zodra de officier van justitie, na een machtiging van een rechter-commissaris, een bevel heeft afgegeven (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 16).[20] Een bevel wordt afgegeven voor hoogstens vier weken en kan steeds voor een periode van maximaal vier weken worden verlengd (artikel 126nba, lid 3).

Na afgifte van het bevel voert het technisch team een technische voorverkenning uit (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 16). Hieruit moet blijken of een geautomatiseerd werk in gebruik is bij de verdachte (*Kamerstukken II* 2017/18, 34 372, nr. 27). Op basis daarvan wordt een plan van aanpak opgesteld waarin wordt beschreven hoe in een geautomatiseerd werk binnengedrongen zal worden. Dit is een ander plan van aanpak dan het zojuist genoemde plan van aanpak dat betrekking had op de uitvoering van het onderzoek. Dit tweede plan van aanpak zal eerst worden getest in een 'proefopstelling' (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 16).

### *2.3.5 Fase 2 – Binnendringen*

Na het testen in een proefopstelling start de volgende fase, het daadwerkelijk binnendringen in een geautomatiseerd werk. In de nota naar aanleiding van het verslag staat dat binnendringen 'het plaatsen en verwijderen van een technisch hulpmiddel met behulp waarvan gegevens kunnen worden vastgelegd' omvat (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 63). De bedoeling is dat het binnendringen gebeurt op de manier zoals dat in het plan van aanpak (volgend uit 'technische voorverkenningen') beschreven staat (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 16).[21] In de memorie van toelichting staat dat voor de regeling rondom het binnendringen aansluiting is gezocht bij de regeling computervredebreuk in het Wetboek van Strafrecht. Dat betekent dat van binnendringen in elk geval sprake is 'indien de toegang tot het geautomatiseerde werk wordt verworven door het doorbreken van een beveiliging, door een technische ingreep, met behulp van valse signalen of een valse sleutel, of door het aannemen van een valse hoedanigheid (artikel 138ab, eerste lid, Sr)' (*Kamerstukken II* 2016/17, 34 372, nr. 3, p. 15).
Voor het binnendringen kunnen volgens de wetgever verschillende technieken worden gebruikt (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 16). In de eerste

[20] Gedurende de plenaire behandeling van de wet in de Eerste Kamer, zet de minister de hier beschreven werkwijze uitgebreid uiteen (*Kamerstukken I*, Handelingen 19 juni 2018, nr. 34, p. 19).
[21] In de memorie van toelichting staat een aantal manieren beschreven, maar deze opsomming is niet limitatief (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 34).

plaats kan het tactisch team binnendringen met behulp van inloggegevens die door *social engineering* of het gebruik van kunstmatige intelligentie worden verkregen. Ten tweede kunnen personen wiens inloggegevens in het bezit van de politie moeten komen, verleid worden om te reageren op een e-mailverzoek.[22] Als de politie op deze wijze inlogggegevens verkrijgt, is het mogelijk om *malware* te plaatsen waardoor de toegang tot het geautomatiseerde werk 'open' staat en een '*bug*' of '*keylogger*' geplaatst kan worden. Beide kunnen gebruikt worden om na het binnendringen onderzoekshandelingen te verrichten (zie volgende paragraaf). Een derde manier om binnen te dringen is door gebruik te maken van kwetsbaarheden in een computer. Dat zijn bijvoorbeeld fouten en lekken in bestaande software (*Kamerstukken II*, 2015/16, 34 372, nr. 3, p. 34). Er wordt verder geen specifieke informatie gegeven over de wijze van binnendringen, ook al bestaat die wens er bij sommige politieke partijen wel. Het doen van uitspraken over de door de politie gebruikte methoden en technieken wordt gezien als een 'onaanvaardbaar risico voor de inzetbaarheid van die middelen' waardoor de 'effectiviteit van de opsporing' afneemt (*Kamerstukken II* 2016/17, 26 643, nr. 6, p. 58). Wel worden in de nota naar aanleiding van het verslag een aantal nieuwe opties toegevoegd, bijvoorbeeld dat 'brute force' een voorbeeld is waarbij binnengedrongen wordt met behulp van kunstmatige intelligentie (*Kamerstukken II* 2016/17, 26 643, nr. 6, p. 72).

**Kwetsbaarheden**

Zoals gezegd kunnen kwetsbaarheden gebruikt worden om binnen te dringen. Het is niet uitzonderlijk dat software kwetsbaarheden bevat. Softwarefabrikanten zijn continu bezig om hun ontwikkelde software aan te passen (*Kamerstukken II* 2016/17, 26 643, nr. 428, p. 2) en op internet circuleren diverse websites waarop kwetsbaarheden worden gepubliceerd.[23] Tijdens de behandeling van de wet blijken drie soorten kwetsbaarheden onderscheiden te kunnen worden: bekende, bekende onbekende kwetsbaarheden en onbekende onbekende kwetsbaarheden. Een bekende kwetsbaarheid is een kwetsbaarheid die bij een fabrikant van een product reeds bekend is. Fabrikanten van deze producten ontwikkelen regelmatig updates om de bij hun bekende kwetsbaarheden te verhelpen (*Kamerstukken II* 2016/17, 26 643, nr. 428). Dat biedt echter geen garantie dat softwaregebruikers niet meer worden blootgesteld aan de risico's van deze kwetsbaarheid. Zij moeten eerst een update, *patch*, uitvoeren voordat een kwetsbaarheid verholpen is (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 34). Indien een fabrikant geen update verzorgt of indien een softwaregebruiker de update niet installeert, dan blijft de kwetsbaarheid in stand, is deze bekend en kunnen opsporingsinstanties er gebruik van maken.

Een onbekende kwetsbaarheid (zowel bekend onbekend als onbekend onbekend)[24] is een kwetsbaarheid die nog niet via het internet wordt verspreid. Tot het moment van verspreiden is sprake van een *zero day exploit* (*Kamerstukken II* 2015/16, 34 372,

---

22 Hoewel dit als aparte optie in de memorie van toelichting genoemd staat, is ook dit een vorm van *social engineering*. In de nota naar aanleiding van het verslag worden beide begrippen wel van elkaar onderscheiden. Aangegeven wordt dat *social engineering* erop gericht kan zijn 'de verdachte te bewegen handelingen te verrichten zodat software wordt geplaatst op het geautomatiseerde werk dat hij gebruikt, met behulp waarvan verbinding met een andere computer mogelijk wordt gemaakt of met behulp waarvan inloggegevens kunnen worden meegelezen. Met *phishing* wordt geprobeerd de verdachte ertoe te bewegen bepaalde vertrouwelijke gegevens prijs te geven, zoals identificerende gegevens of inloggegevens' (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 72).

23 Zie bijvoorbeeld de websites van het NCSC (NCSC, z.d.).

24 Dit onderscheid wordt in de parlementaire stukken niet altijd expliciet gemaakt, maar kan wel afgeleid worden uit wat staatssecretaris Dijkhoff hierover zegt tijdens de behandeling van de wet in de Tweede Kamer (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34, p. 51).

nr. 3, p. 34).[25] Ook zo'n kwetsbaarheid kan gebruikt worden om een geautomatiseerd werk binnen te dringen. In de memorie van toelichting wordt aangegeven dat het gebruik van *exploits* lastig zal zijn, omdat de kans groot is dat de kwetsbaarheid snel wordt opgelost (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 35).
Bij een bekende onbekende kwetsbaarheid gaat het om een kwetsbaarheid die bekend is bij opsporingsinstanties, maar waarvan de fabrikant nog niet op de hoogte is van het bestaan ervan. In een later toegevoegd wetsartikel, artikel 126ffa Sv, wordt geregeld dat de officier van justitie, na een machtiging van de rechter-commissaris, kan bevelen het melden van een dergelijke kwetsbaarheid uit te stellen (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 15). In deze verplichting ligt impliciet een meldplicht besloten van bekende onbekende kwetsbaarheden in geautomatiseerde werken.

Bij een onbekende onbekende kwetsbaarheid gaat het om een kwetsbaarheid die niet bekend is bij opsporingsinstanties. Zo'n soort kwetsbaarheid kan zich bevinden in software die opsporingsinstanties aanschaffen bij commerciële partijen om 'in bepaalde gevallen het binnendringen in een geautomatiseerd werk' uit te voeren' (*Kamerstukken I* 2016/17, 34 372, D, p. 22). Zo'n commerciële partij zal wel op de hoogte zijn van het gebruik van een onbekende kwetsbaarheid, maar wordt verondersteld deze niet te willen delen. In een memorie van antwoord aan de Eerste Kamer wordt aangegeven dat leveranciers doorgaans niet bereid zijn gedetailleerde informatie over hun product prijs te geven, zoals bijvoorbeeld broncodes (*Kamerstukken I* 2016/17, 34 372, D). Het gevolg hiervan is dat zo'n onbekende kwetsbaarheid niet kan worden gemeld.

In het Besluit staat beschreven dat het gebruik van een commercieel product alleen in een uiterst geval is toegestaan, dat wil zeggen wanneer minder ingrijpende manieren zoals *social engineering* of bekende kwetsbaarheden uitgesloten zijn. De regering wil voorkomen dat de markt van onbekende kwetsbaarheden wordt gestimuleerd, omdat daardoor de veiligheid op het internet negatief beïnvloed zou kunnen worden (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 15). Deze beperking met betrekking tot de aankoop van hacksoftware is ook vastgelegd in het Regeerakkoord 2017-2021 'Vertrouwen in de toekomst'. Slechts 'in een specifieke zaak' mag dit soort software worden gekocht. Bovendien worden er aanvullende eisen gesteld aan de leveranciers van dergelijke software. Zo mogen zij niet verkopen aan dubieuze regimes en zal de AIVD hen screenen (Regeerakkoord Vertrouwen in de toekomst, 2017). Bovendien zal de aanschaf van deze software pas plaatsvinden, nadat dit op centraal niveau binnen het Openbaar Ministerie getoetst is (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 15). Ook wordt de wijze waarop de binnendringingsoftware functioneert getest. Dat gebeurt voordat deze wordt ingezet voor een opsporingsonderzoek. Er zal gekeken worden naar de risico's voor het geautomatiseerde werk dat wordt binnengedrongen, onder andere schade aan derden (*Kamerstukken I* 2017/18, 34 372, G, p. 12).
Omdat de aanschaf van dit soort software te beperken, bestaat de wens dat de politie zelf methoden ontwikkelt om geautomatiseerde werken binnen te kunnen dringen. Ten behoeve hiervan zijn extra financiële middelen vrijgemaakt (*Kamerstukken II* 2018/19, 34 372, 29, p. 9).

[25] In een brief volledig geweid aan de omvang met kwetsbaarheden staat een net iets andere uitleg vermeld. Een kwetsbaarheid die onbekend is bij de fabrikant wordt een '*zero-day vulnerability*' genoemd. Als zo'n kwetsbaarheid gebruikt wordt in software om binnen te dringen, dan wordt gesproken over een '*zero day exploit*' (*Kamerstukken II* 2016/17, 26 643, nr. 428, p. 2).

Voor het binnendringen dient een apart bevel af te worden gegeven. Dit bevel kan gecombineerd worden met het bevel met betrekking tot de te verrichten onderzoekshandelingen (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 63). Het bevel voor de inzet van de bevoegdheid wordt afgegeven voor een periode van vier weken. Het moment van binnendringen kan niet exact worden vastgelegd, maar moet binnen die vier weken gebeuren. Deze periode kan steeds opnieuw worden verlengd (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 51). Als het voor het binnendringen in een geautomatiseerd werk noodzakelijk blijkt om eerst een router binnen te dringen, is daarvoor een bevel van de officier van justitie en een machtiging van de rechter-commissaris vereist. Als van te voren vaststaat dat zowel het geautomatiseerde werk als de router moeten worden binnengedrongen, kan voor beide een bevel worden afgegeven (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 71).

### *2.3.6 Fase 3 – Vijf onderzoekshandelingen*[26]

Nadat het geautomatiseerde werk is binnengedrongen kunnen verschillende onderzoekshandelingen worden verricht (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 16). Het gaat daarbij om onderzoekshandelingen die op afstand worden verricht. Indien dat niet het geval is, is sprake van 'gewone' bijzondere opsporingsbevoegdheden (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 32).
Ten eerste het vaststellen van 'bepaalde' kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit en locatie. Ook het vastleggen van deze kenmerken is hierbij inbegrepen (artikel 126nba, lid 1a). Inzicht in kenmerken wordt van belang geacht, omdat de nieuwe bevoegdheid beperkt is tot een geautomatiseerd werk dat bij de verdachte in gebruik is (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 19). Het geautomatiseerde werk hoeft dus géén eigendom te zijn van de verdachte (*Kamerstukken II* 2017/18, 34 372, nr. 27, p. 12). Deze eerste handeling, te karakteriseren als een virtuele plaatsopneming of inkijkoperatie (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 19), is vooral bedoeld om de inzet van andere onderzoekshandelingen goed voor te bereiden en de verdere richting van het opsporingsonderzoek te bepalen. Een concreet voorbeeld is dat de politie een computer waarvan alleen het Tor-adres bekend is, binnendringt om het IP-adres vast te stellen. Dat adres kan vervolgens gebruikt worden om een bevel tot aftappen en opnemen van communicatie aan de aanbieder te kunnen geven (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 20). Soms zal een 'stapsgewijze aanpak' worden gehanteerd (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 60).
De tweede onderzoekshandeling die onderdeel uitmaakt van de nieuwe bevoegdheid is het uitvoeren van een bevel tot het aftappen en opnemen van communicatie (aftappen van communicatie) of het opnemen van vertrouwelijke communicatie (direct afluisteren; artikel 126nba, lid 1b Sv; Besluit onderzoek in een geautomatiseerd werk, 2018, p. 16; *Kamerstukken I,* Handelingen 19 juni 2018, p. 23).[27] Voor beide geldt dat ze apart geregeld zijn in het Wetboek van Strafvordering en daarom is voor de inzet ervan een afzonderlijk bevel nodig op grond van artt. 126m, 126l, 126s (als sprake is van 126uba Sv), of 126zg Sv (als sprake is van 126zpa Sv). De nieuwe bevoegdheid beperkt zich tot het gebruik van het geautomatiseerde werk om communicatie af te kunnen tappen. Het onderzoek is niet gericht op de gegevens die in het

[26] Een groot deel van deze paragraaf is gebaseerd op de memorie van toelichting en wat hier in het Besluit over geregeld is.
[27] In de oorspronkelijke wetstekst is in artikel 126zpa, lid 1b alleen artikel 126zg (opnemen communicatie die plaatsvindt met gebruikmaking van diensten van een aanbieder) opgenomen en niet artikel 126zf (opnemen vertrouwelijke communicatie). In het voorstel van wet Verzamelwet Justitie en Veiligheid 2022 wordt dit hersteld (*Kamerstukken II* 2021/22, 36 003, nr. 2, p. 17).

geautomatiseerde werk worden opgeslagen behalve de gegevens die betrekking hebben op af te tappen communicatie (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 23).
De derde onderzoekshandeling is het uitvoeren van een bevel tot stelselmatige observatie (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 16). Op afstand kan bijvoorbeeld software op een smartphone worden geïnstalleerd die de GPS-functie activeert. Door een softwareapplicatie op de telefoon te installeren kunnen vervolgens locatiegegevens worden verzonden waardoor het mogelijk wordt om de locatie te bepalen waar die telefoon zich bevindt. Deze locatiebepaling wordt verondersteld nauwkeuriger te zijn dan wanneer mastgegevens worden gebruikt. Een concretere plaatsbepaling komt goed van pas wanneer werkzaamheden van een ObservatieTeam (OT) niet of nauwelijks tot resultaten leiden. Ook kan deze onderzoekshandeling behulpzaam zijn wanneer de politie een verdachte wil aanhouden, maar zijn of haar verblijfplaats onbekend is (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 20). Om een stelselmatige observatie uit te voeren, mag niet heimelijk een woning worden betreden of heimelijk een webcam worden aangezet. Dat geldt ook voor de nieuwe hackbevoegdheid, zo geeft de staatssecretaris aan (*Kamerstukken I* 2016/17, 34 372, D, p. 3). Wel wordt voorgesteld 'de bevestiging van een technisch hulpmiddel op een persoon mogelijk te maken in het kader van de stelselmatige observatie van een geautomatiseerd werk' (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 52).[28]

Het vastleggen van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen[29] is de vierde onderzoekshandeling die kan worden uitgevoerd (artikel 126nba, lid 1d Sv; Besluit onderzoek in een geautomatiseerd werk, 2018, p. 16). Voor de inzet van deze onderzoekshandeling, en ook voor de ontoegankelijkmaking (zie volgende alinea) gelden strengere inzetvoorwaarden. De vierde onderzoekshandeling is breder dan alleen het vastleggen van bepaalde kenmerken van een geautomatiseerd werk en of de gebruiker. Het gaat zowel om gegevens die al aanwezig zijn in het geautomatiseerde werk als om gegevens die gedurende de tijd waarop het bevel betrekking heeft, worden opgeslagen. Een voorbeeld van dit soort gegevens zijn afbeeldingen van kinderporno of wachtwoorden waarmee de versleuteling van gegevens kan worden verwijderd, bijvoorbeeld van cryptocontainers of van een harde schijf. Gegevens kunnen betrekking hebben op communicatie, maar mondelinge communicatie die niet is opgeslagen, is uitgesloten. Daarvoor moet de bevoegdheid tot het aftappen van telecommunicatie worden gebruikt. Het vastleggen van gegevens moet beperkt blijven tot gegevens die redelijkerwijs nodig zijn om de waarheid te achterhalen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 20-21).

De vijfde onderzoekhandeling tot slot, is het ontoegankelijk maken van gegevens (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 16).[30] De mogelijkheid bestaat dat gedurende een opsporingsonderzoek gegevens worden aangetroffen die gebruikt zijn bij het plegen van een strafbaar feit. Indien het voor het beëindigen van een strafbaar feit en/of het voorkomen dat een nieuw strafbaar feit wordt gepleegd, nodig is om de betreffende gegevens ontoegankelijk te maken, kan de officier van justitie daartoe overgaan. Voor deze onderzoekshandeling wordt aangesloten bij de bestaande wettelijke regeling van het ontoegankelijk maken van gegevens (artikel

[28] Deze uitzondering geldt alleen voor de hackbevoegdheid (Commissie modernisering opsporingsonderzoek in het digitale tijdperk, 2018, p. 171).
[29] De term opgeslagen wordt 'neutraal' gebruikt. Er hoeft niet een specifieke handeling van de gebruiker te zijn verricht met het doel om gegevens te bewaren, bijvoorbeeld het opslaan van een tekstbestand in Word (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 20).
[30] Het ontoegankelijk maken van gegevens is ook geregeld in het nieuwe artikel 125p Sv. In dit artikel gaat het om een vordering aan de *aanbieder* om gegevens ontoegankelijk maken. Daar is bij deze onderzoekshandeling geen sprake van.

125o Sv). Ontoegankelijk maken betekent dat maatregelen worden getroffen om ervoor te zorgen dat een beheerder van een geautomatiseerd werk of derden geen kennis meer kunnen nemen of gebruik kunnen maken van de gegevens. Het kan ook betekenen dat verspreiding van gegevens wordt voorkomen of dat gegevens worden verwijderd. Bij verwijdering is het de bedoeling dat gegevens behouden blijven, zodat ze in het kader van strafvordering kunnen worden ingezet. Verder is de inzet van andere maatregelen mogelijk die voorkomen dat anderen kennis kunnen nemen van de gegevens. Zo kan met hardware een computer (tijdelijk) onbruikbaar worden gemaakt en er bestaat software die gegevens kan versleutelen. Een concreet voorbeeld van deze onderzoekshandeling is het onschadelijk maken van een botnet.[31] Het ontoegankelijk maken betreft een voorlopige maatregel. Een rechter zal bij een einduitspraak dan wel afzonderlijke beschikking een beslissing nemen over wat er moet gebeuren met de gegevens die ontoegankelijk zijn gemaakt.

**Technisch hulpmiddel**
Voor het verrichten van onderzoekshandelingen kan een technisch hulpmiddel worden gebruikt.[32] Een technisch hulpmiddel is een 'softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel' (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 2). Het gebruik van een technisch hulpmiddel is niet 'strikt noodzakelijk'. Soms zullen handelingen 'ad hoc en handmatig' worden verricht (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 16).
Een technisch hulpmiddel kent één of meerdere functionaliteiten zoals het maken van screenshots, het opnemen van geluid, het vastleggen van toetsaanslagen en/of het doorzoeken van bestandsmappen om vervolgens gegevens daaruit vast te leggen. De benodigde functionaliteiten dienen in het bevel van de officier van justitie te worden vastgelegd en gedurende het onderzoek moet het technisch hulpmiddel zodanig zijn ingericht dat alleen de functionaliteiten zoals beschreven in het bevel, daadwerkelijk kunnen worden gebruikt (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 37; artikel 8 Bogw).

Bij het verzamelen van gegevens worden in het geautomatiseerde werk gegevens gedetecteerd. Gedetecteerde gegevens zijn gegevens die het technisch hulpmiddel waarneemt in het geautomatiseerde werk dat onderzocht wordt. Het lezen van een bestand op een computer van een verdachte is hier een voorbeeld van (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 38). Vervolgens vindt registratie van de gedetecteerde gegevens plaats. Dit houdt in dat een technisch hulpmiddel de gedetecteerde gegevens overneemt uit het geautomatiseerde werk, bijvoorbeeld het zojuist genoemde bestand op een computer. Wanneer een technisch hulpmiddel wordt gebruikt om gegevens uit de *cloud* te halen, nadat gebruikersnaam en wachtwoord zijn verkregen, dan vinden detectie en registratie pas in het technisch hulpmiddel zelf plaats (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 39). Na de registratie moeten de gegevens direct getransporteerd worden naar de technische infrastructuur van het technisch team (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 40; artikel 27, lid 1 Bogw). Met een technische infrastructuur wordt bedoeld een 'technische voorziening van een technisch team bedoeld voor de vastlegging van

[31] 'Een botnet is een netwerk van aan het internet verbonden gecompromitteerde (computer)systemen, die op afstand kunnen worden aangestuurd (Van der Waagen & Bernaards, 2018, p. 59)'. Een dergelijk netwerk kan ervoor zorgen dat kwaadaardige software wordt verspreid (Van der Waagen & Bernaards, 2018, p. 60), waardoor bijvoorbeeld toetsaanslagen van de computergebruiker worden vastgelegd (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 22).
[32] Ook voor het binnendringen kan overigens software – dat is een technisch hulpmiddel doorgaans ook – worden gebruikt, alleen valt de software die gebruikt wordt voor het binnendringen niet onder definitie zoals die in het Besluit geformuleerd staat.

gegevens ter uitvoering van een bevel (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 2). Alleen ambtenaren die door de korpschef zijn aangewezen hebben toegang tot deze infrastructuur, zo blijkt uit de memorie van toelichting (*Kamerstukken I* 2016/17, 34 372, D, p. 41) en artikel 28 lid 2 Bogw.
Uit het Besluit blijkt verder dat plaatsing op de infrastructuur ('een technische voorziening') nodig is om de betrouwbaarheid en integriteit van het bewijsmateriaal te waarborgen en 'onbevoegde wijziging of kennisneming hiervan te voorkomen' (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 33).
Het technisch hulpmiddel dient zodanig ontworpen te zijn dat het automatisch verzenden van gegevens daadwerkelijk plaatsvindt. Tijdens het transport moeten de geregistreerde gegevens worden beveiligd om wijziging en toegang door onbevoegden te voorkomen (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 40; artikel 28, lid 1 Bogw). Voor de beveiliging geldt dat deze de 'beïnvloeding van een technisch hulpmiddel van buitenaf naar de stand van de techniek zo goed mogelijk' moeten tegengaan (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 39). Een voorbeeld van een beveiligingsmaatregel is het laten plaatsvinden van authenticatie voor de communicatie met een technisch hulpmiddel. Een andere vorm van beveiliging is de versleuteling van gegevens met een digitale handtekening. Gegevens die middels deze bevoegdheid verzameld worden, kunnen gebruikt worden als bewijs. Daarom moeten de integriteit en betrouwbaarheid 'onomstotelijk' vast staan (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 21).
Verder dient een technisch hulpmiddel een uniek gegeven toe te kennen aan de gegevens die geregistreerd worden (artikel 27, lid 2 Bogw), bijvoorbeeld een code die op het moment dat het technisch hulpmiddel werd geplaatst, is toegevoegd. Ook moet een technisch hulpmiddel in staat zijn om aan de geregistreerde gegevens datum en tijdstip toe te kennen, zodat duidelijk is op welk moment precies de gegevens geregistreerd zijn (artikel 27, lid 3 Bogw). Het gaat daarbij overigens om de 'Nederlandse tijd', ook als de gegevens geregistreerd zijn in een andere tijdszone.

*Keuring technisch hulpmiddel*
In de toelichting op het Besluit wordt duidelijk dat in eerste instantie gebruik zal moeten worden gemaakt van een technisch hulpmiddel dat vooraf goedgekeurd is. Keuring achteraf behoort ook tot de mogelijkheden (artikel 15 lid 1 Bogw). Net zoals het gebruik van een technisch hulpmiddel waarvan de aard ervan zich tegen keuring verzet (artikel 21 lid 4 Bogw). Als dat laatste het geval is, moet de officier van justitie in de processtukken opmerken dat afgezien is van keuring. Tevens dient hij of zij op te nemen welke aanvullende waarborgen zijn getroffen (artikel 21 lid 4 Bogw) om de 'betrouwbaarheid, integriteit en herleidbaarheid van vastgelegde gegevens te garanderen' (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 21).
Indien een technisch hulpmiddel goedgekeurd wordt, kan worden aangenomen dat aan de wettelijke eisen met betrekking tot de betrouwbaarheid, integriteit en herleidbaarheid van gegevens is voldaan (Besluit onderzoek in een geautomatiseerd werk, p. 19). 'In bepaalde gevallen' kan het beter zijn onderzoekshandelingen 'handmatig' te verrichten. Dat laatste wordt als een passende mogelijkheid gezien wanneer gegevens direct na het binnendringen kunnen worden ingezien en overgenomen om de identiteit van een geautomatiseerd werk vast te stellen. Of het nodig is een technisch hulpmiddel te gebruiken wordt onder andere afhankelijk geacht van 'de aard van de inzet, de aard van het geautomatiseerde werk en de vraag of gegevens zonder gebruik van een technisch hulpmiddel als rechtmatig bewijs kunnen worden aangemerkt'.[33] Als de officier van justitie beveelt dat er geen technisch

[33] Bij een onderzoekshandeling zonder technisch hulpmiddel kan het onder andere gaan over het verzamelen van gegevens nadat een methode is toegepast waarbij gebruik wordt gemaakt van bij 'de verdachte

hulpmiddel wordt gebruikt, dan dient het onderzoek te worden uitgevoerd 'aan de hand van de in het bevel omschreven onderzoekshandelingen'. Ook dienen 'procedurele waarborgen' (artikel 21, lid 5 Bogw) genomen te worden om 'de betrouwbaarheid, integriteit en herleidbaarheid van de tijdens het onderzoek vast te leggen gegevens te garanderen'. Het technisch team van de politie zal de politie hierover adviseren en de officier van justitie dient in de processtukken de getroffen procedurele waarborgen op te nemen (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 21).

De wijze waarop een keuring plaatsvindt, zal worden omschreven in een keuringsprotocol. Daarin zullen tevens criteria opgenomen worden die tijdens de keuring worden gebruikt (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 42). In het Besluit zijn op basis van artikel 126ee Sv regels geformuleerd aangaande de onderzoekshandelingen die worden verricht met een technisch hulpmiddel. Deze regels moeten ertoe bijdragen dat de bevoegdheid niet wordt misbruikt en dat de authenticiteit en integriteit van de verkregen gegevens verzekerd kan worden (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 54).
Tijdens de keuring dient gekeken te worden naar alle onderdelen van het hulpmiddel die belangrijk zijn voor de 'detectie, registratie en het transport van de gegevens' (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 42). Op basis van onder andere artikel 14, lid 2 Bogw wordt duidelijk dat tijdens de keuring gekeken wordt naar de artikelen 8 t/m 13 van het Besluit. De Keuringsdienst en het Openbaar Ministerie zijn samen verantwoordelijk voor het opstellen van een protocol, dat de minister voorafgaand aan het gebruik ervan goed moet keuren. Mocht een andere keuringsdienst worden aangewezen, dan heeft de Landelijke Eenheid een 'coördinerende rol' bij het formuleren en het gebruik van het keuringsprotocol (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 42).

Het is de bedoeling dat de keuring 'proefondervindelijk' plaatsvindt (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 43). De verwachting is dat deze keuring enkele maanden in beslag kan nemen, zeker wanneer de gebruikte software nog moet worden aangepast om definitief goedgekeurd te worden (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 40). Op het moment dat de keuring is afgerond, dient de keuringsdienst haar bevindingen vast te leggen in een keuringsrapport. Daarin moet een uniek keuringsnummer worden opgenomen dat in alle processen-verbaal die gedurende het opsporingsonderzoek worden opgesteld, kan worden gebruikt wanneer verwezen wordt naar een technisch hulpmiddel. Het veronderstelde voordeel van zo'n uniek nummer is dat verder niets vermeld hoeft te worden over de precieze werking van het hulpmiddel waardoor de kans kleiner is dat opsporingsbelangen geschaad worden. Technische details hoeven immers niet te worden prijsgegeven. Bovendien hebben rechters en advocaten de garantie dat het hulpmiddel dat is ingezet voldoet aan alle wettelijke eisen (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 43). Soms zal het onmogelijk zijn dat een hulpmiddel voldoet aan alle technische eisen die worden gesteld. In dat geval moeten vervangende waarborgen worden ingebouwd (artikel 18, lid 3e Bogw; in de toelichting (p. 43) wordt gesproken over 'vervangende procedurele waarborgen'). Een voorbeeld van een technische eis die niet altijd kan worden ingewilligd is een datum/tijdfunctie. Zo'n functie zorgt er onder andere voor dat precies kan worden vastgelegd wanneer een e-mail is verzonden. In het opsporingsonderzoek zullen maatregelen moeten worden genomen waardoor het ontbreken van een datum/tijd functie niet meer problematisch is. Deze maatregelen

buitgemaakte inloggevens' of 'gegevens die aan een website of het achterliggende systeem onttrokken zijn' (*Kamerstukken II* 2018/19, 34 372, nr. 29, p. 13).

dienen in het proces-verbaal te worden vastgelegd (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 43).

De geldigheidsduur van het keuringsrapport zal vermeld worden in het rapport. Indien binnen die periode de werking van een technisch hulpmiddel of een onderdeel hiervan op zo'n manier wijzigt dat het niet meer aan de gestelde technische eisen kan voldoen, moet een herkeuring worden uitgevoerd. Alle keuringsrapporten worden centraal geregistreerd bij de Landelijke Eenheid. De Inspectie houdt toezicht op de wijze waarop de keuringsprocedure wordt nageleefd (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 43).

**Logging**
Logging, ofwel het continu vastleggen van onderzoekshandelingen die verricht worden, is (ook) een manier om de betrouwbaarheid, integriteit en herleidbaarheid van bewijs te waarborgen. Vier vormen van logging kunnen worden onderscheiden, zo blijkt uit het Besluit (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 17-18).

1 Inzetlogging. Deze logging heeft betrekking op het automatisch vastleggen van het beeldscherm en de toetsaanslagen van de opsporingsambtenaar van het technisch team. Ook betreft deze vorm van logging de communicatie tussen de technische infrastructuur en het geautomatiseerde werk, de gebruikte scripts en softwareversies en het journaal dat de opsporingsambtenaar bijhoudt. In principe is het de bedoeling dat alles automatisch wordt vastgelegd. Indien dat niet mogelijk blijkt, dan moet binnen de politieorganisatie worden vastgelegd dat de logging handmatig gebeurt.
2 Bewijslogging. Dit is een onderdeel van de zojuist besproken inzetlogging. Bewijslogging gaat over het vastleggen van gegevens gedurende de onderzoeksfase, al dan niet met behulp van een technisch hulpmiddel. Deze gegevens kunnen gebruikt worden in een strafzaak.
3 Systeemlogging. Deze vorm heeft betrekking op de logging die reeds plaatsvindt door (alle) gebruikte systemen en die op centraal niveau wordt verzameld en vastgelegd. Systeemlogging moet ertoe bijdragen dat problemen met betrekking tot de betrouwbaarheid, integriteit en de beschikbaarheid van de technische infrastructuur worden gesignaleerd en opgelost.
4 Authenticatie- en autorisatielogging, een subonderdeel van systeemlogging dat betrekking heeft op de toegang tot een technisch hulpmiddel.

Naar aanleiding van een vraag van D66 legt de minister uit dat logbestanden worden opgeslagen op een infrastructuur die het technisch team gebruikt. Deze gegevens mogen niet worden bewerkt en zijn alleen toegankelijk voor opsporingsambtenaren die daartoe geautoriseerd zijn door de korpschef. Ook moeten deze gegevens beveiligd zijn tegen 'wijziging of onbevoegde' kennisneming (*Kamerstukken II* 2017/18, 34 372, nr. 27, p. 12).
Indien uit loggegevens blijkt dat een onregelmatigheid heeft plaatsgevonden die de betrouwbaarheid en integriteit van de verzamelde gegevens beïnvloedt, dan dient de opsporingsambtenaar van het technisch team een proces-verbaal op te maken (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 18). Het melden van een eventuele (technische) onregelmatigheid in een proces-verbaal is in het Besluit opgenomen naar aanleiding van een advies van de Raad voor de Rechtspraak (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 46). Een officier van justitie en een rechter zullen vervolgens een oordeel vellen over de vraag of de onregelmatigheid van invloed is op de bewijskracht van de gegevens. Ook de Inspectie heeft toegang tot

logginggegevens. Zij kan deze gebruiken in het kader van het toezicht dat zij uitvoert op de bevoegdheid (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 18). Mochten er tijdens een rechtszaak twijfels zijn over de betrouwbaarheid en integriteit van het bewijsmateriaal dan kan de rechter om meer informatie vragen of een deskundige raadplegen. De rechter beschikt hierbij over de procedure zoals die vastgelegd is in artikel 187d Sv. Dat betekent dat de rechter-commissaris kan voorkomen dat de verdachte(-n) en zijn of haar advocaat kennis nemen van de informatie die aan de rechter wordt verstrekt. Dat is toegestaan indien er voldoende aanwijzingen zijn dat openbaarmaking opsporingsbelangen schaadt (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 22).

**Deskundigheid team**

Zoals eerder aangegeven houdt het technische team zich bezig met zowel het binnendringen als met het verrichten van onderzoekshandelingen. Een belangrijke vereiste voor teamleden is dat zij beschikken over 'specialistische kennis en vaardigheden' op het gebied van ICT (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 13), een reden waarom ook buitengewone opsporingsambtenaren aangewezen worden. Deze specialistische kennis moet ervoor zorgen dat onderzoekshandelingen op professionele wijze worden uitgevoerd, zodat bijvoorbeeld computersystemen waarin deze handelingen plaatsvinden, blijven werken. Ook kennis over het juridisch kader waarbinnen het onderzoek in een geautomatiseerd werk plaatsvindt en vaardigheden met betrekking tot het opmaken van een proces-verbaal behoren tot het kwalificatiepakket waaraan een technisch teamlid zou moeten voldoen (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 35). Een opsporingsambtenaar kan lid worden van het technisch team indien hij of zij voldoet aan de kwalificaties zoals deze zijn aangewezen door de Minister van Justitie en Veiligheid. Welke kwalificaties dat precies zijn, is verder uitgewerkt in een ministeriële regeling (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 14).[34] Omdat het lidmaatschap van een technisch team een specialistische functie betreft, wordt verwacht dat de leden ervan vooral zijinstromers zijn. Een volledige politieopleiding is niet nodig (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 35). De korpschef zal één of meer ambtenaren aanwijzen die de toegang tot technische hulpmiddelen registreert (artikel 22, lid 1 Bogw). Deze kan vervolgens een collega ('een met plaatsing belaste opsporingsambtenaar) toegang geven tot het technisch hulpmiddel (artikel 22, lid 2 Bogw). In incidentele gevallen is het toegestaan dat het technisch team samenwerkt met andere opsporingsambtenaren. Dat geldt bijvoorbeeld voor situaties waarin deze ambtenaren beschikken over unieke vaardigheden en kennis die nodig kunnen zijn om op een goede manier uitvoering te geven aan een bevel. De korpschef velt hier een oordeel over en als dat oordeel positief uitvalt, wordt de opsporingsambtenaar tijdelijk toegevoegd aan het technisch team. Gedurende zijn/haar deelname aan het team is het de bedoeling dat een al bestaand lid van het technische team hem of haar begeleidt (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 14).

### *2.3.7 Fase 4 – Afsluiten onderzoek*

Op het moment dat het technisch team het doel van het onderzoek in een geautomatiseerd werk heeft bereikt, of de geldigheidsduur van het bevel is verlopen, zal het technisch team het onderzoek beëindigen. Als gebruik is gemaakt van een technisch hulpmiddel, dan wordt dit zoveel als mogelijk verwijderd, zodat de server van de politie geen gegevens meer kan ontvangen. Soms verwijdert het technisch

[34] Deze regeling staat gepubliceerd in de Staatscourant 2019, nr. 10910.

team zelf een technisch hulpmiddel, soms beschikt een technisch hulpmiddel over een functionaliteit die zorgt voor automatische vernietiging na een vooraf ingestelde periode. Rondom het verwijderingsproces is het niet uitgesloten dat sporen achterblijven van het technisch hulpmiddel dat is gebruikt. Deze kunnen ontstaan als gevolg 'van de invloed van het geïnstalleerde technisch hulpmiddel op het geautomatiseerde werk, of van handelingen die het technisch team uitvoerde om het middel te plaatsen en of te verwijderen' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 36). Er kunnen zich situaties voordoen waarin besloten wordt om een technisch hulpmiddel niet te verwijderen of de aangebrachte wijzigingen aan het geautomatiseerde werk niet ongedaan te maken. Aan een dergelijke beslissing dienen zwaarwegende belangen ten grondslag te liggen. Daarbij kan gedacht worden aan de reële kans dat de verwijdering een flink risico oplevert voor het systeem waarbinnen het geautomatiseerde werk is geïnstalleerd. Mocht een middel niet volledig verwijderd worden, dan zorgt het technisch team ervoor dat de politie geen data meer kan ontvangen van het betreffende geautomatiseerde werk (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 36; artikel 26, lid 1 Bogw). Bovendien zal de officier van justitie, indien het niet volledig verwijderen risico's oplevert voor het functioneren van het geautomatiseerde werk, de beheerder van het geautomatiseerde werk op de hoogte stellen en informatie verstrekken zodat (sporen van) de software verwijderd kunnen worden (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 36-37; artikel 26, lid 2 Bogw). Van de verwijdering van het technisch hulpmiddel of van het feit dat het transport van gegevens stop is gezet, dient een proces-verbaal opgemaakt te worden (artikel 26, lid 3 Bogw). Op basis van logging zou kunnen worden gecontroleerd of het ontvangen van gegevens op de technische infrastructuur daadwerkelijk gestopt is. De Inspectie Justitie en Veiligheid neemt het verwijderproces mee in haar toezicht (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 47).

Het is de bedoeling dat het technisch team de resultaten van het onderzoek overdraagt aan het tactisch team (artikel 29 lid 1 Bogw). Mocht het binnen de reikwijdte van het bevel passen en in het kader van het opsporingsonderzoek nodig zijn, dan kunnen gegevens worden gefilterd. Dat gebeurt onder andere bij het aftappen en opnemen van telecommunicatie. Ten behoeve van de inzet van een dergelijke bevoegdheid wordt een lijst opgesteld van e-mailadressen waarvan het communicatieverkeer bijgehouden dient te worden. Gedurende de inzet van de bevoegdheid kunnen gegevens worden verzameld van personen die géén onderwerp van onderzoek zijn in het opsporingsonderzoek (en dus niet op de vooraf opgestelde lijst staan). Het technisch team filtert deze gegevens eruit, omdat het tactisch team alleen het e-mailverkeer krijgt van personen die op de lijst staan (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 48). Het filteren moet met een forensisch kopie van de vastgelegde gegevens gebeuren en het technisch team dient de bewerkingen die zij uitvoert vast te leggen (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 17; artikel 29 lid 2 en 3 Bogw).
Voor geheimhoudersgegevens gelden de reeds bestaande wettelijke kaders zoals vastgelegd in artikel 126aa Sv.

Processen-verbaal worden gebruikt om in een strafzaak verantwoording af te leggen (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 22). Gestreefd wordt naar een 'zo spoedig mogelijke afronding van het proces-verbaal (*Kamerstukken II* 2016/17, 34 372, nr. 3, p. 78). Ook 'andere voorwerpen waaraan gegevens kunnen worden ontleend die voor het onderzoek in de zaak van betekenis zijn' kunnen worden gebruikt. Het kan zijn dat wordt gekozen voor 'een minder gedetailleerde verantwoording'. Dat wordt gerechtvaardigd geacht wanneer 'bijzondere belangen' in

het spel zijn zoals de 'afscherming van opsporingsmethodieken en –middelen'. Het is aan de officier van justitie om hier een oordeel over te vellen (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 22). Indien tijdens het onderzoek gebruik is gemaakt van een goedgekeurd technisch hulpmiddel, kan worden aangenomen dat de gegevens betrouwbaar, integer en herleidbaar zijn. In dat geval dient in het proces-verbaal alleen te worden verwezen naar het keuringsnummer en hoeft géén informatie te worden gedeeld over de samenstelling van het hulpmiddel. Als onderzoekshandelingen hebben plaatsgevonden zonder goedgekeurd technisch hulpmiddel, dan moet de officier van justitie in de processtukken aangegeven welke aanvullende waarborgen zijn getroffen (artikel 21, lid 4 Bogw) in het kader van de betrouwbaarheid, integriteit en herleidbaarheid (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 22). Indien geen technisch hulpmiddel wordt gebruikt, dienen procedurele waarborgen te worden getroffen (artikel 21, lid 5 Bogw; Besluit onderzoek in een geautomatiseerd werk, 2018, p. 22).[35]

**Bewaren en vernietigen van gegevens**

Gegevens die op de technische infrastructuur worden vastgelegd zijn persoonsgegevens waarop de Wet politiegegevens (Wpg) van toepassing is. Dat geldt voor alle soorten gegevens die gedurende het opsporingsonderzoek beschikbaar zijn. Daarbij gaat het om de door het technisch team verzamelde en bewerkte gegevens, logbestanden en gegevens die het tactisch team tot haar beschikking heeft en krijgt. Op basis van het Besluit blijkt dat de bewaartermijn van de gegevens afhangt van het doel waarvoor de gegevens verzameld worden. De verwachting is dat opsporingsinstanties het grootste deel van de gegevens verwerken in het kader van een opsporingsonderzoek (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 22). Op het moment dat gegevens niet langer nodig zijn voor het doel van het onderzoek, mogen zij maximaal een halfjaar worden bewaard om te bekijken of zij aanleiding geven tot een nieuw onderzoek of een nieuwe verwerking. Hoe lang een periode duurt totdat gegevens niet meer nodig zijn, is niet exact vastgelegd, maar is, aldus het Besluit, afhankelijk van het moment waarop de rechter een beslissing heeft genomen die onherroepelijk is. Het komt voor dat een zaak niet wordt ingezonden aan het Openbaar Ministerie, omdat deze niet is opgelost. De zaak wordt dan doorgaans op een lager pitje voortgezet. Ook gedurende die periode mogen gegevens bewaard worden, niet oneindig maar tot het moment waarop de feiten die in het onderzoek centraal staan, zijn verjaard (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 22-23). Daarna mogen gegevens nog vijf jaar worden bewaard ten behoeve van de afhandeling van eventuele klachten en of verantwoording van onderzoeksactiviteiten die hebben plaatsgevonden. Na die vijf jaar dienen gegevens gearchiveerd of vernietigd te worden (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 23).[36]

Voor het verwijderen van gegevens van 'onschuldige derden' gelden verschillende verwijderingsregimes, zo blijkt uit een Verslag van een schriftelijk overleg over het Besluit (*Kamerstukken II* 2018/19, 34 372, nr. 29, p. 14). Het verwijderregime is

[35] Bij een niet (goed-)gekeurd middel gaat het om aanvullende waarborgen (artikel 21, lid 4) en bij een inzet zonder technisch hulpmiddel om procedurele waarborgen (artikel 21, lid 5). De aanvullende waarborgen dienen opgenomen te worden in de processtukken als keuring achterwege blijft of als geen gebruik wordt gemaakt van een technische hulpmiddel (Besluit onderzoek in een geautomatiseerd werk, p. 22.). Onduidelijk is wat er met de procedurele waarborgen moet gebeuren.

[36] De officier van justitie houdt gegevens beschikbaar voor het onderzoek die verkregen zijn door observatie, het opnemen van vertrouwelijke communicatie en het opnemen van telecommunicatie met een technisch hulpmiddel en die niet bij de processtukken zijn gevoegd. Twee maanden na het beëindigen van het onderzoek en het op de hoogte stellen van betrokkenen dat bevoegdheden zijn ingezet, vernietigt de officier van justitie de processen-verbaal en andere voorwerpen (Besluit onderzoek in een geautomatiseerd werk, p. 23).

afhankelijk van de onderzoekshandeling die is uitgevoerd. Wanneer het gaat om handelingen met als doel om telecommunicatie af te tappen of vertrouwelijke communicatie op te nemen, dan dienen gegevens binnen twee maanden te worden vernietigd na beëindiging van het onderzoek. Tenzij de gegevens kunnen worden gebruikt voor een ander strafrechtelijk onderzoek (artikel 126cc Sv). Als gegevens verzameld zijn door andere onderzoekshandelingen dan geldt het regime van de Wet Politiegegevens. Binnen de wet wordt onderscheid gemaakt tussen verschillende doelen in het kader waarvan gegevensverzameling heeft plaatsgevonden. De algemene regel is dat 'politiegegevens worden verwijderd zodra ze niet meer nodig zijn voor het doel waarvoor ze worden verwerkt of zodra de termijn voor de verwerking is verlopen'. Daarna worden de gegevens verwijderd. De bewaartermijn voor de verwijderde gegevens is vijf jaar. De verwijderde politiegegevens zijn niet langer toegankelijk voor operationele doeleinden. De gegevens worden als het ware apart gezet en kunnen niet aan derden worden verstrekt. Wel kunnen de verwijderde gegevens worden gebruikt ten behoeve van de afhandeling van klachten en de verantwoording van verrichtingen. Nadat de periode van vijf jaar is verstreken, worden de verwijderde politiegegevens vernietigd. Van de vernietiging kan worden afgezien voor zover de waarde van de archiefbescheiden als bestanddeel van het cultureel erfgoed of voor historisch onderzoek zich daartegen verzet' (*Kamerstukken II* 2018/19, 34 372, nr. 29, p. 14).

## 2.4 Waarborgen voor controle

De controle rondom de inzet van de bevoegdheid vindt plaats op grofweg drie momenten in de tijd[37] te weten voorafgaand, gedurende en na afloop van de inzet. Daarbij zijn verschillende actoren betrokken die in de komende subparagrafen de revue passeren. Achtereenvolgens wordt aandacht besteed aan het Openbaar Ministerie (paragraaf 2.4.1), de rechter (paragraaf 2.4.2), de keuringsdienst (paragraaf 2.4.3), de Inspectie Justitie en Veiligheid (paragraaf 2.4.4) en andere actoren (paragraaf 2.4.5).

### *2.4.1 Het Openbaar Ministerie*

Binnen het Openbaar Ministerie is er vanuit verschillende niveaus betrokkenheid bij de controle op de inzet van de bevoegdheid, zowel voorafgaand aan de inzet als tijdens de inzet. Een deel van die betrokkenheid vloeit logisch voort uit artikel 126nba, lid 1 Sv. Zoals eerder beschreven stelt de officier van justitie een vordering tot machtiging op voor de rechter-commissaris en later, als de machtiging wordt verleend, een bevel voor de politie. Voorafgaand hieraan is ook de landelijk officier van justitie betrokken die deze bevoegdheid in zijn of haar portefeuille heeft (*Kamerstukken I*, Handelingen 19 juni 2018, nr. 34, p. 19).[38] Voordat de officier van justitie definitief een vordering tot machtiging doet, wordt de voorgenomen inzet voorgelegd is aan de Centrale Toetsingscommissie (CTC). De CTC is een intern adviesorgaan binnen het Openbaar Ministerie. Zij toetst de inzet aan wet- en regelgeving, jurisprudentie, proportionaliteit, subsidiariteit en de mogelijke afbreukrisico's. Daarnaast overweegt de CTC de effectiviteit van de bevoegdheid en het afbreukrisico tegen het belang van de hantering van de bevoegdheid in een concreet geval. De CTC legt haar advies

[37] Deze momenten zijn niet altijd scherp te onderscheiden, maar voor de leesbaarheid van de tekst en het begrip worden ze op deze wijze besproken.

[38] Deze functie is pas gedurende het wetgevingstraject ontstaan. In de memorie van toelichting bijvoorbeeld bestond deze functie van een aparte landelijk officier van justitie nog niet.

vervolgens voor aan het College van Procureurs-Generaal (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 38), die een definitieve beslissing neemt. Daarbij wordt onder andere het rechtsmatigheidscriterium meegenomen (*Kamerstukken I* 2016/17, 34 372, D). De toetsing door de CTC kan via een spoedprocedure verlopen. Een zaak wordt in dat geval zo snel mogelijk getoetst en het advies wordt (mondeling) voorgelegd aan het College van PG's. Die kan op haar beurt een (mondelinge) beslissing nemen (*Kamerstukken II* 2016/17, 34 372, nr. 6).

Gedurende het onderzoek houdt de officier van justitie toezicht op de toepassing van opsporingsbevoegdheden.[39] Als leider van het opsporingsonderzoek (en gerechtelijke ambtenaar) controleert hij/zij het werk van opsporingsambtenaren (*Kamerstukken I* 2016/17, 34 372, D). Er is een aantal specifieke onderwerpen ten aanzien waarvan de officier van justitie beslissingen dient te nemen. Eén daarvan is de keuze om een technisch hulpmiddel later of helemaal niet te laten keuren. De officier van justitie zal moeten afwegen of hij/zij van deze mogelijkheid gebruik wil maken. Bovendien dient hij/zij, indien de aard van het technisch hulpmiddel zich verzet tegen een keuring, in de processtukken te vermelden welke aanvullende waarborgen ingebouwd zijn om de betrouwbaarheid, herleidbaarheid en integriteit van de verzamelde gegevens te garanderen (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 21). Ook is de officier van justitie betrokken bij de verlenging van een inzet (artikel 126nba Sv, lid 5) en bij het uitstellen van het melden van kwetsbaarheden (artikel 126ffa Sv). Als gevolg van de machtigingsstructuur dient de rechter-commissaris over beide punten een uitspraak te doen.

### *2.4.2 De rechter*

In het Wetboek van Strafvordering is in de fase voordat een bevoegdheid wordt toegepast een belangrijke rol weggelegd voor de rechter-commissaris (*Kamerstukken II* 2015/16, 34 372, nr. 4). Deze rol is afhankelijk van de inbreuk op de privacy die de bevoegdheid maakt en het risico voor de beheersbaarheid en de integriteit van de opsporing. In het geval van de hackbevoegdheid beoordeelt de rechter-commissaris de vordering tot machtiging die de officier van justitie aan hem/haar doet. In de machtiging moet een aantal inhoudelijke punten worden uitgelicht waardoor de rechter-commissaris tot een onderbouwd oordeel kan komen. De volgende aspecten komen hierbij aan de orde (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 38; *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 30):

1 Het misdrijf inclusief de feiten en omstandigheden die ten grondslag liggen aan de verdenking (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 30).
2 identificatie geautomatiseerd werk, bijvoorbeeld een IP-adres. Het is belangrijk om hier inzicht in te hebben zodat de reikwijdte van de bevoegdheid voldoende kan worden afgebakend. Bovendien is deze informatie nodig om uitspraken te kunnen doen over de proportionaliteit van de bevoegdheid. Indien gedurende het opsporingsproces duidelijk wordt dat een extra geautomatiseerd werk moet worden binnengedrongen, dan is een aanvullende machtiging van de rechter-commissaris nodig. Dat geldt overigens ook als gedurende het onderzoek een nieuw strafbaar feit boven tafel komt (*Kamerstukken II* 2016/17, 34 372, nr. 6).
3 Locatie van het geautomatiseerde werk. Indien bekend is dat een geautomatiseerd werk zich *niet* in Nederland bevindt of indien de locatie onbekend is, dan dient de rechter-commissaris hiervan op de hoogte te worden gesteld.

[39] In de empirische hoofdstukken zal blijken dat de zaaksofficier het tactisch team aanstuurt en de landelijk officier van justitie het technisch team (zie onder andere hoofdstuk 3).

4 Doel bevoegdheid. Duidelijk moet worden welke concreet doel in het opsporingsonderzoek behaald moet worden door de inzet van de bevoegdheid.
5 Technisch hulpmiddel. Als voor het verrichten van onderzoekshandelingen gebruik wordt gemaakt van een technisch hulpmiddel, dan moeten de aard en functionaliteit ervan worden vermeld, het deel van het geautomatiseerde werk waarop het hulpmiddel geplaatst wordt en de categorie gegevens die verzameld wordt.
6 Tijdsduur van de inzet van de bevoegdheid (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 30).
Extra informatie over de afzonderlijke bevoegdheid. Indien in het bevel de inzet van afzonderlijke bijzondere opsporingsbevoegdheden aan de orde is, zoals direct afluisteren, het aftappen van communicatie en stelselmatige observatie, dan kan in het bevel aandacht worden besteed aan gegevens die in een afzonderlijk bevel voor de toepassing van die bevoegdheden moeten worden opgenomen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 30).

Aan de hand van deze informatie toetst de rechter-commissaris de reikwijdte van het onderzoek en of de inzet proportioneel en subsidiair is (*Kamerstukken II* 2016/17, 34 372, nr. 6).[40] Voor zowel het binnendringen als voor de afzonderlijke onderzoekshandelingen zijn machtigingen nodig van de rechter-commissaris. Deze mogen worden samengenomen in één machtiging (*Kamerstukken II* 2016/17, 34 372, nr. 6). De rechter-commissaris kijkt in principe niet of de uitvoering van de bevoegdheid op correcte wijze verloopt. Hij/zij kan echter wel bepalen dat het binnendringen en of het uitvoeren van bepaalde onderzoekshandelingen in zijn/haar aanwezigheid moet gebeuren. Die keuze is aan de rechter-commissaris (*Kamerstukken II* 2016/17, 34 372, nr. 6). Hij/zij neemt ook een besluit over de vraag of de inzet van de bevoegdheid met vier weken verlengd mag worden (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34), een stapsgewijze aanpak nodig is (*Kamerstukken II* 2016/17, 34 372, nr. 6) en of het melden van een kwetsbaarheid uitgesteld kan worden (*Kamerstukken I* 2018/19, 34 372, L).

Op het moment dat het opsporingsonderzoek is afgerond, kan een zaak voor de rechter worden gebracht. Deze zittingsrechter beoordeelt de manier waarop het bewijs is verzameld inclusief de bevoegdheden die zijn ingezet. Zowel de rechter-commissaris als de rechter hebben een rol met betrekking tot het toetsen van de rechtmatigheid van de inzet (*Kamerstukken I* 2016/17, 34 372, D). Ook kan de rechter alle beschikbare informatie opvragen of een deskundige raadplegen wanneer er twijfels zijn over de betrouwbaarheid en integriteit van het bewijs (Besluit onderzoek in een geautomatiseerd werk, 2018).

### *2.4.3 De Keuringsdienst*

Gedurende het onderzoek kan, zoals eerder aangegeven, besloten worden om een technisch hulpmiddel te gebruiken. Om de betrouwbaarheid, herleidbaarheid en integriteit van de verzamelde gegevens te kunnen garanderen zijn diverse eisen gesteld aan dit hulpmiddel (Besluit onderzoek in een geautomatiseerd werk, 2018, , p. 18-19). Elk technisch hulpmiddel dient in principe aan een keuringsdienst te worden voorgelegd om te beoordelen of aan de gestelde eisen wordt voldaan (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 21). De Dienst Landelijke

[40] In een antwoord op vragen van D66 legt de minister in de Eerste Kamer uit dat de rechter-commissaris ook naar de wijze van binnendringen zal kijken, omdat dat behoort tot de 'methodische aanpak' (*Kamerstukken I*, Handelingen 34, 19 juni 2018, p. 16).

Operationele Samenwerking van de politie zal de keuringstaak op zich nemen.[41] Zij moet ervoor zorgen dat een 'objectief en onafhankelijk oordeel' wordt gegeven over het hulpmiddel. Overigens staat in het Besluit beschreven dat eventueel ook een andere organisatie kan worden aangewezen als keuringsdienst (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 42). De korpschef zal het technisch hulpmiddel bij de keuringsdienst aanbieden om gekeurd te worden (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 43).

### *2.4.4 De Inspectie Justitie en Veiligheid*

Het zogenoemde 'systeemtoezicht' is in handen van de Inspectie Justitie en Veiligheid (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34).[42] Wettelijk is vastgelegd dat deze Rijksinspectie (*Kamerstukken II* 2016/17, 34 372, nr. 6) toezicht houdt op de wijze waarop de politie haar taak uitvoert. Vanuit die rol houdt zij (ook) toezicht op 'het functioneren van het wettelijke systeem rond de uitvoering van een bevel tot onderzoek in een geautomatiseerd werk' (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 23; artikel 126nba, lid 7 Sv). Daarbij neemt zij de regels en voorschriften mee die in het Wetboek van Strafvordering en het Besluit technische hulpmiddelen Strafvordering zijn neergelegd (*Kamerstukken II* 2016/17, 34 372, nr. 6).[43] Het toezicht heeft zowel betrekking op zaken die na een opsporingsonderzoek worden voorgelegd aan de rechter als op zaken waarbij dat laatste niet aan de orde is. De Inspectie kan haar toezicht zelf vormgeven. Zij is niet afhankelijk van meldingen die van buitenaf komen (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34, p. 47). De Inspectie neemt in haar toezicht diverse onderwerpen mee (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 23-24). Zo dient zij aandacht te besteden aan de autorisatie van de betrokken opsporingsambtenaren en hun kennis en expertise, de inzet van technische hulpmiddelen (inclusief de vraag of gegevens op een zorgvuldige manier en binnen de bestaande kaders worden verwerkt (*Kamerstukken II* 2017/18, 34 372, nr. 27), de naleving van technische vereisten en de keuringsprocedure (Besluit onderzoek in een geautomatiseerd werk, 2018), logging en de beveiliging van gegevens en de manier waarop deze worden gebruikt, bewaard en vernietigd (*Kamerstukken I* 2016/17, 34 372, D)). Het toezicht richt zich niet alleen op de fase nadat een onderzoek heeft plaatsgevonden, maar de Inspectie kan ook steekproefsgewijs meekijken in de praktijk bij het daadwerkelijk binnendringen en onderzoek doen in een geautomatiseerd werk (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 24). Haar bevindingen legt de Inspectie jaarlijks vast in een Verslag dat openbaar wordt gemaakt. Indien structurele problemen worden geconstateerd, kan zij de politie vragen een 'verbeterplan' op te stellen. Ook kan besloten worden om het toezicht op sommige terreinen verder 'te intensiveren' (*Kamerstukken I* 2017/18, 34 372, G).

De taken van de Inspectie hebben betrekking op de uitvoering (vindt de inzet plaats volgens 'relevante wet- en regelgeving en binnen de kaders van het bevel van de officier van justitie en de machtiging van de rechter-commissaris'; *Kamerstukken I* 2017/18, 34 372, G), maar zij toets niet de rechtmatigheid van de concrete inzet. Dat is aan de rechter ter terechtzitting (*Kamerstukken II* 2016/17, 34 372, nr. 6).[44]

---

41 De Raad voor de Rechtspraak en de Nederlandse Vereniging voor Rechtspraak hadden liever gezien dat de keuringstaak buiten de politie zou zijn neergelegd (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 43).

42 Het systeemtoezicht en de uiteindelijke rol van de Inspectie hierin is een belangrijk discussiepunt geweest gedurende het wetgevingstraject. Zie bijlage 3.

43 Uiteindelijk is het Besluit er bijgekomen.

44 Op basis van de Kamerstukken lijkt de minister zichzelf enigszins tegen te spreken. In de Eerste Kamer geeft hij aan dat de Inspectie ook kijkt naar rechtmatigheid van de inzet van de hackbevoegdheid. Het

Vanwege de werkzaamheden die de Inspectie in het kader van de nieuwe bevoegdheid moet gaan verrichten, is het Besluit politiegegevens licht aangepast: er is een verplichting gekomen tot het verstrekken van politiegegevens ten behoeve van de toezichthoudende taak van de Inspectie (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 24).

### *2.4.5 Andere actoren*

Naast bovengenoemde actoren speelt een aantal andere actoren een rol met betrekking tot toetsing en toezicht. In de eerste plaats de politie zelf. Binnen de politieorganisatie houden leidinggevenden toezicht op de uitvoering van het bevel (*Kamerstukken II* 2016/17, 34 372, nr. 6). Uitvoerende medewerkers maken hun werk inzichtelijk doordat zij processen-verbaal opmaken waarin zij zo snel mogelijk hun opsporingshandelingen moeten beschrijven (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34). Ten tweede houdt de Autoriteit Persoonsgegevens toezicht op de naleving van wetgeving op het terrein van het beschermen van persoonsgegevens door organisaties die zich bezig houden met rechtshandhaving (*Kamerstukken I* 2016/17, 34 372, D). De Autoriteit Persoonsgegevens heeft géén rol bij de voorafgaande keuring van een technisch hulpmiddel (*Kamerstukken II* 2017/18, 34 372, nr. 27). De Nationale Ombudsman is een derde toezichtsactor. Indien burgers klachten hebben over het strafvorderlijk optreden van een institutie, kan de Nationale Ombudsman aanvullende rechtsbescherming bieden. Een voorwaarde hierbij is dat burgers géén toegang hebben tot een rechter of dat deze 'zich niet heeft uitgelaten over een gedraging die een strafvorderlijk aspect kent (*Kamerstukken I* 2016/17, 34 372, D). Met betrekking tot de nieuwe bevoegdheid geldt dat bijvoorbeeld voor een situatie waarin niet vervolgd wordt en niet aan de notificatieplicht wordt voldaan (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34).

## 2.5 Grondrechten en waarborgen

Eerder is duidelijk geworden dat de nieuwe bevoegdheid raakt aan de grondrechten van burgers (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 50). In de memorie van toelichting wordt de meeste aandacht besteed aan het recht op de bescherming van de persoonlijke levenssfeer, kortweg privacy. Daarbij wordt het Europees Verdrag voor de Rechten van de Mens (EVRM) gevolgd, meer in het bijzonder het beoordelingskader van artikel 8 EVRM. Het recht op de bescherming van de persoonlijke levenssfeer betekent dat de overheid respect moet hebben voor de persoonlijke levenssfeer van burgers en dat burgers het recht hebben om 'met rust gelaten te worden' en om 'onbevangen zichzelf te kunnen zijn' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 52). Het beperken van dit recht kan alleen als dit bij wet geregeld is. Verder moet, volgend uit artikel 8 lid 2 EVRM, de beperking noodzakelijk zijn in een democratische samenleving in het kader van 'de openbare veiligheid of het voorkomen van wanordelijkheden en strafbare feiten'. Deze noodzakelijkheid wordt onder andere bepaald door de beginselen proportionaliteit en subsidiariteit (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 52). Naast proportionaliteit en subsidiariteit dient de

begrip rechtmatigheid heeft betrekking op een rechtmatige toepassing. Het is niet de bedoeling dat de Inspectie kijkt naar de oordeelsvorming van de officier van justitie en de rechter-commissaris (*Kamerstukken I* 2017/18, 34 372, G). Het handelen van de officier wordt getoetst door de Procureur-Generaal bij de Hoge Raad en de rechter ter terechtzitting. De Inspectie kan wel de PG-HR op de hoogte stellen wanneer sprake is van 'schendingen van wettelijke voorschriften door of in opdracht van de officier van justitie'. Ook kan zij de Autoriteit Persoonsgegevens informeren wanneer sprake is van een mogelijke schending van de regels rond de bescherming van persoonsgegevens (*Kamerstukken II* 2016/17, 34 372, nr. 6).

kwaliteit (toegankelijkheid en kenbaarheid) van het recht op orde te zijn. In de memorie van toelichting wordt aangegeven dat uit artikel 126nba Sv voldoende duidelijk wordt wat de bevoegdheid inhoudt. Toch dienen in het recht altijd *waarborgen* te zijn opgenomen die moeten voorkomen dat de bevoegdheid wordt misbruikt en er sprake is van willekeurige inmenging in het leven van burgers (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 52). De waarborgen worden strikter naarmate een bevoegdheid ingrijpender wordt en een heimelijke toepassing ervan mogelijk is (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 52).

Vanwege de ingrijpendheid van de bevoegdheid zijn diverse waarborgen ingebouwd (*Kamerstukken II* 2016/17, 343372, nr. 6, p. 93; *Kamerstukken I*, Handelingen 19 juni 2018, nr. 34).[45] Voor de 'wettelijke voorwaarden' is aangesloten bij de criteria die gelden voor het toepassen van andere, reeds bestaande ingrijpende (bijzondere) opsporingsbevoegdheden (*Kamerstukken I* 2016/17, 34 372, D). Verder zou het proces rondom het inzetten van de bevoegdheid moeten voldoen aan de vereisten die voortkomen uit de Europese jurisprudentie (*Kamerstukken I* 2016/17, 34 372, D, p. 4). Ook zouden de waarborgen vergelijkbaar zijn met de waarborgen die gelden voor verschillende vormen van communicatie zoals elektronische communicatie en communicatie die plaatsvindt met behulp van telefoon op brief (*Kamerstukken II* 2015/16, 34 372, nr. 3). In de memorie van toelichting (*Kamerstukken II* 2015/16, 34 372, nr. 3, o.a. p. 28) wordt geschreven dat de verschillende waarborgen en voorwaarden ertoe moeten leiden dat sprake is van een zorgvuldige en rechtmatige inzet van de bevoegdheid. Ook moeten deze voorkomen dat ongericht gegevens worden verzameld (*Kamerstukken I* 2017/18, 34 372, G, p. 2).

In de rest van de paragraaf wordt nader ingegaan op de diverse voorwaarden en waarborgen, hierna: waarborgen. Deze hebben, hoewel dit onderscheid niet altijd zo scherp te maken is, betrekking op drie momenten in de tijd: voorafgaand, gedurende en na afloop van de inzet van de bevoegdheid. Omdat veel van de waarborgen in eerdere paragrafen al aan de orde zijn geweest volgen hierna tabellen 2.1 t/m 2.3 waarin de verschillende waarborgen zijn opgenomen, inclusief een korte toelichting.

### *2.5.1 Voorafgaand aan de inzet*

**Tabel 2.1 Waarborgen voorafgaand**

| Waarborg | Toelichting |
|---|---|
| Reikwijdte | De bevoegdheid kan niet voor alle misdrijven worden ingezet en ten behoeve van een beperkt aantal onderzoekshandelingen. |
| Gerichte inzet & definitie geautomatiseerd werk | De bevoegdheid dient gericht te worden ingezet: op bepaalde personen en op bepaalde gegevens. Verder kunnen veel verschillende geautomatiseerde werken onder de definitie van een geautomatiseerd werk worden geplaatst (*Kamerstukken II* 2015/16, 34 372, nr. 6, p. 13). De bevoegdheid is niet bedoeld voor het 'hacken van software die apparatuur betreft die in het lichaam is geplaatst, zoals pacemakers of inwendige gehoorapparaten' (*Kamerstukken I*, Handelingen 19 juni 2018, nr. 34, p. 23). |

[45] Over de ingrijpendheid van de bevoegdheid op de persoonlijke levenssfeer is veel gesproken gedurende het wetgevingstraject, zie bijlage 3.

| Waarborg | Toelichting |
|---|---|
| Beperkte periode | De bevoegdheid mag voor een periode van maximaal vier weken worden toegepast. Deze periode kan steeds met een periode van ten hoogte vier weken worden verlengd (artikel 126nba, lid 3; *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 54). |
| Controle door OvJ, CTC en RC | De controle door verschillende actoren van de inzet van de bevoegdheid voorafgaand aan de inzet ervan wordt aangemerkt als één van de 'strikte voorwaarden' en 'stevige waarborgen'. Het gaat daarbij onder andere om de officier van justitie, de CTC en de rechter-commissaris (*Kamerstukken I* Handelingen 19 juni 2018, nr. 34). Zij beoordelen onder andere het geautomatiseerde werk waarin wordt binnengedrongen (*Kamerstukken II* Handelingen 13 december 2016, nr. 34) en of sprake is van een ernstige inbreuk op de rechtsorde en een dringend opsporingsbelang (*Kamerstukken I* 2018/19, 34 372, L). |
| Eisen technisch hulpmiddel | In het Besluit zijn diverse eisen opgenomen die ervoor moeten zorgen dat een technisch hulpmiddel in staat is om op een herleidbare, betrouwbare en integere manier gegevens te verzamelen (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 19). |
| Keuring technisch hulpmiddel door Keuringsdienst | Voordat een technisch hulpmiddel wordt gebruikt dient het hulpmiddel in principe goedgekeurd te zijn door de keuringsdienst (artikel 21, lid 1 Bogw; Besluit onderzoek in een geautomatiseerd werk, 2018, p. 19). De keuring moet voorkomen dat software wordt gebruikt die niet aan de gestelde eisen voldoet. Volgens de reactie op het advies van de Raad van State zouden ervaringen met softwareapplicaties in het buitenland laten zien dat een 'zorgvuldige keuringscertificering' belangrijk is (*Kamerstukken II* 2015/16, 34 372, nr. 4). Ook zou de keuring ervoor moeten zorgen dat derden een kwetsbaarheid niet misbruiken (*Kamerstukken II* 2016/17, 34 372, nr. 6). De keuring richt zich niet op de wijze waarop op een geautomatiseerd werk wordt binnengedrongen. Het binnendringen heeft volgens de minister géén invloed op de betrouwbaarheid van de verzamelde gegevens (Besluit onderzoek in een geautomatiseerd werk, 2018, p 20; *Kamerstukken II* 2018/19, 34 372, nr. 29, p. 13). |
| Treffen aanvullende (procedurele) waarborgen | Het kan voorkomen dat een technisch hulpmiddel wordt gebruikt 'dat zich naar zijn aard niet leent voor een voorafgaande keuring'. Het onderzoeksbelang kan dit dringend vorderen, aldus de toelichtende tekst op het Besluit (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 21). De officier van justitie dient dit in zijn/haar bevel te vermelden en het technisch hulpmiddel zal dan achteraf gekeurd moeten worden (artikel 15, lid 1 Bogw). Ook hierop is een uitzondering mogelijk (artikel 15, lid 2 Bogw), namelijk op het moment dat aan het einde van het onderzoek blijkt dat 'de aard van het hulpmiddel' zich volgens de officier van justitie 'verzet' tegen keuring. Als dat aan de orde is moet de officier van justitie in de processtukken opmerken dat afgezien is van keuring. Tevens dient hij of zij op te nemen welke aanvullende waarborgen zijn getroffen (artikel 21, lid 4 Bogw) om de 'betrouwbaarheid, integriteit en herleidbaarheid van vastgelegde gegevens te garanderen' (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 21). |

### 2.5.2 *Tijdens de inzet*

**Tabel 2.2 Waarborgen tijdens**

| Waarborg | Toelichting |
|---|---|
| Technisch team en functiescheiding | Er is aan apart team binnen de politie dat uitvoering geeft aan het toepassen van de bevoegdheid. Dit technisch team is gescheiden van het tactisch team dat het opsporingsonderzoek uitvoert. (*Kamerstukken I*, Handelingen 19 juni 2018, nr. 34). Functiescheiding is één van de waarborgen die ervoor moet zorgen dat er géén sprake is van willekeurige inmenging in het leven van burgers door de overheid en misbruik van de bevoegdheid (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 54). Het onderscheid betekent onder andere dat het technisch team gegevens 'filtert' en dat het tactisch team 'nooit iets anders dan dat te zien' krijgt (*Kamerstukken I*, Handelingen 19 juni 2018, nr. 34; bijvoorbeeld 'bijvangst'). De deskundigheid binnen dit technisch team moet ervoor zorgen dat de risico's die verbonden zijn aan het binnendringen worden 'beheerst dan wel beperkt'. In het Besluit zijn regels opgenomen over de deskundigheid van opsporingsambtenaren (artikel 3 en 4). Functiescheiding moet er ook voor zorgen dat het technisch team niet wordt beïnvloed als zij afwegingen maakt aangaande de haalbaarheid van een onderzoek en de uitvoering ervan. (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 14). |
| Logging | Logging is een belangrijke waarborg in het kader van inbreuk op de persoonlijke levenssfeer (*Kamerstukken I*, Handelingen 19 juni 2018, nr. 34).[a] Er zijn vier verschillende vormen van logging onderscheiden. |

a Logging wordt ook al genoemd in de memorie van toelichting (*Kamerstukken II* 2015/16, 34 372, nr. 3).

### 2.5.3 *Na afloop van de inzet*

**Tabel 2.3 Waarborgen na afloop**

| Waarborg | Toelichting |
|---|---|
| Verwijdering technisch hulpmiddel | Het technisch hulpmiddel dient verwijderd te worden. Indien deze niet volledig verwijderd kan worden, en de achtergebleven sporen risico's opleveren voor het geautomatiseerde werk, zal de officier de beheerder informeren en informatie aanleveren zodat de software alsnog verwijderd kan worden (*Kamerstukken II* 2015/16, 34 372, nr. 43). |
| Zittingsrechter | De toetsing door de zittingsrechter is de 'beste waarborg voor onafhankelijkheid, onpartijdigheid en een degelijke procedure'. (*Kamerstukken I*, Handelingen 19 juni 2018, nr. 34, p. 20). Ook zou de rechterlijke toetsing, inclusief de toetsing vooraf door de rechter-commissaris 'een willekeurige toepassing van de bevoegdheid' uitsluiten (*Kamerstukken I* 2016/17, 34 372, D). |
| Inspectie Justitie en veiligheid | Ook de Inspectie houdt toezicht op de inzet van de bevoegdheid. Dit gebeurt overigens niet alleen achteraf, maar kan ook tijdens de inzet gebeuren. |

| Waarborg | Toelichting |
|---|---|
| Notificatieverplichting | In aansluiting op de regeling voor de notificatie van bijzondere opsporingsbevoegdheden (artikel 126bb Sv.) is er de verplichting om betrokkenen op de hoogte te brengen dat de bevoegdheid is ingezet. Zodra het belang van het onderzoek het toelaat, doorgaans is dat na afronding van het opsporingsonderzoek, geldt deze notificatieplicht aan de betrokkenen. Als het proces-verbaal van de toepassing van de bevoegdheid is toegevoegd aan de processtukken, is notificatie niet vereist (*Kamerstukken II* 2016/17, 34 372, nr. 6).<br>De notificatieplicht betekent dat degene wiens geautomatiseerde werk is binnengedrongen op de hoogte moet worden gesteld dat dit heeft plaatsgevonden. Een globale aanduiding (schriftelijk) van de aard van de gegevens volstaat: degene die het notificatiebericht ontvangt, moet in staat zijn om te beoordelen of zijn of haar rechten zijn geschonden. Het notificeren van een verdachte kan worden uitgesteld bij een onderzoek in een andere strafzaak waarbij de verdachte betrokken is of bij een onderzoek tegen meerdere verdachten dat nog niet in zijn geheel is afgerond. (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 40). Ook wanneer een geautomatiseerd werk in het buitenland wordt binnengedrongen is notificatie vereist. Soms zal het echter lastig zijn om de betrokkenen te traceren waardoor de notificatie achterwege blijft. (*Kamerstukken II* 2016/17, 34 372, nr. 6). De notificatieplicht is in lijn met de eisen vanuit het EHRM dat een betrokkene achteraf in kennis wordt gesteld dat een bevoegdheid is ingezet en dat deze eventueel 'genoegdoening kan zoeken voor een eventuele inbreuk op zijn privacy' (*Kamerstukken I* 2016/17, 34 372, D, p. 6). Ook volgt de notificatieplicht logisch voort uit de plaatsing van de bevoegdheid in het wetboek. |

## 2.6 Binnendringen en onderzoek doen in een internationale context

Een geautomatiseerd werk dat onderwerp van onderzoek is, bevindt zich lang niet altijd in Nederland (*Kamerstukken II* 2015/16, 34 372, nr. 3). Hoewel het voor opsporingsinstanties mogelijk is de beschikking te krijgen over gegevens die daarop staan, is het ingewikkelder om vast te stellen op welke fysieke locatie(s) de benodigde gegevens zich bevinden. Internetgebruikers doen vaak moeite om anoniem te blijven (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 42). In de periode dat de Wet CCIII tot stand is gekomen was er (nog) geen internationaalrechtelijk kader dat zich richt op de toepassing van uitvoerende rechtsmacht[46] bij de bestrijding van computercriminaliteit.[47] Wel was er het Cybercrimeverdrag van de Raad van Europa waarin een regeling is opgenomen voor grensoverschrijdende toegang tot computergegevens. Het gaat daarbij om twee soorten gegevens (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 44). Ten eerste openbare gegevens (open bronnen) die zijn opgeslagen. Het maakt voor deze gegevens niet uit op welke locatie deze zich bevinden. Ten tweede de toegang tot opgeslagen gegevens bij een andere

[46] Bij het begrip rechtsmacht spelen twee componenten een rol. Wetgevende rechtsmacht heeft betrekking op de toepasselijkheid van de Nederlandse wet. Uitvoerende rechtsmacht gaat over het verrichten van handelingen door Nederlandse rechtshandhavingsactiviteiten met als doel de opsporing en vervolging in Nederland (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 43).

[47] Dit is inmiddels achterhaald. Het comité van de Ministers van de Raad van Europa heeft een tweede aanvullend protocol bij het Verdrag aangenomen. Dat Verdrag heeft betrekking op hechtere samenwerking en het openbaar maken van elektronisch bewijsmateriaal (Bijzonder strafrecht, z.d.).

verdragspartij, die verkregen kan worden door middel van een netwerkzoeking. Van belang is dat sprake is van rechtmatige en vrijwillige instemming van een verdachte, van een ander individueel persoon of van een aanbieder die gerechtigd is de gegevens via het computersysteem aan de verzoekende partij te verstrekken. Het is de verschillende partijen nog niet gelukt om het eens te worden over de voorwaarden waaronder toegang tot gegevens mogelijk is in andere situaties (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 44).
In de memorie van toelichting wordt aangegeven dat een verdere ontwikkeling van het internationaalrechtelijk kader de voorkeur heeft, maar dat de ontwikkeling ervan 'een ideaal is dat slechts op langere termijn kan worden gerealiseerd' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 46). In de tussentijd zijn er twee opties. De eerste is dat géén onderzoek plaatsvindt als onbekend is waar gegevens zich bevinden. Dat zou betekenen, zo staat beschreven in de memorie van toelichting, dat het internet 'een vrijplaats is voor criminaliteit' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 46). Aangezien die optie onwenselijk wordt gevonden, is gekozen voor de tweede optie, namelijk het 'zelfstandig op een zorgvuldige wijze uitoefenen van rechtsmacht bij de bestrijding van computercriminaliteit waarbij zo veel mogelijk rekening wordt gehouden met verschillende belangen' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 46).[48]

In een OM-aanwijzing[49] staat beschreven hoe gehandeld dient te worden wanneer een geautomatiseerd werk zich in het buitenland bevindt. Duidelijk wordt dat een verzoek tot rechtshulp moet worden gedaan wanneer opsporingshandelingen betrekking hebben op gegevens die zich op buitenlands grondgebied bevinden. In uitzonderlijke omstandigheden moet het echter mogelijk zijn zonder voorafgaande toestemming van het buitenland op te treden. In de OM-aanwijzing staan verschillende scenario's geschetst waarin optreden zonder toestemming aan de orde kan zijn (Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid, 2019). Het eerste scenario betreft een situatie waarin de locatie van gegevens bekend is, er een rechtshulpverzoek is gedaan, maar waarin niet langer gewacht kan worden op een reactie dan wel dat het niet in de verwachting ligt dat het land waarbij het rechtshulpverzoek is ingediend, zal reageren. In het tweede scenario is de locatie onbekend op het moment dat de bevoegdheid wordt ingezet, maar wordt de plek van het geautomatiseerde werk op een later moment in het onderzoek bekend. Er zijn dan twee mogelijkheden. De eerste mogelijkheid is dat zo snel mogelijk een rechtshulpverzoek wordt gedaan en dat het onderzoek stil wordt gelegd totdat de toestemming er is. Bij de tweede mogelijkheid wordt ook een rechtshulpverzoek gedaan, maar in plaats van het tijdelijk stopzetten van het onderzoek, wordt in de tussentijd de inzet van de bevoegdheid wel voltooid (zonder dat daar officieel toestemming voor is). Bij beide scenario's dient de zaaksofficier van justitie de 'context van de aanvaarde soevereiniteitsschending' te bespreken met de landelijk officier van justitie bij het Landelijk Parket. Deze is zoals gezegd nauw betrokken bij de voorbereiding voor en de inzet van de bevoegdheid. De zaaksofficier zal vervolgens het besluit ter instemming voorleggen aan de rechercheofficier van justitie van zijn of haar arrondissementsparket (Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid, 2019, p. 2-3). Bij optreden zonder toestemming dienen in de overweging de volgende elementen te worden meegenomen: de ernst of onmiddellijkheid van de gevolgen van de aanval of dreiging, de aard en ernst van het

[48] Inzetten op buitenlands grondgebied zijn een belangrijk discussiepunt geweest gedurende het wetgevingstraject, zie bijlage 3.
[49] Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid (Staatscourant, 26 februari 2019, nr. 10277).

strafbare feit en de vluchtigheid van de gegevens of informatie die wordt gezocht, en of die moet worden veiliggesteld, dan wel ontoegankelijk moet worden gemaakt. Daarnaast moet gedacht worden aan de mate van betrokkenheid van de Nederlandse rechtsorde en de gevolgen daarvoor (inclusief het belang van slachtoffers), de aard van de te verrichten opsporingshandelingen en de risico's voor het geautomatiseerde werk.
Het derde scenario houdt in dat de locatie niet middels redelijke inspanning kan worden vastgesteld. In dat geval wordt ervan uitgegaan dat de gegevens zich in Nederland bevinden en dat betekent dat de Nederlandse rechtsregels kunnen worden toegepast. Wat precies redelijk is, zal per geval moeten worden vastgesteld. Een redelijke inspanning betekent onder meer dat de tijd en moeite voor het vaststellen van een specifieke geografische locatie in een reële verhouding staan tot de noodzakelijkheid van onverwijld optreden (bijvoorbeeld de online dienstverlening van een overheidsinstelling die gedurende langere tijd stil ligt), de doorlooptijd en de tijdsdruk van het onderzoek (Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid, 2019, p. 3).

# Inleiding op de empirische hoofdstukken

In de komende hoofdstukken wordt uiteengezet hoe de uitvoering van de hackbevoegdheid er in de praktijk uitziet (deelvragen 2 tot en met 5). In hoofdstuk 3 staat het traject voorafgaand aan de daadwerkelijke uitvoering centraal (deelvraag 2). Ingegaan wordt onder andere op de wijze waarop de inzet van de bevoegdheid wordt getoetst door de daartoe aangewezen actoren. In de hoofdstukken 4 en 5 richt de aandacht zich op wat er allemaal gebeurt tijdens de uitvoering van de bevoegdheid. Hoofdstuk 4 gaat over het binnendringen, het uitvoeren van onderzoekshandelingen en de inzetten met een internationale component (deelvraag 3). Hoofdstuk 5 richt zich op de controle gedurende de uitvoering van de bevoegdheid (deelvraag 4). In dat hoofdstuk is onder andere aandacht voor de Keuringsdienst en de Inspectie Justitie en Veiligheid. In hoofdstuk 6 staat de afronding van de inzet centraal en de vervolgstappen die ondernomen worden (deelvraag 5).
Om de inhoud van de zojuist geschetste hoofdstukken goed te kunnen begrijpen volgt in de rest van deze inleiding een toelichting op de belangrijkste actoren die betrokken zijn bij de inzet van de hackbevoegdheid.

## Digit-politie

Bij de inzet van de hackbevoegdheid heeft Digit (*Digital Intrusion Team*) een centrale rol. Digit zelf kent twee onderdelen: Digit-politie en Digit-OM.
De uitvoering van de hackbevoegdheid is in handen van Digit-politie, een deel van hen is het technisch team waarnaar in de wetsgeschiedenis wordt verwezen. Digit-politie is een specialistisch team, ondergebracht bij de landelijke eenheid van de Nationale Politie. Digit-politie bestaat uit een aantal (kleine) subonderdelen: inzet, *research & development*, infra en security.
Het inzetteam (technisch team in de wetsgeschiedenis) bestaat uit twaalf personen[50] en houdt zich bezig met het binnendringen in geautomatiseerde werken en het verrichten van onderzoekshandelingen. Daarnaast stelt zij een haalbaarheidsonderzoek op en voert zij testen uit. Hieraan worden soms medewerkers van andere onderdelen (tijdelijk) toegevoegd. Binnen het inzetteam werken nog twee tactisch coördinatoren. Zij monitoren het verloop van de inzetten en zijn, samen met een inzetverantwoordelijke uit het inzetteam, het belangrijkste aanspreekpunt voor het tactisch team van de politie.
Het *research and development* team telt acht personen. Naast het zoeken naar bekende kwetsbaarheden die gebruiksklaar gemaakt kunnen worden (het research-gedeelte), verricht dit team ontwikkelwerkzaamheden (de ontwikkeltak). Grofweg gaat het daarbij om twee soorten werkzaamheden. In de eerste plaats zijn er langer lopende projecten waarin Digit zelf technische hulpmiddelen ontwikkelt die (in de toekomst) gebruikt kunnen worden om onderzoek te doen in een geautomatiseerd werk. Daarnaast ondersteunen ontwikkelaars, indien nodig, het inzetteam bij de verschillende inzetten die Digit uitvoert. Wanneer gewerkt wordt met een technisch hulpmiddel dat Digit zelf ontwikkeld heeft, kan een ontwikkelaar tijdelijk toegevoegd worden aan het inzetteam.

[50] Het genoemde aantal betreft het aantal personen dat ten tijde van de dataverzameling voor dit onderzoek onderdeel uitmaakte van het team. Inmiddels (april 2022) is dit aantal niet meer actueel. Dit geldt deels ook voor de aantallen die genoemd worden bij de andere teams binnen Digit-politie.

Hij/zij kan dan helpen met het testen en met het daadwerkelijk uitvoeren van het onderzoek. Het ontwikkelteam werkt in principe vraaggericht. Dat betekent dat de producten die zij ontwikkelt afhankelijk zijn van de onderzoeksvraag van het tactisch team.
Naast bovenstaande twee teams werkt nog een aantal mensen bij team Infra en één persoon bij Security.[51] Team infra is verantwoordelijk voor alle hard- en software die bij Digit in haar eigen omgeving wordt gebruikt. Security houdt zich bezig met het 'veilig houden' van Digit. Dat betekent dat er aandacht is voor informatiebeveiliging, meer praktische aspecten zoals de uitgifte van ICT-middelen en het meedenken over daadwerkelijke inzetten.
Naast bovenstaande teams werken bij Digit twee dossiervormers, een 'eigen' jurist, een beleidsadviseur en een teamleider.

### Digit-OM

Digit-politie wordt aangestuurd door Digit-OM, ondergebracht bij het Landelijk Parket. Digit-OM bestaat uit twee personen: een officier van justitie en een parketsecretaris. Naast de aansturing door Digit-politie is Digit-OM voor alle betrokken actoren aanspreekpunt en vraagbaak. Deze rol vervult Digit-OM vanaf het moment dat er plannen bestaan om de bevoegdheid in te zetten tot en met het moment dat een zaak definitief afgehandeld is bij de rechter (als een zaak waarin een inzet heeft plaatsgevonden op zitting wordt behandeld). De Digit-officier van justitie vervult de schakelfunctie die in de wetsgeschiedenis oorspronkelijk was toebedeeld aan een tactisch zaaksofficier van justitie (zie hoofdstuk 3).

### Tactisch-OM en tactisch team politie

Een inzet van Digit vindt plaats binnen een opsporingsonderzoek waarin de hackbevoegdheid doorgaans één van de (vele) bijzondere opsporingsbevoegdheden is die wordt ingezet. Dat opsporingsonderzoek wordt uitgevoerd door een tactisch team van de politie, bijvoorbeeld een team van de districtsrecherche of Team High Tech Crime. Het tactisch team werkt onder gezag van een tactisch zaaksofficier van justitie (hierna zaaksofficier). Deze zaaksofficier is eindverantwoordelijk voor het opsporingsonderzoek waarbinnen Digit een inzet doet en hij/zij dient verantwoording af te leggen in de rechtbank als de zaak op zitting wordt behandeld.

[51] Dit zijn niet de teams Infra en Security van de Landelijke Eenheid van de Nationale Politie.

# 3 Voorbereiden en verkenning inzet hackbevoegdheid

## 3.1 Inleiding

Dit hoofdstuk richt de aandacht op de wijze waarop de verkennende fase verloopt die voorafgaat aan de daadwerkelijke inzet van de bevoegdheid (deelvraag 3). Na een korte samenvatting van het wettelijk kader wordt ingegaan op redenen waarom een zaaksofficier van justitie de hackbevoegdheid in zijn/haar opsporingsonderzoek wil inzetten. Ook wordt kort ingegaan op redenen om uiteindelijk niet over te gaan tot een inzet. Daarna wordt aandacht besteed aan wat er gebeurt zodra vanuit een zaaksofficier van justitie en of een tactisch team van de politie de wens bestaat om de bevoegdheid in te zetten. Twee processen worden onderscheiden: het operationele proces en het toetsingsproces. Beide worden in dit hoofdstuk nader uiteengezet.
In dit hoofdstuk wordt het tactisch perspectief beperkt belicht, omdat slechts zeven tactisch officieren van justitie zijn gesproken en aanvraag-processen verbaal zijn bestudeerd. In het tweede deel van de evaluatie zal dit perspectief uitgebreider bestudeerd worden. Datzelfde geldt voor het inzichtelijk maken van de manier waarop de rechter-commissaris een inzet toetst. Voor dit onderzoek zijn slechts twee, weliswaar gespecialiseerde, rechters-commissarissen gesproken. In deel twee van de evaluatie zal ook uitgebreider aandacht worden besteed aan die toetsing.

## 3.2 Samenvatting wettelijk kader

In de memorie van toelichting komen, zoals eerder beschreven, drie technologische ontwikkelingen naar voren die maken dat de inzet van de hackbevoegdheid nodig kan zijn: versleuteling, *cloud computing* en draadloze netwerken (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 7-12). De inzet van de hackbevoegdheid wordt gezien als een zwaar middel. Indien een tactisch team de bevoegdheid wil inzetten, dient zij te onderbouwen waarom de inzet nodig is. Als door de zaaksofficier de inschatting wordt gemaakt dat de inzet proportioneel en subsidiair is, dan wordt een rapport haalbaarheidsonderzoek opgesteld voor de officier van justitie inclusief een plan van aanpak hoe het onderzoek zal worden uitgevoerd (Besluit onderzoek in een geautomatiseerd werk, p. 16). Indien verschillende actoren, betrokken bij de toetsing van de inzet, oordelen dat een inzet kan en mag plaatsvinden, stelt het technisch team een (tweede) plan van aanpak op met betrekking tot het binnendringen. Dat plan van aanpak wordt getest in een ‘proefopstelling’ (Besluit onderzoek in een geautomatiseerd werk, p. 16).
Bij de toetsing of de inzet van de bevoegdheid überhaupt plaats kan vinden, zijn diverse actoren betrokken. Allereerst het Openbaar Ministerie (onder andere artikel 126nba Sv, lid 1). Indien een zaaksofficier van justitie de bevoegdheid in zijn of haar onderzoek wil inzetten, stelt zij op basis van een aanvraagproces-verbaal een vordering tot machtiging op aan de rechter-commissaris. Voorafgaand daaraan dient de CTC akkoord te gaan met een mogelijke inzet (*Kamerstukken II*, 2015/16, 34 372, nr. 3, p. 38). De CTC adviseert het College van PG’s over de inzet. Vervolgens beoordeelt de rechter-commissaris de vordering tot machtiging die de officier van justitie aan hem/haar doet (artikel 126nba Sv, lid 4). In de machtiging moet een aantal inhoudelijke punten worden uitgelicht waardoor de rechter-commissaris tot een onderbouwd oordeel kan komen (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 38).

De toetsing door de CTC kan via een spoedprocedure verlopen. Een zaak wordt in dat geval zo snel mogelijk getoetst en het advies wordt (mondeling) voorgelegd aan het College van PG's. Die kan op haar beurt een (mondelinge) beslissing nemen (*Kamerstukken II* 2016/17, 34 372, nr. 6). Het bevel kan alleen worden gegeven na een schriftelijke machtiging van de rechter commissaris (artikel 126nba, lid 4).

## 3.3 Keuze en aanvraag voor de inzet van de hackbevoegdheid

Versleuteling is voor tactische onderzoeksteams een belangrijke reden om de hackbevoegdheid in te zetten. Dat blijkt uit het feit dat in de interviews vaak de versleuteling van gegevens wordt genoemd. Ook in de lijst met inzetten die Digit-politie in de afgelopen twee jaar is gestart, waren veel inzetten te zien waarbij sprake was van versleuteling van gegevens(-dragers). Bij veel inzetten ging het om telefoonzaken waarbij de politie zicht wilde krijgen op de communicatie van een verdachte en waarbij andere opsporingsbevoegdheden (bijvoorbeeld telefoontaps en opnemen vertrouwelijke communicatie (OVC) niks opleverden. In die zaken bestond een sterk vermoeden dat onderlinge communicatie tussen verdachten plaatsvond via versleutelde maar vrij gangbare berichtenapps op de telefoon. Bij dit soort zogenoemde standaardinzetten hanteert Digit een min of meer standaard werkwijze. Daarnaast zijn er zogenoemde 'maatwerkinzetten'. Een voorbeeld van zo'n maatwerkinzet is een onderzoek naar een server die een centrale functie had bij de verspreiding van malware en die zich (tijdelijk) in Nederland bevond. Eén van de geïnterviewden vertelt dat voor dit soort inzetten Digit zelf 'iets moet ontwikkelen'. Daar gaat 'veel tijd inzitten' en dat is 'vaak technisch uitdagend'.

In lijn met de wetsgeschiedenis wordt de bevoegdheid ook in de praktijk gezien als zwaar middel dat als laatste redmiddel kan worden ingezet. In een groot deel van de bestudeerde zaken zijn binnen een opsporingsonderzoek diverse andere bevoegdheden ingezet die niet tot het gewenste resultaat hebben geleid. Bij één van de geselecteerde inzetten bijvoorbeeld verliet de verdachte zijn huis niet of nauwelijks. Er waren verschillende (bijzondere) opsporingsbevoegdheden ingezet die niets opleverden, zoals IP-taps, observaties en financieel onderzoek. In die zaak 'bleef er weinig anders over' dan een inzet van de hackbevoegdheid. Dat betekent overigens niet dat binnen alle opsporingsonderzoeken de nieuwe bevoegdheid wordt gezien als uiterste middel. Soms is op voorhand al te onderbouwen waarom andere (minder zware) bijzondere opsporingsbevoegdheden niet succesvol zullen zijn. Bijvoorbeeld door gedragingen van de verdachte of de locatie waar men onderzoek wil doen. Betrokken verdachten kunnen 'moeilijk bereikbaar' of 'scherp' zijn en met de inzet van de standaard klassieke opsporingsmiddelen komen de opsporingsinstanties niet verder. Overigens zijn deze afwegingen niet uniek voor de hackbevoegdheid. Het grote opsporingsbewustzijn van met name verdachten op het terrein van georganiseerde criminaliteit is vaker een reden om bepaalde bijzondere opsporingsbevoegdheden (BOB-middelen) in te zetten (Kruisbergen et al., 2010).
Het kan ook zijn dat binnen een opsporingsonderzoek een zodanig urgente dreiging is dat sneller overgegaan wordt tot de inzet van bevoegdheden en dus ook de hackbevoegdheid. Bij één van de geselecteerde inzetten ging het bijvoorbeeld om een concrete ernstige dreiging in de richting van een functionaris betrokken bij de opsporing.

Als een zaaksofficier van justitie de hackbevoegdheid binnen zijn of haar opsporingsonderzoek wil inzetten, wendt hij/zij zich tot Digit-OM. Soms meldt een

tactisch team van de politie zich bij Digit-politie. Digit-politie en /of –OM maken vervolgens een eerste inschatting van de praktische en technische mogelijkheden die er zijn om de hackbevoegdheid in te zetten. Lang niet alle verzoeken worden uiteindelijk gehonoreerd. Hoe dit intakeproces precies verloopt wordt in de komende paragrafen nader besproken.

In de periode 2019 tot en met maart 2021 heeft Digit ongeveer 60 verzoeken afgewezen en 27 verzoeken ingewilligd. In totaal zijn er dus zo'n 90 verzoeken binnengekomen, waarvan het merendeel niet kon worden opgepakt.[52] De meest voorkomende reden om aanvragen af te wijzen was de beperkte capaciteit bij Digit, al dan niet in combinatie met de technische complexiteit van de inzet. Immers, hoe complexer een inzet, hoe meer er ook van de capaciteit van het team gevraagd wordt. Andere redenen om af te zien van een inzet waren dat op voorhand al duidelijk was dat een inzet om technische redenen niet haalbaar bleek of dat het doel van het tactisch team niet scherp genoeg geformuleerd was. Daarnaast kiest een tactisch team er soms zelf alsnog voor van een inzet af te zien, zo wordt vanuit Digit verteld. Bijvoorbeeld omdat de kans klein is dat de beoogde doelen behaald worden, de doorlooptijd van een inzet of de voorbereiding te lang is of omdat een onderzoek al is 'geklapt'.
Als een zaaksofficier van justitie inschat dat de inzet van de hackbevoegdheid van meerwaarde kan zijn voor het opsporingsonderzoek en dat de inzet van de bevoegdheid proportioneel en subsidiair is, moet zowel aan de kant van het Openbaar Ministerie als aan de kant van de politie een aanmeld- of intakeprocedure worden doorlopen waarin keuzes worden gemaakt en onderbouwd rondom de inzet van de hackbevoegdheid. Binnen dit intakeproces kunnen twee processen worden onderscheiden die deels op elkaar aansluiten en deels simultaan plaatsvinden. Aan de ene kant is er het operationele proces waarbij Digit-OM, Digit-politie en het tactisch team en de zaaksofficier betrokken zijn. Aan de andere kant is er de procedure rondom toetsing en controle waarin de zaaksofficier, Digit-OM, de rechercheofficier, de hoofdofficier van justitie, de Centrale Toetsingscommissie (CTC), het College van Procureurs Generaal (hierna College van PG's) en de rechter-commissaris een rol hebben. Deze twee processen worden in de onderstaande paragrafen vanwege analytische redenen apart van elkaar besproken.

### *3.3.1 Hoofdpunten*

- Het intakeproces bestaat uit twee processen die deels op elkaar aansluiten en deels simultaan plaatsvinden: een operationeel proces en een procedure rondom de toetsing van de inzet.
- Aan ruim twee derde van de verzoeken van de tactische teams wordt geen uitvoering gegeven door Digit. Daarbij spelen zowel tactische als technische argumenten een rol.
- De versleuteling van gegevens(dragers) is in elk geval bij de inzetten die nader bestudeerd zijn de belangrijkste aanleiding om de hackbevoegdheid in te zetten.

[52] Het gaat hier om een globaal beeld dat op verzoek van de onderzoekers is samengesteld. Deze cijfers worden niet structureel bijgehouden. Niet alle afwijzingen volgden na formele aanvragen. Soms werd ook na het eerste telefonisch contact duidelijk dat inzet niet haalbaar zou zijn.

## 3.4 Operationeel proces

### *3.4.1 Intake - OM*

Binnen het Openbaar Ministerie heeft Digit-OM onlangs een OM-instructie opgesteld, vastgesteld door het College van PG's, waarin toegelicht is welke stappen gezet moeten worden als binnen een opsporingsonderzoek de inzet van de hackbevoegdheid overwogen wordt (Openbaar Ministerie, z.d.). Deze instructie is gebaseerd op de ervaringen die in de eerste periode opgedaan zijn met de uitvoering van de hackbevoegdheid. In de instructie staat beschreven dat een zaaksofficier die voornemens is gebruik te maken van de hackbevoegdheid dit voorlegt aan de Digit-officier van justitie. De Digit-officier maakt vervolgens een eerste inschatting van de juridische haalbaarheid en inventariseert 'eventuele gevoeligheden'. Hij vraagt Digit-politie om een eerste inschatting te maken van de technische haalbaarheid en stemt de haalbaarheid en operationele aspecten van een mogelijke inzet af met de teamleiding van Digit-politie. Deze eerste beoordeling zou dan vervolgens besproken moeten worden met de zaaksofficier. In onderling overleg wordt vervolgens bepaald of de inzet van de hackbevoegdheid gewenst is. De zaaksofficier beslist uiteindelijk, als leider van het opsporingsonderzoek, in samenspraak met Digit-OM of overgegaan kan worden tot de inzet van de hackbevoegdheid. Daarna volgt nog een procedure binnen het Openbaar Ministerie (onder andere CTC; Openbaar Ministerie, z.d.).

In de praktijk verloopt het contact tussen een zaaksofficier en de Digit-officier laagdrempelig en informeel. Doorgaans is sprake van een eerste telefonisch contact waarin globaal wordt uitgevraagd om wat voor type zaak het gaat om een inschatting te kunnen maken of de ernst en/of urgentie van de zaak hoog genoeg is om de hackbevoegdheid in te zetten. Digit-OM kan op die manier prioriteren. Ook wordt gevraagd wat het tactisch onderzoeksteam wil en dat wordt voorgelegd aan Digit-politie, zodat een eerste schifting gemaakt kan worden tussen haalbare en minder haalbare zaken. Als de conclusie is dat een inzet technisch, juridisch en qua prioriteiten en capaciteit bij Digit doorgang kan vinden, dan wordt met de zaaksofficier besproken dat het traject vervolgd kan worden. De zaaksofficier heeft tijdens deze intake niet alleen contact met Digit-OM. Ook met het tactisch politieteam is in deze fase contact in verband met de nodige afstemming over het nut en de noodzaak om binnen een bepaald onderzoek de hackbevoegdheid in te zetten.

In de OM-instructie is een duidelijke scheiding tussen de werkzaamheden van de zaaksofficier en die van de Digit-officier beschreven (Openbaar Ministerie, z.d.). De zaaksofficier van justitie heeft de leiding over en is eindverantwoordelijk voor het opsporingsonderzoek waarin de bevoegdheid wordt ingezet. De Digit-officier heeft de leiding over en is verantwoordelijk voor de uitvoering van het bevel door het technisch team van Digit-politie. Deze verdeling van verantwoordelijkheden en taken wordt in de praktijk ook nageleefd. Vanwege de specialistische aard van de bevoegdheid speelt Digit-OM wel een belangrijke rol bij het informeren en adviseren van zaaksofficieren, bijvoorbeeld wanneer de inzet van de hackbevoegdheid overwogen wordt. Dat gaat onder andere over het maken van een inschatting of een inzet doorgang moet vinden. Eén van de geïnterviewden vertelt:

> *'Het is heel erg het bewaken aan de poort. Want de trajecten die daarna komen, richting rechter-commissaris en richting CTC, zijn arbeidsintensieve trajecten. Die kosten van iedereen veel tijd. Die wil je eigenlijk alleen maar ingaan voor de zaken waar je ook het idee voor hebt dat die haalbaar zijn om te doen.'*

Verder wordt door Digit-OM benadrukt dat het belangrijk is dat beide partijen nauw contact hebben met elkaar en dat het tactisch team 'bij het minste of geringste' kan bellen en dat er 'open lijnen' zijn tussen beide partijen. Die samenwerking is belangrijk, omdat de zaaksofficier, vanwege de afscherming van onderzoeksmethoden, geen kennis heeft over de precieze wijze waarop de hackbevoegdheid wordt uitgevoerd. Digit-OM vervult in dat opzicht een 'schakelfunctie' richting het tactisch OM, vergelijkbaar met de wijze waarop Digit-politie een schakelfunctie vervult naar het tactisch team van de politie. Dat is anders dan de wetgever het oorspronkelijk bedacht had. Die voorzag dat de zaaksofficier van justitie een schakelfunctie zou vervullen tussen het technisch (Digit) en het tactisch team. Vanuit Digit-OM wordt verteld dat, onder andere vanwege de technische complexiteit van de hackbevoegdheid, vrij snel besloten is om een gespecialiseerde landelijk officier van justitie aan te stellen (in plaats van alles over te laten aan individuele zaaksofficieren). Dit is vergelijkbaar met de manier waarop dat geregeld is rondom WOD (werken onder dekmantel)-trajecten en het Team criminele inlichtingen. Eén van de geïnterviewden verwacht dat die specialistische functie nog wel een tijdje nodig zal zijn, omdat technische ontwikkelingen snel gaan waardoor het goed is dat iemand daar 'dedicated' mee bezig is.

Digit-politie vindt de schakelfunctie die Digit-OM vervult prettig. Eén van hen vertelt:

> *'Deze bevoegdheid is eigenlijk te specialistisch voor individuele zaaksofficieren. Die krijgen er maar in een enkele zaak mee te maken. Kun je dan verwachten dat ze het helemaal snappen, vraagt* [de geïnterviewde] *zich hardop af. Je ontkomt niet aan een schakel als de Digit officier.'*

In de praktijk is te zien dat er (veel) contact is tussen de zaaksofficieren en Digit-OM en dat beide partijen elkaar gemakkelijk weten te vinden, niet alleen voorafgaand aan de inzet overigens, maar ook tijdens een inzet. De zaaksofficier schrijft uiteindelijk een oplegnotitie voor de CTC, maar ook dat gaat in nauwe samenwerking met Digit-OM.

### *3.4.2 Intake - Politie*

Wanneer een tactisch politieteam[53] gebruik wil maken van de bevoegdheid om heimelijk en op afstand onderzoek te doen in een geautomatiseerd werk moet een intakeformulier worden ingevuld. Op het intakeformulier staat de achtergrond van de zaak, namen en informatie over de verdachte(-n). Op het intranet van de politie staat een pagina met informatie over team Digit en de werkzaamheden die het uitvoert. Op deze pagina staat ook een intakeformulier dat een aanvrager (een tactisch team) kan indienen. Dit formulier komt direct binnen in de mailbox van Digit-politie. Vanuit Digit-politie wordt aangegeven dat er niet actief geworven wordt. Er is beperkte capaciteit bij Digit-politie en de bevoegdheid is nog relatief onbekend.
Het invullen van het intakeformulier gebeurt bij voorkeur door het tactisch team in samenspraak met een (aangewezen) medewerker van Team Digitale Opsporing (TDO). Elke politie-eenheid kent een TDO. Het aantal fte waaruit zo'n team bestaat varieert per eenheid. De betrokkenheid van een medewerker van team TDO bij de aanvraag wordt noodzakelijk gevonden, omdat het voor de volledige inhoudelijke beoordeling van een aanvraag en het inschatten van de haalbaarheid nodig is om over gedetailleerde technische informatie over het geautomatiseerde werk en de verdachte

[53] Waar tactisch team staat worden alle teams bedoeld die een 126nba Sv in kunnen (laten) zetten. Dat kunnen tactische rechercheteams zijn van de politie, maar ook van de KMar of van een bijzondere opsporingsdienst zoals de FIOD.

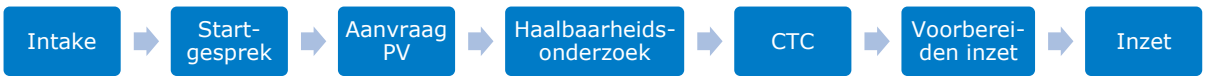
te beschikken. Ook kan de TDO-er Digit-politie informatie verschaffen die zij nodig heeft om een inschatting te maken van de mogelijkheden zoals een wifiscan of tapinformatie. Geïnterviewden vertellen dat het intakeformulier in de praktijk niet altijd even goed en volledig wordt ingevuld.

Op basis van het ingevulde intakeformulier maakt Digit-politie een eerste beoordeling van de technische en tactische mogelijkheden en bepaalt op die manier, in nauw overleg met Digit-OM, of Digit een inzet gaat doen. Verschillende geïnterviewden vertellen over de criteria die hierbij een rol spelen. Ten eerste gaat het om het soort misdrijf. Niet voor elk misdrijf mag de bevoegdheid worden ingezet. Ook kan meewegen of bij een bepaald misdrijf al eerder een inzet is gedaan. Eén van de geïnterviewden vertelt dat als er bijvoorbeeld veel inzetten zijn gedaan rondom verdovende middelen, er een volgende keer sneller gekozen zal worden voor een witwaszaak. Daarnaast wordt gekeken naar het geautomatiseerde werk. Gestreefd wordt naar een breed palet aan geautomatiseerde werken, zodat Digit ervaring kan opdoen en van de betreffende inzetten kan leren. Voor telefoons geldt een beperking op het aantal inzetten dat tegelijkertijd mogelijk is.[54] Ten derde kan het technisch hulpmiddel een rol spelen. Op het moment dat met een middel nog geen ervaring is opgedaan (op een bepaald geautomatiseerd werk), dan kan ook dat een reden zijn om een inzet te willen doen. Ten vierde wordt het aanvragende team meegenomen bij de afweging een inzet wel of niet te doen. In principe kan een aanvraag binnenkomen vanuit alle politie-eenheden en andere (bijzondere) opsporingsdiensten binnen Nederland. Het liefst bedient Digit verschillende partijen. Eén van de geïnterviewden vertelt dat het niet zo moet zijn dat Digit alleen inzetten doet voor de Landelijke Eenheid van de politie (Digit is hier zelf een onderdeel van). Een zesde criterium is dat gekeken wordt naar de gedragingen van de verdachte. Als deze zich bijvoorbeeld vaak in het buitenland bevindt, dan zal Digit niet snel een inzet doen. Los van deze criteria geldt dat 'prangende zaken' in principe altijd zullen worden opgepakt.

Wanneer Digit-politie besluit om binnen een opsporingsonderzoek een inzet te willen doen, wordt het tactisch team gevraagd een aanvullend aanvraagformulier in te vullen. Dat bevat onder meer een beschrijving van de verdachte, de verdenking, de noodzaak om de onderzoeksbevoegdheid toe te passen en de gewenste resultaten van de toepassing van de bevoegdheid. Bij binnenkomende aanvragen wordt dus naast technische haalbaarheid ook kritisch gekeken naar de tactische toegevoegde waarde. Zoals één van de geïnterviewden opmerkt: 'het is geen middel voor 'niet geschoten, altijd mis'.

In figuur 3.1 is het intakeproces van Digit-politie vereenvoudigd en schematisch weergegeven. De periode van intake tot en met bevel duurt ongeveer twee à drie weken. In de volgende paragrafen wordt dieper ingegaan op de verschillende onderdelen binnen dit proces.

**Figuur 3.1 Operationeel proces van intake naar inzet**




[54] Deze beperking gold gedurende de periode dat data verzameld werden. Inmiddels is deze beperking niet meer actueel.

### *3.4.3 Startgesprek*

Bij een voorlopige eerste positieve beoordeling, maakt Digit-politie een afspraak met het tactisch team voor een uitgebreider startgesprek. Bij dat gesprek wordt meer uitleg gegeven over de werkwijze van Digit-politie. Ook wordt dieper ingegaan op de wensen van het tactisch team, welk doel zij wil behalen en hoe dat bereikt kan worden. Bij dit gesprek zijn vanuit het tactisch team in ieder geval de teamleider en de TDO-er uit de eenheid aanwezig. Vanuit Digit-politie zijn tegenwoordig een zaaksverantwoordelijke vanuit het inzetteam en een tactisch coördinator aanwezig.

Het startgesprek begint met nogmaals een korte samenvatting van het opsporingsonderzoek. Er moet goed worden uitgelegd waarom een tactisch team denkt dat de informatie die zij wil hebben alleen op een specifiek geautomatiseerd werk te vinden is en waarom die informatie alleen met de hackbevoegdheid kan worden verkregen. Digit-politie vraagt hier ook op door, zo wordt uitgelegd door één van de geïnterviewden vanuit Digit:

> *'Er zal dan eerst gevraagd worden wat het doel is van de inzet van de bevoegdheid. Bijvoorbeeld: waaruit blijkt dat er communicatie is over de telefoon? Je hoort dan bijvoorbeeld dat er informatie over de tap komt, maar dat deze informatie versleuteld is. Een andere vraag die ze stellen is hoe ze weten welke app* [applicatie] *een verdachte gebruikt om te communiceren. Ook dat kan over de tap gehoord zijn (…). Dit soort vragen vanuit Digit zijn nodig, omdat de inzet op een telefoon duur, complex en arbeidsintensief is. Er kan veel informatie beschikbaar komen en het is de vraag of dat tot resultaat gaat leiden. Daarom moet goed verantwoord worden waarom je de bevoegdheid op een specifiek apparaat wilt inzetten. Dan heb je ook de grootste kans op resultaat.'*

Tijdens het gesprek worden verder de mogelijkheden en onmogelijkheden van de hackbevoegdheid besproken, om zowel aan de 'tactische' kant als aan de 'technische'[55] kant te zorgen voor realistische verwachtingen. Er wordt bijvoorbeeld stilgestaan bij het feit dat het om een relatief nieuwe bevoegdheid gaat waarbij alle betrokken partijen nog lerende zijn en dat hacken niet gebeurt door een 'druk op de knop' op afstand, maar behoorlijke voorbereidingstijd van Digit vergt. Verder wordt besproken dat er inspanningen van het tactisch team nodig (kunnen) zijn voor en tijdens de inzet en dat een inzet lang niet altijd slaagt (intern document 2). Het kan bijvoorbeeld veel tijd kosten om op een geautomatiseerd werk binnen te komen. Bij een 'makkelijke' inzet duurt het ongeveer één week, bij een hele moeilijke inzet kan het wel twee of drie maanden duren volgens één van de medewerkers van Digit-politie. Niet in elk onderzoek kan een tactisch team zich die tijd permitteren. Het is daarom belangrijk dat een tactisch team dat weet, zodat het daarop kan anticiperen.

Tijdens deze bijeenkomst wordt ook stilgestaan bij de werkafspraken: bijvoorbeeld de scheiding tussen tactiek en techniek, waardoor niet alle informatie door Digit-politie gedeeld kan worden (meer over deze functiescheiding in paragraaf 4.4.10). Digit vertelt daarentegen wel zo veel mogelijk tactische informatie nodig te hebben om een gedegen plan van aanpak te kunnen maken en de kans op een geslaagde inzet te vergroten. Tactische informatie kan helpen om risico's goed in te kunnen schatten en een inschatting te maken van de proportionaliteit van de inzet. Ook is voor Digit contact met het tactisch team noodzakelijk, omdat soms afstemming moet worden gezocht of extra informatie voorafgaand aan een inzet nodig is, bijvoorbeeld het

[55] Met technische kant wordt naar Digit-politie verwezen.

plaatsen van een IP-tap. Een ander voorbeeld van een situatie waarbij contact met het tactisch team noodzakelijk is, is bij de inzet van een 'ruisstrategie'. Een ruisstrategie moet ervoor zorgen dat een verdachte (extra) gaat communiceren. Die strategie wordt altijd door de tactische teams bepaald, maar moet wel worden afgestemd met Digit-politie om de timing van het binnendringen te bepalen. Als Digit-politie bijvoorbeeld meer tijd nodig heeft om binnen te kunnen dringen, wordt de ruisstrategie uitgesteld. Om bovenstaande redenen vraagt Digit-politie aan het tactisch politieteam toegang tot het registratiesysteem waarin het tactisch team informatie bijhoudt over de stand van zaken in het opsporingsonderzoek. Sinds 2020 hebben medewerkers van Digit, na het volgen van een cursus, hier toegang toe. Daardoor blijven zij goed op de hoogte van (de ontwikkelingen binnen) een zaak en van achtergrondinformatie over de interesses en gedragingen van een verdachte. Eén van de geïnterviewden vertelt:

> '[Het registratiesysteem] *levert knetterveel informatie op, bijvoorbeeld achtergrondinformatie over de verdachte, welke contacten hij heeft, het soort device* [geautomatiseerd werk] *dat hij gebruikt etcetera. Het is informatie die door het tactisch team is verzameld. Die informatie is nodig zodat je kunt acteren op een verdachte, bijvoorbeeld op hoe hij handelt. Dat soort informatie is soms nodig om als inzetteam goed je werk te kunnen doen.'*

Het komt voor dat een tactisch team bepaalde informatie niet deelt, omdat zij niet altijd goed weet welke informatie relevant is voor Digit. Inzage in het registratiesysteem biedt Digit de mogelijkheid om alsnog zicht te krijgen op informatie, zodat deze gebruikt kan worden in het kader van een inzet. Bovendien kan informatie verstrekt door het tactisch team (extra) worden gecontroleerd, bijvoorbeeld gegevens over het geautomatiseerde werk van de verdachte. Eén van de geïnterviewden legt uit dat toegang tot het registratiesysteem ook belangrijk is in het kader van 'BOB-aanvragen' die een tactisch team doet. Soms heeft Digit extra informatie nodig om een inzet te kunnen doen. In sommige gevallen kan die extra informatie worden verkregen met behulp van een (andere) bijzondere opsporingsbevoegdheid, bijvoorbeeld het vorderen van gegevens (artikel 126ng Sv). Het tactisch team moet een aanvraag voor zo'n bevoegdheid doen en er wordt verteld dat het daarbij van belang is dat geredeneerd wordt vanuit het tactisch opsporingsonderzoek in plaats van dat die bevoegdheid bijvoorbeeld wordt ingezet 'omdat Digit dat wil'. Op die manier wordt voorkomen dat te veel informatie prijs hoeft te worden gegeven over de door Digit gehanteerde methodes.

Verder wordt gedurende de bijeenkomst besproken dat het uitgangspunt is dat per opsporingsonderzoek één geautomatiseerd werk tegelijkertijd (dat geldt zeker voor telefoons) onderwerp van onderzoek is.[56] In de beginperiode is het voorgekomen dat meerdere telefoons onderwerp van onderzoek waren. Vanwege capaciteitsoverwegingen is afgesproken het aantal geautomatiseerde werken te beperken. Eén van de geïnterviewde zaaksofficieren vertelt dat capaciteit ook aan de tactische kant een knelpunt kan zijn. Er moet voldoende tijd zijn om de binnengekomen gegevens tijdig te analyseren. Dat er in principe géén capaciteit is voor het binnendringen van meerdere telefoons tegelijkertijd betekent dat een tactisch team keuzes moet maken welke telefoon het meest kansrijk is en dat het risico bestaat dat niet de juiste telefoon gekozen wordt (zie ook hoofdstuk 6).

[56] Deze afspraak wordt inmiddels (na de periode waarin de dataverzameling voor dit onderzoek heeft plaatsgevonden) niet meer zo strikt gehanteerd.

Het tactisch team bepaalt dus in principe welke verdachte of welk geautomatiseerd werk 'getarget' wordt. Wel kan Digit-politie meedenken over de technische haalbaarheid wanneer er meerdere verdachten en/of geautomatiseerde werken zijn. Gedurende het startgesprek wordt ook ingegaan op de mogelijke manieren van binnendringen en de afbreukrisico's die daarmee gepaard gaan. Tot slot wordt de procedure rondom de inzet verder toegelicht. Er wordt onder andere aandacht besteed aan wie bij welke stappen in het proces betrokken moet zijn vanuit de politie en het Openbaar Ministerie, welke stukken en informatie op welk moment moeten worden aangeleverd (bijvoorbeeld het plan van aanpak) en aan de afscherming van methodieken en gegevens. Indien gewenst sluiten Digit-OM en de zaaksofficier aan bij het zojuist beschreven startgesprek.

**Afstemming Digit en tactiek**
Vanaf het eerste moment dat een inzet wordt overwogen zijn er voortdurend contactmomenten tussen Digit-OM en Digit-politie en het tactisch politieteam en de zaaksofficier. Soms zijn dat fysieke overleggen in groter comité, maar vaker ook korte telefonische contacten. Na de intake en het startgesprek blijven die contactmomenten bestaan. Er moet een aanvraagproces-verbaal worden opgesteld en stukken voor de CTC moeten worden voorbereid. Gedurende de inzet is er contact over het verloop van de inzet en ook bij afronding is er overleg onder andere in verband met de processen-verbaal die moeten worden opgesteld. Digit-OM ziet binnen dit gehele traject een belangrijke adviserende rol voor zichzelf weggelegd.

### *3.4.4 Aanvraagproces-verbaal*

Digit vraagt het tactisch team, na de intake en het startgesprek, zo spoedig mogelijk een (concept) aanvraagproces-verbaal op te stellen en dat naar de parketsecretaris van Digit-OM te versturen. Het aanvraagproces-verbaal volgt een vast format waarin een aantal thema's aan de orde komt. Zo is er ten eerste aandacht voor de verdenking. Ten tweede wordt stilgestaan bij de tactische aanleiding om de hackbevoegdheid in te willen zetten. Wat zijn eerdere onderzoeksbevindingen en wat is het belang van het onderzoek? Ook wordt ingegaan op de proportionaliteit en subsidiariteit van een inzet. Staat het belang van het onderzoek in verhouding tot de inbreuk die ermee gemaakt wordt? Er kan bijvoorbeeld sprake zijn van een feit dat 'de rechtstaat hevig heeft geschokt'. Ook moet onderbouwd worden waarom de inzet van andere opsporingsbevoegdheden niet heeft geleid tot het vergaren van de noodzakelijke informatie. Bijvoorbeeld dat via een andere bijzondere opsporingsbevoegdheid is gebleken dat een verdachte zegt dat hij bepaalde dingen niet over de telefoon doet, maar via een andere weg zal communiceren. Verder moet worden uitgelegd waarom niet te verwachten valt dat door de inzet van andere en minder vergaande opsporingsbevoegdheden de noodzakelijke informatie binnen aanzienlijke termijn alsnog kan worden vergaard. Daarnaast is aandacht voor het geautomatiseerde werk waarop zal worden binnengedrongen, bijvoorbeeld dat met een andere bijzondere opsporingsbevoegdheid is vastgesteld dat de verdachte een bepaald geautomatiseerd werk gebruikt. Op die manier kan het gekozen geautomatiseerd werk onderbouwd worden. Tot slot wordt aandacht besteed aan eventuele risico's voor het geautomatiseerde werk die het binnendringen en het doen van onderzoek met zich mee kunnen brengen. Dat risico wordt door Digit doorgaans als gering of nihil ingeschat.

Ook bij dit proces is Digit-OM nauw betrokken. De teksten van bijvoorbeeld het aanvraagproces-verbaal worden meegelezen op wet(technische) aspecten. Op die

manier wordt regie gehouden en wordt voorkomen dat er 'onnodige fouten' in de stukken komen te staan. Dat helpt wanneer het stuk naar de CTC gaat. Voorbeelden van fouten die door één van de geïnterviewden worden genoemd zijn het zetten van verkeerde vinkjes bij de subs A t/m E, of het niet volledig duidelijk omschrijven van de functionaliteiten van het technisch hulpmiddel. De controle wordt belangrijk gevonden, omdat slordigheden in het aanvraag proces-verbaal juridisch consequenties kunnen hebben. Eén van de geïnterviewden legt uit:

> *'Dit* [foutjes in het proces-verbaal] *zit met name aan* [de tactische] *politiekant (…). Je levert een format aan waar ze mee moeten werken en dan toch besluiten dat een bepaald tekstblok niet nodig is en eruit halen. (…) Dat is funest, want dat staat er met een reden in. En niet kunnen overzien wat daar dan de consequentie van is. Eigenlijk zit het hem op dat soort stukken. Het zijn de verkeerde vinkjes, niet de juiste tekstblokken erbij hebben, nog met een oude versie werken.'*

### *3.4.5 Haalbaarheidsonderzoek*

In de uitvoeringspraktijk wordt binnen het operationele proces na het verkennende gesprek een (technisch) haalbaarheidsonderzoek uitgevoerd. Dit onderzoek wordt opgesteld door Digit-politie. Het inzetteam van Digit maakt hierin een inschatting van de technische haalbaarheid. De operationeel coördinatoren van Digit-politie beoordelen (in samenspraak met hun leidinggevende) de operationele haalbaarheid. In het haalbaarheidsonderzoek worden bijvoorbeeld variabelen in kaart gebracht die belangrijk zijn voor het binnendringen van een geautomatiseerd werk. Naast een inschatting van de haalbaarheid van het te verrichten onderzoek wordt een inschatting gemaakt van de mogelijke afbreukrisico's. Wat is de kans dat een verdachte iets te weten komt over de inzet? Bestaat de kans dat derden schade ondervinden, bijvoorbeeld wanneer meerdere personen gebruikmaken van een server? Ook wordt de uitvoering van het onderzoek in het geautomatiseerde werk nader uitgewerkt. In het rapport haalbaarheidsonderzoek beschrijft Digit onder andere welke bevelen nodig zijn en of software van derden moet worden aangeschaft. Het rapport dat wordt opgesteld ten behoeve van het haalbaarheidsonderzoek volgt een vast format en daarin komen de volgende thema's aan bod:

- doelstelling van het onderzoek (subA t/m E);
- omschrijving van het geautomatiseerde werk;
- inzet met of zonder technisch hulpmiddel;
- tactische haalbaarheid met betrekking tot verdachten;
- afbreukrisico;
- risicoanalyse (kans op schade) voor derden;
- inschatting van de haalbaarheid;
- vertragende en belemmerende factoren;
- inspanningsverplichtingen tactisch team
- uitvoeringstermijn.

Voor met name de laatste punten, die betrekking hebben op risicoanalyses en werkafspraken, lijken in de voor dit onderzoek geselecteerde inzetten min of meer standaardteksten gebruikt te worden.

Als Digit een inzet haalbaar acht, meldt de Digit-officier aan de zaaksofficier dat de voorgenomen inzet van de bevoegdheid voorgelegd kan worden aan de CTC. Het haalbaarheidsonderzoek is één van de aspecten die in een CTC-vergadering besproken wordt. Op de advisering door de CTC wordt nader ingegaan in paragraaf 3.5.1.

Vanwege de afscherming van de werkzaamheden van Digit (voorkomen moet worden dat technische details van het binnendringen worden prijsgegeven) wordt het haalbaarheidsonderzoek met daarin technische details over het binnendringen niet verstrekt aan het tactisch team of de zaaksofficier, maar enkel aan de Digit-officier en de CTC.[57] Wel wordt de zaaksofficier vanuit dit haalbaarheidsonderzoek door de Digit-officier voorgelicht over de kansen en risico's van een inzet. Dat is belangrijk, omdat de zaaksofficier eindverantwoordelijk is voor de wijze waarop het opsporingsonderzoek wordt uitgevoerd en daarover eventueel in het strafproces verantwoording af moet leggen. De informatie die de zaaksofficier krijgt over de haalbaarheid kan hij of zij ook gebruiken voor zijn/haar toelichting en oplegnotitie richting de CTC en de rechter-commissaris.

### *3.4.6 Plannen van aanpak*

Digit-OM en Digit-politie hebben ervoor gekozen het plan van aanpak waarin de uitvoering van het onderzoek wordt beschreven niet op te nemen in het haalbaarheidsonderzoek, maar te behandelen als een intern (vertrouwelijk) document. Vanuit Digit-politie wordt aangegeven dat dat onder andere is gebeurd omdat er te veel vertrouwelijke informatie in het plan van aanpak staat. In plaats daarvan is de keuze gemaakt om bij de CTC een gedetailleerdere mondelinge toelichting te geven op hoe het onderzoek zal worden aangepakt.
De zaaksverantwoordelijke vanuit het inzetteam moet ervoor zorgen dat, na de toestemming van het college van PG's, een tweede plan van aanpak voor het binnendringen wordt opgesteld (dat is een ander plan van aanpak dan het hiervoor genoemde plan van aanpak dat betrekking heeft op de uitvoering van het gehele onderzoek, zie paragraaf 2.3.4). In het plan van aanpak voor de uitvoering moet de totale inzet kort beschreven worden met de bijbehorende wettelijke grondslag van de inzet (intern document 3).[58] Het plan van aanpak voor het binnendringen dient vervolgens getest te worden in een proefopstelling. De zaaksverantwoordelijke moet ervoor zorgen – in samenspraak met de operationeel coördinatoren van Digit-politie – dat het plan van aanpak opgesteld wordt en getest in een proefopstelling. Deze handeling moet vastgelegd worden in de systemen van Digit. Uit de rapporten van de Inspectie (2020, 2021, 2022) blijkt dat niet alle gevallen een plan van aanpak voor het binnendringen is opgesteld.

Vooral vanuit Digit-OM wordt kritisch gekeken naar het opstellen van een plan van aanpak dat Digit moet opstellen. Zo zou het niet realistisch zijn om een perfect dekkend plan van aanpak te hebben. Het is eventueel mogelijk om een aantal verschillende scenario's uit te werken, maar in de praktijk kunnen onvoorziene omstandigheden zich voordoen. Een geïnterviewde opsporingsfunctionaris legt uit:

> *'Het idee dat je al in je haalbaarheidsonderzoek (…) een plan kan hebben, niet in die fase. En daarbij werkt hacking ook niet zo dat je met een vastomlijnd plan dat kan doen. Dat is een creatief proces waarbij je al gaande,* trial and error *proberend erachter komt of het wel of niet lukt. Dat wil je beheerst en netjes doen, dat je geen dingen stukmaakt en dat je niet buiten de kaders van je bevel gaat in ons geval. Maar (…) een vastomlijnd plan (…) hebben (…) dat gaat niet.'*

[57] Inmiddels (dit betreft de periode nadat de dataverzameling voor dit onderzoek heeft plaatsgevonden) maakt het haalbaarheidsonderzoek deel uit van een breder advies. Dat stuk wordt ook gedeeld met een tactisch team en de zaaksofficier. Bij de onderzoekers is verder niet bekend welke informatie precies in dit brede advies staat. Dat kan in het tweede deel van de evaluatie aan de orde komen.

[58] De WODC-onderzoekers hebben geen plannen van aanpak ingezien. De plannen van aanpak worden wel bekeken door de Inspectie.

Deze geïnterviewde zegt te snappen dat het belangrijk is dat bij de uitvoering van de hackbevoegdheid 'zorgvuldig en beheerst' te werk moet worden gegaan. Voorkomen moet worden dat Digit 'als een stel cowboys' gaat 'rondrennen' in een geautomatiseerd werk. Toch vraagt deze geïnterviewde zich af of een plan van aanpak de manier is om dat te waarborgen. Volgens deze geïnterviewde zou er meer vertrouwen moeten zijn in 'ambtseed relaterende en werkende opsporingsambtenaren' die de uitvoering van de bevoegdheid voor hun rekening nemen.

### *3.4.7 Proefopstelling*

Het plan van aanpak voor het binnendringen wordt uiteindelijk getest in een proefopstelling. Dat betekent dat bijvoorbeeld gekeken wordt of op een geautomatiseerd werk binnengedrongen kan worden en onderzoekshandelingen kunnen worden verricht. Het testen moet gebeuren door opsporingsambtenaren die hiervoor zijn aangewezen en gecertificeerd. Zij dienen te beschikken over de juiste kwalificaties.[59] Op dit moment voldoen vooral de leden van het inzetteam aan deze eisen. De Inspectie Justitie en Veiligheid constateert een aantal aandachtspunten wat betreft de aanwijzing van leden en van deelnemers aan het technisch team. In haar eerste Verslag merkt zij op dat de aanwijzingsbesluiten niet altijd op orde waren (Inspectie JenV, 2020) en in het tweede Verslag dat in minstens twee zaken de bevoegdheid is toegepast door opsporingsambtenaren die niet als lid of als deelnemer waren aangewezen (Inspectie JenV, 2021). In het derde Verslag staat vermeld dat deelnemers achteraf zijn aangewezen en dat de aanwijzing op structurele basis plaatsvindt, in plaats van op incidentele basis. Dit is niet in lijn met het Besluit. Verder vindt de begeleiding van deelnemers, die tijdelijk aan het technisch team worden toegevoegd, niet permanent plaats. Dat zou volgens het Besluit wel moeten. In plaats daarvan worden deelnemers, vanwege de uitvoerbaarheid van deze regel, tijdens briefings ingelicht (Inspectie JenV, 2022). Ook over het testen in een proefopstelling is de Inspectie kritisch. Zij constateert dat er niet altijd een verslag aanwezig is van het testen in een proefopstelling en de resultaten van het testen (Inspectie JenV, 2020, 2021, 2022).[60]
Als een proefopstelling wordt gemaakt, dan wordt gecontroleerd of alles functioneert zoals het zou moeten functioneren. Als het geautomatiseerde werk waarop moet worden binnengedrongen bijvoorbeeld een telefoon is, dan wordt, voorafgaand aan de daadwerkelijke inzet, precies dezelfde telefoon gekocht, inclusief de juiste software. Vervolgens wordt met die telefoon een aantal testen uitgevoerd. Ook andere geautomatiseerde werken die worden binnengedrongen, anders dan een telefoon, worden getest.
In de uitvoeringspraktijk wordt verteld dat het zorgen voor een proefopstelling die zo veel mogelijk lijkt een kostbare aangelegenheid is. In de wetsgeschiedenis staat overigens nergens vermeld dat er een proefopstelling moet zijn die zo veel mogelijk lijkt, al is het natuurlijk wel de vraag in hoeverre het zin heeft een test uit te voeren op een apparaat dat niet voldoende lijkt op het apparaat dat moet worden binnengedrongen. Door Digit wordt verteld dat in de periode maart 2019-maart 2021 voor ongeveer € 200.000 aan gelijkende apparatuur is aangeschaft. Telkens nieuwe toestellen aanschaffen is volgens Digit-politie niet haalbaar. Dit zou namelijk inhouden

[59] Deze kwalificaties staan beschreven in de Regeling betreffende de kwalificaties van opsporingsambtenaren die door de korpschef kunnen worden aangewezen als lid van een technisch team (Staatscourant, 2019, nr. 10910).

[60] In het derde Verslag (2022, p. 12) constateert de Inspectie verder dat zij begrip heeft voor het feit dat de mate waarin getest wordt afhankelijk is van 'de aard en complexiteit van de zaak en de daartoe in te zetten middelen'. Ook schrijft zij dat Digit heeft aangegeven te werken aan een nieuwe opzet van de haalbaarheidsonderzoeken en plannen van aanpak.

dat ze een 'warehouse' met 'honderden telefoons' hebben liggen. Dat is zonde omdat elke testtoestel in principe slechts eenmalig wordt gebruikt. Voor een volgende inzet moet vaak een ander apparaat worden aangeschaft, omdat dit apparaat net weer anders is.
Eén van de geïnterviewden geeft aan dat het eigenlijk voldoende zou moeten zijn wanneer het testen met een toestel met een bepaalde softwarevariant zodanig duidelijk wordt beschreven dat op basis daarvan een inschatting kan worden gemaakt of een inzet op een bijna gelijk apparaat ook succesvol zou kunnen zijn. Als op zo'n manier getest kan worden, hoeft niet steeds een nieuw toestel te worden aangeschaft. Dat biedt ook een uitweg, als in een onderzoek een verdachte een sterk verouderd toestel heeft dat niet of nauwelijks meer te koop is. Of als het wel lukt om dat toestel aan te schaffen, maar het niet mogelijk blijkt om hier een verouderde softwarevariant op te installeren.

In principe mag Digit-politie pas aan de slag met een technische voorverkenning en met het testen van de gekozen methode in een proefopstelling nadat de rechter-commissaris de machtiging heeft afgegeven en er een bevel is van de officier van justitie (Besluit onderzoek in geautomatiseerd werk, 2018, p. 16). Dat kan pas *na* een positief advies van de CTC en het College van PG's. In de praktijk loopt die route soms anders. Het testen of het lukt om het toestel binnen te dringen vindt bijvoorbeeld soms plaats *voordat* het haalbaarheidsonderzoek en het aanvraagproces-verbaal zijn afgerond.

Vanuit Digit wordt kritiek gegeven op de testopstelling. Deze kritiek is vergelijkbaar met de kritische noten ten aanzien van het plan van aanpak. Er wordt uitgelegd dat nooit helemaal zeker zal zijn wat aangetroffen wordt in een geautomatiseerd werk, ondanks alle voorbereidingen die hebben plaatsgevonden. Het is bijvoorbeeld de vraag of het gelukt is om tot een goedlijkende proefopstelling te komen, omdat onzeker is hoe een telefoon eruit ziet. Welke hardware en softwareversie bevinden zich op de telefoon? Welke applicaties staan erop? Welke virusscanner is geïnstalleerd? Dat de werkelijkheid wat grilliger zou zijn dan in de wet is voorzien wordt geïllustreerd door één van de geïnterviewden:

> *'In de wet is er dus vanuit gegaan dat het hacken een soort toveroperatie is. Een operatie waarbij de politie alles al weet over de manier waarop zij het aan wil pakken, dat alle deuren meteen opengaan, dat alles getest kan worden en dat ook een inschatting kan worden gemaakt over hoe het hacken precies gaat verlopen. De praktijk is anders. Bij hacken werkt het zo dat je eigenlijk pas een goede inschatting kunt maken als je op het geautomatiseerde werk zit. Je kunt je wel verdiepen in de hard- en software, maar je weet pas echt wat er aan applicaties en dergelijke op een* device *staat als je binnen bent.'*

Een laatste kanttekening die vanuit Digit wordt gemaakt ten aanzien van de testopstelling is dat het testen slechts een momentopname is. Een geslaagde test geeft géén garanties dat op elk moment erna binnengedrongen kan worden en onderzoek kan worden gedaan. Eén van de geïnterviewden zegt: 'Wat vandaag lukt, lukt morgen misschien niet meer en andersom kan ook het geval zijn.'

### *3.4.8 Hoofdpunten*

- Bij het intakeproces (de allereerste beoordeling of de bevoegdheid binnen een opsporingsonderzoek überhaupt zou kunnen worden ingezet) wordt naar juridische, tactische en technische aspecten gekeken.
- Digit kan vanuit capacitair oogpunt een beperkt aantal inzetten voor haar rekening nemen. Bovendien vergt elke inzet veel voorbereidingstijd.
- Het werken met een proefopstelling, onder andere bedoeld om te kijken naar neveneffecten, wordt kritisch bekeken, omdat de omgeving waarin gehackt wordt niet volledig voorspelbaar is. Bovendien zijn er hoge kosten verbonden aan het testen vanwege de wens om een identiek toestel aan te schaffen. In de wetsgeschiedenis wordt overigens niet duidelijk in welke mate een testapparaat moet lijken op het apparaat dat zal worden binnengedrongen.

## 3.5 Waarborgen voor controle voorafgaand aan de inzet

Voorafgaand aan de daadwerkelijke inzet van de hackbevoegdheid wordt een uitgebreide toetsingsprocedure gehanteerd (zie ook bijlage 4). Deze procedure is in figuur 3.2 schematisch weergegeven.

**Figuur 3.2 Toetsingsprocedure**


In de eerder genoemde OM-instructie (Openbaar Ministerie, z.d.) voor de inzet van de hackbevoegdheid zijn alle stappen die moeten worden gezet wat betreft de controle door het Openbaar Ministerie uitgebreid beschreven. Een mogelijke inzet wordt pas ter toetsing voorgelegd aan de CTC als Digit-OM er vertrouwen in heeft dat er een positief advies komt. Er gaat immers veel werk zitten in de voorbereiding van de CTC-bijeenkomst.
In de volgende paragrafen wordt nader ingegaan op de rollen van de CTC en de rechter-commissaris. De rollen van de rechercheofficier en de hoofdofficier zijn gedurende dit onderzoek zeer beperkt aan bod gekomen. Verschillende geïnterviewden geven aan de inzet voor te leggen aan de rechercheofficier. Vaak vindt dit overleg mondeling plaats waarna instemming volgt voor een inzet. Eén van de geïnterviewden vertelt zich als rechercheofficier ook gedurende de inzet bemoeid te hebben met een zaak, omdat het vermoeden van deze rechercheofficier was dat de informatie op basis waarvan besloten was tot een inzet over te gaan, niet klopte. Dat vermoeden bleek juist en op basis daarvan is de inzet gestopt. Een andere geïnterviewde merkt op dat, na de rechercheofficier, de hoofdofficier er 'heel formeel nog tussen zit'. Hij/zij tekent het verzoek om een inzet te doen, voordat het richting de CTC gaat. Het kan voorkomen dat de rol van de hoofdofficier groter is. Zo vertelt een andere geïnterviewde dat in de zaak waarin deze geïnterviewde de zaaksofficier was regelmatig overleg plaatsvond met zowel de recherche- als de hoofdofficier. Beiden waren op die manier betrokken bij de zaak, omdat het geen 'doorsnee zaak' betrof. De hoofdofficier had naar aanleiding van de inzet een aantal 'verduidelijkingsvragen'.

### *3.5.1 Advisering door de CTC en besluit College van PG's*

Wanneer de rechercheofficier en de hoofdofficier hebben ingestemd, legt de zaaksofficier de voorgenomen inzet voor aan de CTC. De CTC komt wekelijks in een vergadering bijeen. Meestal worden twee à drie verzoeken per vergadering behandeld. Daar zitten overigens ook verzoeken tussen die betrekking hebben op andere bijzondere opsporingsbevoegdheden dan de hackbevoegdheid.
Verzoeken die de hoofdofficier van justitie indient, worden bij het secretariaat van de CTC aangemeld. Bij het verzoek worden een aanvraagproces-verbaal van de politie gevoegd en een oplegnotitie van de zaaksofficier. Daarin staat een toelichting bij het verzoek beschreven en een omschrijving van de zaak inclusief aandacht voor de aanleiding van en verdenking in het onderzoek. Ook wordt in de oplegnotitie aandacht besteed aan de stand van zaken van het opsporingsonderzoek en de reden om op dat moment de hackbevoegdheid in te willen zetten. De oplegnotitie wordt door de zaaksofficier in samenspraak met de Digit-officier opgesteld. Indien bij het uitvoeren van onderzoekshandelingen gebruik wordt gemaakt van een niet gekeurd technisch hulpmiddel (ex artikel 21 lid 2 Bogw), wordt tegenwoordig ook een plan van aanpak voor het treffen van aanvullende waarborgen[61] (als bedoeld in artikel 21 lid 4 Bogw) meegezonden naar de CTC.
Tijdens de CTC-bijeenkomst wordt de aanvraag van de hackbevoegdheid in twee gescheiden delen behandeld. Er is een tactisch deel en een technisch deel. Tijdens het tactisch gedeelte geeft de zaaksofficier een toelichting op de zaak. Verteld wordt dat tijdens dit gedeelte onder andere ingegaan wordt op tactische vragen zoals waarom moet de hackbevoegdheid binnen het onderzoek worden ingezet? Wat is de meerwaarde van de inzet? Ook wordt stilgestaan bij de proportionaliteit en de subsidiariteit van de inzet.
Na het tactische deel is er aansluitend een separate bijeenkomst waarin de Digit-officier en, indien nodig, Digit-politie een toelichting geven op het haalbaarheidsonderzoek. Soms wordt tijdens dit tweede deel de technische uitvoering besproken, maar over de technische componenten 'laat de CTC zich niet erg uit'. De nadruk van de bijeenkomst ligt vooral op de haalbaarheid en afbreukrisico's van de inzet van de hackbevoegdheid.
Omdat het technisch gedeelte van de inzet van de hackbevoegdheid maar minimaal wordt beoordeeld tijdens de CTC-vergadering, vervult Digit-OM (ook) in het CTC-traject een belangrijke adviesrol. Eén van de geïnterviewden vertelt:

> *'In de tussentijd* [in aanloop naar de vergadering van de CTC en de periode dat Digit een haalbaarheidsonderzoek opmaakt] *bekijken wij: is dit een zaak waarin wat bijzonders zit wat we de CTC specifiek moeten meegeven? Als dat zo is, dan geven we dat aan, zodat we in ieder geval uitgenodigd worden of we nodigen onszelf uit. (…) En (…) zeker in de beginperiode, toen de CTC ons nog veel vroeg, eigenlijk was dat elke week gewoon wel een moment met de CTC om ze bij te praten.'*

Het geven van uitleg bij de CTC is, vanwege de technische complexiteit, niet altijd gemakkelijk. Dezelfde geïnterviewde vertelt dat wel eens een binnendringoptie is voorgelegd waarmee de CTC instemde. Naar aanleiding van een vraag van één van de WODC-onderzoekers vertelt deze geïnterviewde dat een keuze hieromtrent erg specialistische kennis vereist waarover de CTC 'beperkt' zou beschikken. De geïnterviewde vond het echter wel belangrijk om de gemaakte keuze voor te leggen, omdat slechts een klein clubje mensen (twee vanuit de politie en twee vanuit DIGIT-

[61] Zie uitgebreid paragraaf 5.2.8.

OM) in de praktijk de verschillende opties tegen elkaar afwegen. Toch blijft het lastig om dit soort zaken aan de betrokken partijen (CTC, RC, rechercheofficieren) op een begrijpelijke manier uit te leggen.

Inmiddels is de CTC wat vertrouwder geraakt met de bevoegdheid en wordt Digit-OM vooral rondom telefoonzaken niet of nauwelijks meer om advies gevraagd.
Na het tactisch en technisch gedeelte, vindt overleg plaats tussen de CTC-leden over de vraag of de voorgenomen inzet de CTC-toets kan doorstaan. De CTC beoordeelt het verzoek aan de hand van (onder meer) de verdenking, proportionaliteit, subsidiariteit, de kans van slagen van de inzet en eventuele gevoeligheden/risico's. Op basis van de beoordeling van die criteria stelt zij een advies op voor het College van PG's.
Het beslismoment om positief of negatief te adviseren volgt meestal direct na de technische en tactische toelichting. In de overgrote meerderheid van de voorgelegde inzetten is het advies positief (zie tabel 3.1).

**Tabel 3.1 Overzicht CTC-adviezen hackbevoegdheid[a]**

| Advies | 2019[b] | 2020 | 2021 |
|---|---|---|---|
| Positief | | | |
| Positief advies CTC en toestemming college | 14 | 19 | 41 |
| Deels positief advies CTC en toestemming conform advies | | 1 | 1 |
| Negatief | | | |
| Negatief advies CTC en aanvraag ingetrokken door OVJ | 0 | 2 | 1 |
| Verlengingen[c] | | | |
| Verlenging, positief advies CTC + toestemming college | 10 | 28 | 14 |
| Verlenging, deels positief advies CTC + toestemming college | | 1 | 0 |
| Verlenging, negatief advies CTC + daarna ingetrokken door OvJ | | 1 | 1 |

a De aantallen in deze tabel gaan over verzoeken en niet over geautomatiseerde werken. Het aantal unieke geautomatiseerde werken waarvoor jaarlijks een 126nba-verzoek wordt gedaan wordt niet apart bijgehouden.

b Over 2019 zijn minder cijfers aangeleverd. Een lege cel betekent dat er geen gegevens bekend zijn.

c Verlengingen kunnen ook betrekking hebben op inzetten die in een eerder jaar zijn gestart. Een zaak die bijvoorbeeld in 2019 bij de CTC is geweest voor een eerste verzoek tot inzet van de hackbevoegdheid kan in 2020 wederom bij de CTC zijn geweest voor een verlenging. Daarnaast kan het zo zijn dat er ten aanzien van één inzet meerdere keren wordt verzocht om een verlenging. In 2020 werd als toestemmingstermijn vier weken aangehouden. Na vier weken moest de zaaksofficier terugkomen en een verlenging aanvragen. In sommige gevallen was het binnendringen in een bepaald geautomatiseerd werk erg lastig. Het was niet ondenkbaar dat een zaaksofficier dan drie keer terug moest komen om een verlenging aan te vragen van de toestemming tot inzet.

Vervolgens wordt alles wat besproken is op schrift gesteld en naar het College van PG's gestuurd. Het College krijgt alleen het advies van de CTC en niet de onderliggende inhoudelijke stukken. De adviezen van de CTC en de stukken die aan de CTC ter beschikking zijn gesteld, zijn geen processtukken en worden om die reden niet aan het strafdossier toegevoegd. De beslissing om al dan niet toestemming te verlenen wordt, inclusief het CTC-advies, teruggekoppeld aan het aanvragende parket. Het advies wordt inmiddels ook teruggekoppeld aan Digit-OM, zodat zij ziet wat de CTC overwogen heeft.

**Voorbereiding op de CTC**
De CTC-vergadering wordt zowel door Digit-OM als door Digit-politie nauwkeurig voorbereid. Voorafgaand aan de bijeenkomst bij de CTC wordt met de betrokken actoren (Digit-politie, Digit-OM, de zaaksofficier en de teamleider van het tactisch team) bij het landelijke parket een overleg gepland. Tijdens dit overleg worden de inzet en de daarbij behorende technische en juridische mogelijkheden, grenzen en risico's voor het geautomatiseerde werk en derden nader besproken.
Direct aansluitend aan de CTC-bijeenkomst wordt een startbijeenkomst gepland met Digit, het tactisch politieteam en de zaaksofficier waarbij met elkaar wordt gesproken over onder andere de haalbaarheid, afbreukrisico's en procesrisico's en op welke wijze in het onderzoek verder zal worden samengewerkt. Tijdens deze overleggen worden werkafspraken en voorwaarden besproken waaronder de hackbevoegdheid kan worden ingezet. Ook vindt nog een operationeel overleg plaats tussen Digit-politie en Digit-OM voorafgaand aan de CTC-bijeenkomst. Er wordt dan onder meer besproken op welke wijze de onderzoekshandelingen worden uitgevoerd (al dan niet met een technisch hulpmiddel),[62] wat de risico's zijn voor het geautomatiseerde werk en derden en of er een afbreukrisico bestaat voor het opsporingsonderzoek.

### *3.5.2 Rechter-commissaris*

Voorafgaand aan de inzet dient de rechter-commissaris een machtiging af te geven. In principe kan elke rechter-commissaris die zich bezighoudt met zwaardere zaken te maken krijgen met een onderzoek waarin de hackbevoegdheid wordt ingezet. Om die reden is voor rechters-commissarissen een instructie opgesteld die opgenomen staat in een (intern) handboek. Op basis van de eerste ervaringen die met de bevoegdheid zijn opgedaan, staat in die instructie uitleg over de bevoegdheid, eisen voor toepassing ervan en de mitsen en maren van een inzet geformuleerd. Zo staat bijvoorbeeld genoemd dat het lastig is gebleken om een technisch hulpmiddel al voorafgaand aan een inzet goedgekeurd te krijgen. Ook is in deze instructie een laagdrempelige verwijzing opgenomen naar Digit-OM, omdat zij alles kan vertellen over de in te zetten middelen, de techniek erachter en de eventuele risico's (wat ook van belang is voor de proportionaliteitstoets).
Verder is door het Kenniscentrum Cybercrime[63] een omvangrijk wetgevingsbericht en checklist opgesteld met daarin aandachtspunten rondom de beoordeling in het kader van het afgeven van een machtiging tot het binnendringen in een geautomatiseerd werk.
In Nederland zijn er enkele rechters-commissarissen die, vanwege hun specialisme, meer ervaring hebben met de inzet van de hackbevoegdheid. Hoewel deze rechters-commissarissen niet elke zaak waarin de hackbevoegdheid wordt ingezet behandelen, worden zij regelmatig benaderd door collega-rechters-commissarissen met het verzoek om mee te denken en te adviseren als deze te maken krijgen met een zaak waarin de wens bestaat om de hackbevoegdheid in te zetten.

**Afwegingen**
Een rechter-commissaris kan op verschillende manieren op de hoogte gebracht worden van het opsporingsonderzoek waarbinnen de wens bestaat om de hackbevoegdheid in te zetten. Soms zijn in een opsporingsonderzoek eerder al andere bevoegdheden ingezet waarvoor een machtiging van de rechter-commissaris nodig was, waardoor de

[62] Zie ook Intern document 4.
[63] Het Kenniscentrum Cybercrime verzamelt en beheert kennis en informatie over cybercrime voor alle rechtbanken en gerechtshoven in Nederland. Het Kenniscentrum Cybercrime is onderdeel van het Gerechtshof Den Haag (Derechtspraak.nl, z.d.).

rechter-commissaris de inhoud van het opsporingsonderzoek al kent. In andere gevallen kan het aanvraagproces-verbaal worden gebruikt om de rechter-commissaris een overzicht van het opsporingsonderzoek te verschaffen en inzicht te geven in het nut en de noodzaak van de inzet van de hackbevoegdheid. De twee rechters-commissarissen die in het kader van deze eerste evaluatie gesproken zijn, geven beiden aan dat er naar aanleiding van de startinformatie over een opsporingsonderzoek altijd wel onderwerpen zijn waarover zij als rechter-commissaris meer willen weten.
Digit-OM heeft een notitie opgesteld waarin staat beschreven welke informatie wel, en welke informatie géén onderdeel uitmaakt van de machtiging van de rechter-commissaris (intern document 5). Dat heeft geleid tot een aantal uitgangspunten bij het informeren van de rechter-commissaris bij de inzet van de hackbevoegdheid. Deze punten komen grotendeels tegemoet aan de informatiebehoefte die bij de twee rechters-commissarissen bestond die in het kader van het eerste deel van de evaluatie geïnterviewd zijn. Zo moet de rechter-commissaris actief geïnformeerd worden over de te verrichten onderzoekshandelingen en de wijze waarop die worden uitgevoerd. Ook over de mate waarin het binnendringen en/of de onderzoekshandelingen risico's met zich meebrengen voor het functioneren van het geautomatiseerde werk of derden, wordt de rechter-commissaris actief geïnformeerd. Die informatie is nodig om een proportionaliteits- en subsidiariteitsafweging te maken. Ook aan een eventueel internationale component moet aandacht worden besteed. Indien de gegevens niet in Nederland zijn opgeslagen/het geautomatiseerde werk zich in het buitenland bevindt, wordt hier in de vordering tot machtiging en in het bevel melding van gemaakt.
De methode van binnendringen maakt géén onderdeel uit van het bevel en de machtiging tot het verlenen van dat bevel. Daar hoeft een rechter-commissaris dus ook niet over geïnformeerd te worden. Over het binnendringen in een geautomatiseerd werk en de wijze waarop dit gebeurt, kan de landelijk Digit-officier de rechter-commissaris, indien gewenst, wel (mondeling) informeren. Daarbij is het voor Digit-OM zoeken hoe ver de informatie gaat die aan de rechter-commissaris verstrekt wordt, bijvoorbeeld over het binnendringen of over de technische aspecten rondom een technisch hulpmiddel. De geïnterviewde rechters-commissarissen benadrukken op hun beurt dat het van belang is om echt goed te begrijpen wat er gebeurt voordat een machtiging wordt afgegeven. Soms zijn dat vragen over technisch aspecten, bijvoorbeeld hoe wordt binnengedrongen? Wat zijn de risico's? Ook kan het voorkomen dat behoefte is aan informatie over de werking van het technisch hulpmiddel. Dat zijn doorgaans onderwerpen die (bewust) niet op papier worden vastgelegd. Het komt voor dat de zaaksofficier soms al met de Digit-officier gebeld heeft om de rechter-commissaris van extra informatie te voorzien. De rechter-commissaris neemt soms ook zelf rechtstreeks contact op met Digit-OM. Eén van hen vertelt:

> *'(..) dat is gewoon heel fijn, want dan krijg je* [van de Digit-officier] *allemaal informatie die je niet van de zaaksofficier krijgt, want die heeft dat ook niet. En dat schrijven we ook niet op* [in de machtiging]*. Maar wel dat er een toelichting is gekomen* [die vanwege zwaar opsporingsbelang niet kan worden gedeeld]*.'*

Hoewel de geïnterviewde rechters-commissarissen aangaven dat het van belang is om goed te snappen wat er gebeurt voordat er een machtiging wordt afgegeven, is dat niet altijd haalbaar. Enerzijds heeft dat te maken met het (wisselende technische) kennisniveau. Vaak is een rechter-commissaris al verbonden aan een zaak voordat de inzet van de hackbevoegdheid in beeld komt. Er zijn daarom ook niet of minder technisch onderlegde rechters-commissarissen betrokken bij de inzetten van Digit. Anderzijds kan, ook als de kennis wel aanwezig is, niet alle informatie worden gedeeld

in verband met de afscherming van de werkwijze van Digit. Dat maakt dat de rechter-commissaris bij het vormen van zijn oordeel deels ook moet vertrouwen op de kennis, expertise en professionaliteit van anderen, zoals onderstaand fragment uit een interview met één van hen illustreert:

> *'Onderzoeker: dat is misschien een lastige vraag, snappen jouw collega's wat er precies gebeurt? Of snap jij wat er precies gebeurt?'*
>
> *'Dat is wel een gewetensvraag, want je weet niet wat je niet weet. En ik denk wel dat er een verschil is tussen een positie van een officier en van een rechter-commissaris. Dat is ook de reden denk ik dat er een hele gespecialiseerde officier bij Digit zit, die echt van de hoed en de rand weet, en die moet het aan ons kunnen uitleggen. En de precieze technische werking hoef ik niet te weten. Ik moet het alleen (…) weten, zodat ik het kan meenemen in mijn proportionaliteitstoets. Eventueel subsidiariteit, maar volgens mij speelt het meer in het kader van de proportionaliteit. (…) Het gaat toch vooral om schade aan derden, of aan het geautomatiseerde werk, waar je goed over ingelicht wil worden. En dan staat er bijvoorbeeld nihil, dat is duidelijk. Maar soms staat er: gering, en dan wil ik weten wat (…) gering betekent.'*

Wanneer een machtiging wordt afgegeven, kan er variatie zijn wat betreft de mate waarin de rechter-commissaris voorwaarden verbindt aan de machtiging. Eén van de geïnterviewde rechters-commissarissen geeft aan de uitvoering van de bevoegdheid (tot nog toe) niet te veel hebben willen inperken, omdat daar geen aanleiding toe was. Volgens een andere geïnterviewde, een zaaksofficier, komt het toch wel eens voor dat een rechter-commissaris zich meer mengt in de inzet. Deze geïnterviewde vertelt dat de rechter-commissaris die een machtiging moest afgeven in het opsporingsonderzoek waarbij deze geïnterviewde betrokken was er 'heel strak inzat'. De rechter-commissaris wilde 'elke dag een update' hebben. Volgens deze geïnterviewde deed de betreffende rechter-commissaris steeds navraag bij de cyberofficier van justitie. Daaraan zou je hebben kunnen merken dat de bevoegdheid voor de rechter-commissaris 'nieuw en wennen' was.

In de uitvoeringspraktijk blijkt dat de rechter-commissaris in de zaken die zijn bestudeerd niet definitief beslist geen machtiging af te geven. Wel wordt tijdens interviews aangegeven dat een vordering tot machtiging dan wel het onderliggende proces-verbaal soms moet worden aangevuld. Eén voorbeeld van een in eerste instantie afgewezen verzoek ging over een gewenste inzet waarbij het geautomatiseerde werk niet bij de verdachte zelf in gebruik was, maar bij een ander. Vervolgens volgde een proces-verbaalverdenking van die persoon en kon de machtiging alsnog worden afgegeven. Ook komt het voor dat de rechter-commissaris aanvullende vragen heeft of beperkingen opneemt in de machtiging, bijvoorbeeld over de looptijd van de inzet, in het geval van OVC is dat soms twee in plaats van vier weken, of de hoeveelheid gegevens die verzameld mag worden. Dat kan bijvoorbeeld betrekking hebben op een mailaccount dat de verdachte meer dan tien jaar gebruikt, aldus één van de geïnterviewde rechters-commissarissen. Het binnendringen van zo'n account zou betekenen dat de gehele inhoud van die mailbox kan worden binnengehaald. Wat deze geïnterviewde betreft is dat 'onnodig privacy schendend' en kun je om die reden proberen de periode te beperken waarover gegevens worden binnengehaald. Overigens is het aanbrengen van zo'n gewenste beperking soms technisch niet mogelijk. Dat kan een extra reden zijn voor de rechter-commissaris om zich goed te laten voorlichten over de werking van een technisch hulpmiddel. In zo'n

geval kan ervoor gekozen worden om de beperking op te nemen dat alleen de gegevens van de afgelopen twee jaar in het onderzoek mogen worden gebruikt. De rechters-commissarissen die in het kader van deze evaluatie gesproken zijn, geven aan dat het voor de afgifte van de machtiging niet meeweegt of een technisch hulpmiddel is goedgekeurd. Een van hen zegt:

> *'(…) ik kan me eigenlijk geen situatie voorstellen waarvan je denkt: nou nu het een niet goedgekeurd middel is, doe ik het maar niet. Nee. Je weet dat dat later in de procedure, dat dat misschien problemen op gaat leveren. (…). Wie zegt dat de resultaten die jullie zeggen te hebben uit dat onderzoek komen? Komt het wel uit die hack? Maar, nee… validatie, dat is wel een beetje een ding, maar dat is ook wel een beetje latere zorg (…).'*

Ook wat betreft proportionaliteit en subsidiariteit is er doorgaans geen reden om van een machtiging af te zien. Er wordt verteld dat beide eerder al uitvoerig getoetst zijn en dat de aangedragen inzetten, inzetten betroffen in opsporingsonderzoeken naar zeer ernstige delicten waarbij het nut en de noodzaak om de hackbevoegdheid in te zetten duidelijk waren gemotiveerd. Dezelfde geïnterviewde vermoedt dat er ook een soort 'natuurlijke drempel' is om de bevoegdheid in te zetten, onder andere vanwege de kosten van een inzet en alle werkzaamheden die Digit dient te verrichten.

### *3.5.3 Machtiging en afgifte bevel*

Een machtiging wordt meestal afgegeven voor de duur van vier weken. Soms wordt daarvan afgeweken, vooral bij de inzet van OVC. Dan kan de duur van de inzet vaker beperkt worden tot twee weken. Eén van de geïnterviewden, betrokken bij de toetsing van de inzet van de bevoegdheid, legt uit dat dat vooral bedoeld is om 'meer de vinger aan de pols' te kunnen houden op welke momenten de bevoegdheid wordt ingezet. Met een 'gewone OVC' (zonder binnendringen) is er doorgaans ook meer controle, in plaats van dat de toestemming voor een maand wordt gegeven.

Na een machtiging van de rechter-commissaris kan de zaaksofficier de inzet van de bevoegdheid bevelen. Een bevel kan na machtiging schriftelijk worden gewijzigd, aangevuld, verlengd of beëindigd. Bij dringende noodzaak kunnen de beslissing van de officier van justitie en de machtiging van de rechter-commissaris mondeling worden gegeven en deze dienen daarna op schrift te worden gesteld. Deze mondelinge optie is er alleen voor een verlenging van een inzet, en niet voor de eerste inzet binnen een opsporingsonderzoek. Eén van de geïnterviewden vanuit Digit vertelt dat het lastig is dat er voor het verkrijgen van het eerste bevel geen 'mondelinge spoedprocedure' is die binnen een bepaalde periode schriftelijk kan worden bevestigd. Een andere geïnterviewde, ook werkzaam bij Digit, legt uit dat het in de praktijk mogelijk is gebleken om binnen zes uur een bevel te krijgen. Tegelijkertijd vertelt deze geïnterviewde[64] dat in een recente zaak Digit met spoed een inzet wilde doen, maar dat dit niet is gelukt, omdat de schriftelijke stukken niet op tijd in orde waren. Zodra het bevel is afgegeven, wordt deze aan Digit-politie en aan Digit-OM toegestuurd. Digit start met haar inzet op de startdatum die in het bevel staat opgenomen (intern document 1).

Een bevel kan voor de duur van vier weken worden verstrekt en kan telkens voor een periode van ten hoogste vier weken worden verlengd. De termijnen dienen door de

[64] Deze geïnterviewde vertelt op eigen initiatief over dit voorbeeld toen de periode van dataverzameling voor het eerste deel van de evaluatie al afgerond was.

zaaksofficier te worden bewaakt. De inhoud van een verlengingsaanvraag wordt door Digit-politie afgestemd met Digit-OM. Na akkoord kan het aanvraag proces-verbaal worden ingediend bij de zaaksofficier.

### *3.5.4 Betrokkenheid verschillende actoren*

In het voorgaande is duidelijk geworden dat verschillende actoren betrokken zijn, voordat de bevoegdheid daadwerkelijk wordt ingezet. Voordat een zaak naar de CTC gaat, hebben op tactisch niveau een rechercheofficier en een hoofdofficier naar de zaak gekeken als eerste toets. De procedure die doorlopen moet worden voordat de hackbevoegdheid kan worden ingezet wordt gezien als een arbeidsintensief traject. Het is intensief omdat er veel partijen bij betrokken zijn, en er veel checks plaatsvinden, met name met en door Digit-OM. Dat geldt zowel voor de CTC-stukken als voor de stukken die richting de rechter-commissaris moeten. Eén van de geïnterviewden vraagt zich af of de betrokkenheid van de CTC er altijd zal moeten zijn:

> *'Als je het vanuit dat perspectief bekijkt, dan kun je je afvragen of dat hele traject richting de CTC noodzakelijk is. Je zou kunnen zeggen: de onbekendheid met het middel op dit moment én de verstrekkendheid, de potentiële verstrekkendheid, én we weten eigenlijk nog niet zo goed wat er gebeurt, rechtvaardigt, zeker in deze fase, nog wel de CTC. Gewoon dat je dat technisch, maar ook gewoon juridisch gewoon wil zien in de praktijk. Nou dat doe je nu met het onderzoek, maar je kunt je afvragen of dat op termijn nog noodzakelijk zal zijn. Tenzij, maar dat hangt er een beetje van af hoe je het gaat gebruiken, als je bijvoorbeeld de microfoon van zo'n telefoon gaat gebruiken, ja dan wordt het misschien weer een andere afweging. Omdat die op plaatsen kan komen waar je niet zo maar mag zijn. Dus dan wordt misschien het gebruik ervan wel bepalend voor welke waarborgen je op voorhand inzet. Maar als je gewoon kijkt naar wat voor informatie haal je binnen, ja dan rechtvaardigt dat op zichzelf, nou wel een rechterlijke toets, maar misschien niet een zware CTC- en College-toets. Dus zo kijk ik er een beetje naar op termijn, omdat het wel goed is om er op deze manier mee bezig te zijn.'*

Een andere geïnterviewde geeft daarentegen aan juist goed te snappen waarom de toetsingsprocedure zo zwaar is aangezet:

> *'Het is een middel wat, je moet door heel veel hoepels springen, (…) wil je toestemming krijgen en dat is denk ik ook wel terecht, want het is het meest schokkende opsporingsmiddel dat we hebben (…). Alhoewel, dat hangt er natuurlijk helemaal vanaf hoe iemand zijn telefoon gebruikt. In potentie is het een heel zwaar BOB-middel, dus dat betekent logischerwijs, net zoals bij de andere BOB-middelen, want zo spannend is het ook weer niet, dat je gewoon goed moet kijken naar de proportionaliteit en de subsidiariteit.'*

Ondanks het feit dat meerdere partijen betrokken zijn bij het toezicht, vaart een groot deel van deze actoren op de kennis van Digit-politie en –OM. Eén van de geïnterviewden vertelt dat dat wel eens ingewikkeld is:

> *'En dat is het lastige ook* [om precies te snappen wat Digit doet]*. Het is zo specialistisch dat je (..), wat ik net zei, zo diep in het konijnenhol* [zit] *dat je, ik denk dat wij het behoorlijk goed snappen, maar ik denk dat er binnen het OM weinig mensen zitten die op hetzelfde niveau zitten. Dat kan ook niet, want daar ben je specialist voor. En het is voor mij heel erg zaak om te zorgen dat ik aan de*

*ene kant bij de CTC en aan de andere kant bij de rechercheofficieren van het Landelijk Parket steeds blijf toetsen: Is dit nou wat ik hier bedenk, kan dit wel of kan die niet? En zorg dat ik het hen op een manier uitleg zodat zij* [het] *begrijpen. Maar dat is wel een lastige.'*

### *3.5.5 Hoofdpunten*

- Verschillende actoren zijn betrokken bij de vraag of de bevoegdheid in een concreet opsporingsonderzoek daadwerkelijk kan en mag worden ingezet. Digit-OM speelt hierbij, als vraagbaak en adviseur, een belangrijke rol. Vooral met betrekking tot de technische aspecten van een inzet.
- Details over de exacte wijze waarop binnengedrongen wordt maken geen onderdeel uit van de toetsing door de CTC en de rechter-commissaris.
- De uitgebreide toetsingsprocedure is een arbeidsintensief traject in vergelijking met sommige andere bijzondere opsporingsbevoegdheden. Voor de opsporingspraktijk kan het lastig zijn dat in geval van spoed er geen mondelinge procedure bestaat, zoals dat wel het geval is bij een verlenging.

# 4 Binnendringen en onderzoekshandelingen

## 4.1 Inleiding

In dit hoofdstuk richt de aandacht zich op de uitvoering van de hackbevoegdheid: het binnendringen en het verrichten van onderzoekshandelingen (deelvraag 3). Voordat op deze onderwerpen wordt ingegaan, wordt stilgestaan bij het soort misdrijven waarvoor de bevoegdheid wordt ingezet en de geautomatiseerde werken die onderwerp van een inzet waren (paragraaf 4.2). Vervolgens komen het binnendringen zelf (paragraaf 4.3) en de uitgevoerde onderzoekshandelingen aan bod (paragraaf 4.4). Afgesloten wordt met de werkwijze ten aanzien van de inzetten met een internationale component (paragraaf 4.5). Net zoals in hoofdstuk 3 start elk subhoofdstuk met een korte samenvatting van het wettelijk kader inclusief discussiepunten. Daarna volgt een beschrijving van de uitvoering in de praktijk. Elk subhoofdstuk sluit af met een opsomming van de hoofdpunten.

## 4.2 Misdrijven en geautomatiseerde werken

### *4.2.1 Samenvatting wettelijk kader*

De bevoegdheid kan worden ingezet bij strafbare feiten die volledig in de digitale wereld plaatsvinden en bij andere vormen van criminaliteit. Het soort misdrijven waarvoor de bevoegdheid mag worden ingezet is nader gespecificeerd en kent een gedifferentieerde opbouw. Ten eerste mag de bevoegdheid worden ingezet voor de opsporing van misdrijven als bedoeld in artikel 67 eerste lid Sv, zogenoemde voorlopige hechtenis-feiten (‘VH-feiten’) en voor misdrijven die een ernstige inbreuk op de rechtsorde opleveren (artikel 126nba Sv, lid 1). Ten tweede is de bevoegdheid bedoeld voor een onderzoek naar personen ten aanzien van wie een redelijk vermoeden bestaat dat zij zich bezighouden met het beramen en/of plegen van misdrijven in georganiseerd verband (artikel 126uba Sv). Ten derde kan de bevoegdheid worden ingezet wanneer er aanwijzingen zijn voor een terroristisch misdrijf (artikel 126zpa Sv). Indien de politie gegevens wil vastleggen (artikel 126nba Sv lid 1d) of gegevens ontoegankelijk wil maken (artikel 126nba, lid 1e ), dient sprake te zijn van een misdrijf waarop een gevangenisstraf van acht jaar of meer mogelijk is en of van een misdrijf dat opgenomen staat in het Besluit (artikel 126nba, lid 1). Voor die misdrijven geldt doorgaans dat er geen gevangenisstraf van acht jaar of meer kan worden opgelegd.

In tegenstelling tot het soort misdrijven is er géén lijst van geautomatiseerde werken waarin de politie zou mogen binnendringen. Die wens was er wel bij een aantal politieke partijen (zie bijlage 3). Alle geautomatiseerde werken die vallen binnen de definitie ‘een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken’ (artikel 80sexies Sr), kunnen worden binnengedrongen. In het debat met de Kamer heeft de minister toegezegd dat de politie geen pacemakers of inwendige gehoorapparaten zal binnendringen (*Kamerstukken I Handelingen* 19 juni 2018, nr. 34, p. 23).

Hoewel verschillende soorten geautomatiseerde werken binnengedrongen kunnen worden, dient een inzet wel gericht plaats te vinden. Dat betekent dat het geautomatiseerde werk bij de verdachte in gebruik moet zijn (artikel 126nba, lid1).

### *4.2.2 Misdrijven*

In de periode maart 2019 tot en met maart 2021 is voor 25 inzetten een eerste bevel afgegeven.[65] In tabel 4.1 staat een gedetailleerd overzicht van het soort misdrijven waarvoor de hackbevoegdheid is ingezet.

**Tabel 4.1 Soorten misdrijven**

| Misdrijf | Aantal inzetten |
|---|---|
| Traditionele criminaliteit | |
| Moord/doodslag en of poging daartoe en of voorbereiding | 7 |
| Combinatie met WWM en brandstichting | 1 |
| Opiumwet | 3 |
| Combinatie met omkoping en witwassen | 1 |
| Combinatie met omkoping, heling, witwassen en criminele organisatie | 1 |
| Combinatie met opium, witwassen, valsheid in geschifte en WWM | 1 |
| Combinatie met WWM en criminele organisatie | 1 |
| Combinatie met witwassen | 1 |
| Valsheid in geschrifte en oplichting | 1 |
| Lidmaatschap criminele organisatie | 2 |
| Witwassen | 2 |
| Combinatie met criminele organisatie | 1 |
| Zeden | 1 |
| Organisatie terroristisch misdrijf | 1 |
| Cybercriminaliteit in enge zin | |
| Computervredebreuk | 1 |

De naam computercriminaliteit suggereert wellicht dat de hackbevoegdheid vooral wordt ingezet voor cybercriminaliteit in enge zin. Bovenstaand overzicht laat echter zien dat het overgrote deel van de inzetten betrekking had op opsporingsonderzoeken naar zware vormen van meer traditionele criminaliteit, zowel wat betreft de proportionaliteit (feiten waarvoor een substantiële gevangenisstraf kan worden opgelegd en die de rechtsorde schaden) als wat betreft de subsidiariteit (andere bijzondere opsporingsbevoegdheden hebben weinig opgeleverd). Eén van de geïnterviewden zegt hierover:

> *'Team Digit werkt vooral aan traditionele zaken, zoals drugshandel, met een kleine digitale component, bijvoorbeeld gebruikte telefoons. Het team richt zich op de communicatie in dat soort zaken, omdat die gebruikt wordt om de handel te ondersteunen. Digit richt zich dus minder op louter malware of ransomware.'*

[65] Dit aantal betreft het aantal op basis waarvan onderzoekers een selectie hebben gemaakt van inzetten die diepgaander zijn bestudeerd (zie bijlage 2).

Binnen een groot deel van de onderzoeken waarbinnen Digit een inzet heeft gedaan (8 van de 25) was sprake van een misdrijf binnen de opiumwet, al dan niet in combinatie met andere delicten zoals witwassen, omkoping en misdrijven gerelateerd aan de Wet Wapens en Munitie. Ook moord/doodslag of een poging daartoe was in een aanzienlijk deel van de zaken een delict waarnaar een tactisch team van de politie onderzoek deed (8 van de 25). Naast deze vormen van criminaliteit is onderzoek gedaan naar, al dan niet in combinatie, valsheid in geschrifte, lidmaatschap van een criminele organisatie, witwassen, terrorisme en een zedengerelateerd misdrijf (onder andere ontucht). Slechts één inzet betrof cybercriminaliteit in enge zin. Hierbij ging het om het ontoegankelijk maken van een botnet.

Binnen alle inzetten zijn gegevens vastgelegd (subD) en/of gegevens ontoegankelijk gemaakt (subE). Voor de inzet van subD en subE gelden strengere eisen wat betreft de misdrijven waarvoor deze onderzoekshandelingen kunnen worden ingezet. Uit tabel 4.2 blijkt dat bij 12 van de 25 inzetten sprake was van ten minste één misdrijf waarvoor maximaal acht jaar gevangenisstraf (of meer) kon worden opgelegd. Bij 5 van de 25 inzetten was sprake van ten minste één misdrijf dat op de AMvB-lijst stond en in acht van de inzetten was sprake van een combinatie van de categorieën acht jaar en AMvB-lijst.

**Tabel 4.2 Eisen inzet subD en subE**

| Eisen inzet | Aantal |
|---|---|
| Maximale gevangenisstraf van acht jaar of hoger | 12 |
| AMvB-lijst | 5 |
| Combinatie acht jaar en AMvB-lijst | 8 |

### *4.2.3 Geautomatiseerde werken*

Bij de 25 inzetten waarvoor een eerste bevel is afgegeven, zijn 38 geautomatiseerde werken onderwerp van onderzoek geweest.[66] In tabel 4.3 staat een overzicht van de verschillende soorten geautomatiseerde werken die zijn binnengedrongen.
Zoals tabel 4.3 laat zien betreft het overgrote deel van de geautomatiseerde werken waarop is binnengedrongen (30 van de 38) een inzet op een telefoon, zogenoemde standaardinzetten. Er lijken verschillende redenen te zijn waarom Digit tot nu toe vooral telefooninzetten heeft gedaan, al worden inmiddels ook (meer) inzetten verricht op andere geautomatiseerde werken. Eén van de redenen is dat Digit vraaggericht werkt. Ze is afhankelijk van de aanvragen van tactische teams. Vanuit Digit wordt verteld dat deze teams Digit vooral weten te vinden voor telefooninzetten. Daarbij komt dat een telefoon veel informatie oplevert over een verdachte. Daarnaast staan veel servers in het buitenland, aldus één van de geïnterviewden, waardoor Digit niet altijd wat kan doen. Verder is het binnendringen op andere soorten geautomatiseerde werken meestal complex, waardoor er geen garantie is dat de inzet bijtijds kan plaatsvinden. Binnen Digit wordt, ondanks de vele telefooninzetten, geprobeerd meer diversiteit aan te brengen qua inzetten zodat ervaring kan worden opgedaan met het binnendringen in verschillende geautomatiseerde werken.

[66] Bij dit aantal gaat het om het aantal geautomatiseerde werken waarin ten minste een poging is gedaan om binnen te dringen. Niet meegenomen zijn de geautomatiseerde werken waarbij gedurende het onderzoek besloten is om niet binnen te dringen, bijvoorbeeld omdat tijdens de voorbereiding bleek dat het technisch niet mogelijk zou zijn.

### Tabel 4.3 Soorten geautomatiseerde werken

| Geautomatiseerd werk | Aantal |
|---|---|
| Telefoon | 22 |
| Telefoon in combinatie met tweede geautomatiseerd werk | 8 |
| Laptop | 2 |
| Router/modem | 2 |
| Server | 3 |
| Wireless Access Point (WAP) | 1 |
| **Totaal** | **38[a]** |

a Dit aantal is groter dan 25 (het totaal aantal inzetten), omdat per inzet meerdere geautomatiseerde werken onderwerp van onderzoek kunnen zijn.

Digit beschikt over de capaciteit om vier tot maximaal acht inzetten (op unieke geautomatiseerde werken) tegelijkertijd te doen. Een inzet vindt altijd plaats binnen een tactisch opsporingsonderzoek/een zaak. Voor telefoons hanteert Digit zoals gezegd inmiddels de richtlijn dat per inzet één telefoon tegelijkertijd wordt binnengedrongen.

Het binnendringen in een geautomatiseerd werk moet zoals eerder genoemd gericht gebeuren. Dat betekent dat de verdachte hoofdgebruiker is van het geautomatiseerde werk. Tijdens de intake met het tactisch team wordt hierop gelet. Eén van de geïnterviewden, een zaaksofficier, vertelt dat dit een criterium blijft, ook als een inzet gestart is, bijvoorbeeld of een inzet door moet blijven gaan. Een andere geïnterviewde van de politie merkt op dat die gerichte inzet ervoor zorgt dat de privacy van 'onschuldige burgers' minder in geding is dan wanneer bijvoorbeeld een gegevensdrager in beslag wordt genomen.

Vooral in de beginperiode richtte het bevel zich op één specifiek geautomatiseerd werk. In het geval van een telefoon is daar op een gegeven moment verandering in gekomen. Bij latere inzetten is het meer gangbaar geworden om een tweede geautomatiseerde werk standaard in het bevel te betrekken. In die gevallen volstond één bevel.

Het voorgaande laat zien dat de reikwijdte van wat als geautomatiseerd werk kan worden gezien door de tijd heen kan fluctueren. Dat geldt niet alleen voor de zojuist beschreven standaardinzet waarbij één telefoon tegelijkertijd wordt binnengedrongen. Een voorbeeld van zo'n andersoortige inzet is het binnendringen van een server om vervolgens een botnet ontoegankelijk te maken. Hoewel wordt binnengedrongen op een server, wordt toegang verkregen tot veel verschillende geautomatiseerde werken die het botnet met elkaar verbindt (en die niet allemaal apart vermeld staan in het bevel). Bij zo'n inzet blijven de onderzoeksactiviteiten die Digit uitvoert niet beperkt tot één of twee apparaten, zoals dat bij veel andere inzetten wel het geval is. Een geïnterviewde die betrokken is bij het toetsingsproces merkt op dat een dergelijke interpretatie van de reikwijdte van een geautomatiseerd werk niet direct vanzelfsprekend was. Bij de inzet waarover deze geïnterviewde spreekt (een andere dan de botnetzaak) twijfelde deze geïnterviewde of de keuze om het betreffende geautomatiseerde werk slechts te zien als een geheel van samenhangende apparaten wel gerechtvaardigd was en of het niet vooral een 'tactische keuze' was om verschillende geautomatiseerde werken onder één geautomatiseerd werk te laten

vallen. Aan dat ene geautomatiseerde werk waren vele andere geautomatiseerde werken gekoppeld die door deze wijze van definiëren niet apart in een bevel genoemd hoefde te worden. Uiteindelijk heeft deze geïnterviewde ingestemd, omdat Digit uit de gekoppelde geautomatiseerde werken niet allerlei gegevens zou halen waardoor de inbreuk uiteindelijk 'erg meeviel'. Deze geïnterviewde merkt op benieuwd te zijn wat een zittingsrechter van deze interpretatie vindt, al geeft deze geïnterviewde aan dat het maar de vraag is of dit vraagstuk überhaupt tijdens een zitting behandeld wordt.

#### *4.2.4 Hoofdpunten*

- Inzetten door Digit vinden vooral plaats in opsporingsonderzoeken naar zwaardere vormen van traditionele criminaliteit.
- Er wordt binnengedrongen op een beperkt aantal typen geautomatiseerde werken. In de afgelopen twee jaar vooral op telefoons.
- Meestal beperkt de omschrijving van een geautomatiseerd werk in bijvoorbeeld een aanvraagproces-verbaal zich tot één of twee apparaten.

## 4.3 Binnendringen

#### *4.3.1 Inleiding*

In de komende paragrafen wordt, na wederom een korte samenvatting van het wettelijk kader, uiteengezet hoe het binnendringen in geautomatiseerde werken in de praktijk verloopt. Eerst wordt aandacht besteed aan de vraag wat onder binnendringen moet en kan worden verstaan en de dilemma's die daarbij een rol spelen. Vervolgens wordt ingegaan op de door de politie gehanteerde werkwijze. De exacte wijze waarop de politie een geautomatiseerd werk binnendringt is geheim. Alleen Digit-OM en Digit-politie zijn van alle details op de hoogte. Het tactisch team van de politie en de zaaksofficieren van justitie weten niet hoe Digit uiteindelijk binnenkomt (tenzij dit in de strafzaak van belang is). Vanwege het geheime karakter van het binnendringen, worden in dit rapport géén details over het binnendringen besproken. Afgesloten wordt met het thema kwetsbaarheden en de aanschaf van en het gebruik van commerciële middelen. Dat thema wordt wel uitgebreid belicht, omdat hier gedurende het wetgevingstraject uitgebreid discussie over is geweest (zie bijlage 3) en de uitkomsten hiervan invloed hebben op de wijze waarop de bevoegdheid in de praktijk kan worden uitgevoerd.

#### *4.3.2 Samenvatting wettelijk kader*

In Kamerstukken wordt géén uitputtend overzicht gegeven van manieren waarop kan worden binnengedrongen, omdat het prijsgeven van de precieze methoden invloed zou hebben op de effectiviteit ervan (*Kamerstukken II* 2016/17, 26 643, nr. 6, p. 58). Eén van de manieren om binnen te dringen, en ook meteen degene die het meeste discussie heeft opgeleverd, is het gebruik van kwetsbaarheden, vooral onbekende kwetsbaarheden. Een belangrijk punt van zorg van een aantal politieke partijen was dat het gebruik van kwetsbaarheden het internet onveilig zou maken (*Kamerstukken II Handelingen* 13 december 2016, nr. 34 & *Kamerstukken II* 2015/16, 34 372, nr. 4). Rondom het gebruik van kwetsbaarheden is toegezegd dat de politie in eerste instantie bekende kwetsbaarheden zal benutten. Als dat niet mogelijk is dan kunnen onbekende kwetsbaarheden worden gebruikt (*Kamerstukken I* 2017/18, 34 372, G, p. 7). Het kabinet verwachtte dat in minder dan 10% van de zaken kwetsbaarheden zouden

worden ingezet (*Kamerstukken II Handelingen* 13 december 2016, nr. 34) en dat in veel gevallen het gebruik van bekende kwetsbaarheden zou volstaan (*Kamerstukken I* 2016/17, 34 372, D). Wat betreft bekende onbekende kwetsbaarheden is afgesproken dat de melding van het gebruik ervan kan worden uitgesteld (artikel 126 ffa Sv). In deze verplichting ligt impliciet besloten dat het gebruik van onbekende kwetsbaarheden gemeld dient te worden. De kwetsbaarheden lijken gemeld te moeten worden bij de fabrikant van de producten waarin de kwetsbaarheid zich bevindt (*Kamerstukken II* 1016/17, 26 643, nr. 428, p. 4). Het kan ook voorkomen dat de politie te maken heeft met onbekende onbekende kwetsbaarheden. Dat is het geval als gebruik wordt gemaakt van commerciële binnendringingssoftware waarvan onbekend is welke kwetsbaarheden een leverancier benut. Melden is in dat geval niet mogelijk. Om het gebruik van deze software aan banden te leggen is afgesproken dat deze software beperkt mag worden aangeschaft (Regeerakkoord 2017-2021) en dat voor elke nieuwe zaak een aparte licentie aangeschaft dient te worden (*Kamerstukken I* 2017/18, 34 372, G, p. 11-12). In het Besluit staat beschreven dat het gebruik van een commercieel product beperkt is tot het uiterste geval, dat wil zeggen wanneer minder ingrijpende manieren zoals *social engineering* of bekende kwetsbaarheden niet toereikend zijn (Besluit onderzoek in een geautomatiseerd werk, p. 15).

### *4.3.3 Binnendringen – reikwijdte en behoefte steunbevoegdheid*

Over het binnendringen van een geautomatiseerd werk is weinig vastgelegd in de wet. Dat levert in de uitvoeringspraktijk vragen op. Het is bijvoorbeeld onduidelijk of een bepaalde handeling onder het binnendringen kan worden geschaard. Eén van de geïnterviewden legt uit dat een vergelijking met artikel 138ab Sr (computervredebreuk) niet altijd past. Bij artikel 126nba gaat het om *heimelijk* en *op afstand* binnendringen, terwijl voor artikel 138ab Sr die criteria niet gelden. Als voorbeeld geeft deze geïnterviewde het openen van een laptop waarop geen wachtwoord zit en die zich in een afgesloten ruimte bevindt. Volgens artikel 138ab is dit binnendringen, terwijl dit géén binnendringen is in het kader van de 126nba, omdat het binnendringen niet op afstand gebeurt. Daarnaast is er volgens deze geïnterviewde onduidelijkheid over de vraag wanneer een handeling (juridisch) kan worden gekwalificeerd als binnendringen op een systeem. Die vraag is relevant om te kunnen bepalen of de betrokkenheid van Digit gewenst is, of dat het werk ook door een ander team van de politie kan worden verricht.

Naast dilemma's rondom de vraag wat de definitie van binnendringen is (en welke handeling maakt dat sprake is van binnendringen), speelt in de uitvoeringspraktijk de vraag welke handelingen toegestaan zijn in het kader van het binnendringen. Eén van de dilemma's die daarbij aan de orde is, is dat het in de praktijk soms toch noodzakelijk blijkt om op locatie, bij het geautomatiseerde werk (in de buurt), één of meer handelingen te verrichten om de inzet van de bevoegdheid mogelijk te maken. Artikel 126nba Sv lijkt geen rekening te hebben gehouden met deze optie. De wetgever gaat ervan uit (weliswaar niet in het wetsartikel zelf, maar wel in de introducerende tekst en de memorie van toelichting) dat de bevoegdheid *heimelijk en op afstand* plaatsvindt. Om toch in nabijheid van de verdachte te kunnen verkeren, vinden soms handelingen plaats die passen binnen artikel 3 Politiewet. Het komt echter voor dat er handelingen verricht moeten worden die niet (meer) binnen dit artikel vallen. In die gevallen kan het nodig zijn om een andere opsporingsbevoegdheid (al dan niet bijzonder) in te zetten om toegang tot het geautomatiseerde werk mogelijk te maken. Een deel van de geïnterviewden geeft aan een 'steunbevoegdheid' te missen in dat kader. Daarmee kan een mogelijkheid worden

gecreëerd, vergelijkbaar met bijvoorbeeld het opnemen van vertrouwelijke communicatie (artikel 126l Sv) dat de politie een locatie mag betreden (denk aan een woning of een besloten plaats) om uitvoering te kunnen geven aan de hackbevoegdheid, meer in het bijzonder het binnendringen.

Verschillende geïnterviewden leggen uit dat de politie door het ontbreken van een steunbevoegdheid op dit moment nog te veel afhankelijk is van wat er tot nu toe juridisch mogelijk is. Dat wordt problematisch gevonden, omdat binnendringen op grond van artikel 126nba Sv via artikel 3 Politiewet niet altijd mogelijk is (bijvoorbeeld in verband met de aanwezigheid op locatie) en omdat de politie afhankelijk is van andere opsporingsbevoegdheden (al dan niet bijzonder) die in het kader van het tactisch onderzoek al worden ingezet. Eén van de geïnterviewde opsporingsfunctionarissen vertelt hierover:

> *'We hebben nu een casus lopen waarbij ook een OVC in een pand geplaatst wordt en (...) binnen het plaatsen van die OVC bestaat de bevoegdheid om dat pand te betreden. En daar* [in die casus] *is dus een rechtmatige toegang tot die fysieke locatie. En daar gaat dan iemand van ons mee om op het moment dat daar fysieke toegang is gekregen, ook vanuit onze kant een handeling (…) te verrichten waardoor we (...) het eerste moment* [om] *van afstand toegang tot het apparaat* [te kunnen] *maken, kunnen faciliteren. (...) Op een later moment* [hoeven we dan] *niet meer in die woning aanwezig (...)* [te] *zijn,* [en hebben we] *nog steeds toegang tot het apparaat (...). Dat zoek je dan nu onder de bevoegdheid die aan de OVC hangt (…), maar dan ben je dus wel afhankelijk van of er binnen die bevoegdheid aanleiding is om naar binnen te gaan. Dat is, daar moet je heel zuiver in blijven zitten, dat je daar niet in een andere bevoegdheid, dat er dan gezegd wordt: we gaan nu naar binnen om even met de stofdoekje er over heen te gaan, knipoog, knipoog, zodat we ook voor jullie naar binnen kunnen. En dat is niet hoe het moet. Dus dat beperkt je heel erg, omdat je mee moet liften op de momenten dat er voor zo'n team een andere aanleiding bestaat. Terwijl, als je onder de streep kijkt, de inbreuk die je daar gaat maken, die is niet anders dan waar we bevoegdheden al voor gecreëerd hebben. Ik denk dat ze uiteindelijk nooit onderkend hebben dat je soms fysiek die toegang ook eventjes nodig hebt.'*

Deze geïnterviewde legt verder uit dat, mochten er niet al andere opsporingsbevoegdheden worden ingezet, dat dan een andere oplossing moet worden bedacht of dat Digit geen inzet doet. Voor deze geïnterviewde en een collega is het geen optie om de inzet koste wat kost toch door te laten gaan, zo blijkt uit het antwoord op een vraag van één van de WODC-onderzoekers:

> *'Onderzoeker: Of je doet het* [de inzet] *toch en je ziet wel wat de rechter er van vindt?*
>
> *Geïnterviewde 1: Nooit. Nee.*
>
> *Geïnterviewde 2: Nee. En de rechter gaat er ook nooit wat van vinden want de rechter ziet het* [de manier van binnendringen] *niet. Dus als wij die grens al niet bewaken…*
>
> *Geïnterviewde 1: Wie dan wel. Dat is ook gewoon de positie die we hebben rondom dat binnendringen, dat vergt een hele, hele grote mate van magistratelijk optreden van onze hand. Dus daar zit geen enkel smaakje in van goh we proberen eens wat,*

*of goh we doen iets waarvan we weten dat is eigenlijk over het randje (…) Dat is gewoon niet hoe het werkt.'*

Er wordt verteld dat het wel eens voorgekomen is dat Digit het binnendringen niet heeft kunnen doen vanwege het ontbreken van een steunbevoegdheid. Dat betrof een zaak waarbij de verdachte de gegevens op zijn geautomatiseerde werk goed beveiligd had. Om binnen te kunnen dringen was het nodig in het huis van de verdachte een handeling te verrichten. Er was echter geen mogelijkheid om gebruik te maken van een andere bevoegdheid om de woning te betreden. De politie had in theorie misschien tijdens het plaatsen van een OVC naar binnen gekund, maar het opnemen van vertrouwelijke communicatie was 'geen doel van het onderzoek', dus het binnendringen kon niet via die weg plaatsvinden.
Hoeveel inzetten om deze reden niet uitgevoerd konden worden, is gedurende dit onderzoek niet duidelijk geworden, omdat dit niet wordt bijgehouden. Eén van de geïnterviewde licht toe dat dat ook lastig is, omdat soms bij voorbaat al duidelijk is dat een bepaalde manier van binnendringen niet tot de mogelijkheden behoort. Zo'n werkwijze wordt om die reden niet serieus overwogen en niet geregistreerd.

Het voorgaande laat zien dat binnen de opsporingspraktijk behoefte bestaat aan een steunbevoegdheid. Een door Digit-OM genoemd nadeel van een steunbevoegdheid is dat de inzet van opsporingsbevoegdheden (al dan niet bijzonder) in principe verantwoord dient te worden in het opsporingsdossier. Dat wordt onwenselijk gevonden in verband met de afscherming van de gehanteerde methodes om binnen te dringen. Op die verantwoording is wel een uitzondering mogelijk, namelijk door een verzoek in te dienen bij de rechter-commissaris met de vraag of deze informatie achterwege kan worden gelaten. Vooraf is echter niet duidelijk of de rechter-commissaris dat verzoek zal inwilligen. Het kan zijn dat hij/zij niet akkoord gaat en dat zou betekenen dat deze informatie in het opsporingsdossier moet worden opgenomen. Digit wil echter geen informatie prijsgeven over de manier waarop zij een geautomatiseerd werk binnendringt. Eén van de geïnterviewden zou daarom graag zien dat dergelijke handelingen niet verantwoord hoeven te worden in een opsporingsdossier dat openbaar wordt. Deze geïnterviewde vertelt dat met het binnendringen alleen geen bewijs wordt verzameld, maar dat 'er een mate van controle' op de steunbevoegdheid zou moeten zitten. Als de politie 'dingen doet die niet voor een stafrechter kenbaar' zijn dan zou het wenselijk zijn dat handelen 'objectief getoetst te hebben'. Deze geïnterviewde oppert dat een rechter-commissaris dat buiten de strafzaak om zou kunnen doen.

### *4.3.4 Werkwijze*

Digit maakt in algemene zin onderscheid tussen twee manieren van binnendringen:

1 Een manier waarbij een vorm van interactie nodig is met de gebruiker van het geautomatiseerde werk. Een voorbeeld hiervan is *social engineering*: de politie probeert de verdachte een bepaalde handeling te laten verrichten.
2 Een manier waarbij géén interactie plaatsvindt met een verdachte.

Voor beide manieren geldt dat de politie één of meerdere kwetsbaarheden gebruikt om het geautomatiseerde werk binnen te komen.

Digit kiest in principe per inzet welke werkwijze het meest passend is. De afgelopen twee jaar heeft Digit vooral telefooninzetten gedaan. Voor de zaken is een min of meer

gestandaardiseerde manier van werken ontwikkeld (zie paragraaf 4.3.8). Deze gestandaardiseerde werkwijze neemt niet weg dat in veel dat deze inzetten ook sprake is van een maatwerkcomponent, omdat bij een deel van de inzetten een handeling van de verdachte nodig is. Voor die inzetten bedenkt Digit, op basis van informatie vanuit het tactisch team, op welke manier zij die medewerking voor elkaar kan krijgen. Het uitdenken van een strategie gebeurt tot nu toe door verschillende medewerkers binnen Digit, maar meerdere geïnterviewden geven aan dat ze hiervoor graag een specialistisch iemand zouden willen inschakelen. Inzet van meer specialistische kennis zou er volgens één van hen voor kunnen zorgen dat de kans verkleind wordt dat een verdachte door heeft dat de politie onderzoek naar hem of haar doet. *Social engineering* brengt wat dat betreft een groter 'afbreukrisico' met zich mee. Zo'n inzet heeft daarom niet de voorkeur, maar is geen reden om een inzet niet te gaan doen. Dezelfde geïnterviewde vertelt dat, naar aanleiding van een inzet die vergaande (niet-voorziene) consequenties bleek te hebben voor de verdachte (die uiteindelijk geen verdachte bleek), het voornemen bestaat om een 'beter plan van aanpak' te schrijven waarin meer aandacht is voor de consequenties van een voorgenomen werkwijze. De enige plek waar dit wordt afgewogen, is immers bij Digit en niet bij andere actoren die een beslissing moeten nemen of de bevoegdheid mag worden ingezet, zoals een CTC.

In niet-telefoonzaken is, in tegenstelling tot de telefoonzaken, altijd sprake van maatwerk. Verhoudingsgewijs zijn er veel minder van dit soort inzetten geweest. Bij deze inzetten is gebruikgemaakt van eigen technische hulpmiddelen of was sprake van een handmatige inzet (zie paragraaf 4.4.6). Ook voor deze inzetten geldt dat Digit op basis van informatie uit het tactisch onderzoeksteam een strategie bedenkt op welke manier zij het geautomatiseerde werk (bijvoorbeeld een server of een laptop) kan binnenkomen. Dit kan zowel gebeuren zonder als met behulp van een handeling van een verdachte.

**Op locatie**

In de uitvoeringspraktijk blijkt dat vooral het werken op afstand vragen oproept. Eerder werd al duidelijk dat het soms nodig is dat Digit haar werk doet vanuit een andere plek dan het politiebureau. Dat geldt zowel voor de voorbereiding om te kunnen binnendringen als voor het binnendringen zelf. Om binnen te kunnen dringen kan het nodig zijn om in de buurt van de verdachte te zijn, bijvoorbeeld om in kaart te brengen welke geautomatiseerde werken zich in de nabijheid van de verdachte bevinden.[67] Op die manier kan inzichtelijk wordt gemaakt welke geautomatiseerde werken bij een verdachte in gebruik zijn. Ook voor het daadwerkelijk binnendringen is soms een handeling op locatie nodig. Eén van de geïnterviewde opsporingsfunctionarissen geeft aan dat het uitvoeren van een fysieke handeling in sommige gevallen zelfs de voorkeur heeft:

> *'Als je één keer fysieke toegang tot een apparaat hebt, dan is het op een later moment toegang houden tot het apparaat, is vaak veel makkelijker en minder heftig vorm te geven dan dat je echt helemaal heimelijk van afstand binnendringt op een apparaat. En dat is èn veel bewerkelijker in de tijd, dus je bent gewoon veel langer bezig om daar een plan op te trekken. Maar als je het doet, dan ben je (…) beveiliging aan het doorbreken of je bent mensen aan het verleiden tot gedrag dat we eigenlijk liever niet zien (..). Dus als je het hebt over de impact van je handelingen, is het veel prettiger (…) vanuit het grote plaatje om één keer een*

[67] Dit voorbeeld betreft het binnendringen in een tweede geautomatiseerde werk gedurende een al lopende inzet.

*fysieke toegang tot een apparaat te hebben dan dat je daadwerkelijk alles heimelijk en van afstand doet.'*

Tijdens de interviews blijkt dat er discussie is over wat op afstand precies betekent. Betekent op afstand dat er gewerkt wordt vanuit de politielocatie waar Digit werkzaam is, of is ook sprake van op afstand als Digit zich dichter in de buurt van de verdachte bevindt, maar bijvoorbeeld het geautomatiseerde werk zelf niet in handen heeft? En hoe moet de situatie worden beoordeeld waarin Digit voor een korte periode toegang krijgt tot het geautomatiseerde werk (bijvoorbeeld door mee te gaan met een huiszoeking (zie paragraaf 4.3.3) en daarbinnen een handeling verricht, zodat zij vervolgens op afstand onderzoekshandelingen kan verrichten?

### *4.3.5 Kwetsbaarheden*

Om een geautomatiseerd werk binnen te kunnen dringen worden kwetsbaarheden gebruikt. Hoewel in een Kamerbrief (*Kamerstukken II* 2016/17, 26 643, nr. 428), volledig gewijd aan het gebruik van kwetsbaarheden, uitgelegd wordt wat kwetsbaarheden zijn en welke soorten (bekend en onbekend) onderscheiden worden, roept de definiëring van een kwetsbaarheid in de uitvoeringspraktijk vragen op. Het antwoord op die vragen is nodig, omdat dit bepalend is voor eventuele vervolgacties zoals het melden van een onbekende kwetsbaarheid. Het eerste discussiepunt gaat over de vraag wat überhaupt een kwetsbaarheid is. Eén van de geïnterviewden vertelt dat bijvoorbeeld nagedacht moest worden hoe een misconfiguratie te waarderen. De geïnterviewde geeft het voorbeeld van een server. Daarin kan zich een bug bevinden waardoor het gemakkelijk is om een server te laten crashen zodat vervolgens binnengedrongen kan worden. In dat geval is sprake van een kwetsbaarheid. Het kan echter ook zo zijn dat een 'systeembeheerder iets open heeft laten staan' of een heel gemakkelijk wachtwoord heeft gebruikt. Op zo'n moment is géén sprake van een kwetsbaarheid, maar van een misconfiguratie.
Het tweede discussiepunt heeft betrekking op het soort kwetsbaarheid waarvan sprake is. In de brief aan de Tweede Kamer staat uitgelegd dat een bekende kwetsbaarheid een kwetsbaarheid is waarvan de fabrikant op de hoogte is dat deze in zijn product zit. Dat riep in de uitvoeringspraktijk de vraag op wanneer er vanuit kan worden gegaan dat een fabrikant op de hoogte is. Eén van de geïnterviewden stelt bijvoorbeeld de vraag of een kwetsbaarheid als bekend kan worden verondersteld als die kwetsbaarheid beschreven staat op een 'obscuur Pools hackersforum'. Een andere geïnterviewde stelt gelijksoortige vragen. Omdat daar in de wet geen duidelijke kaders voor zijn, heeft Digit-OM hier zelf invulling aan moeten geven. Zij heeft geen eigen definitie bedacht van een onbekende kwetsbaarheid, maar er is onder andere gekeken naar wat andere partijen die te maken hebben met onbekende kwetsbaarheden hierover op papier hebben gezet en naar wat er in het buitenland onder een onbekende kwetsbaarheid wordt verstaan. In de definitie die Digit nu hanteert, wordt ervan uitgegaan dat sprake is van een kwetsbaarheid die bekend is of bekend had kunnen zijn als informatie over een kwetsbaarheid op het internet staat (bijvoorbeeld een blog op het internet) of als er een andere manier is waarop de fabrikant geïnformeerd kan zijn.

### *4.3.6 Bekende en onbekende kwetsbaarheden*

In de wetsgeschiedenis is het gebruik van bekende kwetsbaarheden om binnen te dringen als voorkeursoptie gepresenteerd. De verwachting was dat vooral van dit soort kwetsbaarheden gebruik zou worden gemaakt. Gedurende de onderzoeksperiode is

echter maar in een beperkt aantal zaken binnengedrongen via een bekende kwetsbaarheid. Een belangrijke verklaring hiervoor is het soort geautomatiseerde werken waarop is binnengedrongen. Bekende kwetsbaarheden zijn vooral bruikbaar gebleken voor de niet-telefooninzetten (maatwerk) en die zijn er veel minder geweest. Binnen Digit-politie houdt een aantal mensen van het ontwikkelteam zich bezig met het zoeken naar bekende kwetsbaarheden. Met alleen het vinden van een kwetsbaarheid op een gepubliceerde lijst is de politie er echter nog niet. Op het moment dat zo'n kwetsbaarheid gevonden wordt, kan deze doorgaans niet direct worden gebruikt. Op basis van de (beperkte) informatie die dan beschikbaar is, maakt de politie een inschatting of de kwetsbaarheid bruikbaar is. Mocht dat het geval zijn, dan maakt de politie hem gebruiksklaar (het zogenoemde *exploiten*) om hem in te kunnen zetten. Een voor de opsporingspraktijk nadeel van het gebruik van een bekende kwetsbaarheid is dat de kwetsbaarheid elk moment onbruikbaar kan worden, bijvoorbeeld omdat een computersysteem geüpdate wordt. 'Wat vandaag over een bekende kwetsbaarheid gezegd wordt, kan morgen alweer anders zijn'.

Net zoals bij een bekende kwetsbaarheid kan bij een onbekende kwetsbaarheid onderscheid worden gemaakt tussen een kwetsbaarheid die nog niet gebruiksklaar gemaakt is en een kwetsbaarheid waarbij dat al wel gebeurd is. Beide soorten (wel en niet-gebruiksklaar) worden te koop aangeboden door een commerciële partij (onbekende onbekende kwetsbaarheden). Daarnaast kan Digit zelf onbekende kwetsbaarheden vinden en er gebruik van maken (bekende onbekende kwetsbaarheden).

### *4.3.7 Bekende onbekende kwetsbaarheden*

Enkele geïnterviewden geven aan dat Digit niet snel bekende onbekende kwetsbaarheden zal gebruiken om binnen te komen. Eén van de redenen hiervoor is dat het niet altijd gemakkelijk is om deze te vinden. Dat geldt zeker voor kwetsbaarheden in geautomatiseerde werken zoals telefoons. Een andere geïnterviewde legt uit dat Digit doorgaans 'chirurgisch' (heel precies) te werk gaat. Dat betekent dat zij niet een brede aanval uitvoert om een geautomatiseerd werk binnen te komen. In plaats daarvan hanteert zij een manier van werken waarbij alleen een heel specifiek doelwit (een bepaald type geautomatiseerd werk, met een bepaalde versie) binnengedrongen wordt. Dat is ingewikkeld, onder andere omdat veel (deskundige) menskracht beschikbaar dient te zijn om dit soort kwetsbaarheden zelf te vinden. Menskracht waarover Digit-politie zelf niet beschikt.
Een ander, vaker genoemd argument voor het niet snel zullen benutten van een bekende onbekende kwetsbaarheid, is de meldplicht. In artikel 126ffa Sv is vastgelegd dat het melden van het gebruik van een onbekende kwetsbaarheid ten behoeve van het binnendringen uitgesteld kan worden. In de toelichting op dit amendement wordt verwezen naar een meldplicht, maar deze is wettelijk niet vastgelegd. In plaats daarvan volgt deze uit een toelichting van de staatsecretaris tijdens de plenaire behandeling van de wet in de Tweede Kamer. Eén van de geïnterviewden verbaast zich over het feit dat alleen de uitzondering en niet de hoofregel in de wet is vastgelegd:

> '*Waar het begint is dat de wetgever niet (..) ergens een basisprincipe* [organiseert]*, wat je als overheid moet met de kennis over een onbekende kwetsbaarheid. Het enige wat ze hebben gedaan is ergens in de blessuretijd* [vlak voor inwerkingtreding van de wet] *een bij amendement stuk regelgeving erin gefietst wat iets organiseert als uitzondering op een hoofdregel die nooit geformuleerd is.*

*Dus we hebben wel de uitzondering, maar ik heb nergens de hoofdregel staan dat ik een onbekende kwetsbaarheid moet melden.'*

Een geïnterviewde, betrokken bij het toezicht, merkt op dat het melden van een onbekende kwetsbaarheid alleen betrekking heeft op het binnendringgedeelte. In de ogen van deze geïnterviewde zouden ook kwetsbaarheden gemeld moeten worden die ingezet kunnen worden voor subE (ontoegankelijkmaking van gegevens) en die invloed hebben op de beschikbaarheid van gegevens ('*denial of service*').

**Toepassing meldplicht en kritiek**

Gedurende de onderzoeksperiode heeft de officier van justitie bij de rechter-commissaris één machtiging gevorderd om het melden van een aantal onbekende kwetsbaarheden uit te stellen. De rechter-commissaris heeft vervolgens, na een belangenafweging, deze machtiging afgegeven voor een periode van een niet openbaar gemaakt aantal maanden. Op het moment van schrijven van dit rapport is deze kwetsbaarheid nog niet gemeld. In de uiteindelijke beslissing van de rechter-commissaris speelden drie factoren een rol. Allereerst 'het gewicht van het opsporingsbelang'. Dat beoordeelde de rechter-commissaris als 'zwaarwegend'. De tweede factor is de aard en gebruikers van de software. De software was door personen met criminele intenties ontwikkeld en zou 'vrijwel alleen' gebruikt worden voor 'criminele doeleinden'. Tevens was in vergelijkbare gevallen niet gebleken dat 'goedwillende derden van deze software gebruikmaken en kwetsbaar raken'. Bovendien werd de software niet in de vitale sector gebruikt of 'regulier en wijdverbreid in de maatschappij'. De derde factor tot slot was 'de kans op misbruik van de kwetsbaarheden door een derde'. Die kans achtte de rechter-commissaris 'zeer gering' (Rechtbank Den Haag, 2021b).
Vanuit de uitvoeringpraktijk is veel kritiek op de meldplicht, en die kritiek gaat niet alleen over de wijze waarop artikel 126 ffa Sv in het Wetboek van Strafvordering terecht is gekomen. De volgende drie kritiekpunten worden in de komende subparagrafen nader uitgewerkt, namelijk er wordt geen onderscheid gemaakt tussen geautomatiseerde werken, de (internationale) samenwerking wordt bemoeilijkt en een relatieve bevoegdheid is niet geregeld.

**Geen onderscheid tussen geautomatiseerde werken**

In artikel 126ffa Sv wordt géén onderscheid gemaakt tussen de geautomatiseerde werken waarin de onbekende kwetsbaarheid gevonden wordt. Dat betekent dat een kwetsbaarheid in een computersysteem dat geproduceerd is door en voor personen met criminele intenties hetzelfde behandeld moet worden als een kwetsbaarheid in een geautomatiseerd werk dat in gebruik is bij een groot deel van de Nederlandse burgers of in een geautomatiseerd werk binnen de 'kritieke infrastructuur'.[68] Meerdere geïnterviewden verbazen zich hierover. In de eerste plaats vertellen enkele geïnterviewden dat Digit dit soort kwetsbaarheden (in geautomatiseerde werken binnen de kritieke infrastructuur of die breed gebruikt worden) zelf niet tegenkomt in de praktijk en ze ook niet zou gebruiken. Eén van hen noemt als voorbeeld een kwetsbaarheid in de dijkbewaking of in een systeem dat binnen een ziekenhuis wordt gebruikt. Zo'n soort kwetsbaarheid gaat het volgens deze geïnterviewde 'niet worden in het gebruik', vanwege de impact die het heeft. In de tweede plaats is er verbazing vanwege het feit dat deze meldplicht ervoor zou zorgen dat opsporingsinstanties het werk van personen met criminele intenties vergemakkelijken. Eén van de

[68] Er is inmiddels jurisprudentie beschikbaar, niet gerelateerd aan de meldplicht, waarin criteria geformuleerd worden op basis waarvan is bepaald dat een aanbieder van PGP-toestellen de omzet haalt uit 'enig misdrijf' (Anti Money Laundering Centre, 2021).

geïnterviewden legt dit uit aan de hand van een hypothetisch voorbeeld. Het betreft een zaak waarin Digit géén inzet heeft gedaan.

> *'(…)* [Er kunnen zich] *gekke situaties voor (…) doen.* [De geïnterviewde] *geeft het voorbeeld van een kwetsbaarheid in de malware die criminelen gebruiken om de Rotterdamse haven plat te leggen* [Maersk, NotPetya]. *Door die kwetsbaarheid zou binnengedrongen kunnen worden op de server van de verdachte.* [De geïnterviewde] *vindt het gek dat het melden van onbekende kwetsbaarheden ook geldt voor criminele software zoals de malware in het voorbeeld. Nu vertel je de crimineel hoe hij zijn gaten kan dichten. Daar zou eigenlijk een uitzondering voor moeten komen.'*

Het willen binnendringen in 'criminele' systemen is niet alleen een hypothetische situatie gebleken. Een andere geïnterviewde vertelt over de eerder al genoemde 'maatwerkinzetten' die Digit voor haar rekening neemt. Dat zijn doorgaans 'systemen van criminelen gemaakt voor criminelen'. In die systemen zitten soms programmeerfouten die deze 'criminelen' zelf maken. De meldplicht zoals die op dit moment geldt betekent dat deze personen met criminele intenties uiteindelijk op de hoogte moeten worden gesteld dat er een kwetsbaarheid in hun systeem zit, zodat zij dit zelf kunnen dichten en opsporingsinstanties niet meer in het systeem binnen kunnen dringen. Deze geïnterviewde kan zich niet voorstellen dat dat de bedoeling is geweest van de wetgever. Een andere geïnterviewde noemt nog een andere (praktische) reden waarom de meldplicht in dit soort situaties ingewikkeld is. Het is lang niet duidelijk aan wie de melding gericht moet worden.

**Samenwerking**

Een tweede punt van kritiek is dat de meldplicht samenwerking met andere partijen bemoeilijkt, zowel internationaal als nationaal. Volgens enkele geïnterviewden bevindt Nederland zich in een uitzonderingspositie wat betreft de meldplicht. Zij vertellen dat deze uitzonderingspositie ertoe bijdraagt dat voor inzetten waarbij met het buitenland wordt samengewerkt zich situaties voordoen die de samenwerking niet bevorderen. Dezelfde geïnterviewde legt uit dat in sommige landen onbekende kwetsbaarheden staatsgeheim zijn. Dat betekent dat over die kwetsbaarheid niets naar buiten mag komen. Dat is problematisch als zo'n land wil samenwerken met Nederland, omdat Digit-politie deze onbekende kwetsbaarheid (in het andere land een staatsgeheim) moet melden. Om die reden ziet Digit zichzelf genoodzaakt tegen het buitenland te zeggen dat zij beter hun mond kunnen houden, zodra zij iets willen vertellen over de manier waarop zij een computersysteem willen binnendringen. Dat maakt de samenwerking er niet prettiger op. Deze geïnterviewde licht toe:

> *'Het is heel lastig om samen te werken met een land waarin de afspraak is dat een onbekende kwetsbaarheid staatsgeheim moet blijven, terwijl jij een meldplicht hebt. Als je in zo'n geval als Nederland zegt 'wij moeten deze onbekende kwetsbaarheid melden', dan doet dat iets met het vertrouwen van dat andere land. De meldplicht maakt samenwerking met andere landen dus lastig.* [De geïnterviewde] *vertelt dat zij, wanneer zij overleg hebben met partijen waarmee zij samenwerken, altijd open zijn over het feit dat zij een onbekende kwetsbaarheid moeten melden.'*

Ook nationaal gezien vormt Digit een uitzondering wat betreft de meldplicht. In de podcast Cyberhelden (Prins, 2021) vertelt een medewerker van het NFI dat het NFI gebruik maakt van onbekende kwetsbaarheden en dat deze niet gemeld hoeven te

worden. Bij de AIVD en de MIVD geldt het beleid 'melden, tenzij'. Dat betekent dat 'in het belang van de nationale veiligheid' de keuze kan worden gemaakt om 'zwakke plekken (tijdelijk) niet te melden' (AIVD, z.d.).

**Relatieve bevoegdheid niet geregeld**
Zoals eerder aangegeven heeft de Digit-officier van justitie één keer een machtiging gevorderd bij de rechter-commissaris in verband met het uitstellen van het melden van een bekende onbekende kwetsbaarheid. Een praktisch probleem waarop gestuit werd is dat er in artikel 126ffa geen rechtbank geregeld is waarnaar de officier van justitie zijn vordering kan richten. Relatieve bevoegdheidsregels zijn in principe allemaal opgehangen aan de verdachte of aan het strafbare feit. Het melden van een onbekende kwetsbaarheid zou als 'zaaksoverstijgend' kunnen worden gezien. Volgens één van de geïnterviewden is hier geen rekening mee gehouden bij het formuleren van artikel 126ffa Sv:

> *'Als je terug gaat kijken in de toelichting bij ffa* [art 126ffa Sv] *wordt er heel makkelijk gezegd van: ja dat kan dan een beetje aansluitend bij je strafzaak of zoiets dergelijks, of bij je nba* [artikel 126nba Sv]*. Maar daarmee wordt miskend dat bij een nba het zich richt op een verdachte of een zaak of een bepaald doel en die ffa* [heeft betrekking op] *(...) een foutje wat je aantreft die* [je] *(...) gewoon toevallig in die zaak tegenkomt. Maar het zegt niks over die hele zaak. Dus ook jouw toets of je wel of niet uitstel wilt verlenen, staat los van die hele zaak. Dus het is niet meer een onderdeel van die zaak. En ja, daar is gewoon te veel van uitgegaan* [dat het gerelateerd is aan een concrete zaak]*.'*

Dat deze onbekende kwetsbaarheid als zaaksoverstijgend wordt gezien, betekent dat niet duidelijk is tot welke rechtbank het Openbaar Ministerie zich moet wenden. Uiteindelijk heeft de rechter-commissaris in de uitspraak over het uitstellen van de melding gemotiveerd waarom gevonden werd dat in dit geval kennis genomen mocht worden van de vordering van de officier van justitie (Rechtbank Den Haag, 2021b).

**Alternatieven**
Verschillende geïnterviewden vanuit Digit-politie vertellen dat er volgens hen alternatieven zijn voor de manier waarop de meldplicht op dit moment geregeld is. Enkele geïnterviewden pleiten voor het creëren van een verzamelpunt voor onbekende kwetsbaarheden, vergelijkbaar met de manier waarop dat in de Verenigde Staten gebeurt. In Nederland bestaat het Nationaal Cyber Security Centrum (NCSC), maar die is vooral gericht op kwetsbaarheden in producten (bijvoorbeeld een router), aldus een geïnterviewde. Bij zo'n verzamelpunt zou vervolgens besloten moeten worden hoe ernstig de kwetsbaarheid is (wordt een land er onveiliger door) en of deze aan de fabrikant moet worden gemeld. Volgens een andere geïnterviewde zou de Nederlandse politie ook prima in staat zijn om deze afweging te maken, maar 'is er in Nederland niet het vertrouwen dat de politie dat zelf kan'. Weer een andere geïnterviewde geeft aan dat bij de komst van zo'n meldpunt wel goed nagedacht zou moeten worden over de vraag wie allemaal een dergelijke beslissing kan nemen en over de uitvoerbaarheid van het proces.

Een volgend alternatief is dat duidelijker onderscheid gemaakt kan worden tussen het soort geautomatiseerde werk waarin de kwetsbaarheid zich bevindt. Een onbekende kwetsbaarheid in een KPN-netwerk zou anders behandeld moeten worden dan een kwetsbaarheid in een netwerk dat 'dedicated door criminelen wordt gebruikt'. Verder zouden afspraken gemaakt kunnen worden hoe om te gaan met kwetsbaarheden die

door andere (buitenlandse) partijen gevonden worden. Eén van de geïnterviewden merkt op dat die kwetsbaarheden vrijgesteld zouden kunnen worden van de meldplicht, omdat deze kwetsbaarheden 'eigendom' zijn van het buitenland. Een andere geïnterviewde wijst erop dat maar 'tot op zekere hoogte' een dergelijke afspraak gemaakt kan worden. Een vrijstelling is bijvoorbeeld lastig in het geval een onbekende kwetsbaarheid een veiligheidsprobleem met zich meebrengt. Daarbij komt dat elk land op zijn eigen manier een beoordeling zal maken van de veiligheidssituatie en eigen waarden en normen heeft op dat gebied. Mocht staatsveiligheid als criterium worden meegenomen, dan zullen volgens deze geïnterviewde de veiligheidsdiensten geïnformeerd moeten worden. De kwetsbaarheid kan immers een kwetsbaarheid betreffen die zij in hun onderzoek inzetten.

### *4.3.8 Onbekende onbekende kwetsbaarheden*

In het grootste deel van de inzetten maakt Digit gebruik van binnendringingssoftware die bij een commerciële leverancier (hierna leverancier) is aangeschaft. Deze binnendringingssoftware is doorgaans verwerkt in een product waarmee ook onderzoekshandelingen worden verricht. De samenstelling en werking van dit product is voor Digit een 'zwarte doos', omdat dit tot het bedrijfsgeheim behoort van de leverancier. Dat betekent dat Digit géén kennis heeft van de inhoudelijke samenstelling van het product (welke onbekende kwetsbaarheden erin verwerkt zijn). Toch wordt uitgelegd dat deze producten uit één of meer onbekende kwetsbaarheden moeten bestaan, omdat het anders niet mogelijk zou zijn om ermee binnen te dringen. Meerdere geïnterviewden vertellen dat leveranciers nooit volledig inzage zullen geven in de werking van hun product, omdat dat 'hun goud' is. Zodra informatie over hun product op straat komt te liggen, bestaat het risico dat het niet langer bruikbaar is en dat betekent dat hun investeringen (grote bedragen) voor niks gedaan zijn. Eén van de geïnterviewden zegt (het gaat hierbij over de hypothetische situatie dat informatie op straat komt te liggen door een meldplicht):

> *'Zo'n bedrijf steekt miljoenen in het vinden van een kwetsbaarheid en het ontwikkelen van een product. Als wij die kwetsbaarheid voor één onderzoek zouden gebruiken en de kwetsbaarheid daarna zouden melden, omdat deze nog onbekend is, dan is de investering van zo'n commerciële partij er voor niets geweest. Ook voor al hun andere klanten zal hun product niet meer bruikbaar zijn.'*

Omdat de onbekende kwetsbaarheden onbekend zijn bij Digit, geldt voor deze kwetsbaarheden niet de eerder besproken meldplicht.[69] Enkele geïnterviewden zijn kritisch ten aanzien van de manier waarop dit geregeld is:

> *'Geïnterviewde 1 zegt dat er nu wat hypocriets zit in het omgaan met onbekende kwetsbaarheden. Vooral wat betreft het aanschaffen van commerciële producten. Eigenlijk weet je dat daarin onbekende kwetsbaarheden zitten, maar omdat je dat officieel niet kunt weten, hoeven we het niet te melden en kunnen we dus met deze producten werken. Maar als je het zelf ontdekt, mag het niet op die manier. Dat is hypocriet. Geïnterviewde 2 merkt op dat* [dit] *eigenlijk lijnrecht staat tegenover het feit dat ze gemeld moeten worden. Deze geïnterviewde merkt ook op dat nu eigenlijk van twee walletjes gegeten wordt. Aan de ene kant wordt van je gevraagd kwetsbaarheden op te lossen en aan de andere kant ga je ze kopen om te gebruiken. Dat bijt elkaar.'*

[69] Door het 'zwarte doos' karakter van dit middel weet Digit niet van welke kwetsbaarheid gebruik wordt gemaakt en dus kan zij geen melding doen.

Hoewel dus niet met 100% zekerheid kan worden gezegd dat leveranciers in hun producten gebruikmaken van onbekende kwetsbaarheden, wordt daar in de rest van dit rapport wel vanuit gegaan. Daarom richt de aandacht zich in de komende paragrafen op (de samenwerking met) leveranciers en op hun producten.

**Noodzaak commerciële middelen**

Zoals gezegd is bij de grootste deel van de inzetten gebruikgemaakt van één of meerdere commerciële producten waarin één of meerdere onbekende kwetsbaarheden verwerkt zijn (hierna een commercieel product). Dit ligt niet in lijn met hoe de wetgever dit oorspronkelijk bedacht had. Dat er vooral gebruik is gemaakt van een commercieel product heeft te maken met het feit dat het grootste deel van de inzetten een inzet betrof op een telefoon. Een aantal geïnterviewden merkt op dat Digit dergelijke inzetten niet zonder een commercieel middel kan doen. Daarvoor wordt een aantal redenen genoemd. De eerste is dat het technisch heel ingewikkeld is om binnen te dringen, zeker op geautomatiseerde werken die een groot deel van de Nederlanders gebruikt, zoals een smartphone. Fabrikanten van dat soort producten investeren veel geld om hun product zo veilig mogelijk te krijgen. Om die beveiliging te kunnen doorbreken is veel kennis en menskracht nodig. Eén van de geïnterviewden spreekt over 100+man en dat is volgens deze geïnterviewde nog een optimistische inschatting. Commerciële leveranciers van onder andere binnendringsoftware hebben de beschikking over dit grote aantal medewerkers (en waarschijnlijk meer dan dat), terwijl Digit minder dan tien man hiervoor beschikbaar heeft. In het Regeerakkoord is destijds 10 miljoen euro beschikbaar gesteld, onder andere om Digit zelf producten te laten ontwikkelen. Ook met dat extra bedrag is het volgens sommige geïnterviewden niet realistisch om de samenwerking met commerciële leveranciers volledig los te laten. Niet alleen omdat veel extra personeel moet worden aangenomen, maar ook omdat de kennisachterstand inmiddels zo groot zou zijn dat het kennisniveau van leveranciers niet geëvenaard kan worden. Eén van de geïnterviewden, die aangeeft dat Digit niet te afhankelijk wil zijn van commerciële partijen en er het liefst los van komt, wijst nog wel op een mogelijk alternatief, namelijk het kopen van kwetsbaarheden (in plaats van een heel product). Vervolgens zou Digit die zelf gebruiksklaar kunnen maken. Deze geïnterviewde legt echter uit dat dit géén realistische optie is, omdat afgesproken is dat Digit zelf geen kwetsbaarheden (die nog niet gebruiksklaar zijn) mag inkopen. Een andere geïnterviewde van Digit vraagt zich hardop af of Digit zich wel bezig zou moeten houden met het ontwikkelen van een product vergelijkbaar met dat van een commerciële leverancier. Volgens deze geïnterviewde is Digit er voor de opsporing en is het team 'geen *software development* bedrijf'.

Een tweede argument, dat nauw samenhangt met het voorgaande, is dat leveranciers ook het onderhoud van hun product voor hun rekening nemen. Bij de aanschaf van een product sluit Digit een onderhoudscontract af, zodat de continue werking ervan zo veel mogelijk gewaarborgd kan blijven. Volgens één van de geïnterviewden hebben leveranciers er belang bij dat hun product zo goed mogelijk functioneert, omdat ze anders snel hun klantenkring kwijt raken. Als Digit zelf het onderhoud voor haar rekening zou moeten nemen en eventuele alternatieven (andere kwetsbaarheden) in huis moet hebben, dan zou daarvoor extra menskracht nodig zijn die er niet is. Bovendien zou Digit deze alternatieven moeten melden.

Het derde argument tot slot heeft te maken met de meldplicht. Mocht het mogelijk zijn voor Digit om een zelf gevonden onbekende kwetsbaarheid gebruiksklaar te maken, eerder is gebleken dat dit vooral vanwege de technische complexiteit een zo goed als hypothetische situatie is, dan vormt de meldplicht een belemmering. Het zelf vinden van een kwetsbaarheid betekent dat deze gemeld moet worden en dat de kwetsbaarheid, waarin veel energie gestoken is om die gebruiksklaar te maken, voor

één of hooguit twee zaken kan worden gebruikt. Eén van de geïnterviewden is daarom blij dat er een mogelijkheid is om met commerciële middelen te werken. Volgens deze geïnterviewde zou het een ramp zijn als commerciële middelen niet meer zijn toegestaan en ze tegelijkertijd de bekende onbekende kwetsbaarheden moeten blijven melden. Een andere geïnterviewde merkt op dat ze bij Digit in zo'n geval 'geblinddoekt zijn en dat hun handen op hun rug zijn vastgebonden'.

Vanwege de geschetste afhankelijkheid van commerciële middelen pleit weer een andere geïnterviewde van de politie voor het aangaan van 'strategische samenwerking': publiek-private samenwerking tussen de markt (cybersecuritybedrijven) en de publieke sector waaronder defensie en mogelijk ook inlichtingen- en veiligheidsdiensten. Deze samenwerking zou in de ogen van de geïnterviewde, naast binnendringen en onderzoekshandelingen, ook betrekking kunnen hebben op andere onderdelen zoals de technische infrastructuur waarmee Digit werkt.

**Aanschaf middel**

*Binnendringen gecombineerd met onderzoekshandelingen*
Leveranciers van commerciële middelen maken, in tegenstelling tot de wetgever, doorgaans géén onderscheid tussen binnendringen en onderzoekshandelingen. Vaak wordt een kant-en-klaar product verkocht. Enkele geïnterviewden lichten toe dat leveranciers wereldwijd werken en daarom generieke producten willen maken. Een leverancier kijkt anders naar zijn producten dan de wetgever in Nederland dat doet. Er wordt verteld dat in het ideale geval alleen binnendringingsoftware wordt aangeschaft, die vervolgens gecombineerd wordt met een eigen door Digit ontwikkeld technisch hulpmiddel waarmee de onderzoekshandelingen kunnen worden verricht. Eén van de geïnterviewden, werkzaam bij Digit, vertelt dat het de afgelopen tijd wel mogelijk is gebleken om met een leverancier afspraken te maken over het aanbrengen van wijzigingen aan het standaardproduct dat zij levert. Op die manier zou het product beter passen in de context van de Nederlandse wetgeving. Er zijn wijzigingen aangebracht waardoor beter aan de elementen uit het bevel kan worden voldaan. Het technisch hulpmiddel beschikt over de volgende functionaliteiten (waarvan overigens, vanwege technische redenen, niet altijd gebruik kon worden gemaakt): het overnemen van (lokaal opgeslagen) gegevens, het maken van afbeeldingen, het opnemen van beeld en geluid, waaronder communicatie, en locatiebepaling.
Uiteindelijk hoopt Digit het proces van in- en exfiltreren van elkaar te kunnen scheiden waardoor alleen voor het binnendringen een commercieel product nodig is en voor het uitvoeren van onderzoekshandelingen niet meer.

**Aankoopproces**

*Leveranciers*
Informatie over leveranciers waarvan Digit haar producten afneemt is vertrouwelijk en daarom niet gedeeld met de auteurs van dit rapport. Eén van de geïnterviewden licht toe dat Digit met aan aantal partijen 'optrekt'. Deze partijen opereren volgens de geïnterviewden in een 'nichemarkt'. Hoeveel leveranciers er exact zijn, weet deze geïnterviewde niet, maar zijn inschatting is 'tientallen'. Niet alle leveranciers zijn voor Digit interessant. Door Digit wordt verteld dat bij leveranciers in bepaalde landen géén middelen gekocht worden. De ervaringen met de leverancier die producten levert zijn positief. Eén van de geïnterviewden bij Digit beschrijft dat een leverancier 'kwaliteit levert en zeer integer werkt'. Als een leverancier onderhoud aan het product moet

plegen, vraagt hij hiervoor altijd eerst toestemming. Deze geïnterviewde heeft nog nooit meegemaakt dat dat niet gebeurde. Ook de integriteit en de continuïteit van onderzoeksgegevens zouden volgens deze geïnterviewde gewaarborgd zijn. De leverancier zou weliswaar gegevens kunnen inzien (zie volgende paragraaf), maar zou deze niet kunnen aanpassen. De Keuringsdienst en de Inspectie zijn kritisch op deze werkwijze.

*Digit-politie*
Binnen Digit-politie houden enkele medewerkers zich bezig met het aanschaffen van een middel en het onderhouden van contacten met (mogelijke) leveranciers. Aan de uiteindelijke beslissing om een middel aan te schaffen gaat een uitgebreid proces vooraf. Dat begint met het onderhouden van een relatie met mogelijke leveranciers. Eén van de geïnterviewden vertelt dat het in de wereld van commerciële leveranciers draait om vertrouwen en dat het belangrijk is om een band op te bouwen. Dat is volgens deze geïnterviewde een traject van jaren waarin je contacten legt en onderhoudt en leert begrijpen hoe de wereld van deze commerciële producten in elkaar steekt. Eén van de activiteiten die Digit in dit kader onderneemt is dat zij op bezoek gaat bij leveranciers. Dat kost tijd en veel geld, maar dat is het volgens deze geïnterviewde wel waard. Bij zo'n bezoek heeft deze geïnterviewde onder andere de mogelijkheid om bij de afdeling *Research & Development* te kijken hoe het er daar aan toegaat.

Op het moment dat er een product is waarin Digit geïnteresseerd is, wordt een aantal stappen doorlopen om te bekijken of een product bruikbaar zou kunnen zijn,[70] aldus deze geïnterviewde. Verteld wordt dat deze stappen niet heel veel anders zijn dan degene die worden doorlopen bij andere producten die de politie aanschaft. Er worden gesprekken gevoerd, presentaties bekeken en er wordt een demonstratie gegeven. Gedurende het proces om tot de aankoop van een product over te gaan, speelt vertrouwen in de leverancier en zijn product zoals eerder genoemd een belangrijke rol. Er wordt uitgelegd dat een leverancier afhankelijk is van het vertrouwen dat in hem gesteld wordt en dat hij om die reden er alles aan zal doen om de goede naam hoog te houden die hij heeft opgebouwd. Eén van de geïnterviewde vanuit Digit geeft aan:

> *'Volgens mij is in deze branche het belangrijkste bezit van een marktpartij niet het product, maar de 'naam' en integriteit. Als die niet kloppen dan kan het product nog zo goed zijn, maar dan kom je* [als leverancier] *gewoonweg niet binnen* [bij een klant, in dit geval de politie]*.'*

Digit heeft op haar beurt weinig andere opties dan te varen op vertrouwen, omdat Digit niet precies weet hoe het product werkt. Dat is ook niet mogelijk, omdat de leverancier het product niet volledig uit handen geeft. De politie werkt weliswaar met een computer die '*stand alone*' bij haar op locatie staat, zo wordt door Digit uitgelegd, maar het beheer van het product, onder andere het verzorgen van updates, ligt in handen van de leverancier. Dat het beheer door de leverancier zelf wordt gedaan, betekent dat de leverancier toegang kan hebben heeft tot de data die de politie verzamelt. Digit is zich bewust van deze mogelijkheid, maar geeft aan dat hierover contractuele afspraken zijn gemaakt met de leverancier. Bovendien zouden deze leveranciers moeten voldoen aan hun eigen exportregime wat onder andere inhoudt dat zij géén inzage mogen hebben in de data van hun klanten. Eén van de geïnterviewden vanuit Digit legt uit dat bij de inzet van een commercieel product, vanwege de zojuist geschetste onzekerheden die ermee gepaard gaan, altijd een

[70] Deze stappen staan overigens niet uitgeschreven/ zijn niet geformaliseerd.

risicoanalyse wordt gemaakt. Voor een 'politiek gevoelige zaak' gebruikt Digit liever geen commercieel middel, terwijl dat voor een drugszaak waarin sprake is van cocaïnesmokkel anders ligt. Deze geïnterviewde vraagt zich hardop af hoe belangrijk het is dat er in zo'n laatste soort zaak geen enkel risico wordt genomen.
Deze geïnterviewde vertelt dat Digit in het contact en in de samenwerking met de leverancier altijd een gezonde vorm van wantrouwen heeft. Digit houdt er rekening mee dat een leverancier nooit helemaal volledig te vertrouwen is. Een andere geïnterviewde merkt op, in relatie tot hetzelfde gezonde wantrouwen, dat vraagtekens geplaatst moeten worden als een leverancier 'gouden bergen' belooft. Uitgelegd wordt dat er altijd vragen aan een leverancier kunnen worden gesteld en dat Digit dat ook moet doen om een inschatting te kunnen maken of een product aangeschaft kan worden. Bij die vragen en de antwoorden moet je er als Digit vanuit kunnen gaan dat de leverancier vragen eerlijk beantwoord en ter onderbouwing daarvan wordt (wederom) verwezen naar het belang van het hoog houden van een goede naam:

> *'Geïnterviewde zegt dat we* [onderzoekers] *ons ook moeten realiseren dat als zij liegen, dat ze dan hun eigen ramen ingooien. Digit heeft contacten in binnen- en buitenland en zoiets spreekt zich rond. Het is een klein wereldje. Als geïnterviewde iets slechts hoort over een bedrijf* [bijvoorbeeld een 'achterdeurtje dat wordt ingebouwd']*, dan is het ook meteen klaar.'*

Voor Digit is het verlies van een goede naam van de leverancier een belangrijk argument om de mogelijke (theoretische) risico's die gepaard gaan met het gebruik van een commercieel product te accepteren.

*Regiegroep*
Het zojuist beschreven proces vindt plaats bij Digit-politie. Eén van de geïnterviewden geeft aan dat Digit-OM ook al graag bij dit proces betrokken zou willen zijn. Volgens deze geïnterviewde is het belangrijk dat in deze fase niet alleen een technische afweging wordt gemaakt, maar ook een juridische. Technisch kan een middel misschien goed werken, maar het is de vraag of wat een middel technisch kan, ook altijd juridisch toegestaan is, bijvoorbeeld met betrekking tot soevereiniteitskwesties. Deze geïnterviewde vertelt dat binnen het Openbaar Ministerie nog een discussie gevoerd zal worden over wat de precieze rol is van de Digit-officier van justitie.

Op het moment dat Digit een keuze voor een product heeft gemaakt, is er in elk geval een rol weggelegd voor het Openbaar Ministerie. Er is een regiegroep die op basis van informatie van Digit beslist of het product aangeschaft kan worden. Deze regiegroep bestaat uit een rechercheofficier, een vertegenwoordiger van het Landelijk Parket, van de politie, van Defensie en van de FIOD. Eén van de geïnterviewden vertelt dat in die regiegroep, toen de keuze moest worden gemaakt over het aanschaffen van het eerste commerciële product, onder andere gesproken is over de kosten van het middel en een aantal veiligheidskwesties zoals de vraag of het middel voldoende veilig en integer zou zijn. Uiteindelijk heeft de regiegroep positief geoordeeld, omdat het ontwikkelen van een eigen middel niet haalbaar zou zijn. De inschatting was ook dat het door Digit naar voren gebrachte product een 'goed middel' was.

*Screening AIVD*
Potentiële leveranciers van producten worden gescreend door de AIVD. Eén van de geïnterviewden vertelt dat zowel potentiële leveranciers waarbij Digit een product wil aanschaffen als leveranciers waarbij Digit al besloten heeft een product te willen kopen, aangemeld worden voor een screening. Vanuit het ministerie van Binnenlandse

Zaken wordt aangegeven, in lijn met de beantwoording van Kamervragen (Bruins, Slot & Yeşilgöz-Segerius, 2022),[71] dat de AIVD de procedure uitvoert 'als een naslagverzoek conform de F-taak in de Wiv 2017 onder artikel 8 lid 2f. Dit artikel betekent dat de AIVD in de eigen systemen naar een specifieke persoon of instantie een naslag kan doen op verzoek van anderen, conform de Regeling naslag Wiv 2017'. Of er screenings hebben plaatsgevonden, hoeveel en wat uit de screening kwam, daar kan de AIVD 'gezien de wettelijke geheimhoudingsplicht in de WiV 2017' in het openbaar geen mededelingen over doen. Vanuit de politie wordt de screening van de AIVD omschreven als een 'stille procedure'. Als na enkele weken er geen reactie van de AIVD is, kan er vanuit worden gegaan dat een product bij de gescreende leverancier kan worden aangeschaft. Tot nu toe heeft Digit bij de leveranciers die aangemeld zijn voor een screening niks teruggehoord van de AIVD. Naast een screening wordt gekeken of de leverancier zaken doet met 'foute regimes'. Dat gebeurt bij de politie. De politie vraagt, zo blijkt uit een Kamerbrief (Bruins, Slot & Yeşilgöz-Segerius, 2022), de leverancier 'niet te hebben geleverd aan landen waartegen vanuit de Europese Unie of de Verenigde Naties restrictieve sancties bestaan'. Daarnaast 'wordt gecontroleerd of in het land waar de leverancier is gevestigd een exportcontroleregime bestaat waar mensenrechten een onderdeel is in de beoordeling voor het verstrekken van een exportvergunning'.

*Licentiemodel*
In het Regeerakkoord is, zoals eerder beschreven, afgesproken dat de aanschaf van commerciële middelen zo veel mogelijk dient te worden beperkt. Om die reden mag een aangeschaft middel voor één zaak worden ingezet. Mocht het middel daarna voor een nieuwe inzet nodig zijn, dan dient het product opnieuw te worden aangeschaft. Deze afspraak bepaalt in grote mate hoe Digit werkt. Een middel wordt inclusief onderhoudspakket aangeschaft. Daarnaast koopt Digit per inzet een nieuwe licentie. Die nieuwe licentie wordt pas aangeschaft als met een testlicentie (één licentie die voor alle testen kan worden gebruikt) vastgesteld is dat het product werkt en als het bevel van de officier van justitie binnen is.[72] Zo'n test biedt overigens géén garantie op een succesvolle inzet. Het is voorgekomen dat toch niet kon worden binnengedrongen. Vanuit Digit wordt aangegeven dat dit bij twee à drie inzetten het geval was. Op dat moment is een licentie die 'ontzettend duur' was, voor niks aangeschaft. Een geïnterviewde legt uit dat het uiteindelijk van verschillende factoren afhankelijk is of een inzet slaagt (zie paragraaf 4.3.9).

Toen de wet net in werking was getreden, werd voor elke telefoon die werd binnengedrongen een licentie gekocht, ook als binnen één inzet meerdere telefoons werden binnengedrongen. Inmiddels koopt Digit, vanwege de hoge kosten, per inzet 1 licentie, los van het aantal toestellen dat tijdens die betreffende inzet moet worden binnengedrongen. In het Regeerakkoord is de afspraak immers per zaak gemaakt. Eén van de geïnterviewden vertelt dat dit in de praktijk betekent dat per inzet de licentie voor maximaal twee telefoons wordt gebruikt.
Verschillende geïnterviewden zijn kritisch op het licentiemodel. Eén van hen geeft aan dat het een 'draak van een regel is'. Deze geïnterviewde licht toe:

> '*(..) deze regel was bedoeld om te voorkomen dat de markt gestimuleerd zou worden. Geïnterviewde durft de stelling aan dat met deze regel de markt juist*

[71] Het betreft Kamervragen over het gebruik van hacksoftware, gesteld door Tweede Kamerleden Omtzigt en Van Dijk.
[72] De Inspectie constateert dat achteraf in elke zaak minstens één licentie is aangeschaft (Inspectie JenV, 2021).

*gestimuleerd wordt, omdat je zowel betaalt voor de aanschaf van de software als voor een licentie bij elke inzet. (…) Daar verdienen bedrijven enorm veel geld aan. Je betaalt nu namelijk voor een product, elke keer opnieuw voor een licentie en er moeten onderhoudskosten worden betaald, in plaats van dat je één keer over een totaalprijs onderhandelt voor de aanschaf en een X-aantal licenties.'*

Op een ander moment vertelt deze geïnterviewde dat de leverancier van een product wel eens heeft gevraagd of Digit niet liever af zou willen van telkens opnieuw een licentie kopen. Hij kon zich niet voorstellen dat de manier waarop Digit op dit moment het product aankoopt de bedoeling was. Deze geïnterviewde zou het liefst een product aanschaffen met daarbij standaard tien licenties. Mocht op een bepaald moment een verzoek komen voor een elfde inzet, dan kan die inzet pas plaatsvinden als een andere inzet afgerond is. Deze geïnterviewde schat in dat op dit moment de aanschafprijs twee keer betaald is als gevolg van de licenties die steeds opnieuw moeten worden gekocht. Hoeveel de politie precies voor een product betaalt wil zij niet zeggen in verband met afspraken die met de leverancier gemaakt zijn. Het zou gaan om 'enkele miljoenen'. Dat bedrag ligt in lijn met wat Perlroth (2021) beschrijft. Zij deed onderzoek naar de markt van *zero day's*.

*Gebruik te verantwoorden*

Verschillende geïnterviewden realiseren zich wat de mogelijke risico's zijn van de inzet van commerciële middelen. Dat neemt niet weg dat zij het gebruik van deze middelen toch (goed) te verantwoorden vinden, mits duidelijke afspraken worden gemaakt. Allereerst wordt het gebruik ervan noodzakelijk geacht om het werk goed te kunnen doen. Eén van de geïnterviewden vanuit Digit vertelt graag zo ethisch mogelijk te willen werken. Het uitbannen van commerciële middelen zou het werk meer ethisch maken, maar zonder deze middelen kan de politie haar werk niet goed doen. Een andere geïnterviewde die niet direct betrokken is bij het uitvoeringproces herkent dat beeld. Deze geïnterviewde geeft aan 'buiten het operationele proces' te staan en daardoor 'moreel zuiver' te kunnen blijven. Maar degene die daadwerkelijk bezig zijn met opsporingsonderzoeken hebben 'lastige keuzes' te maken.

Een tweede argument is de eerder al beschreven goede naam die leveranciers hoog te houden hebben. Het derde argument dat wordt genoemd is dat in Nederland voldoende 'checks and balances' bestaan om dit soort producten verantwoord in te zetten. Eén van de geïnterviewde opsporingsfunctionarissen vertelt over het wettelijk kader in Nederland, met onder andere een rechter-commissaris die onafhankelijk is, een Openbaar Ministerie dat 'magistratelijk is, op afstand staat van de politie en kritisch is op haar optreden' en een CTC. Dat zouden voldoende *check and balances* moeten zijn. Bovendien screent de AIVD alle potentiële leveranciers. Een vierde argument tot slot heeft betrekking op de bijzondere positie die wordt toegekend aan commerciële leveranciers en hun producten. Een aantal geïnterviewden legt uit dat de politie voor bijvoorbeeld hardware ook afhankelijk is van commerciële leveranciers en hun producten. Denk daarbij aan laptops en mobiele telefoons waar Google (weliswaar geanonimiseerd) op draait. Een andere geïnterviewde betrokken bij het toezicht op de bevoegdheid vindt die vergelijking niet goed opgaan, omdat aan de commerciële software die voor de hackbevoegdheid worden ingezet allerlei eisen zijn gesteld en dat door het gebruik van deze commerciële software 'echt inbreuk wordt gemaakt op de privacy' van burgers.

### *4.3.9 Looptijd & resultaat*

Bij een groot deel van de inzetten is het (uiteindelijk) gelukt om op één of meerdere momenten binnen te dringen.[73] Dat geldt voor vier van de zes maatwerkinzetten en voor zeventien van de negentien telefooninzetten.[74] Als het eenmaal gelukt is om een geautomatiseerd werk binnen te dringen, betekent dit overigens niet dat de politie gedurende de looptijd continu binnengedrongen blijft op het geautomatiseerde werk. Tijdens een inzet is het niet uitzonderlijk dat meerdere malen opnieuw moet worden binnengedrongen. Een geïnterviewde vertelt over zijn ervaringen tijdens een inzet van Digit:

> *'(..) waar we last van hebben gehad, is dat ie niet continu heeft gewerkt. We hebben meer tijd gehad dat we er niet in konden dan dat we er wel in konden* [in het geautomatiseerde werk]. *En als je er vandaag in kon, dan wilde dat niet zeggen dat je er morgen weer inzat.'*

Deze geïnterviewde vertelt gedurende de inzet, die meer dan een jaar geduurd heeft, steeds op de hoogte te zijn gehouden of de politie wel of niet in het geautomatiseerde werk aanwezig was. Een andere geïnterviewde heeft een gelijksoortige ervaring met een inzet die één keer verlengd is.

> *'Het is verre van een rustig bezit, zo'n hack. Ik dacht aan het begin, ze doen het één keer en dan heb je het voor altijd. Dat is helemaal niet zo. Kost echt wel veel gedoe om erin te komen, (..), en dan verliezen ze* [de verbinding] *weer, en komt het weer terug* [de verbinding]*.'*

Het is niet altijd duidelijk geworden/bekend waarom het binnendringen niet (continu) succesvol was. Meer in algemene zin is het succes van het binnendringen van verschillende factoren afhankelijk. Grofweg kan onderscheid worden gemaakt tussen technische factoren gerelateerd aan het geautomatiseerde werk en factoren die te maken hebben met (het gedrag van) de verdachte. Op de technische factoren kan in dit openbare rapport, vanwege de afscherming van opsporingsmethoden, niet nader worden ingegaan. Over de andere categorie kan beperkt iets worden gezegd. Het binnendringen kan afhankelijk zijn van de locatie waar een geautomatiseerd werk zich bevindt. Zodra een verdachte naar het buitenland vertrekt, wordt doorgaans niet op het geautomatiseerde werk binnengedrongen. Daarnaast is het, zoals gezegd, soms nodig om bij een geautomatiseerd werk in de buurt te zijn om het binnendringen voor elkaar te kunnen krijgen. Aanwezigheid op locatie is een risico, omdat de politie betrapt kan worden. Verder speelt de deskundigheid van de verdachte op technisch gebied een rol. Bij een verdachte die technisch goed onderlegd is, kan het lastig zijn om binnen te dringen. Tot slot kan het gebrek aan (onbewuste) bereidheid van een verdachte om een bepaalde handeling te verrichten een oorzaak zijn van het feit dat niet kan worden binnengedrongen. Dat is ook één van de redenen dat Digit op een verkeerd toestel is binnengedrongen.[75] Daarbij ging het om een situatie waarin in de interactie met de verdachte een handeling plaatsvond vanuit de verdachte die niet voorzien was.

---

[73] De onderzoekers gaan hier uit van het aantal inzetten op basis waarvan een selectie is gemaakt van inzetten die diepgaander bestudeerd zijn.

[74] Bij sommige inzetten is geprobeerd meerdere telefoons binnen te dringen. Indien het bij één of meer van deze telefoons is gelukt om binnen te dringen, is deze inzet bestempeld als gelukt om binnen te dringen.

[75] Zie het tweede Verslag van de Inspectie JenV (2021). Om te voorkomen dat dit nogmaals gebeurt is volgens één van de geïnterviewden het werkproces rondom het binnendringen ('een *check before flight*-lijstje') aangescherpt. Er wordt daarnaast verteld dat aanpassingen zijn gedaan aan een middel dat wordt gebruikt zodat meer recht gedaan kan worden aan de elementen uit het bevel.

### *4.3.10 Hoofdpunten*

- Het uitvoeren van de hackbevoegdheid kan niet altijd volledig op afstand gebeuren. Daarom heeft Digit behoefte aan een (heimelijke) steunbevoegdheid.
- Om binnen te dringen op telefoons is gebruikgemaakt van een commercieel middel.
- Digit is zich bewust van het feit dat er risico's zitten aan het gebruik van zo'n middel. Het gebruik ervan wordt echter noodzakelijk geacht om op een bepaald type geautomatiseerd werk (telefoons) binnen te kunnen dringen. Op dit type geautomatiseerd werk vindt het grootste deel van de inzetten plaats.
- Het licentiemodel, dat voortvloeit uit het Regeerakkoord, maakt de aanschaf van een commercieel middel duur. Het is dan ook de vraag of dit model ertoe leidt dat de markt van onbekende kwetsbaarheden minder gestimuleerd wordt.[76]
- De meldplicht geldt ook voor geautomatiseerde werken die vrijwel alleen voor criminele doeleinden worden gebruikt. Dat betekent dat personen met criminele intenties uiteindelijk op de hoogte moeten worden gesteld dat in hun systeem zich een kwetsbaarheid bevindt, zodat zij veiliger gebruik kunnen (blijven) maken van hun systeem.
- De meldplicht van onbekende kwetsbaarheden kent nog een ander nadeel, namelijk dat de samenwerking met binnen- en buitenlandse partijen lastiger wordt, omdat zij doorgaans geen (vergelijkbare) meldplicht kennen.
- De meldplicht, in combinatie met de wens om het gebruik van commerciële middelen te beperken, is voor Digit ingewikkeld, omdat de meldplicht ervoor zorgt dat een eventueel eigen door Digit ontwikkeld product slechts één of twee keer bruikbaar is.
- Succesvol binnendringen is afhankelijk van een mix van factoren en omstandigheden.

## 4.4 Onderzoekshandelingen

### *4.4.1 Inleiding*

In de komende paragrafen richt de aandacht zich, na een samenvatting van het wettelijk kader, allereerst op de onderzoekshandelingen waarvoor de bevoegdheid is ingezet en de dilemma's die daarbij een rol spelen. Vervolgens wordt ingegaan op de manier waarop de onderzoekshandelingen worden uitgevoerd en de technische hulpmiddelen die daarbij al dan niet worden gebruikt. Daarna komen de gegevens die Digit verzamelt aan de orde en wordt ingegaan op de samenwerking tussen het technisch en het tactisch team, zowel aan politie- als aan OM-zijde.

### *4.4.2 Samenvatting wettelijk kader*

Nadat de politie is binnengedrongen, kan zij, op afstand (Besluit onderzoek in een geautomatiseerd werk, p. 32), vijf onderzoekshandelingen verrichten. De verschillende onderzoekshandelingen zijn vastgelegd in de artikelen 126nba lid 1a t/m 1 e Sv. Het gaat om de volgende onderzoekshandelingen: het vastleggen van kenmerken van het geautomatiseerde werk en of de gebruiker ervan (lid 1a), de uitvoering van een bevel tot het aftappen van telecommunicatie (126m Sv) of het opnemen van vertrouwelijke communicatie (126l Sv) (lid 1b) en de uitvoering van een bevel stelselmatige observatie (artikel 126g Sv), waarbij de officier van justitie kan bepalen dat ter uitvoering van het bevel een technisch hulpmiddel op een persoon wordt bevestigd

[76] De Inspectie trekt een soortgelijke conclusie (Inspectie JenV, 2021, p. 14).

(lid 1c). Daarnaast, en hiervoor gelden strengere eisen, het vastleggen van gegevens die in het geautomatiseerde werk zijn opgeslagen, of die eerst, na het tijdstip van afgifte van het bevel, worden opgeslagen (lid 1d) en de ontoegankelijkmaking van gegevens (lid 1e), bedoeld in artikel 126cc vijfde lid. Soms kan gewerkt worden met een stapsgewijze aanpak (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 68). Dat betekent dat wordt binnengedrongen om kenmerken vast te stellen (lid 1a) en dat op basis van die informatie bepaald wordt welke handelingen nog meer verricht dienen te worden (lid 1b t/m lid 1e). Voor het binnendringen en de onderzoekshandelingen dienen aparte bevelen te worden afgegeven. Beide kunnen gecombineerd worden in één bevel (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 63).
De onderzoekshandelingen moeten worden uitgevoerd door het technisch team van de politie (artt. 3 lid 2 Bogw & 24, lid 1 Bogw). Daarbij kan het team gebruikmaken van een technisch hulpmiddel. Dat is een 'softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht uitvoering van een bevel' (Besluit onderzoek geautomatiseerd werk, 2018). Het gebruik van een technisch hulpmiddel is niet 'strikt noodzakelijk'. Soms zullen handelingen, afhankelijk van onder andere de aard van het onderzoek, 'ad hoc en handmatig' worden verricht (Besluit onderzoek geautomatiseerd werk, 2018; artikel 126nba Sv, lid 1).

In wet- en regelgeving is vastgelegd dat gedurende het verloop van een opsporingsonderzoek sprake moet zijn van functiescheiding tussen het tactisch en het technisch team (*Kamerstukken II* 2015/16, 34 372, nr. 3). Functiescheiding moet een bijdrage leveren aan een zorgvuldig verloop van een inzet (*Kamerstukken I* 2016/17, 34 372, D, p. 6) en ervoor zorgen dat géén beïnvloeding plaatsvindt van het technisch team als zij afwegingen maakt over de haalbaarheid van een onderzoek en de uitvoering ervan (Besluit onderzoek geautomatiseerd werk, p. 14).
Digit dient de verzamelde gegevens, al dan niet gefilterd, met behulp van een forensisch kopie over te dragen aan het tactisch onderzoeksteam (artikel 29 Bogw). Verder dient sprake te zijn van logging. Logging is een belangrijke waarborg in het kader van een mogelijke inbreuk op de persoonlijke levenssfeer. Er worden vier vormen van van logging onderscheiden (Besluit onderzoek in een geautomatiseerd werk, p. 17-18).

### *4.4.3 Juiste sub bepalen*

Digit (OM en politie) en het tactisch team (OM en politie) bepalen in overleg met elkaar op basis van welke subs (de vijf onderzoekhandelingen, sub 1a t/m sub1e) gehandeld wordt. Bijna elke sub (behalve subE - ontoegankelijkmaking) levert gegevens op, bijvoorbeeld app-berichten verstuurd met een mobiele telefoon. In de uitvoeringpraktijk zorgt het onderscheid tussen de subs voor discussie, omdat niet elke categorie gegevens 'in een apart hokje' kan worden geplaatst. Technisch gezien kunnen nagenoeg alle gegevens op een geautomatiseerd werk een vastgelegd gegeven betreffen (subD). Een dergelijke interpretatie is echter problematisch omdat onder meer voor subD, het vastleggen van gegevens, een strenger inzetcriterium geldt. Bovendien, zo legt een geïnterviewde opsporingsfunctionaris uit, is het belangrijk dat de bevoegdheid wordt ingezet zoals deze bedoeld is door de wetgever, anders dreigt 'devaluatie':

> *'Je krijgt dan heel snel devaluatie van je bevoegdheden. Als je bij alles de overtreffende trap gaat inzetten. (…) Een voorbeeld is (…), is een chat in een telefoon nou een vastgelegd gegeven of niet? Als je daarvan zegt, het zekere voor*

*het onzekere, het is een vastgelegd gegeven, dan betekent het dat je in een zaak waarin je niet aan subD toe zou komen, dat* [je de bevoegdheid] *niet zou kunnen inzetten. Dat moet niet het doel worden, maar je moet zuiver blijven redeneren, (…) om zo dicht mogelijk bij de bedoeling van de wetstekst te blijven.'*

Bij het kiezen van de juiste sub wordt daarom gekeken welke handeling moet worden uitgevoerd om de onderzoeksvraag van het tactisch team te kunnen beantwoorden. Is observatie aan de orde? Dan is subC aangewezen. Of is het juist nodig dat er wordt getapt? In dat laatste geval is sprake van subB.[77] Wat betreft subB en subD heeft Digit-OM, op basis van de teksten uit de memorie van toelichting, zich op het standpunt gesteld dat subB kan worden gebruikt indien alleen communicatie moet worden vastgelegd (intern document 7). Een gelijksoortige discussie speelt rondom subA (vastleggen kenmerken) en subC (observatie). Het maken van foto's met behulp van het geautomatiseerde werk kan gebruikt worden om zeker te weten of een verdachte (en niet iemand anders) het geautomatiseerde werk gebruikt. In dat geval is de foto bedoeld om de gebruiker van het geautomatiseerde werk te identificeren (subA). Die identificatie is belangrijk, omdat de bevoegdheid gericht moet worden ingezet. Vanuit Digit wordt aangegeven dat onder andere met de CTC gesproken is over de vraag of het maken van die foto inderdaad geschaard kon worden onder subA of dat deze handeling toch als een vorm van stelselmatige observatie van een verdachte (subC) moest worden aangemerkt. Uiteindelijk heeft de Digit-officier van justitie de overwegingen van de CTC voorgelegd aan de zaaksofficier en medegedeeld dat aan de keuze voor subA 'een zeker procesrisico' kleeft, maar dat dat risico beperkt is waardoor in de ogen van Digit-OM gehandeld kon worden op basis van subA. Overigens merkt één van de geïnterviewden op, betrokken bij de toetsing, dat een discussie over de verschillende subs gezien kan worden als een wat 'academische discussie'. Voor deze geïnterviewde is het vooral belangrijk dat bij een inzet aan alle voorwaarden wordt voldaan, zo blijkt uit het volgende citaat.

*'Inderdaad die onderverdeling in die* [subs] *A,B,C,D en E, dat zijn* [niet in alle gevallen] *waterdichte schotten daartussen. Aan de andere kant: als het aan de zwaarste voorwaarden van D en E voldoet, heb ik er ook niet zo heel veel moeite mee, want dan is aan de randvoorwaarden eigenlijk wel voldaan. En de uitvoering snap ik ook. En of het dan meer onder d of onder b past, is uiteindelijk dan ook een beetje een academische kwestie. Ik denk ook niet dat dat ooit tot een succesvol verweer zal leiden. In welke belangen ben je geschaad? Het is getoetst, het voldoet aan alle strenge voorwaarden.'*

Hoe een zittingsrechter uiteindelijk de inzet van deze bevoegdheid weegt en beoordeelt is gedurende de looptijd van dit onderzoek niet duidelijk geworden, omdat nog geen zaken inhoudelijk behandeld zijn. Dit onderwerp zal in het tweede deel van de evaluatie hopelijk meegenomen kunnen worden.

### *4.4.4 Meerdere onderzoekshandelingen*

**Telefooninzetten**

Bij telefooninzetten wordt in de meeste gevallen subA tot en met subD ingezet (als het technisch mogelijk is). Eén van de geïnterviewden legt uit dat dit logisch is. In de

[77] Eén van de geïnterviewden merkt op dat er ook binnen een sub onduidelijkheid kan bestaan, en dat die onduidelijkheid niet per se gerelateerd is aan deze bevoegdheid. Binnen subB kan zowel telecommunicatie worden opgenomen als vertrouwelijke communicatie. De grens hiertussen is volgens deze geïnterviewde niet altijd duidelijk.

opsporingsonderzoeken waarin dit soort inzetten worden gedaan wil het tactisch team graag alle informatie uit de telefoon hebben, wat volgens deze geïnterviewde goed uit te leggen is, omdat een telefoon veel inzicht biedt in het leven van een verdachte.
Bij het uitvoeren van onderzoekshandelingen op een telefoon is er voor de uitvoeringspraktijk een aantal aandachtspunten. De eerste betreft het feit dat niet doorlopend gegevens kunnen worden binnengehaald. Dat betekent in de eerste plaats dat niet alle onderzoekshandelingen waarvoor een bevel is afgegeven altijd uitgevoerd kunnen worden. Daarnaast zorgt dit ervoor dat ook bij het inzichtelijk krijgen van chatgesprekken het nodig kan zijn om subD in te zetten.
Het tweede aandachtspunt betreft het opnemen van vertrouwelijke communicatie (subB). Die onderzoekshandeling is plaatsgebonden. Dat betekent dat per inzet bepaald wordt op welke plekken de politie een verdachte mag afluisteren. Voordat Digit-politie een microfoon aanzet, wil zij daarom eerst zeker weten of de verdachte zich bevindt op een locatie waarop het toegestaan is gesprekken op te nemen. In het verleden is dit niet altijd goed gegaan en zijn gesprekken opgenomen waarbij dat niet had gemogen. Digit wil om die reden tegenwoordig via diverse wegen (zowel technisch als tactisch) de locatie van een verdachte bevestigd zien. Op die manier kan bepaald worden wanneer de microfoon aan moet, maar ook weer uit moet. Twee geïnterviewden vertellen dat tijdens de inzet het observatieteam op een gegeven moment zag dat een auto van het advocatenkantoor ter plaatse kwam. Op dat moment is gezegd dat het opnemen van vertrouwelijke communicatie gestopt moest worden, omdat mogelijk sprake zou zijn van communicatie met een geheimhouder. In dit geval lukte het om het afluisteren tijdig te beëindigen. Het blijft echter ingewikkeld om een 'connectie tussen persoon en apparaat' vast te stellen. De politie moet het bijvoorbeeld doorhebben als een verdachte naar een plaats gaat waar géén toestemming voor is, bijvoorbeeld als hij koffie gaat drinken bij de buren.

Naast het vastleggen van locaties, dient er voor subB een apart bevel te zijn, ook al is er in de zaak waarbinnen Digit een inzet gaat doen al een machtiging afgegeven voor een traditionele OVC (zonder dat de politie heimelijk en op afstand binnendringt). Het is niet uitzonderlijk dat er al zo'n machtiging ligt, omdat in opsporingsonderzoeken waarbij Digit betrokken wordt doorgaans meerdere bijzondere opsporingsbevoegdheden zijn ingezet. Ook het afgeven van een apart bevel is niet altijd goed gegaan. Eén van de geïnterviewden vertelt dat er recent een inzet is geweest waarin er toestemming was voor OVC in een woning, maar niet voor in de auto. In die auto was alleen traditionele OVC toegestaan. Toch had Digit-politie ook in de auto de microfoon aangezet. Uiteindelijk is in die zaak door de rechter-commissaris besloten dat het opgenomen gesprek niet hoefde te worden vernietigd, omdat eerder al goed gevonden was dat in de auto gesprekken werden opgenomen.

Indien er een bevel is, en er wordt communicatie opgenomen, dan is er géén garantie dat de onderzoekshandeling bruikbare data oplevert, bijvoorbeeld vanwege omgevingsgeluiden. Ook kan het voorkomen dat de microfoon net te laat aan wordt gezet. Eén van de geïnterviewden licht toe:

> *'Wij hebben bijvoorbeeld letterlijk op een gegeven moment vastgesteld dat verdachte 1 een ontmoeting had op een parkeerplaats in (plaats in Land2) waar wij al beeld hadden hangen omdat we wisten, daar zijn vaker interacties, maar we wilden eigenlijk weten waar gaat het nou over? Toen wilden we die OVC aanzetten, dat hebben we ook gedaan en het eerste wat je dan hoort is, ja, prima (…), bedankt tot volgende week. (…) In de praktijk moet je hem aan kunnen zetten op*

*het juiste moment. In de praktijk moet je hem ook uit kunnen zetten op het moment dat het nodig is. En dat is wel lastig.'*

**Maatwerkinzetten**
Bij maatwerkinzetten lijken de gekozen onderzoekshandelingen minder voor de hand te liggen. Meestal wordt gebruikgemaakt van subA en D. En een enkele keer wordt daar nog een andere sub aan toegevoegd. Zo zijn bij één van de geselecteerde inzetten eerst twee servers binnengedrongen om te kijken hoe de structuur van het botnet eruit zag (subA) om vervolgens deze informatie vast te leggen (subD). Daarna zijn die gegevens gebruikt om het botnet ontoegankelijk te maken (subE).

### *4.4.5 Stapsgewijze aanpak*

In zowel telefoon- als maatwerkinzetten heeft Digit-politie meerdere onderzoekshandelingen uitgevoerd. Hierbij was doorgaans geen sprake van een 'stapsgewijze aanpak' zoals in het wetgevingstraject geschetst. Vaak werd direct een bevel afgegeven voor meerdere onderzoekshandelingen tegelijkertijd in plaats van dat er aparte bevelen werden afgegeven. Volgens enkele geïnterviewden is zo'n stapsgewijze aanpak ook niet realistisch. Eén van hen vertelt bijvoorbeeld dat het voor kan komen dat een verdachte met behulp van technische maatregelen (*intrusion detection*) ervoor gezorgd heeft dat het moeilijk is – zo niet onmogelijk – om toegang te houden tot zijn computersysteem. Daardoor kan het zijn dat de politie slechts voor een korte periode toegang heeft tot het systeem van een verdachte. In die korte tijd zouden al gegevens kunnen worden binnengehaald. Wanneer echter gekozen wordt voor een stapsgewijze aanpak, vervalt die mogelijkheid, omdat voor het verzamelen van gegevens een nieuw bevel moet komen. Tegen de tijd dat dat bevel er is, is de kans reëel dat het niet meer mogelijk is om toegang te krijgen. Een ander bezwaar is dat het onnodig veel tijd zou kosten om stapsgewijs te werken. Er zou dan namelijk twee keer een traject bij de CTC doorlopen moeten worden.

Hoewel geen stapsgewijze werkwijzes zijn gehanteerd zoals bedoeld in het wetgevingstraject, is in één van de geselecteerde zaken wel een ander soort stapsgewijze aanpak gevolgd. Dit betreft de eerder beschreven inzet waarbij een botnet ontoegankelijk is gemaakt. Die ontoegankelijkmaking was de tweede stap. Voorafgaand eraan werden servers verkend en werden gegevens opgeslagen. Naast deze stapsgewijze aanpak is het voorgekomen dat op basis van gegevens die verzameld werden gedurende een eerste ronde onderzoekshandelingen een bevel werd gevraagd voor een nieuw geautomatiseerd werk. In één van de geselecteerde inzetten bestond het vermoeden dat de verdachte meer geautomatiseerde werken in gebruik had dan de politie in eerste instantie vermoedde. Om die reden is op een gegeven moment een bevel gevraagd om een extra geautomatiseerd werk te onderzoeken.

### *4.4.6 Uitvoeren onderzoekshandelingen*

**Onderscheid technisch hulpmiddel en handmatige inzet**
Onderzoekshandelingen kunnen zowel met een technisch hulpmiddel worden verricht als handmatig. In de uitvoeringspraktijk bestaan vragen over wat het precieze onderscheid is tussen beide. Meerdere geïnterviewden geven aan dat beide begrippen niet altijd goed van elkaar gescheiden kunnen worden en dat er grijze gebieden zijn. Een goede interpretatie van deze begrippen is relevant, omdat technische hulpmiddelen in principe vooraf ter keuring aangeboden dienen te worden aan de Keuringsdienst. Hierop wordt in het hoofdstuk 5 uitgebreid ingegaan. Over een

handmatige inzet hoeft de Keuringsdienst zich niet te buigen. In de uitvoeringspraktijk blijkt het keuringstraject een knelpunt te zijn voor Digit.

Om voor zichzelf duidelijkheid te scheppen hebben Digit-OM en -politie, op basis van de wetsgeschiedenis, gezamenlijk overleg gehad wat volgens hen onder een technisch hulpmiddel moet worden verstaan.[78] Daarvoor was het ook nodig om invulling te geven aan de begrippen detectie, registratie en transport. In de wetsgeschiedenis staat immers vermeld dat dat is wat een technisch hulpmiddel doet. Uiteindelijk is in een intern OM-document vastgelegd, opgesteld door Digit-OM en -politie, wat onder een technisch hulpmiddel moet worden verstaan, namelijk: 'een technisch hulpmiddel is een softwareapplicatie waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel die gegevens detecteert, registreert en automatisch transporteert naar een technische infrastructuur van het technisch team' (intern document 8[79]).
Ook een handmatige inzet is gedefinieerd: handmatig onderzoek is 'onderzoek verricht door een volgens het Besluit aangewezen opsporingsambtenaar waarbij één of meerdere van de fases – detectie, registratie en of transport, *zonder* gebruik van een technische *tool*, met directe betrokkenheid van eerstgenoemde opsporingsambtenaar, worden uitgevoerd' (intern document 8[80]). Vertaald naar twee concrete voorbeelden betekent dit het volgende. Als Digit een softwareapplicatie gebruikt die automatisch gegevens detecteert en registreert en een script dat automatisch de geregistreerde gegevens transporteert naar de technisch infrastructuur is sprake van de inzet van een technisch hulpmiddel. Als Digit de mailbox van een verdachte is binnengedrongen, kan zij handmatig mailtjes van een bepaalde afzender (visueel) detecteren. Vervolgens kan het registeren en transporteren van de e-mails geautomatiseerd plaatsvinden. Bij deze handeling is géén sprake van een technisch hulpmiddel, omdat detectie handmatig plaatsvindt.

Digit OM en politie betrekken in hun standpuntbepaling niet de passage in het Besluit waarin wordt aangegeven dat de politie voor onderzoekshandelingen gebruik kan maken van een script dat 'semi-handmatig' wordt ingezet. Wat precies onder 'semi-handmatig' wordt verstaan, wordt niet nader toegelicht. In de toelichting op het Besluit staat alleen beschreven dat zo'n script een voorbeeld is van een technisch hulpmiddel dat zich naar zijn aard niet leent voor voorafgaande keuring en daarom achteraf gekeurd dient te worden (Besluit onderzoek in geautomatiseerd werk, 2018, p. 21). Vanwege deze passage in de toelichting op het Besluit, heeft de Inspectie Justitie en Veiligheid kritiek op de wijze waarop Digit-politie en -OM beide begrippen definiëren. In haar ogen dient een script (handmatig in de ogen van Digit) te worden gezien als een technisch hulpmiddel waarnaar de Keuringsdienst moet kijken (Inspectie JenV, 2021). Vanuit Digit wordt kritiek geuit op deze interpretatie van een technisch hulpmiddel, omdat daardoor ook applicaties gekeurd dienen te worden die breed gebruikt worden, bijvoorbeeld een e-mailprogramma. Er wordt aangegeven dat de verwachting is dat zo'n veelgebruikt e-mailprogramma niet door de keuring heen zal komen. Of een rechter uiteindelijk een oordeel zal hebben over de door Digit gehanteerde definitie is op dit moment nog niet duidelijk.

**Ontwikkeling eigen hulpmiddelen**
De politie heeft gebruikgemaakt van twee soorten technische hulpmiddelen om onderzoekshandelingen uit te kunnen voeren: commerciële producten en eigen

[78] Uiteindelijk is dit vastgelegd in een kader dat Digit-OM geformuleerd heeft voor Digit-politie.
[79] Tekst is gelijk aan intern document 4.
[80] Tekst is gelijk aan intern document 4.

ontwikkelde hulpmiddelen. Bij het grootste deel van de inzetten is zoals eerder aangegeven een product aangeschaft dat is aangeschaft bij een commerciële leverancier. Dit onderwerp is eerder al uitgebreid besproken. Daarom ligt in deze paragraaf de nadruk op de hulpmiddelen die Digit zelf ontwikkeld heeft. Ook voor deze hulpmiddelen geldt dat in dit rapport, in verband met afscherming van onderzoeksmethoden, niet alle details over de werking ervan uit de doeken kunnen worden gedaan.

De ontwikkeling van een technisch hulpmiddel is in handen van het *Research en Development* team van Digit. In de afgelopen twee jaar heeft Digit drie technische hulpmiddelen ontwikkeld[81] waarvan er tot nu toe twee goedgekeurd zijn door de Keuringsdienst. De functie van de ontwikkelde hulpmiddelen is, kort door de bocht geformuleerd, dat data die relevant zijn in het kader van een tactisch onderzoek (denk aan chatberichten, e-mails, geluidsbestanden) opgehaald worden bij de verdachte en worden opgeslagen in de digitale omgeving van Digit. Welk soort data uiteindelijk wordt binnengehaald is afhankelijk van de functionaliteiten waarover het technisch hulpmiddel beschikt. Deze functionaliteiten zijn afhankelijk van de onderzoekshandelingen die Digit mag verrichten en die in het bevel staan vastgelegd. Enkele geïnterviewden vanuit Digit leggen uit dat het voordeel van een (eigen ontwikkeld) technisch hulpmiddel (in vergelijking met een handmatige inzet) is dat nagenoeg alle handelingen geautomatiseerd gebeuren. Eén van hen geeft het voorbeeld van een eigen middel waarmee e-mails kunnen worden binnengehaald. Enerzijds kan tijd worden bespaard omdat niet elk mailtje apart moet worden binnengehaald door een opsporingsambtenaar. Anderzijds wordt de kans op fouten verkleind, bijvoorbeeld doordat een opsporingsambtenaar een mailtje kan overslaan in de mailbox. Het idee was om technische hulpmiddelen te ontwikkelen die voor meerdere inzetten gebruikt kunnen worden. De praktijk is dat een hulpmiddel slechts voor één inzet kan worden gebruikt en dan moet worden aangepast.

Een technisch hulpmiddel bestaat doorgaans uit één of twee componenten. De eerste component is de *remote* component. Deze wordt geplaatst op het geautomatiseerde werk van de verdachte. De tweede component betreft de lokale component. Dat is de component die zich bij Digit bevindt en waarnaar de data van de verdachte worden verstuurd en zeer tijdelijk kunnen worden opgeslagen. Deze component wordt op een server gezet die voor elke zaak anders is. Of een technisch hulpmiddel uit één of twee componenten bestaat is afhankelijk van het geautomatiseerde werk dat de politie onderzoekt. Naast de *remote* en de lokale component is de technische infrastructuur van belang. Daarbinnen worden data min of meer definitief opgeslagen (voor zolang dat wettelijke toegestaan is).

Bij de ontwikkeling van een technisch hulpmiddel moet Digit rekening houden met de technische eisen zoals die zijn vastgelegd in de artikelen 8 t/m 13 van het Besluit. Eén van de geïnterviewden vertelt dat Digit bij de ontwikkeling van een hulpmiddel altijd een lijstje (dat niet beschikbaar is) langsloopt om te kijken of alles op een goede manier is ontworpen, bijvoorbeeld of een bestand op de juiste manier bij Digit aankomt. Digit maakt voor zichzelf een risicoanalyse waarin dat wordt nagegaan.[82] De regels in het Besluit moeten ervoor zorgen dat het bewijs dat verzameld wordt

[81] Het exacte aantal is overigens afhankelijk van de organisatie aan wie de vraag gesteld wordt. Volgens de Keuringsdienst zijn meer dan drie hulpmiddelen ter keuring aangeboden. Zij beschouwen de aanpassingen (zogenoemde 'iteraties') die Digit aan een (nog) niet goedgekeurd middel aanbrengt als een nieuw technisch hulpmiddel.

[82] Werken op basis van een risicoanalyse botst met de manier waarop de Keuringsdienst (en de Inspectie) naar technische hulpmiddelen kijken. Zie hoofdstuk 5.

betrouwbaar, integer en herleidbaar is. De regels hebben betrekking op de manier waarop de verschillende componenten hun werk doen en op de wijze waarop data tussen de verschillende componenten worden verstuurd. De reikwijdte van de regels reikt in principe tot aan de technische infrastructuur van Digit. Een voorbeeld van de wijze waarop Digit zich vertelt rekenschap te geven van deze regels is dat bij één van de technische hulpmiddelen ervoor gezorgd wordt dat data versleuteld worden opgeslagen en dat een *hash* wordt berekend.[83] Zowel *hashing* als encryptie zijn bedoeld om ervoor te zorgen dat met meer zekerheid kan worden gezegd dat de data die bij Digit binnen zijn gekomen exact hetzelfde zijn als de data die op het geautomatiseerde werk van de verdachte stonden.

**Generieke technische hulpmiddelen**
Digit zou het liefst werken met enkele eigen generieke hulpmiddelen die voor meer dan één zaak kunnen worden gebruikt, vergelijkbaar met de wijze waarop met het technisch hulpmiddel wordt gewerkt dat aangeschaft is bij een commerciële leverancier. Tot nu toe is het echter nog niet gelukt om exact hetzelfde middel voor meer dan één zaak te gebruiken. Elke inzet is wat dat betreft maatwerk, omdat een hulpmiddel voor een nieuwe inzet moet worden aangepast. Voor elke inzet wordt bijvoorbeeld een nieuwe digitale omgeving ingericht waarin (een deel van) de onderzoekshandelingen plaatsvindt. Daarnaast kan het zijn dat een nieuwe functionaliteit moet worden toegevoegd (niet alleen schermafbeeldingen maar ook toetsaanslagen). Eén van de geïnterviewden maakt een vergelijking met het Covidvaccin.

> *'(...) ieder geautomatiseerd werk is uniek, dus dat betekent dat je voor iedere inzet iets anders moet hebben. (...) net zoals bij het vaccin voor Covid. Je kunt wel steeds dingen ontwikkelen, en je hebt misschien een goede basis, maar je zal hem altijd op maat moeten gaan maken voor die inzet. En als je dus binnen die inzet ook nog kan hebben dat je geautomatiseerd werk weer een nieuwe update krijgt, dan is het zelfs binnen je eigen zaak weer achterhaald.'*

Dat bij een eigen ontwikkeld hulpmiddel sprake is van maatwerk, is volgens één van de geïnterviewden vanuit Digit de reden dat er niet een soort plank is van waaruit deze middelen kunnen worden verstrekt. In artikel 12 van het Besluit is opgenomen dat er een 'centraal uitgiftepunt' zou moeten zijn voor technische hulpmiddelen. Zo'n uitgiftepunt is er tot nu toe (nog) niet.[84] Een centraal uitgiftepunt bestaat wel voor de meer traditionele technische hulpmiddelen zoals een baken of een microfoon. Bij de technische hulpmiddelen die Digit gebruikt zou eerder sprake zijn van een aantal basissubonderdelen dat gebruikt kan worden in plaats van een standaard product dat al volledig inzetklaar is. Vanuit Digit wordt verteld dat al vanaf de eerste dag waarop de wet in werking trad, besloten is om op dit punt af te wijken van het Besluit. Volgens een geïnterviewde bij Digit zou het uitgiftepunt betekenen dat elk technisch hulpmiddel bij wijze van spreken op een cd zou moeten worden gebrand. Dat zou niet de bedoeling zijn. Bovendien, zo vertelt een andere geïnterviewde, is een uitgiftepunt niet realistisch gezien de grootte (ook fysiek) van sommige technische hulpmiddelen. Verder zou de uitgifte van software 'geen toegevoegde waarde' hebben en zou alles bij

[83] Versleuteling is bedoeld om data te kunnen beveiligen, zodat deze niet aangepast kunnen worden. Op die manier kan de betrouwbaarheid van gegevens worden gewaarborgd. Met een *hash* wordt een unieke code berekend op basis van de (set van) data. Als op een later moment (op het moment dat de data ergens anders staan) de *hash* opnieuw wordt berekend en deze hetzelfde is als de eerder berekende *hash*waarde, dan is dat een aanwijzing dat aan de data niets veranderd is. Een *hash* zorgt ervoor dat de integriteit van de gegevens is gewaarborgd.

[84] Ook de Inspectie (2020, p. 18 & 2021, p. 18) constateert de afwezigheid van een dergelijk proces.

Digit gelogd worden. Verschillende geïnterviewden vanuit Digit vertellen dat het uitgiftepunt één van de voorbeelden is waaraan je kunt zien dat het Besluit gebaseerd is op het Besluit dat er lag en vooral gericht is op de meer traditionele technisch hulpmiddelen.

Hoewel elk technisch hulpmiddel tot nu toe maatwerk is gebleken, is volgens Digit niet altijd sprake van een *volledig nieuw* technisch hulpmiddel, maar van *een deels bestaand* technisch hulpmiddel met een zelfontwikkelde basis, slechts uitgebreid met een extra functionaliteit. Wat dat betreft zou gezegd kunnen worden dat elk technisch hulpmiddel bestaat uit een (groot) aantal subonderdelen waarvan er enkele zijn die gestandaardiseerd kunnen worden. Binnen Digit wordt om die reden gesproken over minimaal keurbare producten (MKP; de basis en dat is één of enkele subonderdelen) en minimaal inzetbare producten (MIP; de basis plus bijvoorbeeld een extra functionaliteit die in een bepaalde zaak nodig is, dat is een aantal extra subonderdelen toegevoegd). Een voorbeeld van een minimaal keurbaar product zijn één of enkele subonderdelen die ervoor zorgen dat een bestand bij het geautomatiseerde werk van een verdachte opgehaald wordt (transport) volgens de regels zoals die staan vastgelegd in het Besluit. Dit MKP zou alvast gekeurd kunnen worden, maar is nog niet klaar voor een inzet. Door het toevoegen van een aantal subonderdelen, waardoor een functionaliteit zoals het vastleggen van toetsaanslagen worden toegevoegd (dat overigens ook moet worden goedgekeurd) wordt een middel wel geschikt voor een inzet in een opsporingsonderzoek. Op dat moment is het hulpmiddel 'inzetklaar' en verandert het MKP in een MIP. Het grootste voordeel voor Digit van een werkwijze waarin een technisch hulpmiddel stapsgewijs gekeurd wordt, is dat zij hoopt dat daarmee het keuringsproces versneld kan worden. De Keuringsdienst maakt echter géén onderscheid tussen MKP's en MIP's. Zij ziet elk hulpmiddel als een nieuw middel, ook al bestaat het uit een aantal eerder gekeurde subonderdelen.
Ondanks het voorgaande gebruikt Digit inmiddels enkele standaard subonderdelen die zijn goedgekeurd. Hierbij kan gedacht worden aan de manier waarop gegevens min of meer definitief veilig kunnen worden veiliggesteld en beschermd op de technische infrastructuur van Digit.

**Ontwikkeltijd**
In 2019 is één hulpmiddel ter keuring aangeboden. Dat middel is niet goedgekeurd (Inspectie JenV, 2020, p. 8-9). In 2020 zijn drie hulpmiddelen ter keuring aangeboden. Twee ervan zijn goedgekeurd (Inspectie JenV, 2021, p. 9).[85] Eén van de geïnterviewden vanuit Digit merkt op dat het ontwikkelwerk 'zeer weinig heeft opgeleverd', zeker als je de inzet van eigen middelen vergelijkt met het aantal inzetten waarin gebruik is gemaakt van een commercieel middel. Volgens deze geïnterviewde zouden er stemmen opgaan om het ontwikkeltraject door een andere partij te laten doen zodat ontwikkelaars zich kunnen richten op ad hoc zaken. Deze geïnterviewde vindt dat 'niet ideaal', maar ziet tegelijkertijd dat de wijze waarop een hulpmiddel op dit moment ontwikkeld wordt 'een struikelblok' is. In de ogen van Digit is een belangrijk knelpunt rondom de ontwikkeling van eigen middelen de tijd die het kost om een technisch hulpmiddel te ontwikkelen, maar vooral ook om het (goed-)gekeurd te krijgen. Meerdere geïnterviewden merken op dat dat een langlopend proces is. Het ontwikkelen van een (eerste versie van een) technisch hulpmiddel duurt al gauw vier weken (indien sprake is van een eenvoudig technisch hulpmiddel). Nadat een hulpmiddel klaar is, moet het gekeurd worden. Dat traject duurt ook minimaal vier weken, maar vaker is meer tijd nodig, al gaan op dit moment de keuringen sneller dan

[85] Uit het derde Verslag van de Inspectie blijkt inmiddels dat zeven technische hulpmiddelen ter keuring zijn aangeboden en dat er vijf zijn goedgekeurd (Inspectie JenV, 2022, p. 7).

vlak na de inwerkingtreding van de wet. Omdat het (nog) niet is voorgekomen dat een hulpmiddel in één keer goedgekeurd werd, worden daarna nog één of meerdere versies ontwikkeld ('iteraties'), inclusief per versie een nieuw keuringstraject. Alles bij elkaar duurt het minstens vier maanden om goedkeuring te krijgen voor een middel, of er komt helemaal geen goedkeuring.

Een lange ontwikkeltijd blijkt niet altijd goed samen te gaan met de termijn waarop een tactisch team behoefte heeft aan een inzet van Digit. Een geïnterviewde, betrokken bij het toetsingstraject, zegt hierover:

> *'Het dringend onderzoeksbelang: dat vind ik, hoe langer ik er over nadenk, vind ik dat best een interessante. Want dringend onderzoeksbelang wil volgens mij ook iets zeggen van: (…) het is echt nodig om het onderzoek vooruit te brengen. En dan heb je bijvoorbeeld een technisch hulpmiddel waarvan het Besluit zegt: in principe moet dat een goedgekeurd middel* [technisch hulpmiddel] *zijn. Nou, dat zullen jullie ook wel gehoord hebben, de trajecten die daarvoor gelden om dat* [technisch hulpmiddel] *goedgekeurd te krijgen zijn enorm lang. Ja, hoe verhoudt zich dat tot een dringend onderzoekbelang?'*

Hoewel Digit eigen middelen in een onderzoek heeft kunnen inzetten, is het ook voorgekomen dat het ontwikkeltraject te lang duurde om een technisch hulpmiddel nog in te kunnen zetten in een zaak.
Digit mag een niet vooraf (goed)gekeurd middel inzetten, maar dit dient wel een uitzondering te zijn (Besluit onderzoek in geautomatiseerd werk, 2018, p. 14). Bij een aantal inzetten is dit gebeurd. Toch werkt Digit liever niet op die manier, omdat het hulpmiddel dan achteraf gekeurd dient te worden en het maar de vraag is, op basis van de keuringservaringen tot nu toe, of het hulpmiddel op een later moment wel goedgekeurd wordt. Eén van de geïnterviewden vanuit Digit vertelt dat de keuring achteraf plaatsvindt van het middel zoals dat ten tijde van de inzet gebruikt is, zonder eventuele verbeteringen die op een later moment zijn toegevoegd. In dat opzicht zou de mogelijkheid om achteraf te keuren vooral een 'administratieve' mogelijkheid zijn.

**Handmatige inzet**
In twee van de geselecteerde inzetten heeft Digit (deels) een handmatige inzet gedaan. In de uitvoeringspraktijk wordt een handmatige inzet steeds vaker overwogen, onder andere omdat het ontwikkelen van een eigen technisch hulpmiddel veel tijd kost. Eén van de geïnterviewden vanuit Digit vertelt dat Digit steeds vaker neigt naar een handmatige inzet, omdat goedkeuring van de keuringsdienst tot nu toe altijd gepaard gaat met extra vervangende waarborgen waaraan Digit uitvoering moet geven. Die waarborgen maken soms dat werken met een technisch hulpmiddel geen voordelen meer heeft ten opzichte van een handmatige inzet. Wanneer sprake is van een handmatige inzet dan dient over de inzet (uitgebreider) verantwoording afgelegd te worden in het opsporingsdossier. Er is immers geen stempel van de keuringsdienst dat laat zien dat het hulpmiddel betrouwbaar, integer en herleidbaar bewijs kan verzamelen. Een andere geïnterviewde, ook werkzaam bij Digit, licht toe dat het in die gevallen belangrijk is om op een zodanige manier te werken dat over de precieze werkwijze uiteindelijk niets prijsgegeven hoeft te worden. Zo veel mogelijk werken met 'standaardtooltjes' kan hierbij helpen.

### *4.4.7 Gegevens binnenhalen en opslaan*

**Onderzoeksgegevens**
Nadat Digit gegevens binnen heeft gehaald, worden de gegevens geautomatiseerd doorgestuurd naar een omgeving binnen de technische infrastructuur van Digit. De omvang van de data is afhankelijk van de hoeveelheid en het soort gegevens dat verzameld wordt. Op basis van de onderzoeksvraag van het tactisch team overhandigt het technisch team in principe ongefilterd gegevens in een gangbaar bestandsformaat. Meestal neemt de TDO-er van een eenheid deze gegevens in ontvangst. Bij specialistische teams, bijvoorbeeld THTC, kan dat anders geregeld zijn. Vanuit Digit wordt verteld dat sommige tactische teams graag direct de gegevens ontvangen op het moment dat deze bij Digit binnenkomen. Dat is voor Digit, vanwege tijdtechnische redenen, niet haalbaar. Daarom is de afspraak gemaakt dat gegevens dagelijks op een vast tijdstip worden overgedragen. Hiervan kan worden afgeweken indien sprake is van een 'dringend opsporingsbelang'. Soms is het bijvoorbeeld nodig het tactisch team direct op de hoogte te brengen van een afspraak die een verdachte heeft, omdat het handig is als daar een observatieteam bij is. De wijze waarop gegevens worden overgedragen is in ontwikkeling. Eén van de geïnterviewden, werkzaam bij Digit, vertelt dat Digit in de loop van de tijd selectiever is geworden in de gegevens die worden verstrekt. In de begintijd werden in principe alle gegevens overgedragen, inclusief grote bestanden zoals foto's die zich in een chatgesprek bevonden. Nu kiest men ervoor om eerst de chatgesprekken door te sturen. Indien een chatgesprek relevant is voor het opsporingsonderzoek, worden de bijbehorende (grotere) bestanden nagestuurd.

**Monitorgegevens**
Naast gegevens die Digit verzamelt op verzoek van het tactisch team ('bewijslogging'), moeten gegevens worden bijgehouden van de handelingen die Digit uitvoert ('inzet-, systeem en autorisatie- en authenticatielogging', hierna samengenomen tot monitorgegevens).[86] Bij die handelingen gaat het om binnendringen, onderzoekshandelingen die (deels) handmatig en/of geautomatiseerd (volledig door een technisch hulpmiddel) plaatsvinden en de afronding van de inzet. Omdat de Inspectie Justitie en Veiligheid in haar Verslagen aandacht besteedt aan het bijhouden van deze gegevens, wordt in dit rapport beperkt op dit onderwerp ingegaan.

Een deel van de monitorgegevens dient geautomatiseerd bijgehouden te worden, bijvoorbeeld met behulp van schermopnames en toetsaanslagen. In de begintijd is dat lastig gebleken, omdat de daarvoor aangeschafte systemen niet goed werkten. Bovendien werd soms pas achteraf duidelijk dat een systeem niet gefunctioneerd had. Inmiddels zou het maken van schermopnames en het bijhouden van toetsaanslagen weer goed werken en heeft Digit een systeem ontwikkeld dat dit in de gaten houdt. Vanuit de Inspectie wordt echter aangegeven dat de logging nog niet op orde is.[87] Enkele geïnterviewden vanuit Digit hebben kritiek op het feit dat continu gekeken zou moeten worden of de monitoring nog goed werkt. 'Hoe ver ga je met de controle van het controleren'? Daarnaast zou het lastig gebleken zijn, onder andere vanwege 'de uitgebreide technische infrastructuur en technische hulpmiddelen' om het bijhouden van monitorgegevens goed op orde te krijgen en te houden. Die lastigheid geldt zeker voor de situatie waarin Digit op locatie aan het werk is (en niet op haar eigen

[86] Om verwarring te voorkomen tussen de verschillende vormen van logging worden deze drie laatste vormen van logging monitorgegevens genoemd.
[87] In haar derde Verslag (2022, p. 27) wordt geconstateerd dat de volledigheid van de vastgelegde beeldschermopnames in 2021 'sterk is verbeterd'. Ook stelt de Inspectie vast dat in het begin van 2021 de logging niet op orde was. In de loop van 2021 is dit verbeterd (Inspectie JenV, 2022, p. 31).

systemen). Volgens één van de geïnterviewden, werkzaam bij Digit, is het organiseren van dat soort logging 'een uitdaging' die nadere ontwikkeling vraagt aan de kant van Digit. Bij één van de geselecteerde inzetten op locatie zijn bodycams gebruikt om alle handelingen te filmen die werden uitgevoerd. In de praktijk bleek dat met deze methode niet alles even duidelijk werd geregistreerd. Daarnaast heeft op een externe locatie een camera 24/7 meegedraaid om het geautomatiseerde werk in de gaten te houden (zodat niemand anders dan Digit er toegang toe zou hebben gekregen). Dit heeft uiteindelijk zoveel beeldmateriaal opgeleverd dat er géén ruimte was om die goed op te slaan. Bovendien zijn vanwege de omvang deze beelden nooit teruggekeken, aldus deze geïnterviewde. Deze geïnterviewde vraagt zich om die reden af wat het nut is van het maken van dat soort opnames. Bij nieuwe inzetten is besloten om niet meer op deze manier te werk te gaan. Een andere geïnterviewde vertelt dat de wetgever er te veel vanuit is gegaan dat Digit op een vaste locatie 'vanuit een luie stoel klikkend' haar werk doet. Dat blijkt in de praktijk niet altijd het geval te zijn en dat zou er mede voor zorgen dat de eisen die aan het bijhouden van monitorgegevens gesteld worden, lastig zijn.

### *4.4.8 Vastleggen gegevens*

Naast monitorgegevens waarvan het de bedoeling is dat die (grotendeels) geautomatiseerd worden vastgelegd, legt Digit zelf (handmatig) ook een aantal dingen vast. Dat vastleggen gebeurt op twee manieren: journaliseren/muteren en verbaliseren. Journaliseren, vergelijkbaar met het bijhouden van een logboek, gebeurt in een eigen intern systeem van Digit en wordt niet openbaar gemaakt in bijvoorbeeld in een procesdossier (in tegenstelling tot een proces-verbaal). Het is de bedoeling dat medewerkers van Digit in principe elke handeling vastleggen. Eén van de geïnterviewden vertelt dat dit zo uitgebreid mogelijk moet gebeuren en dat informatie die gemuteerd is, terug te zien zou moeten zijn in de logging die in het geautomatiseerd werk plaatsvindt (dat geldt overigens ook voor een deel van de informatie die geverbaliseerd wordt). Deze geïnterviewde vertelt dat het belang van muteren er echt 'ingestampt' wordt bij de medewerkers van Digit-politie. Deze geïnterviewde legt uit dat muteren belangrijk is, omdat alles wat gedaan wordt door Digit herleidbaar moet zijn. Bovendien kan het zijn dat op een later moment een proces-verbaal wordt opgemaakt en dan biedt een mutatie 'houvast'. In de praktijk wordt binnen Digit nog niet alles structureel gemuteerd. Een andere geïnterviewde vertelt dat niet elke medewerker het belang van muteren inziet. Toch zou inmiddels een 'stijgende lijn' zichtbaar zijn wat betreft het vastleggen van informatie, het sneller op papier zetten en het hebben van overzicht. Binnen Digit houdt een dossiervormer in de gaten hoe er gemuteerd wordt. Naast journaliseren/muteren dienen medewerkers bepaalde handelingen te verbaliseren. Hierop wordt in hoofdstuk 6 verder ingegaan.

### *4.4.9 Samenwerking en functiescheiding*

In de praktijk werken Digit en het tactisch team samen. Deze samenwerking vindt plaats op verschillende momenten gedurende het opsporingsonderzoek en is er eigenlijk al op het moment dat een tactisch team bij Digit een verzoek indient voor een inzet en Digit in gesprek gaat wat de centrale vraagstelling is. Maar ook als nagedacht wordt over hoe Digit het beste zou kunnen binnendringen. Ook gedurende een inzet vindt samenwerking plaats, bijvoorbeeld om te bepalen op welk moment vertrouwelijke communicatie kan worden opgenomen. Een observatieteam moet Digit op de hoogte brengen wanneer een verdachte zich op een plek bevindt waar dat is toegestaan. Andersom komt het voor dat Digit het observatieteam ondersteunt door

een locatie door te geven waarop de verdachte zich bevindt zodat het observatieteam daar getuige van kan zijn. Op dat moment is Digit 'oog en oor' voor het observatieteam.

Uit het voorgaande blijkt dat géén sprake is van 'strikte functiescheiding'. Hierin wijkt de praktijk af van het uitgangspunt in de wet dat die scheiding er wel zou moeten zijn tussen het tactisch team en Digit. Digit legt het begrip functiescheiding echter op zo'n manier uit dat samenwerking met het tactisch team niet volledig uitgesloten hoeft te zijn. Eén van de geïnterviewden vertelt dat functiescheiding vooral één kant op werkt. Dat betekent dat het tactisch team geen invloed mag uitoefenen op de werkzaamheden van Digit, maar dat Digit wel kennis mag hebben over het tactisch onderzoek. Verschillende geïnterviewden benadrukken dat die kennis nodig is om een inzet goed uit te kunnen voeren. Eén van de geïnterviewden vertelt in dat kader dat het werk dat Digit doet verschilt van andere ondersteunende diensten waarvan een tactisch team gedurende het onderzoek gebruik kan maken.

> *'I&S* [Interceptie & Sensing] *houdt zich onder andere bezig met tappen. Zij zijn niet heel betrokken bij de inhoud van een zaak. Voor het werk dat Digit doet moet je volgens geïnterviewde intiem betrokken zijn bij het onderzoek, zeker als je dat goed wil doen. (…)* [Je moet] *in het hoofd van de verdachte kruipen. Dat is nodig om de risico's en kansen in te kunnen schatten (...). I&S is in een zaak niet echt een opsporingsambtenaar. Voor Digit zou het helpen als zij meer betrokken zou kunnen zijn bij het onderzoek.'*

Tijdens de interviews is diverse malen de noodzaak van samenwerking benadrukt. Eerder is al een aantal voorbeelden voorbij gekomen waarvoor dat geldt. Bij deze voorbeelden gaat het om tactische informatie die Digit nodig heeft. Er zijn ook inzetten waarbij Digit niet alleen behoefte heeft om tactische kennis te ontvangen, maar ook om op technisch vlak met het tactisch team van gedachte te kunnen wisselen. Dit betreft inzetten in opsporingsonderzoeken met een 'high tech' component, uitgevoerd door THTC. Bij inzetten in dat soort opsporingsonderzoeken kan het tactisch team (THTC) een 'fijne sparringpartner' zijn, aldus één van de geïnterviewden. Zo'n tactisch team is in staat om te snappen wat er gebeurt bij Digit en kan bijvoorbeeld helpen met het maken van een risico-inschatting van een bepaalde manier van binnendringen. Andere tactische teams, bijvoorbeeld afkomstig van de districtsrecherche, zullen daartoe niet of minder in staat zijn, waardoor het voor dat soort inzetten niet relevant is om technische informatie te delen.

Met betrekking tot enkele geselecteerde inzetten is gevraagd hoe de samenwerking met het tactisch team verlopen is. Doorgaans ging dat goed. Dat had vooral te maken met het feit dat mensen vanuit Digit en het tactisch team (inclusief soms de TDO'er) elkaar veelal kenden uit het verleden. Bij één van de geselecteerde inzetten werd de samenwerking als prettig ervaren, omdat beide teams 'dezelfde (technische) taal' spraken. Een belangrijk aandachtspunt dat wordt genoemd met betrekking tot samenwerking met tactische teams is om aandacht te hebben voor wat tactische teams wel en niet van Digit kunnen verwachten. Sommige tactische teams denken bijvoorbeeld dat een inzet waardevollere informatie oplevert dan Digit daadwerkelijk kan bieden. Daarnaast wordt wel eens verwacht dat bij Digit alles geautomatiseerd gebeurt, terwijl voor een aantal handelingen Digit op het politiebureau aanwezig moet zijn. Dat betekent dat een gewenste handeling vanuit het tactisch team niet altijd direct kan worden verricht. Tot slot is het bij een aantal inzetten belangrijk gebleken

dat een tactisch team voldoende capaciteit beschikbaar heeft om Digit bij haar werkzaamheden te ondersteunen en om de verzamelde gegevens te kunnen verwerken. Zo is voor inzetten van Digit met enige regelmaat een observatieteam nodig en moet voldoende analysecapaciteit aanwezig zijn om alle gegevens die Digit verzamelt te kunnen analyseren.

### *4.4.10 Samenwerking Digit- en zaaksOM*

Net zoals aan de kant van de politie hebben Digit-OM en het zaaks-OM contact met elkaar en dat gebeurt ook tijdens de inzet. Een zaaksofficier krijgt alleen informatie 'als dat relevant is in een strafzaak', bijvoorbeeld omdat de verwachting is dat hij/zij daar op zitting ter verantwoording over zal worden geroepen. Vanuit Digit wordt uitgelegd dat het vooral rondom de inzet van technische hulpmiddelen balanceren is tussen welke informatie wel en welke informatie niet aan het zaaksOM meegegeven wordt. Voor de rest geldt dat de zaaksofficier erop moet vertrouwen dat Digit 'handelt binnen de grenzen van de wet'. Niet de zaaksofficier maar Digit-OM heeft contact met Digit-politie. Daarnaast krijgt de zaaksofficier van justitie de beschikking over de (summiere) processen-verbaal die Digit opstelt. De kaders voor de inhoud daarvan worden door Digit-OM gesteld. Dat geldt ook voor de kaders voor de inzet in meer algemene zin. Meerdere geïnterviewden geven aan het niet problematisch te vinden dat zij niet weten hoe Digit precies te werk gaat. Bij andere middelen, zoals een tap, weten zij dat ook niet, zo is het argument. Overigens geeft een aantal geïnterviewden aan dat zij wel *iets* denken te weten over de wijze waarop de politie haar werk doet. Gedurende de inzet is er vooral overleg over 'operationele zaken' die zich voor kunnen doen, bijvoorbeeld of alle gegevens die verzameld zijn aan het tactisch team overgedragen kunnen worden (in het kader van mogelijke geheimhoudersgegevens). Daarnaast is er contact op het moment dat een beslissing moet worden genomen over verlenging van de inzet en over de beëindiging ervan.

### *4.4.11 Hoofdpunten*

- In de wet wordt onderscheid gemaakt tussen verschillende onderzoekshandelingen die kunnen worden verricht (de verschillende opsporingsdoelen, subA t/m E). In de uitvoeringspraktijk blijkt een onderzoekshandeling onder meerdere subs te kunnen vallen. Dat gegeven is in de uitvoeringspraktijk soms onderwerp van discussie.
- In de praktijk wordt doorgaans géén stapsgewijze aanpak gehanteerd, waarbij eerst verkennend (subA) gestart wordt.
- De ontwikkeling van eigen hulpmiddelen (en ze vooraf goedgekeurd krijgen) is nauwelijks haalbaar gebleken in de praktijk in verband met de tijd die het kost om een volledig goedgekeurd middel te ontwikkelen.
- Eigen door Digit ontwikkelde hulpmiddelen worden tot nu toe slechts voor één zaak gebruikt, omdat een nieuwe zaak doorgaans vraagt om aanpassingen van het hulpmiddel.
- Digit kan ook een handmatige inzet doen en die optie wordt (steeds) vaker overwogen.
- Het is ingewikkeld gebleken om een goed werkend systeem te implementeren waarmee monitorgegevens (logging) worden bijgehouden. In het derde Verslag van de Inspectie (Inspectie JenV, 2022, p. 31) blijkt dat het proces van logging verbeterd is.
- Digit en het tactisch team werken nauw met elkaar samen. Strikte functiescheiding blijkt in de opsporingspraktijk niet haalbaar, omdat beide teams elkaar nodig hebben bij de uitvoering van de hackbevoegdheid.

## 4.5 Buitenland

### *4.5.1 Inleiding*

In de komende paragrafen wordt nader ingegaan op de wijze waarop de internationale component een rol speelt in de uitvoeringspraktijk, een onderwerp waarover veel discussie was gedurende het wetgevingstraject (zie bijlage 3). Allereest wordt ingegaan op inzetten vanuit Nederland in het buitenland. Daarbinnen wordt onderscheid gemaakt tussen standaardinzetten en maatwerkinzetten. Daarna richt de aandacht zich op inzetten vanuit het buitenland in Nederland. Beide categorieën zijn overigens niet altijd scherp van elkaar te scheiden, maar vanwege analytische redenen worden beide los van elkaar besproken. De paragraaf besluit met de wijze waarop inzetten met een internationale component getoetst worden.

### *4.5.2 Samenvatting wettelijk kader*

Hoewel ten tijde van de totstandkoming van de wet er nog geen internationaalrechtelijk kader beschikbaar was dat in alle gevallen de toegang tot gegevens op buitenlands grondgebied regelt, heeft de wetgever in Nederland ervoor gekozen dat het toch mogelijk moest zijn om in het kader van de bestrijding van computercriminaliteit gegevens te kunnen verzamelen. Regels hieromtrent zijn vastgelegd in een Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid (Staatscourant, 26 februari 2019, nr. 10277), hierna OM-aanwijzing. Uitgangspunt is dat Nederland een rechtshulpverzoek doet, indien zij de beschikking wil krijgen over gegevens die zich op buitenlands grondgebied bevinden. In uitzonderlijke gevallen moet het echter mogelijk zijn om zonder (voorafgaand) rechtshulpverzoek te werken. In de OM-aanwijzing zijn verschillende scenario's geschetst wanneer dat aan de orde kan zijn en aan welke voorwaarden in die gevallen moet worden voldaan. Deze scenario's hebben zowel betrekking op situaties waarin de locatie van gegevens bekend is/bekend wordt gedurende het onderzoek als op situaties waarin de locatie niet 'middels redelijke inspanning' kan worden vastgesteld. Voor alle scenario's geldt dat de zaaksofficier van justitie, in overleg met de Digit-officier, bepaalt of een inzet zonder voorafgaand rechtshulpverzoek plaats kan vinden waarna ook de rechercheofficier toestemming moet geven.

### *4.5.3 Inzetten in het buitenland*

Voor standaardinzetten is de afspraak gemaakt dat in principe niet wordt binnengedrongen op een telefoon die zich buiten Nederland bevindt. Hiervoor lijken twee redenen te zijn. De eerste is dat het technisch niet (altijd) mogelijk is om binnen te dringen op een telefoon die zich in het buitenland bevindt. De tweede reden is dat voor het binnendringen op een telefoon, in lijn met de OM-aanwijzing, een rechtshulpverzoek moet worden ingediend. De locatie van de telefoon is doorgaans bekend, bijvoorbeeld omdat men weet dat de kans bestaat dat de verdachte zich naar een bepaald buitenland verplaatst. Een nadeel van het indienden van een rechtshulpverzoek is dat van sommige landen bekend is dat het heel lastig wordt om op hun grondgebied gegevens te verzamelen. In dat soort landen is de kans op het verkrijgen van toestemming zeer klein, en als de toestemming komt, dan gaat daar veel tijd overheen. Een ander nadeel is dat in het rechtshulpverzoek informatie moet worden gegeven over de gebruikte opsporingsmethoden. Tot nog toe is de keuze gemaakt om aan landen waarmee niet of nauwelijks wordt samengewerkt en/of onbekend is of zij op een zelfde soort manier werken als Nederland géén informatie

prijs te geven over de manier waarop Nederland uitvoering geeft aan de hackbevoegdheid. In die landen wordt om die reden in principe ook geen inzet gedaan. Daarbij komt dat binnendringen op een telefoon die zich tijdelijk in het buitenland bevindt lang niet altijd nodig is om aan de benodigde gegevens te komen.

Bij één van de voor dit onderzoek geselecteerde inzetten bestond, ondanks de mogelijkheid om historische gegevens binnen te halen, vanuit het zaaksOM toch de wens om ook gegevens binnen te halen gedurende de periode dat de telefoon zich in het buitenland bevond. Daarbij ging het om OVC. De betreffende zaak had een grote internationale component en de verdachten waren met enige regelmaat in het buitenland te vinden, waarbij één specifiek land veelvuldig werd bezocht. Dit betrof een land waarmee Nederland een goede samenwerkingsrelatie heeft. Voor deze inzet zijn verschillende Europese onderzoeksbevelen (EOB)[88] ingediend, waarna toestemming volgde om vertrouwelijke communicatie op te nemen. In de EOB's is overigens (bewust) geen informatie prijsgegeven over de wijze waarop de OVC kon plaatsvinden. Dat was in Nederland al geregeld en kon daardoor in het EOB in het midden worden gelaten. Eén van de geïnterviewde opsporingsfunctionarissen vertelt dat het uitwisselen van dit soort gegevens, OVC en ook tapresultaten, in Europa geregeld is. Voor OVC dient een apart onderzoeksbevel te komen (zoals dat met het EOB gebeurd is) en in het geval van tappen, kan Nederland achteraf toestemming vragen. Voor het verstrekken van vastgelegde gegevens (subD) zouden nog géén internationale afspraken bestaan.

Naast standaardinzetten kunnen maatwerkinzetten een buitenlandcomponent bevatten, bijvoorbeeld een server die verbonden is met verschillende geautomatiseerde werken in het buitenland. Ook voor dit soort opsporingsonderzoeken geldt dat niet in elk land een inzet door Digit voor de hand ligt. Eén van de geïnterviewde opsporingsfunctionarissen vertelt dat dat, in tegenstelling tot de standaardinzetten, niet zozeer te maken heeft met het niet prijs willen geven van gehanteerde opsporingsmethoden, maar vooral met de reeds bestaande relaties tussen landen. Voorkomen moet worden dat Digit in de positie komt dat zij als 'statelijke actor' wordt gezien, waardoor (politieke) problemen kunnen ontstaan, omdat op ander grondgebied opgetreden wordt. Indien al een goede samenwerkingsrelatie met een land bestaat, dan ligt een inzet in dat land meer voor de hand. Een voorbeeld van zo'n inzet is het onderzoek naar een botnet dat in veel verschillende landen slachtsoffers maakte. In 2019 raakte THTC betrokken bij een internationaal opsporingsonderzoek hiernaar. Nadat THTC eerst in het kader van die internationale samenwerking zelf allerlei onderzoekshandelingen had uitgevoerd, was in 2020 de inzet van Digit nodig om binnen te dringen in de servers die in Nederland bleken te staan. Vraag aan Digit was om kenmerken van het geautomatiseerde werk en de daarin aangetroffen gegevens vast te leggen. Daarna was het de bedoeling het botnet uit de lucht te halen. Voor het binnendringen in de server heeft Digit gebruikgemaakt van eigen ontwikkelde software en voor de uiteindelijke ontoegankelijkmaking is gebruikgemaakt van software gemaakt door een ander land. Deze geïnterviewde vertelt dat deze inzet ten minste twee juridische uitdagingen kende. In de eerste plaats is voor deze inzet wereldwijd binnengedrongen op verschillende computers verspreid over ten minste 190 landen. Hoewel niet duidelijk was op welke computers precies werd binnengedrongen, was wel een groot deel van de landen bekend (en dus de locatie van het geautomatiseerde werk). Dat betekende

[88] Een EOB gaat over een opsporingsvraag binnen de Europese Unie en maakt het voor justitiële autoriteiten makkelijker om in ander EU-land bewijsmateriaal op te vragen. Verzoeken die binnenkomen vanuit landen buiten de Europese Unie worden gegoten in een klassiek rechtshulpverzoek (Van Berkel et al., 2021).

dat de eerder geschetste uitzonderingssituaties in de OM-aanwijzing niet van toepassing waren en rechtshulpverzoeken moesten worden ingediend. Uiteindelijk is daarvoor niet gekozen. In plaats daarvan is besloten dat het 'uitlegbaar' was om de inzet zonder rechtshulpverzoeken plaats te laten vinden. Vanuit Digit wordt verteld dat de CTC het hiermee eens was en dat de minister over de keuze geïnformeerd is. Dat laatste was nodig, omdat anders dan de OM-aanwijzing voorschrijft gehandeld werd. Voorkomen moest worden dat internationaal politieke onenigheid zou ontstaan over de gehanteerde werkwijze. Uitgelegd wordt dat discussies over territorialiteit en soevereiniteit op politiek niveau vaak ingewikkeld zijn. Op uitvoeringsniveau daarentegen worden weinig problemen of bezwaren gezien als gewerkt moet worden aan een concrete zaak.

Een tweede juridische uitdaging had betrekking op de door het buitenland ontwikkelde code waarmee het botnet onschadelijk kon worden gemaakt. In die code was opgenomen dat de gegevens naar een server van Land X zouden worden gestuurd. Het Openbaar Ministerie uit Land X had al toestemming gekregen om de code in te zetten. Bij die toestemming was echter niet inbegrepen dat de gegevens van een server in Land X naar een Nederlandse server mochten worden verstuurd. Uiteindelijk is de bevoegdheid om die reden gedeeltelijk op de Nederlandse titel ingezet (subA en subD), zo vertelt één van de geïnterviewden. Het gebruik van de code uit Land X en de daaraan gekoppelde handelingen (subE) hebben uiteindelijk op basis van een rechtshulpverzoek uit Land X, waar de code was ontwikkeld, plaatsgevonden. De inzet zelf is verder getoetst zoals dat met de Nederlandse inzetten ook gebeurt. Daarnaast is nog een ambtsbericht naar het College van PG's gestuurd en is de buitenlandse code door Digit gecontroleerd en licht aangepast. De code is verder niet voorgelegd aan de Keuringsdienst. Wel is afgesproken dat de code die Land X heeft ontwikkeld na de inzet openbaar zou worden gemaakt in verband met transparantie. Voor zover bekend is deze afspraak nageleefd.

### *4.5.4 Inzetten in Nederland (door het buitenland)*

Het is ook voorgekomen dat op verzoek van het buitenland (een ander land dan Land X) een inzet in Nederland heeft plaatsgevonden. Eén van de geïnterviewde opsporingsfunctionarissen merkt op dat voor dat soort gevallen niets geregeld is. Gedurende de wetsgeschiedenis is vooral aandacht geweest voor wat er zou gebeuren als Nederland een inzet in het buitenland zou doen, maar niet of nauwelijks voor de 'gespiegelde' situatie. Deze geïnterviewde vertelt dat hierdoor bij één van de inzetten 'kunst- en vliegwerk' moest worden uitgehaald om de inzet juridisch mogelijk te maken. De inzet betrof een opsporingsonderzoek waarbij een Digit-achtig team in het buitenland een *remote-access tool*[89] over wilde nemen. Vervolgens zou daarop een update worden geplaatst die wereldwijd naar allerlei gebruikers zou worden gestuurd. Door deze inzet werd binnengedrongen in Nederlandse geautomatiseerde werken. Vervolgens zouden verzamelde gegevens weer richting het buitenland gaan en op een later moment ook door het buitenland met Nederland worden gedeeld. Het betreffende buitenland heeft aan Nederland toestemming gevraagd voor een inzet. Voor het buitenland was het in principe voldoende dat Nederland een formulier, aangereikt vanuit het buitenland, zou ondertekenen. In Nederland is echter meer nodig om de bevoegdheid in te kunnen zetten (zie hoofdstuk 3). Uiteindelijk is in overleg besloten dat het buitenland een rechtshulpverzoek aan Nederland zou doen. Vervolgens is dat in Nederland op de gebruikelijke wijze (zoals dat met de hackbevoegdheid gaat) getoetst. De geïnterviewde vertelt dat normaal gesproken een marginale toetsing

[89] Een *Remote Access Tool* (RAT) geeft een persoon de mogelijkheid om een computer op afstand te beheren.

wordt gedaan, omdat het verzoekende buitenland een 'fatsoenlijk' land was waarbij er vanuit kan worden gegaan dat dat land het onderzoek op een fatsoenlijke manier heeft gedaan. Vanuit Nederland is uiteindelijk toestemming gekomen om de bevoegdheid in te zetten. Er was echter wel een probleem, omdat een Nederlandse officier van justitie alleen een bevel kan afgeven aan een Nederlandse opsporingsambtenaar, maar die kon het bevel niet uitvoeren, omdat dat technisch niet mogelijk was. Digit kon ook niets, omdat ze daarvoor naar het buitenland moest afreizen en dan zou precies hetzelfde probleem spelen (inzet op buitenlands grondgebied). Om die reden is een tweede rechtshulpverzoek ingediend, maar nu richting het buitenland, waarin het buitenland verzocht werd bepaalde handelingen uit te voeren. Deze geïnterviewde vindt een dergelijke werkwijze 'raar'. Volgens deze geïnterviewde zou er een mogelijkheid moeten komen dat het buitenland zelf op Nederlands grondgebied een hack mag uitvoeren, zoals dat ook het geval is met observaties op andermans grondgebied.

**Verlofprocedure**
Voor verschillende bijzondere opsporingsbevoegdheden bestaat een verlofprocedure. Dat betekent dat, indien het buitenland een bijzondere opsporingsbevoegdheid in Nederland wil inzetten en daar toestemming voor is, de rechter-commissaris nog toestemming moet geven voor de daadwerkelijke overdracht van gegevens die met de bijzondere opsporingsbevoegdheid verzameld zijn. Voor de hackbevoegdheid bestaat een dergelijke procedure niet tot verbazing van twee opsporingsfunctionarissen.

### *4.5.5 Toetsing inzet in het buitenland*

In het voorgaande is de toetsing van een inzet met een internationale component al een aantal keer voorbij gekomen. In principe vindt een zelfde soort toetsing plaats als bij een inzet in Nederland, inclusief de daarbij betrokken actoren. Een zaaksofficier van justitie zal moeten beslissen of een hack in het buitenland nodig is (en kansrijk is) en vervolgens moet gemotiveerd worden waarom dat het geval is, zodat andere actoren (rechercheofficier, CTC, College van PG's, rechter-commissaris) een oordeel kunnen vellen. De CTC neemt bij haar advies mee of een inzet mogelijk in het buitenland plaatsvindt. Eén van de geïnterviewden legt uit dat de zaaksbeschrijving die de CTC voorgeschoteld krijgt hier wel aanleiding toe moet geven. Als uit die beschrijving blijkt dat een verdachte zich mogelijk (tijdelijk) in het buitenland bevindt, dan vraagt de CTC daarop door. In principe ziet de CTC liever géén inzet in het buitenland, tenzij het niet anders kan. Vanuit de rechters-commissarissen wordt aangegeven dat de buitenlandcomponent een beperkte rol speelt bij hun toetsing. Uitgelegd wordt dat de officier van justitie gaat over de rechtmatigheid van het onderzoek. Daar hoort volgens één van de geïnterviewden de omgang met een buitenlandcomponent ook bij. Dat uiteindelijk in het bevel vermeld moet worden dat gegevens zich mogelijk in het buitenland bevinden, is volgens deze geïnterviewde bovendien een extra waarborg voor een zorgvuldige voorbereiding van de inzet van de bevoegdheid door de officier van justitie waarover rekenschap moet worden afgelegd bij de rechter-commissaris. Hoewel er dus een beperkte rol is voor rechters-commissarissen, geeft deze geïnterviewde ook aan dat rechters-commissarissen niet uit het oog moeten verliezen dat de rechter-commissaris bij het verlenen van een machtiging onderdeel is van een overheid die eventueel een soevereiniteitsschending begaat. Daarom vindt deze geïnterviewde het als rechter-commissaris wel belangrijk om te weten dat er een internationale component aan het onderzoek zit. In een aantal machtigingen (met betrekking tot de geselecteerde inzetten) wordt door de betreffende rechter-

commissaris vermeld dat indien het geautomatiseerde werk buiten Nederland wordt gebruikt, toestemming moet worden gevraagd aan het betreffende land.
Verder wordt uitgelegd dat de rol van de rechter-commissaris bij 'hacken-light' anders ligt.[90] Met hacken-light wordt bedoeld dat de politie met rechtmatig verkregen inloggegevens inlogt op een account om gegevens te verzamelen. Hacken-light vindt op dit moment plaats op basis van artikel 181 juncto artikel 177 Sv met een analoge toepassing van artikel 126ng Sv en is een opsporingsbevoegdheid waarvoor de rechter-commissaris, door tussenkomst van een officier van justitie, een opdracht aan de politie geeft. Dat betekent dat wanneer bij het inloggen in het buitenland mogelijk sprake is van een soevereiniteitsinbreuk deze primair plaatsvindt onder verantwoordelijkheid van de rechter-commissaris en niet onder die van de officier van justitie (zoals bij een inzet op basis van 126nba Sv). Uit artikel 181 Sv volgt immers dat de rechter-commissaris de onderzoekshandelingen verricht (op vordering van een officier van justitie), of deze laat verrichten met toepassing van artikel 177 Sv. Wat dat betreft is er een verschil tussen 'zelf onderzoek doen of laten doen en een machtiging afgeven', aldus een geïnterviewde betrokken bij de toetsing van de bevoegdheid.

### *4.5.6 Hoofdpunten*

- Digit is betrokken geweest bij een beperkt aantal inzetten met een internationale component. Het gaat hierbij om inzetten vanuit Nederland in het buitenland en om inzetten vanuit het buitenland in Nederland.
- Wat betreft standaardinzetten is in principe de afspraak dat niet op een telefoon wordt binnengedrongen die zich in het buitenland bevindt. Voor de maatwerkinzetten is wel of niet de bevoegdheid inzetten afhankelijk van de relatie met het betreffende land.
- De OM-aanwijzing wordt gebruikt als leidraad voor inzetten in het buitenland, maar is niet altijd toereikend (indien veel verschillende geautomatiseerde werken in het spel zijn zoals bij een botnet). In het geval dat van de OM-aanwijzing wordt afgeweken, wordt de Minister van Justitie en Veiligheid geïnformeerd.
- Inzetten met een internationale component kunnen vooral politiek ingewikkeld zijn.
- Inzetten door het buitenland in Nederland zijn op dit moment niet geregeld, ook niet in de OM-aanwijzing. Buitenlandse opsporingsfunctionarissen mogen geen hack uitvoeren op Nederlands grondgebied. Daardoor moeten ingewikkelde juridische constructies worden bedacht.

[90] Een voorbeeld hiervan is het inloggen op *Facebook* om vervolgens gegevens vast te mogen leggen (Rechtbank Den Haag, 2021). Oerlemans (2019, p. 3) is kritisch op deze vorm van hacken-light, omdat niet aan de bepalingen in het Wetboek van Strafvordering wordt voldaan.

# 5 Waarborgen voor controle

## 5.1 Inleiding

Gedurende de inzet zijn verschillende actoren betrokken bij de controle op de uitvoering van de hackbevoegdheid: de Inspectie Justitie en Veiligheid (hierna Inspectie), de Keuringsdienst en het Openbaar Ministerie.[91] In dit hoofdstuk wordt beschreven hoe de controle door deze actoren in de praktijk vorm krijgt (deelvraag 4). Allereerst komen de Keuringsdienst (paragraaf 5.2) en de Inspectie (paragraaf 5.3) aan de orde. Vervolgens richt de aandacht zich op het Openbaar Ministerie (paragraaf 5.4). In paragraaf 5.5 wordt de verlenging van een inzet besproken, inclusief de actoren die daarbij betrokken zijn. Omdat eerder al een samenvatting is gegeven van het wettelijk kader rondom toetsing, worden in dit hoofdstuk alleen samenvattingen gegeven met betrekking tot de onderwerpen die nog niet eerder aan bod zijn geweest.

## 5.2 De Keuringsdienst

### *5.2.1 Inleiding*

In dit subhoofdstuk staat de keuring van technische hulpmiddelen centraal. Hierop zal uitgebreid worden ingegaan, omdat gedurende de evaluatie bleek dat de keuring van technische hulpmiddelen voor veel discussie zorgt in de uitvoeringspraktijk. In tegenstelling tot een aantal andere onderwerpen (zie bijlage 3) is over de keuring nauwelijks discussie geweest gedurende het wetgevingstraject. Het doel van het uitgebreid uiteenzetten van het keuringsproces is om te begrijpen waarom de keuring van technische hulpmiddelen als belangrijk knelpunt wordt gezien door de opsporingspraktijk. Om de discussie in de uitvoeringspraktijk te schetsen worden twee perspectieven beschreven.
Allereerst wordt aandacht besteed aan de Keuringsdienst en het keuringsprotocol. Vervolgens komt het keuringsproces in de praktijk aan de orde. Daarna wordt ingegaan op waarborgen indien gebruik wordt gemaakt van een niet (vooraf goed-) gekeurd technisch hulpmiddel. Het hoofdstuk besluit met de uiteenzetting van twee (botsende) perspectieven die een belangrijke rol spelen bij de manier waarop het keuringsproces gepercipieerd wordt.

### *5.2.2 Samenvatting wettelijk kader*

Een technisch hulpmiddel dient, voorafgaand aan het gebruik ervan, gekeurd te worden (artikel 14 Bogw). Indien een technisch hulpmiddel goedgekeurd wordt, kan worden aangenomen dat aan de wettelijke eisen met betrekking tot de betrouwbaarheid, integriteit en herleidbaarheid van gegevens is voldaan (Besluit onderzoek in een geautomatiseerd werk, p. 19). Een keuringsdienst neemt de keuring voor haar rekening (artikel 14 lid 1 Bogw). Zij moet ervoor zorgen dat een 'objectief en onafhankelijk oordeel' wordt gegeven over het hulpmiddel. Overigens kan eventueel ook een andere organisatie dan de Keuringsdienst van de Nationale Politie worden aangewezen als keuringsdienst (artikel 16, lid 2 Bogw; Besluit onderzoek in een geautomatiseerd werk, 2018, p. 42).

[91] Ook de Procureur Generaal bij de Hoge Raad (PG-HR) is betrokken bij het toezicht, namelijk op het handelen van het Openbaar Ministerie. De rol van de PG-HR is in dit onderzoek niet meegenomen.

De wijze waarop een keuring plaatsvindt wordt omschreven in een keuringsprotocol (artikel 17 lid 1 Bogw). Daarin worden tevens criteria opgenomen die tijdens de keuring worden gebruikt. De keuringsdienst en het Openbaar Ministerie zijn samen verantwoordelijk voor het opstellen van een protocol dat de minister voorafgaand aan het gebruik ervan goed moet keuren (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 42).
In het Besluit zijn op basis van artikel 126ee Sv regels geformuleerd aangaande de onderzoekshandelingen die worden verricht met een technisch hulpmiddel. De regels in het Besluit moeten ertoe bijdragen dat de bevoegdheid niet wordt misbruikt en dat de authenticiteit en integriteit van de verkregen gegevens verzekerd kan worden (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 54). Het Besluit bevat onder andere regels ten aanzien van de technische eisen die gesteld worden aan een technisch hulpmiddel en de keuring ervan (artt. 8 t/m 20 Bogw). Een voorbeeld hiervan is dat maatregelen genomen moeten worden 'naar de stand van de techniek' die beïnvloeding van buiten kunnen tegengaan (Besluit onderzoek in een geautomatiseerd werk, p. 39).
Bij de keuring dient gekeken te worden naar alle onderdelen van het hulpmiddel die belangrijk zijn voor de 'detectie, registratie en het transport van de gegevens' (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 42). De technische infrastructuur van Digit is géén onderwerp van keuring (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 42). Het is verder de bedoeling dat de keuring 'proefondervindelijk' plaatsvindt (Besluit onderzoek in een geautomatiseerd werk, 2018). De verwachting is dat deze keuring enkele maanden in beslag kan nemen, zeker wanneer de gebruikte software nog moet worden aangepast om definitief goedgekeurd te worden (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 40). Op het moment dat de keuring is afgerond, dient de keuringsdienst haar bevindingen vast te leggen in een keuringsrapport (artikel 18 lid 2 Bogw) inclusief een uniek keuringsnummer (artikel 18 lid 3b Bogw). Het veronderstelde voordeel van zo'n uniek nummer is dat verder niets vermeld hoeft te worden in het dossier over de precieze werking van het hulpmiddel. Daardoor is de kans kleiner dat opsporingsbelangen geschonden worden. Bovendien hebben rechters en advocaten de garantie dat het ingezette hulpmiddel voldoet aan alle wettelijke eisen (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 43).
Een technisch hulpmiddel wordt alleen goedgekeurd als aan alle gestelde eisen in de artikelen 8 t/m 13 van het Besluit wordt voldaan (artikel 14 lid 2 Bogw). Soms zal dat onmogelijk zijn. In dat geval moeten vervangende waarborgen worden genomen (artikel 18, lid 3e Bogw). Indien sprake is van een inzet zonder technisch hulpmiddel, moeten procedurele waarborgen worden getroffen (artikel 21 lid 5 Bogw).

De geldigheidsduur van het keuringsrapport zal vermeld worden in het rapport (artikel 18, lid 3g Bogw). Indien binnen die periode de werking van een technisch hulpmiddel of een onderdeel hiervan op zo'n manier wijzigt dat niet meer aan de gestelde technische eisen kan worden voldaan, moet een herkeuring worden uitgevoerd (artikel 14, lid 3 Bogw). De Inspectie Justitie en Veiligheid houdt toezicht op de wijze waarop de keuringsprocedure wordt nageleefd (Besluit onderzoek in geautomatiseerd werk, 2018, p. 43).
In principe dient gebruik te worden gemaakt van een vooraf gekeurd en goed bevonden technisch hulpmiddel (Besluit onderzoek geautomatiseerd werk, p. 21). Keuring achteraf behoort ook tot de mogelijkheden (artikel 15, lid 1 Bogw). Net zoals het gebruik van een technisch hulpmiddel waarvan de aard ervan zich verzet tegen een keuring (artikel 21, lid 4 Bogw). Als dat laatste aan de orde is, moet de officier van justitie in de processtukken opmerken dat afgezien is van keuring. Tevens dient hij of zij op te nemen welke aanvullende waarborgen zijn getroffen (artikel 21 lid 4

Bogw) om de 'betrouwbaarheid, integriteit en herleidbaarheid van vastgelegde gegevens te garanderen' (Besluit onderzoek in een geautomatiseerd werk, p. 21).

### *5.2.3 Keuringsdienst*

Sinds 2021 neemt de landelijke Keuringsdienst (hierna Keuringsdienst) de keuringen van de voor de hackbevoegdheid ingezette technische hulpmiddelen voor haar rekening. De Keuringsdienst is onderdeel van de Landelijke Eenheid van de Nationale Politie. Vóór 2021 was TNO[92] verantwoordelijk voor de keuring van technische hulpmiddelen die Digit gebruikt. De Keuringsdienst keurt al langere tijd ook de meer traditionele technische hulpmiddelen (zoals bedoeld in het Besluit technische hulpmiddelen strafvordering). Hierbij gaat het bijvoorbeeld om microfoons of bakens. Bij de inwerkingtreding van de Wet CCIII beschikte de Keuringsdienst niet over voldoende 'expertise en capaciteit' om de keuring van nieuwe middelen voor de hackbevoegdheid uit te voeren. TNO moest functioneren 'als een soort tussenpaus' waarna de Keuringsdienst op een gegeven moment zelf de keuringen is gaan doen. TNO is nog tot en met 2022 betrokken gebleven om de Keuringsdienst te ondersteunen. Dat was nodig, omdat bij de Keuringsdienst te weinig personeel was om de keuringen uit te voeren. Vanuit Digit (politie en OM) bestaat de wens om met TNO de wijze waarop technische hulpmiddelen gekeurd worden te evalueren. De wijze waarop het nu gaat zorgt vooral bij Digit voor onvrede. Of die gesprekken nog gaan plaatsvinden, is onduidelijk.

**Onafhankelijkheid**

De Keuringsdienst en Digit-politie maken beide deel uit van hetzelfde organisatieonderdeel binnen de Landelijke eenheid van de Nationale Politie en vallen bovendien onder hetzelfde sectorhoofd. Verschillende geïnterviewden vanuit Digit vertellen dat dit eigenlijk ongewenst is (de slager keurt zijn eigen vlees). Eén van hen merkt op:

> *'Wat een belangrijk punt is (…) is functiescheiding die* [de] *wetgever voorstelt tussen tactiek en Digit. Die zou je eigenlijk ook moeten hebben voor leidinggeven aan een keuringsdienst en leidinggeven aan Digit. Dat is op dit moment nog niet het geval. En dat moet wel gerealiseerd worden. Op dit moment valt alles binnen één onderdeel van de landelijke eenheid, dus dat is absoluut ongewenst.'*

Ook de Keuringsdienst is van mening dat het 'niet handig' is dat de Keuringsdienst en Digit onder dezelfde sectorleiding vallen, vooral in verband met het ter keuring aanbieden van een technisch hulpmiddel. Wellicht om die reden benadrukt de Keuringsdienst haar onafhankelijke positie ten opzichte van degene (in het geval van de hackbevoegdheid is dat Digit) die bij haar een product ter keuring aanbiedt. Deze onafhankelijkheid betekent bijvoorbeeld dat de Keuringsdienst doorgaans een keuring uitvoert en pas aan Digit rapporteert als de volledige keuring is afgerond. Dat geldt ook voor eventuele (kleine) fouten die zij gedurende het keuringsproces tegenkomt. Die worden tussentijds in principe niet gerapporteerd. Ook zal de Keuringsdienst niet adviseren hoe een middel dient te worden aangepast. Op die manier zou zij te veel 'het ontwikkeltraject ingezogen worden'.[93] Ook TNO vindt die onafhankelijke positie van groot belang, maar zij heeft ervoor gekozen de afstand tussen haar en Digit op sommige momenten wat kleiner te laten zijn. Dat deed zij ook vanwege de rol die zij

[92] Formeel gezien was TNO in die tijd de keuringsdienst. Om verwarring te voorkomen wordt op sommige plekken 'TNO' gehanteerd, in plaats van 'keuringsdienst'.

[93] Dit zou de Keuringsdienst ook te veel tijd kosten.

in de beginperiode had bij onder andere het ontwikkelen van een keuringsprotocol en de eerste keuringen. Eén van de geïnterviewden vertelt:

> *'Dat was ook een belangrijk discussiepunt, (…) hoe dicht kunnen wij nou op Digit zitten? (...) Vanuit de historie was* [de Keuringsdienst] *geneigd om zoveel mogelijk op afstand, muur ertussen, om de onafhankelijkheid te waarborgen. Wat denk ik best heel valide is. Wij hebben gezegd (…), als straks alles misschien* in place *is, en je hebt die keuring 30 keer gedaan, dan kan dat. Maar (…) nu (…) moeten we nog zoveel leren over hoe gaat die wet nou echt werken en wat zijn praktische dingen waar je tegenaan loopt? (…) Dus wat we tot nog toe, (…) nog* [tot] *vorig jaar merkten, is dat als we weer een keer (…) lange tijd met mensen van Digit samenzaten, dan hadden zij daarna weer een beter begrip voor wat staat er (…) ook alweer in die wet en waarom is dat relevant? Want zij zijn uiteindelijk techneuten die gewoon hun werk willen doen en bewijsmateriaal verzamelen. En dat wettelijk kader is lastig. En wij hadden weer meer geleerd over (…) hun praktische inzetomgeving, (…) hoe ziet het normale loggingproces eruit? (…) Je moet dan elkaar zoveel mogelijk begrijpen om het werkbaar te maken. Dus dat was ook een keuze.'*

Het feit dat de hackbevoegdheid nieuw was en dat iedereen nog moest uitvinden hoe precies uitvoering te geven aan de wet en vooral ook de aanvullende regelingen is voor TNO aanleiding geweest om zo nu en dan met Digit mee te denken. Dat deed zij onder andere door in de beginfase van de ontwikkeling van een product (telefonisch) contact te hebben met Digit en een eerste reactie te geven op haar ideeën, bijvoorbeeld dat er een vermoeden was dat het middel niet aan de norm van een bepaalde eis uit het Keuringsprotocol voldeed. Vervolgens kwam Digit op een later moment terug bij TNO en dan reageerde TNO ook hier op. Dit alles vond plaats *voordat* het middel gebouwd en ter keuring aangeboden was. Bij dit meedenken was het voor TNO belangrijk om niet 'op de stoel van de ontwerper' te gaan zitten. Voorkomen moest worden dat TNO 'de grens over zou gaan' door zowel ontwikkelaar als keurder te worden.

### *5.2.4 Keuringsprotocol*

De keuring van een technisch hulpmiddel vindt plaats aan de hand van het keuringsprotocol dat TNO heeft ontwikkeld.[94] De technische eisen waaraan een technisch hulpmiddel moet voldoen (artikelen 8 t/m 13 Bogw) hebben de basis gevormd voor dit protocol. Aan de hand van die artikelen en het volledige Besluit en andere wetsteksten heeft TNO voor zichzelf geprobeerd te bepalen hoe de eisen in het Besluit vertaald konden worden naar 'meer technische eisen'. Vervolgens is TNO in gesprek gegaan met de verschillende 'stakeholders' die bij deze nieuwe bevoegdheid betrokken zijn, zoals Digit, de Keuringsdienst, het Openbaar Ministerie en juristen van de Landelijke Eenheid. Doel van die gesprekken was om inzicht te krijgen in hoe een protocol ontwikkeld kon worden dat werkbaar zou zijn in de praktijk. Daarna heeft het Nederlands Forensisch Instituut (NFI) een review uitgevoerd van het protocol en op basis daarvan is nog een aantal wijzigingen aangebracht. Dit proces heeft ongeveer een jaar geduurd.
Het protocol kent zeventien eisen waaraan een technisch hulpmiddel moet voldoen. Bij deze eisen was het de bedoeling om zo dicht mogelijk bij de wetsteksten te blijven. Per eis is vervolgens een aantal normen vastgesteld. Via die normen (56 in totaal) wordt bepaald of een technisch hulpmiddel aan de gestelde eisen voldoet. De normen

[94] Dit keuringsprotocol is géén openbaar document.

moeten worden gezien als richtlijn voor wat 'als goed genoeg' kan worden bestempeld. Eén van de geïnterviewden, betrokken bij het keuringsproces, vertelt dat vooral over die normen discussie kan ontstaan en ook is ontstaan. Volgens deze geïnterviewde kan een keurder ruimte geven aan bepaalde ontwerpkeuzes, zolang maar uitgelegd kan worden dat ook met die keuzes aan de wet is voldaan. De Keuringsdienst heeft het protocol van TNO één op één overgenomen en zij verwacht niet dat aanpassing op korte termijn nodig is, omdat het protocol 'nog prima zou passen'. Later zal blijken dat niet iedereen, vooral Digit, het daar mee eens is (zie paragraaf 5.2.9)

Het is geen eenvoudige opgave gebleken om tot een definitief protocol te komen. De vraag van de opstellers van het protocol was bijvoorbeeld op welk abstractieniveau de eisen en normen geformuleerd dienden te worden. Enerzijds bestond de wens om deze zo concreet mogelijk te maken zodat er géén misverstanden of interpretatieverschillen over het protocol zouden ontstaan. Anderzijds moest het protocol generiek genoeg zijn zodat alle technische hulpmiddelen die verschillend in elkaar zitten en in verschillende contexten worden toegepast, beoordeeld konden worden. Een voorbeeld waarin het gekozen abstractieniveau voor discussie zorgde heeft betrekking op de eisen die worden gesteld aan de versleuteling van gegevens. Die moet, in lijn met de wetgever 'naar de stand der techniek' zijn, zo staat in het Keuringsprotocol geformuleerd. Onduidelijk was echter wat die 'stand der techniek' precies inhoudt. Op basis van wie of wat wordt bepaald of aan die stand is voldaan? Om de formuleringen zoals de 'stand der techniek' meer te concretiseren heeft TNO op een later moment aangegeven dat voor transportencryptie de richtlijnen van het NCSC worden gebruikt om invulling te geven aan de formulering 'stand der techniek'. Digit vindt dat niet al deze eisen goed toepasbaar zijn op de hulpmiddelen die Digit ontwikkelt, bijvoorbeeld wat betreft transportbeveiliging.
Een tweede punt gaat over het feit dat de wetgever niet alle begrippen voldoende duidelijk toegelicht heeft, bijvoorbeeld de technische infrastructuur van Digit. In de nota van toelichting is vermeld dat de technische infrastructuur zelf géén onderdeel uitmaakt van de keuring (Besluit onderzoek in geautomatiseerd werk, 2018, p. 40). Technisch gezien is echter niet altijd duidelijk waar een technisch hulpmiddel ophoudt en de technische infrastructuur begint. Dit onderscheid is relevant, omdat de Keuringsdienst in haar keuring alleen het technisch hulpmiddel en het transport tot de technische infrastructuur van Digit kan betrekken. Om duidelijkheid te scheppen zijn in het keuringsprotocol verschillende situaties geschetst waarbij steeds is aangegeven wat wel en niet tot de technische infrastructuur behoort en waar de Keuringsdienst wel en niet naar kijkt. In de praktijk is hier discussie over.
Een ander punt waardoor het niet eenvoudig was om het protocol te maken is dat de wijze waarop de wetgever sommige aspecten heeft geformuleerd technisch niet altijd even voor de hand liggend zijn. Logging was in dit kader 'één van de moeilijkste dingen', aldus een geïnterviewde betrokken bij het keuringsproces. Deze geïnterviewde licht toe dat de definitie die de wetgever van logging gebruikt een andere is dan wat IT'ers verstaan onder logging. In de wetsteksten zou het vooral gaan om bewijslogging, het feitelijke bewijsmateriaal.[95] Voor IT'ers heeft logging echter vooral betrekking op het bijhouden hoe een systeem functioneert en of dat op een manier gebeurt zoals dat de bedoeling was. De verschillende vormen van logging lopen in het Besluit echter door elkaar heen. Een bijkomend probleem (voor het samenstellen van het protocol) was dat in het Besluit weliswaar over logging wordt

[95] Een geïnterviewde opsporingsfunctionaris pleit, vanwege mogelijke verwarring, ervoor niet langer te spreken over bewijslogging, maar over bewijs of gegevens die verzameld worden ten behoeve van het tactisch team. Ook zou meer in de toelichting duidelijk moeten worden gemaakt wat onder bewijslogging verstaan wordt.

gesproken, maar niet in de artikelen 8 t/m 13 waarop het Keuringsprotocol volgens het Besluit gebaseerd zou moeten worden. Om aan de artikelen 8 t/m 13 te kunnen voldoen was het in de ogen van TNO echter wel belangrijk om (ook) eisen aan logging te kunnen stellen.

### *5.2.5 Keuringsproces*

Zodra (een eerste versie van) een technisch hulpmiddel ontwikkeld is, wordt het hulpmiddel gekeurd. Dit keuringsproces bestaat uit een aantal stappen: de acceptatietest (intake), de keuring zelf (uitvoering) en het keuringsrapport (afronding). Zie bijlage 5 voor een uitgebreidere beschrijving hiervan.
In de informatiebeveiliging speelt de CIA-driehoek (Confidentiality (vertrouwelijkheid), Integrity (integriteit) and availability (beschikbaarheid)) een belangrijke rol. De Keuringsdienst richt zich op twee van deze aspecten, namelijk vertrouwelijkheid (derden mogen niet meelezen) en integriteit (gegevens mogen niet gewijzigd zijn). De beschikbaarheid is géén onderwerp van de keuring. Eén van de geïnterviewden, betrokken bij het keuringsproces, vertelt:

> *'Availability, dat is niet ons pakkie-an. En dat zullen zij* [Digit] *wel moeten testen, (…) valt het* [hulpmiddel] *niet uit elkaar tijdens een operatie? Dat is voor hun belangrijk. (…) zolang bij de rechter aangetoond kan worden: er is niet mee gerommeld en derden hebben niet mee kunnen lezen* [is het voor ons goed]*. Dat is wat wij toetsen.'*

Voor Digit is het lastig dat de Keuringsdienst, want zo geregeld in het Besluit, alleen kijkt naar vertrouwelijkheid en integriteit en niet breder dan dat. Eén van de geïnterviewden, werkzaam bij Digit, legt uit dat de eisen die worden gesteld in het kader van bijvoorbeeld integriteit ervoor zouden kunnen (gaan) zorgen dat een technisch hulpmiddel in de toekomst niet bruikbaar is in de praktijk, omdat de gestelde eisen het risico vergroten dat een verdachte merkt dat er iets met zijn of haar geautomatiseerde werk aan de hand is. In dat opzicht is er een spanningsveld tussen aan de ene kant optimale beschikbaarheid en aan de andere kant optimale vertrouwelijkheid en integriteit.
Nadat de resultaten van de verschillende testen bekend zijn, stelt de Keuringsdienst een keuringsrapport op dat openbaar kan worden gemaakt. Een eventuele goedkeuring wordt afgegeven voor twee jaar. Dat betekent dat binnen die twee jaar in principe niet opnieuw naar dit middel gekeken wordt, tenzij omstandigheden daar aanleiding toe bieden (denk aan een beveiligingsincident) of omdat een middel gewijzigd is. Tot het moment van het schrijven van dit rapport (april 2022) is het niet voorgekomen dat opnieuw naar een goedgekeurd middel gekeken is.
Hoewel de keuringstermijn vier weken zou moeten zijn,[96] is deze termijn in het contract met TNO niet vastgelegd. Ook voor de Keuringsdienst geldt deze termijn niet. Toch hanteert de Keuringsdienst voor zichzelf een termijn van vier weken. In de uitvoeringspraktijk wordt de keuringstermijn niet altijd gehaald. In de beginperiode had dat onder andere te maken met het feit dat de wet net in werking was getreden en werkende weg uitgevonden moest worden hoe uitvoering te geven aan alle verschillende onderdelen van de wet en aanvullende juridische regelingen. Later speelde ook een gebrek aan capaciteit bij de Keuringsdienst een rol. Ook wordt verteld

[96] Artikel 6 in de Regeling van de Minister van Justitie en Veiligheid van 15 februari 2019, nr. 2433978, houdende regels voor de aanwijzing van een keuringsdienst voor het keuren van technische hulpmiddelen waarmee onderzoekshandelingen worden verricht in een geautomatiseerd werk (Staatscourant 2019, nr. 10713).

door iemand betrokken bij het keuringsproces dat de vertraging te maken had met 'externe factoren', zoals 'fouten in software'.
Voor Digit is het lastig dat er een keuringstermijn bestaat van vier weken die vaak meerdere keren doorlopen moet worden. Deze periode zou niet goed te rijmen zijn met de belangen die spelen in een opsporingsonderzoek.[97] Er wordt nog een ander argument genoemd waarom deze termijn niet altijd handig is, namelijk updates van software. Die zouden ervoor kunnen zorgen dat een technisch hulpmiddel niet meer bruikbaar is tegen de tijd dat het goedgekeurd is. Ook zouden deze updates de keuring (van vooral commerciële middelen) bemoeilijken. Eén van de geïnterviewden, werkzaam bij Digit, geeft aan dat een termijn van één of maximaal twee weken meer passend zou zijn.

### *5.2.6 Opnieuw keuren vs herkeuring*

Indien een technisch hulpmiddel of een onderdeel ervan zodanig wijzigt dat redelijkerwijs aangenomen kan worden dat de werking ervan niet langer voldoet aan de artikelen 8 t/m 13 dient het technisch hulpmiddel of een onderdeel ervan herkeurd te worden. Op basis van de toelichting op het Besluit lijkt herkeuring betrekking te hebben op technische hulpmiddelen die in eerste instantie zijn goedgekeurd. In de praktijk hebben zoals gezegd geen herkeuringen plaatsgevonden. Wel zijn hulpmiddelen opnieuw gekeurd. De Keuringsdienst hanteert het uitgangspunt dat een hulpmiddel opnieuw gekeurd moet worden (en dus geen herkeuring) zodra bijvoorbeeld een nieuwe functionaliteit wordt toegevoegd. Ook een verbeterde versie van een in eerste instantie niet goedgekeurd hulpmiddel is een nieuwe keuring. Eén van de geïnterviewden betrokken bij het keuringsproces, vindt herkeuring in het kader van softwareontwikkeling sowieso lastig, omdat een wijziging 'grote gevolgen kan hebben voor het geheel'. Daarom zou een middel volledig opnieuw gekeurd moeten worden, in plaats van dat enkele onderdelen gekeurd worden. Digit kijkt hier anders naar. Zij ziet het toevoegen van een functionaliteit slechts als een belangrijke uitbreiding in plaats van dat er een heel nieuw middel ontwikkeld is. Dat zou betekenen dat een volledig nieuwe keuring in de ogen van Digit niet nodig is en sprake zou kunnen zijn van een vorm van herkeuring. Het voordeel van herkeuring is bovendien dat de doorlooptijd niet maximaal vier weken maar twee weken is. Een paar geïnterviewden vanuit de Inspectie merken in dit kader op dat een aanvulling zou kunnen zijn om de code van een technisch hulpmiddel beschikbaar te stellen aan de Keuringsdienst. Bij een kleine wijziging kan dan een 'codereview' plaatsvinden en hoeft een technisch hulpmiddel niet volledig opnieuw gekeurd te worden. Vanuit een geïnterviewde betrokken bij het keuringsproces wordt echter aangegeven dat niet verwacht wordt dat 'klakkeloos' keuringstesten overgeslagen zullen worden.

### *5.2.7 Moment van keuren*

**Vooraf en achteraf keuren**
In de uitvoeringspraktijk is het niet of nauwelijks haalbaar gebleken om een hulpmiddel (vooraf) goedgekeurd te krijgen, zeker binnen de termijn waarop de inzet nodig wordt geacht binnen een tactisch opsporingsonderzoek. In het eerste jaar is het niet gelukt om een hulpmiddel vooraf goedgekeurd te krijgen (en ook niet achteraf) en in het tweede jaar is één keer een bevel afgegeven voor de inzet met een vooraf goedgekeurd middel (Inspectie JenV, 2020, p. 9; 2021, p. 9). Digit is zich bewust van het beeld dat hierdoor kan worden uitgestraald. Een geïnterviewde verzucht dat een

[97] Dit geldt op dit moment alleen voor eigen ontwikkelde hulpmiddelen. Het commerciële hulpmiddel wordt gezien als een middel waarvan de aard zich verzet tegen een keuring (zie paragraaf 5.2.7).

'waslijst' van niet goedgekeurde technische hulpmiddelen niet goed staat. Volgens deze geïnterviewde zijn de ontwikkelaars geen 'prutsers', maar gaat een groot deel van de bevindingen van de Keuringsdienst over punten waarvan Digit een andere opvatting heeft over 'wat goed genoeg' is dan de Keuringsdienst.
Indien een technisch hulpmiddel niet op tijd goedgekeurd kan worden, kan een hulpmiddel achteraf ter keuring aangeboden worden. Zo is in één van de geselecteerde inzetten een middel ingezet waaraan een extra functionaliteit was toegevoegd. Ten tijde van de inzet was dit middel niet goedgekeurd. Later, toen het hulpmiddel in een andere zaak is gebruikt en aan de aandachtspunten van de Keuringsdienst tegemoet was gekomen, is het middel goedgekeurd.

**Naar zijn aard niet (goed) te keuren**
Er kan ook besloten worden dat de aard van een technisch hulpmiddel zich tegen een keuring verzet. Tot nu toe is alleen ten aanzien van een hulpmiddel, aangeschaft bij een commerciële leverancier, besloten dat de aard ervan zich verzet tegen een keuring. Oorspronkelijk was het de bedoeling om dit hulpmiddel aan de Keuringsdienst aan te bieden. Idealiter zou het mogelijk moeten zijn om een testlicentie van een product te krijgen zodat het product gekeurd kan worden. Bij goedkeuring zou dan tot aanschaf over kunnen worden gegaan. Verteld wordt echter dat leveranciers van dit soort producten doorgaans geen testlicenties verstrekken. Dat betekent dat een product volledig moet worden aangeschaft en dat veel geld wordt betaald, ook al komt een product hoogstwaarschijnlijk niet door de keuring heen.
Voordat Digit het commerciële middel heeft aangeschaft, zijn door Digit pogingen ondernomen om te onderzoeken of het middel (goed-)gekeurd zou kunnen worden. Daaruit bleek dat dit niet goed mogelijk zou zijn. Op een gegeven moment, er was nog geen beslissing genomen over het ter keuring aanbieden van dit middel, werd Digit gevraagd om in een 'urgente zaak' een inzet te doen. Intussen was in een 'Reflectiekamer'[98] bij het Openbaar Ministerie reeds gesproken over de inzet van het middel. Na toetsing door de CTC is besloten om het middel zonder voorafgaande goedkeuring in te zetten. Tot op de dag van vandaag is het uitgangspunt dat de 'aard van het middel zich verzet tegen keuring'. Omdat dit middel bij het overgrote deel van de inzetten is gebruikt, is het gebruik ervan eerder regel dan uitzondering geworden. Dat ligt niet in lijn met hoe de wetgever het oorspronkelijk bedacht heeft.

Hoewel voorafgaand aan inzetten aangegeven is dat het commerciële hulpmiddel niet gekeurd is, en misschien wel helemaal nooit ter keuring aangeboden zal worden, wordt na afloop van een inzet door de Digit officier van justitie een definitieve beslissing genomen of de aard van een technisch hulpmiddel zich verzet tegen een keuring. In de toelichting op het Besluit (p. 42) staat beschreven dat de officier overleg zal hebben met de Keuringsdienst om te kijken of een middel 'naar verwachting aan de eisen zal voldoen'. In de praktijk heeft de Digit officier van justitie geen overleg gehad met de Keuringsdienst over deze beslissing.

Uit de interviews komt een aantal argumenten naar voren waarom het lastig zou zijn om een product van een commerciële leverancier te keuren. In de eerste plaats de updatesnelheid van het product. Verteld wordt dat de gemiddelde updatesnelheid ongeveer zes tot acht dagen is en dat een productversie na een update niet terug te zetten is naar een oudere versie. Dat betekent dat gedurende de vier weken die een inzet ten minste in beslag neemt (looptijd bevel) meerdere versies van het product worden gebruikt. De vraag is welke versie(s) de Keuringsdienst moet keuren. En

[98] Een reflectiekamer is een intern instrument binnen het Openbaar Ministerie om tegenspraak te organiseren, bijvoorbeeld met betrekking tot complexe juridische zaken.

mochten alle versies worden gekeurd, dan past dat niet bij de doorlooptijd die een keuring doorgaans in beslag neemt. De updatesnelheid is vooral ook problematisch, omdat dit product zowel voor het binnendringen als voor het uitvoeren van onderzoekshandelingen kan worden gebruikt. Vooral de updatesnelheid voor binnendringingssoftware is relatief kort. Digit zou het liefst deze twee processen willen scheiden, maar dat is niet hoe leveranciers werken. De verwachting is dat het updateprobleem een minder grote rol speelt als met het product alleen onderzoekshandelingen zouden worden verricht.
Ten tweede het bedrijfsgeheim van de leverancier. Zoals eerder al genoemd is de werking van een commercieel middel voor Digit een 'zwarte doos'. Dat betekent dat ook de Keuringsdienst geen exacte inzage kan krijgen in de wijze waarop het middel werkt. Eén concreet voorbeeld heeft betrekking op de encryptielagen die worden gebruikt. Een deel daarvan blijft geheim, terwijl de Keuringsdienst daar op basis van het keuringsprotocol wel inzage in wil hebben.
Het derde argument heeft te maken met het feit dat de leverancier ten alle tijden toegang wil hebben tot zijn product. Daardoor krijgt de Keuringsdienst geen exclusieve toegang tot het middel, hetgeen voor haar een vereiste is om de keuring te kunnen doen. Eén van de geïnterviewden vanuit Digit vertelt dat de leverancier permanente toegang wil hebben, omdat de leverancier ervoor wil kunnen zorgen dat de veiligheid van zijn systeem op orde is. Een andere geïnterviewde, werkzaam voor de politie, legt uit dat door 'monitoren van de technische werking van het systeem' de leverancier de kwaliteit van zijn product kan garanderen. Dat betekent echter wel dat de leverancier met de verzamelde gegevens mee kan lezen, hoewel contractuele afspraken zijn gemaakt dat dit niet toegestaan is. Het meelezen is problematisch, onder andere in verband met de eisen die het Besluit aan een technisch hulpmiddel stelt. Zo vertelt één van de geïnterviewden, betrokken bij het keuringsproces:

> *'Ten eerste zegt die wet van de vertrouwelijkheid van je zaakgegevens moet gewaarborgd blijven. En het correct functioneren van je systeem moet gewaarborgd blijven. Dus (…) het is toch wel een beetje fishy als je dan een partij hebt die geen opsporingsbevoegdheid heeft, waarvan je weet dat die toegang heeft tot én alle data die er langskomt én het systeem zelf. En daarmee kan doen wat die wil, zonder dat* [je] *het als politie zelfs ooit maar in de gaten hebt. Dat lijkt ons niet conform de wet. En voor onszelf specifiek, hoe kun je van ons verwachten dat wij iets keuren, terwijl we weten dat in ons keuringslab er intussen een lijntje naar buiten loopt, (…) waar iemand hetgene wat wij aan het testen zijn onderweg even kan aanpassen (…)? Dat staat haaks op wat je met een keuring nou juist doet.'*

Van de beslissing dat de aard van een hulpmiddel zich verzet tegen een keuring, wordt door de Digit officier van justitie een proces-verbaal opgemaakt. Naast het proces-verbaal van de landelijk officier van justitie, stelt Digit, sinds het moment dat besloten is dat de aard van het middel zich verzet tegen keuring, een zogenoemd waarborgen proces-verbaal op. Daarin somt zij de genomen technische waarborgen op.

### *5.2.8 Waarborgen*

De Inspectie constateert in haar tweede Verslag dat Digit-politie niet heeft vermeld 'welke (aanvullende) procedurele waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te garanderen' (Inspectie JenV, 2021, p. 15).[99] Ook op andere manieren heeft de Inspectie niet kunnen

[99] In het derde Verslag constateert zij dat niet alle voorgenomen maatregelen in het kader van aanvullende waarborgen getroffen zijn (Inspectie JenV, 2022, p. 21).

vaststellen dat Digit invulling gegeven heeft aan aanvullende waarborgen. Wel merkt zij op dat de zaaksofficier van justitie het tactisch team aanvullende waarborgen kan hebben laten nemen, maar dat die waarborgen buiten het toezicht van de Inspectie vallen (Inspectie JenV, 2021, p. 16). In de uitvoeringspraktijk kan inderdaad onderscheid worden gemaakt tussen waarborgen die vooral voor rekening komen van het technisch team (hierna technische waarborgen) en waarborgen die voor rekening komen van het tactisch team (hierna tactische waarborgen).

**Technische waarborgen**
Digit-politie heeft een document opgesteld (oktober 2020) waarin zij tien verschillende technische waarborgen noemt die het technisch team eventueel zou kunnen nemen. Een deel van die waarborgen zou kunnen worden aangemerkt als aanvullend, omdat ze geen betrekking hebben op de eisen in de artikelen 8 t/m 13 Bogw.[100] Het gaat bijvoorbeeld om het hanteren van het vier-ogen principe. Een ander deel van deze waarborgen komt overeen met één van de zojuist genoemde artikelen, bijvoorbeeld de waarborg dat het transport van gegevens beveiligd dient te worden. In dit document wordt ook een scala aan tactische maatregelen genoemd, gegroepeerd per onderzoekshandeling, die een tactisch team zou kunnen nemen. Daarin staat ook vermeld dat het de bedoeling is dat Digit-OM bij de zaaksofficier van justitie informeert naar het plan van aanpak rondom de aanvullende waarborgen en de uitvoering ervan (intern document 10). Dit plan van aanpak maakt zoals eerder gezegd inmiddels ook onderdeel uit van de toetsing door de CTC.

Naast het zojuist genoemde document heeft Digit processen-verbaal aanvullende waarborgen opgesteld waarin alle genomen technische waarborgen beschreven staan. Een deel ervan is gerelateerd aan de artikelen 8 t/m 13 Bogw. Er is onder andere aandacht voor de vraag of een plan van aanpak is gemaakt. Het waarborgenproces-verbaal is niet direct na afloop van de eerste inzet opgesteld. Eén van de geïnterviewden vanuit Digit legt uit dat dit pas op een later moment gebeurd is, omdat in eerste instantie verondersteld werd dat het hulpmiddel ter keuring aangeboden zou worden.

**Tactische waarborgen**
Tactische waarborgen zijn bedoeld om gegevens verkregen met het niet gekeurde technisch hulpmiddel te kunnen verifiëren. Een van de geïnterviewde zaaksofficieren legt uit dat dit soort verificatiemomenten belangrijk zijn.

> *'Ik kan* [als zaaksofficier van justitie] *verantwoording afleggen voor de afwegingen die zijn gemaakt om het middel toe te passen, niet voor hoe het is gegaan. Maar ik heb (..) wel te maken met de resultaten ervan, dus ik moet ergens wel een waarborg hebben over dat het een berichtje is geweest van verdachte 1. (…). Dat is uiteindelijk wat een rechtbank natuurlijk ook moet kunnen beoordelen. (..). Dus ik moet wel kunnen instaan voor de betrouwbaarheid van de resultaten. En op het onderdeel (…) hoe wordt dat technisch gedaan?,* [dat weet ik niet] *(…), maar (..) daar omheen* [moet ik] *natuurlijk wel zorgen voor waarborgen voor de betrouwbaarheid van de resultaten.'*

Ook het gebruik van en het afleggen van verantwoording over deze waarborgen is pas op een later moment geformaliseerd. Eén van de geïnterviewden werkzaam bij Digit legt uit dat in de begintijd (toen nog onduidelijk was of het hulpmiddel ter keuring

[100] De Inspectie definieert aanvullend als aanvullend op de standaard in het Besluit voorgeschreven maatregelen (Inspectie JenV, 2021, p. 14).

aangeboden zou worden) wel is bedacht dat verificatiemomenten nodig zouden zijn, zodat geen twijfel zou kunnen bestaan over de integriteit van de gegevens. Dat zou toen ook al ter sprake zijn geweest bij de CTC.[101] Op een later moment zijn de verificatiemomenten 'meer geprofessionaliseerd'. Vanaf dat moment is van het tactisch team min of meer verlangd om een verificiatieproces-verbaal op te stellen. Dat was belangrijk, omdat Digit in de rechtszaal geen vragen zal beantwoorden over het technisch hulpmiddel, omdat anders 'te veel informatie wordt prijsgegeven over tactieken'.
Welke verificatiemethode(s) worden gekozen is onder andere afhankelijk van de onderzoekshandelingen die Digit verricht.[102] Een verificatiemethode betreft doorgaans één of meerdere (bijzondere) opsporingsmethoden die het tactisch team uitvoert, gelijktijdig of vlak na een inzet van Digit. Kerndoel van die methode(s) is vast kunnen stellen dat het binnengedrongen geautomatiseerde werk bij de verdachte hoort. Daarnaast kan in een groot deel van de gevallen ook iets worden gezegd over de inhoud van de gegevens, bijvoorbeeld of gegevens verzameld met behulp van verschillende (bijzondere) opsporingsmethoden met elkaar overeenkomen. Eén van de gebruikte verificatiemethodes is het in beslag nemen van het geautomatiseerde werk van de verdachte. Op die manier kunnen de door Digit verzamelde gegevens vergeleken worden met de gegevens die (nog) op het in beslaggenomen geautomatiseerde werk staan. Een nadeel van deze methode is dat de politie niet altijd zal kunnen beschikken over (de benodigde gegevens op) het geautomatiseerde werk. Een andere verificatiemethode is de inzet van een observatieteam. Dit team kan onder andere gebruikt worden om in de gaten te houden op welke momenten een verdachte zijn geautomatiseerde werk gebruikt. Die informatie kan vervolgens worden vergeleken met de momenten waarop Digit gegevens ontvangen heeft vanuit het geautomatiseerde werk.

**Impact niet (goed-)gekeurd hulpmiddel**
Over de vraag in hoeverre het gebruik van een niet (goed-)gekeurd hulpmiddel invloed heeft op het oordeel van de rechter in een strafzaak kunnen op het moment van schrijven van dit rapport géén uitspraken worden gedaan. In het tweede deel van de evaluatie kan dit onderwerp hopelijk uitgebreider aan de orde komen. Wel kan iets worden gezegd over de invloed hiervan op de keuze van controlerende actoren (zaaksofficier en een rechter-commissaris) om uiteindelijk wel of niet met dit hulpmiddel te mogen werken.
Voor beide rechters-commissarissen die in het kader van dit onderzoek gesproken zijn, is het niet direct een probleem dat de politie gebruik maakt van een niet (goed-)gekeurd technisch hulpmiddel. Dat heeft vooral te maken met de criteria (onder andere de proportionaliteit) aan de hand waarvan een rechter-commissaris de inzet dient te toetsen. Eén van hen legt uit:

> *'(..) kijk, ik heb wel eens een zaak gehad met een goedgekeurd* [technisch] *hulpmiddel. Nou, die is er dan toevallig. Maar over het algemeen is het* [de inzet] *met een niet goedgekeurd middel. (...) Uiteindelijk maakt dat voor mijn toets niet echt een heel groot verschil (…). Ik wil vooral weten, en dat is dan ook in het kader van de proportionaliteit: wat doet zo'n middel nu? Bijvoorbeeld, wat voor risico's levert het op? Maar dan vooral niet de risico's voor het onderzoek* an sich*, maar meer voor het geautomatiseerde werk, of voor derden. Heeft het daar invloed op?*

[101] Tijdens deze evaluatie hebben de onderzoekers zeer summier zicht gekregen op de inhoudelijke beslissingen van de CTC. Er was géén toestemming om concrete inhoudelijke beslissingen in te zien. Geprobeerd zal worden om deze in het kader van het tweede deel van de evaluatie wel in te zien.
[102] In verband met de afscherming van onderzoeksmethoden zal in deze paragraaf geen uitputtend overzicht gegeven worden over verificatiemethodes die in een opsporingsonderzoek worden toegepast.

*Kijk, het Openbaar Ministerie wil bewijs verzamelen en dat moet betrouwbaar bewijs zijn. Dat is niet de toets die ik aanleg. Ik moet veel meer de rechtmatigheid toetsen (…).'*

Een andere geïnterviewde rechter-commissaris geeft aan vooral te kijken naar de vraag of op het moment dat de rechter-commissaris zich over een verzoek buigt het te verantwoorden is dat Digit gegevens uit een geautomatiseerd werk haalt en niet over de manier waarop dat gebeurt (met een niet-gekeurd middel).
Ook binnen het tactisch opsporingsonderzoek wordt de inzet van een niet (goed-)gekeurd middel niet als problematisch gezien. De eerder besproken verificatiemethoden spelen daarbij een belangrijke rol. Een geïnterviewde zaaksofficier vertelt dat het geen verschil maakt dat er met een niet gekeurd middel wordt gewerkt, behalve dat de geïnterviewde 'extra scherp' is in het onderzoek.

*'Maar ja, het is natuurlijk wel iets dat je sowieso heel scherp houdt. Ja, kijk, vergelijk het met als je iemand wilt pakken die te hard rijdt en je hebt gewoon een geijkt meetapparaat en het is alleen maar kijk, het staat erop, we zijn klaar. Prima. Maar als je van te voren weet van dat apparaat, dat is niet voldoende, dan ga je ook omstanders horen. Hoe hard reed die auto, kon je daar een inschatting van maken? Dus je gaat er dingen omheen creëren en zo hebben we dat gedaan.'*

Dat er geen belemmeringen worden ervaren neemt niet weg, aldus een paar geïnterviewden, dat het gebruik van een niet (goed-)gekeurd middel mogelijk discussie op kan leveren in de rechtszaal. Voor deze geïnterviewden kwam het goed uit dat bij het opsporingsonderzoek waarbij zij betrokken waren het 'meest relevante deel van het bewijs' verkregen is door inbeslagname van een telefoon. Weliswaar was een deel van die gegevens ook al met behulp van de hackbevoegdheid verzameld, maar in beslagname van bewijs levert wat dat betreft 'een slag zekerder bewijs' op, omdat 'beslag gewoon beslag' is en voor iedereen te controleren. Er hoeft dan verder niet gesproken te worden of een middel wel of niet goedgekeurd is en of het nog goedgekeurd kan worden. 'Al die vragen zijn niet meer relevant als je het gewoon via de weg van het beslag doet', aldus één van hen.

### *5.2.9 Twee perspectieven*

In het voorgaande heeft de aandacht zich gericht op de vraag hoe het keuringsproces in de praktijk vorm heeft gekregen. Van de twee actoren betrokken bij het keuringsproces ervaart Digit dit proces als problematisch. Dat heeft te maken met het feit dat de belangrijkste twee betrokken actoren (Keuringsdienst en Digit) vanuit verschillende perspectieven naar het keuringsproces kijken en deze perspectieven botsen in de uitvoeringspraktijk soms met elkaar. In de komende paragrafen worden deze twee perspectieven daarom nader uiteengezet: het perspectief van de keuringsdienst en het perspectief van Digit. Binnen het perspectief van waaruit de Keuringsdienst kijkt ligt de nadruk vooral op wet- en regelgeving. Binnen het perspectief van waaruit Digit kijkt, staat vooral de uitvoerbaarheid en noodzakelijkheid van alle regels centraal. Belangrijk om op te merken is dat deze perspectieven de zienswijze van de twee actoren weergeven en niet de zienswijze van het WODC. Wel heeft het WODC deze tweedeling gemaakt.

**Perspectief Keuringsdienst**
Zoals eerder duidelijk is geworden, volgt de Keuringsdienst het Keuringsprotocol dat op basis van het Besluit en toelichtende teksten is opgesteld. De regels in het Besluit

zijn onder andere geformuleerd om de betrouwbaarheid, integriteit en herleidbaarheid van bewijsmateriaal te kunnen waarborgen. Het Besluit vindt zijn grondslag in artikel 126ee Sv. Hoewel bij het opstellen van het keuringsprotocol een interpretatieslag moest worden gemaakt en ook nog steeds wordt gemaakt (in dat opzicht zijn niet alleen de regels leidend) vertelt één van de geïnterviewden van de Keuringsdienst dat de Keuringsdienst in principe niet zelf bepaalt aan welke eisen een technisch hulpmiddel moet voldoen. Dat heeft de wetgever zo aangegeven:

> *'Ons* [keurings]*proces zit eigenlijk vrij simpel in elkaar. Als de wetgever stelt, kastjes moeten zwart zijn, en ze* [Digit] *komen met rode kastjes aan, dan keuren wij die af. Het is niet dat wij zelf verzinnen, nou wij vinden rode kastjes niet mooi. Nee, het is, wij toetsen dat aan de wet. Dat is zoals wij hier werken.'*

De Keuringsdienst keurt een hulpmiddel alleen goed als het aan *alle* eisen van het Keuringsprotocol voldoet. Zo is dat ook deels vastgelegd in het Besluit (artikel 14, lid 2 Bogw). In praktijk betekent dit dat Digit bij de inzet van een goedgekeurd middel ook een aantal vervangende waarborgen dient te implementeren. Voor de Keuringsdienst is het belangrijk dat aan *alle* eisen wordt voldaan, omdat op die manier de betrouwbaarheid, integriteit en herleidbaarheid van gegevens gegarandeerd kunnen worden. De Keuringsdienst wil bij de rechter kunnen verklaren dat niks veranderd is aan de gegevens die bij een verdachte opgehaald zijn. Pas als aan alle eisen is voldaan, dan kan de Keuringsdienst die garantie geven. Bij Digit zorgt deze werkwijze voor onbegrip. Volgens één van de geïnterviewden die betrokken is bij de keuringen lijkt Digit echter niet altijd voldoende kennis te hebben over het Besluit en over het waarom van het bestaan van een keuring. Deze geïnterviewde vindt het min of meer logisch dat Digit de regels uit het Besluit volgt. Eén andere geïnterviewde ook betrokken bij de keuringen, zegt te snappen dat de keuring voor Digit een 'blok aan het been is'. Toch meent deze geïnterviewde dat het voldoen aan alle eisen ingewikkeld zal blijven, ook al zou de Keuringsdienst het voor Digit gemakkelijker maken. Deze geïnterviewde merkt op dat 'de wet gewoon lastig is', maar dat uiteindelijk zeker moet zijn waar data vandaan komen en 'dat er niet mee geknoeid is'.

Een keuringsrapport van de Keuringsdienst heeft géén betrekking op wat er met gegevens gebeurt op de technische infrastructuur van de politie. Hoewel dat in lijn ligt met het Besluit, vraagt één van de geïnterviewden, betrokken bij het keuringsproces, zich af wie dan wel de technische infrastructuur keurt. Volgens deze geïnterviewde is het belangrijk dat dat gebeurt, omdat de technische infrastructuur de plek is waar het bewijsmateriaal is opgeslagen. Een andere geïnterviewde, ook betrokken bij het keuringsproces, begrijpt tegelijkertijd dat Digit rondom die technische infrastructuur 'allerlei dingen aan het ontwikkelen is en dat nog niet mee wil geven' aan de Keuringsdienst.
In de uitvoeringspraktijk blijkt dat het beperkte zicht van de Keuringsdienst op de technische infrastructuur van Digit de keuring kan compliceren. Een voorbeeld hiervan heeft betrekking op een hulpmiddel ontwikkeld om e-mails binnen te halen. De eerste eis uit het Keuringsprotocol is dat het technisch hulpmiddel automatisch en doorlopend (meta-)gegevens logt over het functioneren van het technisch hulpmiddel. De Keuringsdienst oordeelde tijdens één van de keuringen van dit technisch hulpmiddel dat niet elke logregel werd voorzien van een timestamp en dat er géén onweerlegbare logging was van de *commandline* (dat laatste betekent dat er geen logging is van de opdrachten die Digit aan het technisch hulpmiddel geeft). In de ogen van Digit waren deze punten wel geregeld, namelijk op de eigen technische infrastructuur van Digit. Eén van de geïnterviewden werkzaam bij Digit legt uit dat in de eigen omgeving van

Digit logging gestandaardiseerd en gecentraliseerd plaatsvindt inclusief het toekennen van een timestamp. De Keuringsdienst ziet die omgeving echter niet, omdat zij in een eigen testomgeving werkt. Die omgeving is dus geen onderdeel van de keuring.[103] Digit is voornemens om bij het aanbieden van volgende technische hulpmiddelen een aantal aanpassingen door te voeren waardoor de omgeving rondom het technisch hulpmiddel die de Keuringsdienst ziet meer lijkt op de omgeving van Digit. Vanuit Digit wordt ook uitgelegd dat de commando's middels *screen recording* worden bijgehouden in de eigen omgeving van Digit. De Inspectie JenV heeft overigens vastgesteld dat *screen recording* niet altijd op orde is (Inspectie JenV, 2021, p. 11).[104] Voor de Keuringsdienst is het problematisch dat Digit een aantal zaken binnen haar eigen omgeving organiseert, omdat die omgeving géén onderdeel uitmaakt van de keuring. Daardoor kan de Keuringsdienst geen uitspraken doen over de integriteit van het hulpmiddel.

**Perspectief Digit**

Net zoals de Keuringsdienst vindt Digit het belangrijk dat bewijs dat verzameld wordt betrouwbaar, herleidbaar en integer is. Digit kijkt echter vanuit een ander perspectief naar dit vraagstuk. Dat betekent dat zij vooral de uitvoerbaarheid en de noodzakelijkheid van sommige bestaande regels en eisen centraal stelt. In de komende paragraaf wordt dit perspectief nader uiteengezet. Allereerst wordt aandacht besteed aan de uitvoerbaarheid van de regels. Ingegaan wordt op de vraag waarom in meer algemene zin de regels uit het Besluit lastig worden gevonden (te veel gebaseerd op een al bestaand Besluit). Daarna wordt de ingewikkeldheid met betrekking tot een concrete keuringseis toegelicht. Vervolgens richt de aandacht zich op de noodzakelijkheid van deze regels en eisen. Daarbij wordt ingegaan op de wens om meer uit te kunnen gaan van risicoanalyses en bewijswaardes.

*Oud Besluit als uitgangspunt*

Het Besluit onderzoek in een geautomatiseerd werk (Besluit) is gebaseerd op het Besluit technische hulpmiddelen strafvordering ('oude' Besluit). Dat het 'oude' Besluit een belangrijkste inspiratiebron is geweest, levert voor de Keuringsdienst weinig problemen op. Het grootste deel van de eisen is 'goed te begrijpen', 'logisch' en 'prima uit te leggen', zeker wanneer het belangrijk is de betrouwbaarheid en herleidbaarheid van gegevens te waarborgen. Er zouden niet zomaar een paar eisen geschrapt kunnen worden. Eén van de geïnterviewden, betrokken bij het keuringsproces, zegt:

> *'Wij vinden, als je (…) wilt voldoen aan die wet, dus als je echt zegt hetgeen waar jullie straks mee naar de rechter gaan en waar wij dus voor instaan, die klopt ook, als je wilt dat dat ook ergens op slaat, dan zijn dit hele redelijke technische eisen.'*

In tegenstelling tot voor de Keuringsdienst vormen de gestelde eisen, geïnspireerd op het 'oude' Besluit, voor Digit wel een knelpunt. Eén van de belangrijkste redenen hiervoor is dat de middelen die Digit gebruikt niet goed zouden passen in de situaties waarvoor het 'oude' Besluit (vooral) ontworpen is. In de beginperiode, toen mee werd gedacht over het Besluit, heeft niet iedereen zich dat direct gerealiseerd. Eén van de geïnterviewde opsporingsfunctionarissen vertelt:

[103] Eén van de betrokkenen bij het keuringsproces wijst erop dat in de toekomst wellicht andere teams dan Digit de bevoegdheid gaan inzetten. Die werken in weer een andere (eigen) omgeving.

[104] In haar derde Verslag wordt geconstateerd dat de volledigheid van de vastgelegde beeldschermopnames in 2021 'sterk is verbeterd' (Inspectie JenV, 2022, p. 27).

*'Tweeënhalf/drie jaar terug voordat we überhaupt begonnen, hadden we echt nog niet zo'n blik over hoe je met* [Digit-]*technische hulpmiddelen om moet gaan. En werd (…), als ik naar mezelf kijk, vooral het voordeel gezien van: oh, dan kan je een technisch hulpmiddel keuren, hoef je niet uit te leggen hoe je het* [de inzet] *hebt gedaan. (…). Ik denk alleen* [dat] *onvoldoende onderkend* [is] *dat technische hulpmiddelen niet meer alleen fysieke apparaatjes zijn.*[105] *En dat je dus in een hele andere dynamiek weer terecht komt.'*

Eén van de aspecten van die andere dynamiek is dat er in het Besluit vanuit zou worden gegaan dat Digit volledige controle heeft over de omgeving waarin een technisch hulpmiddel geplaatst wordt, vergelijkbaar met een baken waarvan de politie zelf de tijd kan instellen. Vanuit Digit wordt verteld dat Digit niet de volledige controle heeft over alle randvoorwaarden waaronder een inzet plaatsvindt. Vanuit Digit wordt in dat kader gesproken over een 'dynamische en vijandige omgeving' waarin zij moet werken. Tijdens deze evaluatie is voor de onderzoekers niet volledig duidelijk geworden waar precies het onderscheid ligt tussen dynamisch en vijandig. Een vijandige een dynamische omgeving heeft in elk geval betrekking op het niet onder controle hebben van de omgeving en de handelingen die een verdachte daarbinnen verricht. Digit kan bijvoorbeeld niet zelf te tijd van het geautomatiseerde werk van de verdachte instellen of bepalen over welke soort verbinding de verdachte gegevens binnenhaalt. Daarnaast heeft Digit géén invloed op wat een verdachte met zijn of haar geautomatiseerde werk doet. Als deze zijn geautomatiseerde werk uitzet, dan is dat problematisch voor de tijdsregistratie en de logging die eigenlijk continu zou moeten plaatsvinden. Vervolgens zou het dan weer ingewikkeld zijn om aan te tonen dat bewijs herleidbaar en betrouwbaar is. Het vinden van een oplossing hiervoor blijkt lastig te zijn. Verder is onduidelijk hoe de omgeving van de verdachte er precies uit ziet. Er kan in beperkte mate een voorverkenning worden gedaan hoe een geautomatiseerd werk eruit ziet, maar Digit weet pas echt hoe de omgeving eruit ziet als zij binnen is.

*Ingewikkelde keuringseisen*

Naast het feit dat het Besluit lastig is in meer algemene zin, vindt Digit ook een aantal specifieke eisen ingewikkeld. Eén daarvan heeft betrekking op de transportbeveiliging van gegevens, dat wil zeggen de beveiliging van gegevens die van de ene plek naar de andere plek worden verstuurd. Zoals eerder beschreven gelden hiervoor de eisen die het NCSC stelt, omdat die eisen gebruikt worden om invulling te geven aan het begrip stand der techniek.[106] Vanuit Digit wordt verteld dat het niet in alle gevallen mogelijk is om aan die eisen te voldoen. Digit kan afhankelijk zijn van de beveiliging van de verbinding waarover een verdachte gegevens binnenhaalt. Op het moment dat die niet voldoet aan de eisen van het NCSC, wordt een technisch hulpmiddel dat die verbinding gebruikt op dit punt afgekeurd. Om het hulpmiddel goedgekeurd te krijgen moet de transportbeveiliging van de verdachte op orde zijn, maar Digit heeft daar geen invloed op. Dat betekent dat géén gebruik kan worden gemaakt van het hulpmiddel en dat overgegaan moet worden op een handmatige inzet. Verschillende geïnterviewden verbazen zich hierover. Een voorbeeld hiervan is het ophalen van e-mails van een e-mailserver. De wijze waarop verbinding kan worden gelegd met deze server is afhankelijk van de instellingen die door de eigenaar zijn gemaakt op de e-mailserver.

[105] In het 'oude' Besluit wordt een aantal concrete voorbeelden genoemd van fysieke hulpmiddelen (Besluit technische hulpmiddelen strafvordering, p. 14-15). In het 'oude' Besluit wordt ook duidelijk dat rekening is gehouden dat software gekeurd kan worden (Besluit technische hulpmiddelen strafvordering, p. 25).

[106] Op dit moment (april 2022) wordt uitgegaan van de volgende richtlijnen: 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)' van het Nationaal Cyber Security Centrum. De Keuringsdienst hanteert het criterium voldoende/goed.

Het is daarom mogelijk dat de verbinding naar de mailserver toe niet voldoet aan de eisen die worden gesteld door het NCSC. In deze situatie kan Digit dus niet volgens de gestelde criteria e-mails ophalen van de server. Een handmatige inzet zou in dit geval een oplossing kunnen bieden, omdat dan direct zonder technisch hulpmiddel de e-mails van de mailserver worden gehaald. Maar ook dat kan tot problemen leiden, omdat voor het binnenhalen van e-mails hoogstwaarschijnlijk een script nodig is, aldus één van de geïnterviewden, en een script is in de ogen van de Inspectie een technisch hulpmiddel waardoor keuring nodig is. In dat opzicht zit Digit klem tussen de Keuringsdienst en de Inspectie. Bovendien druist het binnenhalen van gegevens over een onbeveiligde verbinding in tegen het Besluit: er kan immers niet gegarandeerd worden dat derden niet de gegevens hebben kunnen inzien en of hebben kunnen wijzigen.
Volgens één van de geïnterviewden, betrokken bij het keuringsproces, zou het voorgaande probleem zich overigens niet of nauwelijks voordoen, omdat het niet vaak voor zal komen dat een verdachte gebruik maakt van een slechte verbinding. Een andere geïnterviewde van Digit bevestigt dat het tot nu toe nog niet is voorgekomen dat Digit helemaal niets kon doen, omdat de NCSC-eisen in de weg zaten. Toch vreest deze geïnterviewde dat deze eis in de toekomst voor problemen zal zorgen. Bovendien zou deze eis soms een rol spelen bij de beslissing om wel of geen gehoor te geven aan een verzoek vanuit een tactisch team voor een inzet door Digit. Bovenstaande argumentatie zou aan de tactische teams 'niet uit te leggen zijn'.

Het gevolg van de als ingewikkeld ervaren keuringseisen is dat Digit het gevoel heeft dat zij vooral producten voor de Keuringsdienst aan het ontwikkelen is. Daardoor ontstaan 'onnodige grote middelen'. Dit wordt als problematisch ervaren, omdat op die manier de ontwikkeling van een technisch hulpmiddel extra tijd kost, tijd die er binnen een opsporingsonderzoek niet altijd is. Naast de tijd die het extra inbouwen in beslag neemt, zou de kwaliteit van het hulpmiddel achteruit gaan. Eén van de geïnterviewden, werkzaam bij Digit, legt uit dat de werking van het hulpmiddel niet wordt aangetast, maar dat wel sprake is van 'vertroebeling' van gegevens. Dat meerdere onderdelen hetzelfde werk doen, betekent dat er meer gegevens zijn (bijvoorbeeld unieke ID's die gecreëerd dienen te worden) en dat zou de herleidbaarheid van gegevens niet ten goede komen (door de wirwar aan verzamelde ID's die is ontstaan). Volgens deze geïnterviewde wordt een hulpmiddel 'nu heel ingewikkeld in het gebruik'. Er dienen meer updates plaats te vinden en het onderhoud ervan is complexer geworden. Een andere geïnterviewde, ook werkzaam bij Digit, merkt op dat elke stukje code dat wordt toegevoegd, de kans op fouten vergroot waardoor problemen kunnen ontstaan. Bovendien zouden hulpmiddelen hierdoor zwaarder worden waardoor een 'hulpmiddel zou schreeuwen' dat het afkomstig is van de politie. In dat opzicht zou een hulpmiddel alleen moeten bestaan uit stukjes code die strikt noodzakelijk zijn. Wat echter als strikt noodzakelijk moet worden beschouwd, daarover verschillen Digit en de Keuringsdienst van mening. Het idee dat een product alleen wordt gemaakt voor de Keuringsdienst wordt breder herkend. Toch zou dat vooral in de beginperiode een extra inspanning vergen, aldus één van de betrokkenen bij de keuringen:

> *'Ik denk (…): puur het binnenhalen van die data is vrij makkelijk. Maar om het zo te maken dat je ook (…) kan zeker stellen dat er niet mee geknoeid kan worden (..), dat is inderdaad werk. Maar dat is dus de prijs dat we willen dat het ook in de rechtszaal gebruikt kan worden. Want doe je dat niet, dan heb je data en dan kun je niet uitleggen waarom dat ooit op het device van die verdachte heeft gestaan of wanneer (…)? (…) Die eerste paar keer kost dat heel veel moeite omdat het*

[ontwikkelen van een technisch hulpmiddel] *voor hun* [voor Digit] *ook nieuw was. (…) En als het goed is, als ze dat vaker hebben gedaan, dan hebben ze (…) al een aantal van dit soort componenten. Of in ieder geval weten ze wat er precies verwacht wordt en doen ze dat gelijk goed. Ook dat gaat natuurlijk steeds efficiënter, maar het is wel een ding als je bijvoorbeeld (…) straks ook inzetteams vanuit de regio's of de eenheden krijgt, dan moet je, dat gaat natuurlijk ook weer een leercurve worden. Dus dat, ja, daar hebben ze (…) gelijk in. Het is natuurlijk meer werk.'*

*Risicoanalyse*

Binnen het perspectief van waaruit Digit kijkt vindt men ook dat niet alle regels en eisen noodzakelijk zijn. Een belangrijke reden hiervoor heeft te maken met het feit dat zij vindt dat bij het beoordelen van een hulpmiddel meer uit zou moeten worden gegaan van een risicoanalyse, vergelijkbaar met de waarschijnlijkheidsanalyses waarmee het Nederlands Forensisch Instituut (NFI) werkt (Nederlands Forensisch Instituut, z.d.).[107] Als dit soort analyses een plek zouden kunnen krijgen binnen het werk van Digit, dan kan ook gewerkt worden met hulpmiddelen die door Digit als 'goed genoeg' zijn bestempeld, in plaats van volledig goedgekeurd. Dat geldt bijvoorbeeld voor een technisch hulpmiddel dat een e-mailprotocol bevat dat als 'weinig robuust' wordt gezien, zo vertelt één van de geïnterviewden van Digit. In theorie is het mogelijk dat bij het gebruik van dit protocol enkele e-mails niet binnenkomen bij Digit. Dat zou echter alleen kunnen gebeuren als een verdachte een e-mail naar een andere map verplaatst precies op hetzelfde moment dat Digit die e-mail aan het binnenhalen is. Omdat e-mails binnen het tijdsbestek van een paar seconden worden opgehaald, acht Digit de kans zeer klein dat een e-mail gemist wordt. Om die reden zou het niet problematisch moeten zijn om een technisch hulpmiddel in te zetten dat gebruik maakt van dit protocol.

Een belangrijk argument dat vanuit Digit wordt genoemd waarom een risicoanalyse passend wordt geacht is dat Digit haar werk in een bepaalde context uitvoert. Zo zijn de technische hulpmiddelen die tot nu toe ontwikkeld zijn maatwerkproducten (ze worden voor één inzet gebruikt) en ze worden gebruikt door een specialistisch team dat bovendien heimelijk haar werk doet. Beide aspecten moeten er volgens Digit voor zorgen dat het maken van een risicoanalyse afdoende zou moeten zijn. Twee geïnterviewden vertellen en gaan in op de eerder beschreven beveiligingseisen voorgeschreven door het NCSC:

*'Geïnterviewde 1 geeft aan dat die* [eisen die aan de verbinding worden gesteld] *niet in verhouding staan tot de aanvalsscenario's. Deze beveiligingseisen zijn misschien nodig als er een technisch hulpmiddel ontwikkeld wordt dat de komende vijf jaar grootschalig en continu door alle TDO'ers* [Team Digitale Ondersteuning] *in Nederland moet worden gebruikt. Maar dat is bij de huidige technische hulpmiddelen die ontworpen worden niet het geval. Die worden voor één zaak ingezet en bij die zaak wordt altijd een afweging gemaakt wat de risico's zijn in relatie tot de mogelijke aanvallen die worden gepleegd.'*

Ook het soort opsporingsonderzoeken waarbinnen Digit een inzet doet maken onderdeel uit van de context. Eén van de geïnterviewden vanuit Digit legt uit dat er een verschil is tussen een kwetsbaarheid die in theorie bestaat (beschreven in een wetenschappelijk paper) en een kwetsbaarheid die in de praktijk daadwerkelijk benut

[107] Volgens de Keuringsdienst zou al worden uitgegaan van een risicoanalyse, omdat in het keuringsprotocol opgenomen staat dat het technisch hulpmiddel *voldoende* beschermd dient te zijn.

kan worden. Het NCSC, en als gevolg daarvan de Keuringsdienst, gaat bij haar richtlijnen uit van theoretische kwetsbaarheden, aldus deze geïnterviewde.[108] Dit soort kwetsbaarheden zouden echter alleen door natiestaten benut kunnen worden. De verdachten die in de onderzoeken van Digit centraal staan zouden doorgaans niet interessant zijn voor zulke grote natiestaten. Bovendien beschikken de verdachten in de onderzoeken waarin de hackbevoegdheid wordt ingezet over het algemeen niet over 'technische kennis en vergaande technische middelen' (hierop bestaan overigens uitzonderingen – dit betreft vooral de maatwerkinzetten). Daarom zou een theoretische kwetsbaarheid niet het uitgangspunt moeten zijn. In plaats daarvan kan eerst gekeken worden of een theoretische kwetsbaarheid in de praktijk (bij inzetten zoals Digit die uitvoert) uitgebuit kan worden.
Eén van de betrokkenen bij het keuringstraject herkent de manier waarop naar de eisen van het NCSC gekeken zou kunnen worden. Transportbeveiliging die niet volledig aan de eisen van het NCSC voldoet zal er niet voor zorgen dat iedereen direct mee kan lezen. Toch is het belangrijk om als Keuringsdienst 'ergens vanuit te gaan', in dit geval de NCSC-beveiligingsrichtlijnen. Deze geïnterviewde legt uit dat, hoewel niet iedereen zomaar mee kan lezen, nu eenmaal niet uitgesloten is dat derden, bijvoorbeeld de National Security Agency (NSA) in Amerika (hypothetisch voorbeeld), mee hebben kunnen lezen. Om die reden zal de Keuringsdienst, als niet volledig aan de eisen ten aanzien van transportbeveiliging wordt voldaan, nooit in de rechtszaal kunnen verklaren dat gegevens die met het technisch hulpmiddel verzameld zijn volledig betrouwbaar, herleidbaar en integer zijn.
Vanuit een geïnterviewde van de Inspectie bestaat begrip voor zowel het standpunt van Digit (beveiligingseisen zijn te streng) als voor het standpunt van de keuringsdienst (er moet een referentiekader zijn). Aangegeven wordt dat ten aanzien van beide opvattingen misschien winst behaald kan worden door een hulpmiddel 'niet te rigide af te keuren, maar toch iets open te laten', door bijvoorbeeld een vervangende waarborg toe te staan die later ingebouwd mag worden afhankelijk van de wijze waarop Digit het hulpmiddel heeft gebruikt. Het is vervolgens aan Digit om uit te leggen waarom een theoretische kwetsbaarheid zich in het specifieke geval in de praktijk niet heeft voorgedaan.

*Bewijswaarde*
Naast het meer centraal stellen van risicoanalyses, wordt binnen het perspectief van waaruit Digit kijkt het denken vanuit bewijswaardes gemist. Verschillende geïnterviewden geven aan dat de wijze waarop de keuring op dit moment plaatsvindt er vanuit gaat dat bewijs dat met de hackbevoegd verzameld is, 100% betrouwbaar moet zijn. Een verdachte zou bij wijze van spreken alleen op basis van dit bewijs veroordeeld moeten kunnen worden. Dat zou ook de reden zijn dat een technisch hulpmiddel aan de hoogst haalbare eisen moet voldoen. Vanuit Digit wordt uitgelegd dat het in de praktijk van de rechtspraak niet zo werkt. Niet alle gegevens die met behulp van een (bijzondere) opsporingsbevoegdheid worden verzameld, worden gebruikt als bewijs, bijvoorbeeld in het geval van sturingsinformatie. Mochten de gegevens wel worden gebruikt als bewijs, dan vindt de veroordeling van een verdachte doorgaans plaats op basis van verschillende stukjes bewijs, dikwijls verzameld met behulp van diverse (bijzondere) opsporingsbevoegdheden. Niet elk stukje van dit bewijs zal beschikken over dezelfde bewijswaarde.[109] Eén van de geïnterviewde opsporingsfunctionarissen legt uit:

[108] Een betrokkene bij het keuringsproces merkt op dat de richtlijnen vanuit het NCSC '*common practice*' zijn.
[109] Eén van de betrokkenen bij het keuringsproces geeft aan dat de redenering met betrekking tot bewijswaarde een te beperkte is. Bewijswaarde gaat niet over technische betrouwbaarheid (waarnaar een keuringsdienst kijkt). Technische of forensische betrouwbaarheid is een onderdeel van een oordeel over een

*(…) als je kijkt hoe in een strafzaak een rechter met bewijs omgaat, dan heeft iets een bepaalde bewijskracht. En dat kan soms heel hoog zijn en soms is dat extreem laag. Op het moment dat ik een getuige heb die knettergek is (…) en die heeft een getuigenverklaring afgelegd over marsmannetjes (…), maar ook dat hij op een bepaalde avond, een bepaalde auto met een bepaald kenteken heeft gezien. Dat is niet een getuige waar (…)* [een officier van justitie] *een hele grote bewijskracht aan wil toekennen. (…). Als (…)* [een officier van justitie] *daar tegenover zet, een verbalisant, die in privé tijd, broodnuchter, een zelfde auto met een bepaald kenteken zag, (…)* [dan heeft de officier van justitie] daar *een getuigenverklaring die (…)* [een officier van justitie] *veel betrouwbaarder vindt. Maar dat betekent niet dat wat die knettergekke getuige (…) verteld heeft, niet op enige manier wel kan meewegen in die strafzaak. Het zal bewijs zijn waar (…)* [een officier van justitie] *heel veel bewijs omheen wil verzamelen, steunbewijs, om het toch te kunnen gebruiken (..). Nou, die setting heb je ook in digitale zin. Ik kan mij voorstellen dat we op een manier met Digit ergens informatie verzamelen, waarvan je denkt dit is verdraaide krakkemikkig van hoe dit in elkaar heeft gezeten. Maar die informatie is er wel. Of, we hebben een stuk techniek gebruikt waarvan we niet kunnen vertellen wat het precies doet. (…) Beide zijn situaties waarvan je als rechter moet zeggen, dat is dan geen bewijs dat ik als groot ronkend bewijsmiddel wil gebruiken om aan iemands veroordeling ten grondslag te leggen. Maar het kan wel ontzettend helpen in de richting van een onderzoek, of misschien is het 1 van de 100 bouwsteentje om te zeggen dat iets wel op een bepaalde manier is gegaan.'*

Van gegevens die met een technisch hulpmiddel verzameld worden, dienen de betrouwbaarheid, integriteit en herleidbaarheid gegarandeerd te kunnen worden. Het beoordelen daarvan is de opdracht die de Keuringsdienst van de wetgever heeft meegekregen. Meerdere geïnterviewden vanuit Digit plaatsten echter vraagtekens bij die opdracht. Zo wordt de vraag gesteld of deze strenge eisen ook worden gesteld aan andere organisatieonderdelen binnen de politie die zich bezighouden met netwerkzoekingen en '*open source intelligence*'.[110] Bij deze activiteiten zou het om dezelfde soort gegevens gaan als bij het werk van Digit. Ook vragen geïnterviewden zich af in hoeverre dit soort eisen (inclusief de keuring die erbij hoort) in het buitenland aan de politie worden gesteld. Enkele geïnterviewden vertellen dat Nederland het enige land zou zijn dat het op deze manier heeft georganiseerd. In een apart onderzoek, uitgevoerd door het WODC, wordt nader ingegaan op de werkwijze en gebruikte waarborgen rondom de hackbevoegdheid in het buitenland.[111]

Enkele geïnterviewden vanuit Digit pleiten ervoor dat er meer beoordelingsruimte komt voor het feit dat een stukje bewijs meerdere bewijswaardes kan hebben, in plaats van dat deze bewijswaarde altijd 100% moet zijn. Overigens biedt een goedgekeurd technisch hulpmiddel ook maar een beperkte garantie, zo merkt een geïnterviewde van Digit op. Er kan misschien met 100% zekerheid worden vastgesteld dat een bepaald bericht op het apparaat van de verdachte stond, maar er kan niet (altijd) aangetoond worden dat het ook de verdachte is die dat bericht geschreven heeft.
Meer ruimte betekent volgens een aantal geïnterviewden vanuit Digit dat het makkelijker moet zijn om een niet (volledig) goedgekeurd hulpmiddel in te zetten. Eén

bepaalde bewijswaarde. Echter, bewijswaarde is een veel breder begrip dat onder andere gaat over de waardering van bewijs in de context van een specifieke zaak.

110 *Open source intelligence* is 'onderzoek doen in open bronnen, en dan met name het internet' met het doel om informatie te vinden om een opsporingsonderzoek 'verder te helpen'. Bij open bronnen gaat het onder andere om sociale netwerken, fora en het *darkweb* (Politie, z.d.).

111 Verwachte publicatiedatum is voorjaar 2023.

van de geïnterviewde opsporingsambtenaren legt aan de hand van een voorbeeld uit in welke gevallen gebruik zou kunnen worden gemaakt van een hulpmiddel dat deels goedgekeurd is.[112] Stel dat de politie geïnteresseerd is in de inhoud van een e-mail. Die e-mail kan verkregen worden met een technisch hulpmiddel waarvan de timestamp niet goed functioneert. Er kan dus niet met zekerheid worden gezegd op welk tijdstip [inclusief datum] de e-mail geschreven is. Wel kan worden vastgesteld dat de e-mail bij de verdachte op zijn of haar apparaat stond op het moment dat Digit/een technisch hulpmiddel het op een apparaat zag staan. Volgens de geïnterviewde hoeft dat niet altijd een probleem te zijn. Als de politie alleen geïnteresseerd is in de inhoud en niet in het tijdstip, dan doet het er minder toe op welk tijdstip een e-mail verstuurd is. Is het in een onderzoek wel van belang om een exact tijdstip te bepalen, dan zou de timestamp-functie goed moeten werken. Ook deze geïnterviewde vertelt dat een dergelijke werkwijze nu niet goed mogelijk is, omdat een technisch hulpmiddel alleen volledig kan worden goedgekeurd. In alle andere gevallen wordt een hulpmiddel nog niet goedgekeurd en dient het aangepast te worden.

*Openheid gehanteerde methode*
Enkele geïnterviewden merken op dat de politie bij een niet (volledig) goedgekeurd hulpmiddel/niet gekeurd hulpmiddel aan de rechter uit zal moeten leggen op welke manier zij te werk is gegaan. Er kan dan immers géén gebruik worden gemaakt van een keuringsnummer dat een technisch hulpmiddel krijgt zodra het goedgekeurd is. Op basis van de uitleg over de werking van het niet (volledig goed-)gekeurde hulpmiddel is het vervolgens aan de zittingsrechter om, eventueel na advies van een deskundige, de waarde van het door Digit aangeleverde bewijs te bepalen en een oordeel te vellen over de vraag in hoeverre het problematisch is dat een technisch hulpmiddel niet gekeurd is/niet volledig goedgekeurd is. Een mogelijk nadeel van een dergelijke werkwijze is dat meer bekend zal worden over de gehanteerde opsporingsmethoden en dat verdachten hun gedrag daarop kunnen aanpassen. Dat wordt als problematisch gezien voor het werk van Digit omdat 'goede ideeën om te kunnen binnendringen en onderzoek te doen' niet oneindig beschikbaar zijn, aldus één van de geïnterviewden werkzaam bij Digit. Tegelijkertijd werpen sommige geïnterviewden de vraag op of het in alle gevallen wel nodig is onderzoeksmethodieken volledig af te schermen. Eén van hen, ook werkzaam bij Digit, zou best aan een rechter willen uitleggen dat hij gebruik heeft gemaakt van een verbindingsniveau dat niet volledig aan de eisen uit het keuringsprotocol voldoet. Bovendien zal, indien sprake is van een handmatige inzet, sowieso uitleg moeten worden gegeven aan de rechter. Een andere geïnterviewde merkt op dat het geen probleem zou moeten zijn om meer informatie te geven over de werking van het technisch hulpmiddel. Bij het ene hulpmiddel zal meer mogelijk zijn dan bij het andere hulpmiddel, maar ook dat zou in de ogen van deze geïnterviewde niet problematisch hoeven te zijn, omdat op basis van die informatie, ook al is die beperkt, de rechter het gepresenteerde bewijs kan waarderen (binnen een bandbreedte van 0 tot 100%). Bovendien kan bij die waardering rekening gehouden worden met de getroffen waarborgen zowel technisch als tactisch (zie paragraaf 5.2.8).

*Mogelijke alternatieven*
Vanwege de door Digit ervaren belemmeringen rondom het keuringsproces wordt binnen Digit (OM en politie) nagedacht over mogelijke alternatieven.[113] Bij Digit beseft

[112] Op dit moment kent het besluit de optie 'deels goedgekeurd' niet.
[113] Er was bij Digit ook een plan om met pilots te starten om alternatieven te onderzoeken, maar daar is het tot op heden (april 2022) niet van gekomen.

men dat het belangrijk is dat gekeken wordt naar de middelen die worden ingezet en dat op de een of andere manier een uitspraak gedaan moet worden over de vraag of gegevens die daarmee verzameld worden als betrouwbaar, herleidbaar en integer bewijs kunnen dienen. Toch vraagt men zich bij Digit af of de wijze waarop er op dit moment gekeurd wordt, in stand moet blijven. Er bestaan verschillende ideeën over mogelijke alternatieven. Een aantal geïnterviewden zou graag zien dat het gemakkelijker wordt om met de Keuringsdienst in gesprek te gaan. Op dit moment vinden die gesprekken, over de inhoud van technische hulpmiddelen, niet of nauwelijks plaats vanwege de onafhankelijke positie van de keuringsdienst. Aangegeven wordt dat het mooi zou zijn als er (formele) momenten worden gecreëerd waarop dat gesprek wel mogelijk is en samen gekeken kan worden naar het keuringsprotocol en de werkbaarheid ervan.
Daarnaast wordt geopperd dat Digit uitgebreid zou kunnen worden met een aantal 'testers' werkzaam op de werkvloer bij Digit (en niet zoals de Keuringsdienst op een andere locatie). Zo'n model wordt in bedrijven die zich bezighouden met softwareontwikkeling al toegepast. De verwachting is dat door het gebruik van deze 'testers' de ontwikkeling van een hulpmiddel sneller kan gaan, omdat een product niet eerst helemaal af hoeft te zijn voordat er (door een keuringsdienst) naar gekeken wordt. Die snelheid wordt in de huidige situatie extra van belang geacht, omdat de middelen die tot nu toe ontwikkeld zijn slechts voor één zaak worden ingezet in plaats van dat deze gedurende meerdere jaren in meerdere opsporingsonderzoeken kunnen worden gebruikt. Ook dit model, waarin een technisch hulpmiddel als het ware 'iteratief' ontwikkeld wordt, is op dit moment lastig vanwege de onafhankelijke positie van de Keuringsdienst.
Tot slot zou Digit graag meer ruimte zien voor risicoanalyses en bewijswaardes. Eén van de geïnterviewde oppert een alternatief in die richting. Dit meest vergaande alternatief zou betekenen dat technische hulpmiddelen niet langer door de Keuringsdienst aan de huidige keuringseisen onderworpen worden. Het belangrijkste argument hiervoor is dat de eisen waaraan een technisch hulpmiddel moet voldoen niet goed passen bij de aard van de hulpmiddelen die Digit gebruikt, namelijk software. De software moet immers in een omgeving draaien die Digit, in tegenstelling tot bij de meer traditionele fysieke hulpmiddelen, niet volledig onder controle kan hebben. Daarnaast zou de werking van dit soort producten, vanwege updates die met enige regelmaat worden uitgevoerd, een keuring zoals die op dit moment wordt uitgevoerd in de weg staan. Op het moment dat een middel gekeurd is, is het eigenlijk alweer verouderd. Tot nu toe is overigens niet opnieuw naar een goedgekeurd middel gekeken. Deze geïnterviewde pleit ervoor om in plaats van een keuring verantwoording af te leggen in processen-verbaal waarover de rechter een eindoordeel velt, eventueel na raadpleging van een deskundige. In plaats van een keuring zou sprake moeten zijn van 'verificatie en validatie' door te kijken naar de 'aannemelijkheid' dat bewijs betrouwbaar is.

### *5.2.10 Hoofdpunten*

- De Keuringsdienst keurt technische hulpmiddelen die Digit zelf ontwikkeld heeft aan de hand van een keuringsprotocol. Dit protocol is gebaseerd op een aantal artikelen uit het Besluit dat ervoor moet zorgen dat het bewijs dat wordt verzameld betrouwbaar, integer en herleidbaar is.
- De Keuringsdienst kan alleen varen op wat zij zelf ziet tijdens een keuring. Wat Digit binnen haar eigen omgeving organiseert, wordt niet meegenomen tijdens de keuring, omdat die omgeving, in lijn met het Besluit, géén onderwerp van de keuring is.

- Het ontwikkelen van een (goed-)gekeurd technisch hulpmiddel neemt veel tijd in beslag. Daardoor is de inzet van een vooraf goedgekeurd hulpmiddel nauwelijks haalbaar gebleken in de praktijk.
- Voor Digit is het lastig werkbaar dat een aangepast middel, dat nog niet was goedgekeurd, volledig opnieuw gekeurd moet worden. De Keuringsdienst keurt een aangepast middel opnieuw, omdat alleen dan uitspraken kunnen worden gedaan over de werking van het middel en over de vraag of daarmee gegevens worden verzameld die betrouwbaar, herleidbaar en integer zijn.
- Digit-OM heeft besloten dat de aard van een gebruikt commercieel middel zich verzet tegen een keuring. Het middel zal op basis van het Besluit en de geformuleerde keuringseisen (hoogstwaarschijnlijk) ook niet goedgekeurd kunnen worden.
- Digit (en het tactisch team) nemen maatregelen in het kader van aanvullende tactische en technische waarborgen bij middelen die niet (goed)gekeurd zijn. Voor de tactische waarborgen is in het Besluit geen aandacht en dus worden deze niet meegenomen tijdens de keuring.
- Voor Digit vormt de keuring een belangrijk knelpunt. Dat heeft te maken met het feit dat de twee betrokken actoren (Keuringsdienst en Digit) vanuit verschillende perspectieven naar het keuringsproces kijken. Binnen het perspectief van waaruit de Keuringsdienst kijkt, staan vooral de regels centraal: een hulpmiddel kan alleen goedgekeurd worden als aan alle eisen uit het keuringsprotocol wordt voldaan (eventueel aangevuld met vervangende waarborgen), zodat de betrouwbaarheid, integriteit en herleidbaarheid van de verzamelde gegevens gegarandeerd kunnen worden. Binnen het perspectief van waaruit Digit naar de keuring van technische hulpmiddelen kijkt wordt vooral gekeken naar de uitvoerbaarheid en de noodzakelijkheid van de regels en de daarop gebaseerde eisen. Voor Digit zijn de regels en eisen lastig uitvoerbaar, onder andere omdat ze niet goed zouden passen bij de hulpmiddelen die Digit ontwikkelt. De regels zijn vooral gebaseerd op het 'oude' Besluit. Verder worden niet alle regels noodzakelijk geacht, omdat te weinig rekening is gehouden met risicoanalyses en bewijswaardes. Het zou niet nodig dat een technisch hulpmiddel aan alle keuringseisen voldoet. Digit doet een aantal suggesties die een oplossing zouden kunnen bieden voor de knelpunten die zij tegenkomt.

## 5.3 De Inspectie Justitie en Veiligheid

### *5.3.1 Inleiding*

In dit subhoofdstuk wordt stilgestaan bij de wijze waarop de Inspectie Justitie en Veiligheid toezicht houdt op de uitvoering van de hackbevoegdheid (onderdeel van deelvraag 4). Na een samenvatting van het wettelijk kader, wordt allereerst ingegaan op het gehanteerde toetsingskader. Vervolgens worden de werkwijze van de Inspectie en de wijze waarop Digit medewerking verleent aan het toezicht beschreven. Afgesloten wordt met hoe gereageerd wordt op de Verslagen van de Inspectie, zowel door Digit als door het ministerie van Justitie en Veiligheid.

### *5.3.2 Samenvatting wettelijk kader*

De Inspectie Justitie en Veiligheid (hierna Inspectie) is verantwoordelijk voor het zogenoemde 'systeemtoezicht' (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34). Wettelijk is vastgelegd dat de Inspectie toezicht houdt op de wijze waarop de

politie haar taak uitvoert. In dat licht heeft zij vanuit de wetgever de rol toegekend gekregen om (ook) toezicht te houden op 'het functioneren van het wettelijke systeem rond de uitvoering van een bevel tot onderzoek in een geautomatiseerd werk' (artikel 126nba lid 7). De toezichtstaak van de Inspectie heeft betrekking op de uitvoering (vindt de inzet plaats volgens 'relevante wet- en regelgeving en binnen de kaders van het bevel van de officier van justitie en de machtiging van de rechter-commissaris' (*Kamerstukken I* 2017/18, 34 372, G.), maar zij toets niet de rechtmatigheid van de inzet. Dat is aan de rechter ter terechtzitting (*Kamerstukken II* 2016/17, 34 372, nr. 6). Verder wordt het handelen van de officier van justitie getoetst door de procureur-generaal bij de Hoge Raad (PG-HR) en de rechter ter terechtzitting. De Inspectie kan wel de PG-HR op de hoogte stellen wanneer sprake is van 'schendingen van wettelijke voorschriften door of in opdracht van de officier van justitie'. Ook kan zij de Autoriteit Persoonsgegevens informeren wanneer sprake is van een mogelijke schending van de regels rond de bescherming van persoonsgegevens (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 82-83).
De Inspectie heeft de toezichtsrol toegekend gekregen na een discussie over de noodzaak van (extra) 'systeemtoezicht'.

### *5.3.3 Toezichtskader*

Sinds 2019 houdt de Inspectie toezicht op de wijze waarop uitvoering wordt gegeven aan de hackbevoegdheid. Dat doet zij, zoals dat door de wetgever aangegeven is, aan de hand van de regels en voorschriften die vastgelegd staan in de verschillende wettelijke regelingen (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 82). Al tijdens het wetgevingstraject denkt de Inspectie mee, onder andere tijdens gesprekken met de politie, over hoe haar toezichtsrol vorm zou moeten krijgen. Eén van de geïnterviewden, betrokken bij het toezicht, vertelt dat met Digit veel gesproken is over 'al die regels en verschillende normatieken' rondom de hackbevoegdheid om te bekijken 'wat daar precies achter zat'. Omdat op het moment dat de wet in werking trad bij de Inspectie onvoldoende deskundigheid in huis was, zijn op verschillende momenten in de tijd drie nieuwe senior-inspecteurs aangenomen. Twee van hen hebben een IT-audit achtergrond en de derde een technisch-forensische achtergrond.

De Inspectie houdt toezicht aan de hand van een door haar opgesteld (nog niet openbaar) toezichtskader. Leidend daarbij zijn, net zoals bij de Keuringsdienst, verschillende wettelijke regelingen (vooral het Besluit) en toelichtingen daarop. De Inspectie legt uit dat zij kijkt naar de 'rechtmatigheid' van de inzet. Daarmee bedoelt zij dat gekeken wordt in hoeverre Digit de regels, vastgelegd in wetsteksten, naleeft. Zij velt géén oordeel over de proportionaliteit en de subsidiariteit van een inzet. Ook alle activiteiten die bij het tactisch team plaatsvinden, zoals uitvoering geven aan verificatiemomenten is géén onderwerp van toezicht.
In de afgelopen jaren is discussie ontstaan over de reikwijdte van het toezicht door de Inspectie. Een belangrijk discussiepunt, dat vooral rondom het verschijnen van het tweede Verslag prominenter naar voren is gekomen, is het onderscheid tussen de onderwerpen waarop de Inspectie toezicht houdt en de onderwerpen die het Openbaar Ministerie en de PG-HR controleren.[114] Aanleiding voor deze discussie is de conclusie van de Inspectie in haar tweede Verslag dat het gebruik van een commercieel hulpmiddel, dat in haar ogen niet voldoet aan de eisen die gesteld worden in het Besluit, een risico vormt voor de betrouwbaarheid van het bewijs dat wordt verzameld. De Inspectie vindt dit onder andere een risico, omdat onduidelijk is welke aanvullende

[114] Eén van de geïnterviewden, betrokken bij het toezicht, vertelt dat deze discussie niet alleen speelt op het terrein van het toezicht op de hackbevoegdheid, maar ook bij andere toezichtsthema's.

(technische) waarborgen zijn genomen. Vanuit Digit-OM is kritiek op deze conclusie omdat de Inspectie niet bevoegd zou zijn om uitspraken te doen over de wijze waarop het Openbaar Ministerie haar rol vervult. Of bewijs als betrouwbaar moet worden ingeschat, zou aan een officier van justitie zijn en uiteindelijk aan een zittingsrechter. Daarnaast is het toezicht op het functioneren van het Openbaar Ministerie belegd bij de PG-HR. Volgens een geïnterviewde betrokken bij het toezicht is de kritiek van Digit-OM goed voorstelbaar. Deze geïnterviewde legt uit dat de Inspectie expliciet naar voren is geschoven om toezicht te houden op de hackbevoegdheid. Er bestaan nog veel meer bijzondere opsporingsbevoegdheden waarbij het toezicht niet op deze manier georganiseerd is en waarbij een werkwijze is ontstaan tussen het Openbaar Ministerie en de politie. Deze geïnterviewde kan zich voorstellen dat het lastig is dat de wetgever besloten heeft dat er nu een 'extra partij is' die naar die werkwijze kijkt.

Hoewel de Inspectie intern discussie heeft gehad en met de Advocaat-Generaal bij de Hoge Raad contact heeft gehad over de vraag waar zij wel en géén toezicht op kan houden, is zij het niet eens met de zienswijze van Digit-OM. Dat gaat niet alleen over het zojuist besproken risico ten aanzien van de integriteit van het bewijs, maar bijvoorbeeld ook over de wijze waarop Digit een technisch hulpmiddel definieert. Digit-OM stelt zich op het standpunt dat de Inspectie daar niet over gaat. Een geïnterviewde opsporingsfunctionaris licht toe:

> *'Op sommige punten* [doet] *Digit gewoon simpelweg (…) wat (…)* [Digit-OM] *ze als kader (…)* [stelt]*. Dus dan kun je als Inspectie wel zeggen, dat klopt niet, maar wat je daar dan eigenlijk zegt, is wat de officier als kader heeft gesteld, dat klopt niet en* [dan] *ben je in (...)* [de] *oordeelsvorming* [van de officier] *aan het treden. De vraag of iets een technisch hulpmiddel is of niet, is niet aan de discretie van Digit, maar is aan de discretie van (…)* [Digit-OM]*. En daar was op een gegeven moment discussie over. Script is een technisch hulpmiddel, en Digit ziet het niet als een technisch hulpmiddel. Dat klopt, omdat het in de kaders die* [Digit-OM] *Digit*[-politie] *heeft gegeven geen technisch hulpmiddel is. Dan kom je al in een spanningsveld.'*

De Inspectie heeft een ander oordeel met betrekking tot het bovenstaande. Volgens haar heeft Digit een belangrijke adviesrol richting het Openbaar Ministerie en kan om die reden over het advies van Digit wel iets worden opgemerkt. Een geïnterviewde licht toe:

> *'Hoe we er nou zo tegenaan kijken, is dat je wel kunt zeggen, de politie, Digit, moet ook adviseren richting de officier om een besluit te kunnen nemen. Dus je zou nog wel iets kunnen vinden als Inspectie over het advies wat de politie heeft gedaan. Want dat is echt een verantwoordelijkheid voor de politie. Ook (…) dat Digit in het begin zegt, we gaan hier een middel inzetten, en dat is geen technisch hulpmiddel volgens ons. Dat is een advies richting de officier. Dan kom je dus volgens mij op een terrein, waar wij denk ik gewoon iets over kunnen zeggen. (…). Kijk als Digit had gezegd, dit is een technisch hulpmiddel in advies richting de officier en de officier zegt: ik vind het geen technisch hulpmiddel. Dan is het een besluit van de officier. Andersom vind ik het een andere situatie en dan vind ik dat we daar best iets van kunnen zeggen. Over het advies. Uiteindelijk blijft het de verantwoordelijkheid van de officier om daar iets mee te doen.'*

Er hebben inmiddels gesprekken plaatsgevonden tussen het Openbaar Ministerie en de Inspectie. Vanuit Digit-OM is aangegeven dat de Inspectie wat haar betreft toezicht

zou kunnen houden op een beperkt aantal werkzaamheden van de politie, zoals de opleidingsvereisten en de logging. Eventueel zou de Inspectie, hoewel dubbelop, kunnen beoordelen of de politie zich aan de door het Openbaar Ministerie gestelde kaders houdt. Volgens de Inspectie wordt het toezicht op die manier een 'lege huls' waarin geen ruimte meer is om bepaalde risico's aan te stippen. Er wordt aangegeven dat de Inspecteurs meerdere malen overleg hebben gehad met de Advocaat-Generaal bij de Hoge Raad en dat deze heeft aangegeven dat de Inspectie de door haar gesignaleerde risico's kan noemen.

### *5.3.4 Eerstelijns toezicht & kwaliteitssysteem*

In tegenstelling tot hoe de Inspectie het zelf graag zou zien, heeft tot nu toe vooral 'eerstelijns' toezicht plaatsgevonden. Dat betekent dat de Inspectie zelf als eerste kijkt of allerlei 'operationele' zaken op orde zijn, zoals bijvoorbeeld de autorisaties van opsporingsambtenaren en de logging. Verteld wordt dat deze vorm van toezichthouden niet efficiënt is en niet in lijn ligt met hoe systeemtoezicht eruit zou moeten zien. Systeemtoezicht betekent volgens de Inspectie dat sprake is van toezicht gevoed door een eigen 'kwaliteitssysteem' van de politie waarmee zij haar eigen 'interne controle' organiseert. Enkele geïnterviewden vertellen dat dit soort controlemechanismen nog niet op orde zijn. Dat zou overigens niet alleen gelden voor Digit, maar voor de politieorganisatie in zijn geheel. Om die controlemechanismen vorm te geven adviseert de Inspectie Digit een eigen kwaliteitssysteem in te richten, dat de Inspectie op haar beurt zou kunnen gebruiken voor het uitoefenen van systeemtoezicht. Eén van de geïnterviewden betrokken bij het toezicht legt uit hoe dat werkt:

> *'Maar dat* [een kwaliteitssysteem] *is in feite niet meer, maar ook niet minder dan dat je intern als organisatie je processen beschrijft en de (…) KPI's*[115] *formuleert. Hoe je dat precies doet, dat is aan de organisatie zelf. Maar ik kan mij voorstellen dat zij* [Digit] *in ieder geval een aantal KPI's formuleren die afgeleid zijn van een Bogw (…). Maar daarnaast heb je ook (…) allerlei waarborgen waaraan moet worden voldaan en waar je dus ook gewoon processen voor moet inrichten en waar je ervoor moet zorgen dat je in de gaten houdt of er aan die criteria wordt voldaan. En de gedachte bij het toezicht wat wij houden is (..) dat wij ons systeemtoezicht kunnen uitoefenen en alles kunnen toevertrouwen op, op de uitkomsten (..) van die kwaliteitsmetingen die in de eigen systemen plaatsvinden.'*

Het voorgaande betekent onder andere dat Digit haar werk in zogenoemde 'werkprocessen' zou moeten vastleggen. Eén van de geïnterviewden betrokken bij het toezichtsproces legt uit dat Digit vindt dat zij al veel vastgelegd heeft, maar volgens deze geïnterviewde gaat het daarbij vooral om beschrijvingen van onderwerpen zoals deze in de wet beschreven staan, in plaats van een beschrijving van hoe die onderwerpen in de praktijk worden ingevuld. Dat is waar het volgens deze geïnterviewde over zou moeten gaan.

Het gewenste kwaliteitssysteem leidt in de uitvoeringspraktijk tot discussie. Deze discussie heeft betrekking op twee aspecten: de definitie van een kwaliteitssysteem en de praktische haalbaarheid van zo'n systeem. In de eerste plaats is niet altijd duidelijk wat onder een kwaliteitssysteem moet worden verstaan. Enkele geïnterviewden lichten toe dat het kwaliteitssysteem betrekking heeft op twee aspecten, namelijk

[115] *Key performance indicator* (in het Nederlands kritieke prestatie-indicator). Met behulp van deze indicatoren kunnen prestaties van een organisatie, bijvoorbeeld een politie(-organisatie) inzichtelijk worden gemaakt (Rautiainen et al., 2019).

informatiebeveiliging en de interne controle van verschillende werkprocessen. Beide aspecten zouden aan Digit uitgelegd zijn. Desondanks ziet de Inspectie niet de ontwikkelingen die zij gehoopt had te zien. Dat geldt zowel voor de informatiebeveiliging als voor de wijze waarop de interne controles worden uitgevoerd. Een medewerker vanuit Digit heeft juist begrepen dat het kwaliteitssysteem vooral betrekking heeft op het goed organiseren van de informatiebeveiliging (in plaats van op het uitvoeren van interne controles). Die interpretatie komt ook naar voren in een Kamerbrief van de toenmalig Minister van Justitie en Veiligheid waarin hij een reactie geeft op het tweede verslag van de Inspectie. Daarin spreekt hij over een 'intern kwaliteitssysteem dat zich richt op de informatiebeveiliging om beveiligingsrisico's te beheersen' (Grapperhaus, 2021).
Een tweede discussiepunt heeft betrekking op de praktische haalbaarheid van een kwaliteitssysteem. Een medewerker vanuit Digit merkt op dat het lastig is om werkprocessen op te stellen in verband met de 'operationele drukte' binnen het team. Daardoor zou er minder tijd zijn voor niet-operationele zaken. Een ander punt dat de praktische haalbaarheid in de weg zou staan is dat het werk dat Digit doet 'maatwerk' is en dat het zich daardoor niet goed laat vastleggen in werkprocessen. Eén van de geïnterviewden betrokken bij het toezicht vertelt dit argument te herkennen. De door de Inspectie 'benodigde en gevraagde verantwoording in de praktijk wringt met hoe er gewekt wordt bij de politie'. Een andere geïnterviewde vanuit Digit merkt op dat een kwaliteitssysteem misschien niet als haalbaar wordt gezien, maar dat dat niet betekent dat er geen 'interne mechanisme' moeten zijn om 'interne controle' uit te voeren op de werkzaamheden van Digit. 'De materie is gevoelig en de kans op een klein foutje is makkelijk aanwezig'. Daarom is 'goede controle' nodig, 'op elkaar en op het systeem'.
Een laatste punt met betrekking tot de praktische uitvoerbaarheid heeft te maken met het detailniveau waarop werkprocessen vastgelegd zouden moeten worden. In de zojuist aangehaalde Kamerbrief wijst de minister erop dat het 'uitputtend beschrijven van de toepasselijke werkprocessen niet realistisch is' (Grapperhaus, 2021). Over wat precies moet worden verstaan onder 'uitputtend' bestaat verschil van inzicht. Eén van de geïnterviewden vertelt dat het advies van de Inspectie helemaal niet is geweest om een 'uitputtelijke' beschrijving te geven. Dat is de interpretatie die er in de Kamerbrief aan gegeven wordt. Het enige wat de Inspectie heeft opgeschreven is dat er een kwaliteitssysteem zou moeten komen.

### *5.3.5 Werkwijze*

Voor het uitvoeren van haar toezichtstaak is de Inspectie enkele dagen per week bij Digit aanwezig.[116] Tijdens hun aanwezigheid bekijken de inspecteurs vooral de door Digit gebruikte systemen (bijvoorbeeld de logging en het journaliseersysteem). Op die manier proberen zij onder andere het verloop van een zaak te reconstrueren en beoordelen zij de manier waarop Digit haar werkzaamheden vastlegt. Om dat op een goede manier te kunnen doen, is het van belang dat alle handelingen waarop de Inspectie toezicht dient te houden daadwerkelijk op papier (lees: in de systemen) worden vastgelegd, voor zover dat niet geautomatiseerd gebeurt. In de praktijk wordt echter niet alles vastgelegd. Voor de Inspectie is dat problematisch, omdat zij op die manier niet de gestelde norm kan controleren. Eén van de geïnterviewden betrokken bij het toezicht merkt dat er op zulke momenten frictie ontstaat tussen Digit en de Inspectie:

[116] Inmiddels (april 2022) is de aanwezigheid minder. Vooral in de periode dat een rapportagejaar afgerond wordt, zijn de Inspecteurs enkele dagen per week aanwezig.

*'Dan denken ze van jullie* [de inspecteurs] *zijn auditors, jullie kijken altijd vanuit de regeltjes, jullie kennen de opsporingswereld niet, in de opsporing werken we niet zo. Daar werken we gewoon, we vertrouwen elkaar, beëdigde opsporingsambtenaren. (…). Allemaal professionals. Dus het is eigenlijk helemaal niet nodig om dat allemaal vast te leggen en allemaal controleerbaar te maken, want we werken onder ambtseed. (...) En ik snap het ook wel vanaf hun kant. Maar goed, voor ons, als we het niet kunnen controleren, dan kunnen we ook nooit schrijven van het is goed. Wij kunnen dat niet in ons verslag schrijven. Het zijn allemaal professionals, het zijn beëdigde opsporingsambtenaren. Ze doen zo hun best, dus minister maakt u zich maar geen zorgen. Of Tweede Kamer.'*

Naast het toezicht bij Digit, heeft de Inspectie het keuringsproces onderzocht. Daarvoor heeft zij gesprekken gevoerd met de Keuringsdienst en zijn keuringsdocumenten ingezien. De inspecteurs hebben onder andere de uitgevoerde keuringen onder de loep genomen.

Eerder is al aangegeven dat de Inspectie kijkt of Digit alle regels volgt. Zij houdt zich niet bezig met de vraag in hoeverre de regels uitvoerbaar zijn en wat deze regels betekenen voor de effectiviteit van het optreden van Digit. Eén van de geïnterviewden betrokken bij het toezichtsproces licht toe:

*'Wij kijken echt naar wat staat er in die regelgeving op basis van de artikelen die daar staan en de toelichting in het Besluit. Daar hebben we een set van gemaakt. Dus het is echt daarop gericht. Straks* [op een later moment in het interview] *zullen we nog wel even horen hoe de politie dat ziet. Die verwacht toch iets meer empathie en context, van het is, de effectiviteit, kan het allemaal wel? Uitvoerbaarheid. Onze insteek van dat normenkader is puur gericht op die regels, in het Besluit en in de wetgeving vastgelegd. Dat is op zich een belangrijk uitgangspunt, om dat op voorhand duidelijk te hebben.'*

Vanuit geïnterviewden vanuit de Inspectie wordt aangegeven dat problemen rondom de uitvoerbaarheid van de regels met betrekking tot de hackbevoegdheid op dit moment niet thuishoren bij de Inspectie. Hoewel Digit beseft dat de Inspectie de regels niet kan veranderen, is het voor Digit (zowel politie als OM) lastig dat niet naar die uitvoerbaarheid gekeken wordt, vooral omdat het werken met deze bevoegdheid nieuw is en Digit zich in de ontwikkelfase bevindt. Bovendien bestaat er bij Digit twijfel of ooit wel aan alle eisen die worden gesteld zal kunnen worden voldaan.

**Rapporteren**

De Inspectie rapporteert over één kalenderjaar en na afloop van zo'n jaar verschijnt een openbaar verslag waarin de belangrijkste bevindingen worden gepresenteerd. Voordat het verslag verschijnt, schrijf de Inspectie één of meerdere brieven aan de politie die meer details bevatten en (om die reden) niet openbaar zijn.[117] Inmiddels (voorjaar 2022) wordt overigens niet meer gewerkt met een dergelijk brievensysteem. De brieven vormden een belangrijke bouwsteen voor het verslag[118] en in het Verslag komen alleen de hoofdpunten terug. Sommige van die hoofdpunten zijn in beide Verslagen aan de orde geweest (onder andere logging), terwijl andere punten niet meer in het Verslag zijn opgenomen, ook al kwamen ze gedurende beide verslagjaren naar voren. Een voorbeeld van zo'n laatste punt is functiescheiding. Beide jaren

[117] De WODC-onderzoekers hebben deze brieven niet betrokken in het onderzoek.
[118] Deze werkwijze (combinatie Verslag en brief) hanteert de Inspectie ook bij andere toezichtactiviteiten op andere terreinen zoals de terugkeer van vreemdelingen.

constateerde de Inspectie dat er contact is geweest tussen het technisch en het tactisch team. Dat is niet volgens de regels en daarom heeft de Inspectie het genoemd. In het tweede Verslag is het punt echter niet aan de orde geweest.[119] Twee factoren speelden daarbij een rol. De eerste is dat er andere punten belangrijker werden gevonden. De tweede is dat gekeken is wat de risico's zijn en hoe het er in de praktijk aan toe gaat. Wat betreft dat laatste begrijpt één van de geïnterviewden betrokken bij het toezicht dat een technisch team alleen goed het werk kan doen op basis van informatie uit het tactisch team. Desondanks is functiescheiding wel 'één van de aspecten uit het rechtskader' waarmee de Inspectie wat moet. Daarom blijft de Inspectie dat punt kritisch volgen en noemen wat zij op dat punt ziet.
Naast deze formele momenten waarop gerapporteerd wordt, bestaat het plan dat Digit en de Inspectie maandelijks met elkaar om tafel gaan zitten om te bespreken wat er speelt. Eén van de geïnterviewden betrokken bij het toezicht vertelt dat vanuit Digit deze behoefte bestond. Zij wilde de Inspectie graag meenemen in 'hun denkproces', zodat de Inspectie zou snappen waarom Digit bepaalde dingen doet zoals zij ze doet. De Inspectie ziet ook de voordelen van zo'n afspraak, omdat zij daardoor de mogelijkheid krijgt om meer (meer dan in de systemen te lezen is) te horen krijgt over de inzetten (vooral de handmatige) die Digit van plan is om te doen. Door Covid-19 is het van dit structureel overlegmoment nog niet gekomen, maar de bedoeling is dat dit in de toekomst maandelijks plaats gaat vinden. Vanuit de Inspectie wordt aangegeven dat op dit moment (voorjaar 2022) overleggen 'regelmatig' plaatsvinden, niet alleen met Digit, maar ook met de Keuringsdienst.

Verschillende geïnterviewden vanuit Digit zijn kritisch over de wijze waarop de Inspectie rapporteert. Zo zou er te weinig oog zijn voor de manier waarop Digit werkt en de context waarin zij haar werk moet doen. Een ander kritiekpunt is dat de Inspectie slechts rapporteert over één kalenderjaar, en het Verslag pas een paar maanden na afloop van dat kalenderjaar verschijnt. Daardoor staan in het verslag punten beschreven die in de ogen van Digit verouderd zijn.

### *5.3.6 Medewerking vanuit Digit*

Naast kritiek op rapportages van de Inspectie, wordt binnen Digit enigszins sceptisch gekeken naar de aanwezigheid van de Inspectie. Verschillende geïnterviewden geven aan dat het aan de ene kant goed is dat de Inspectie er is. De Inspectie 'houdt Digit scherp', 'doet wat zij moet doen' en het toezicht zorgt ervoor dat Digit 'naar buiten toe gedekt is'. Aan de andere kant verbaast één van de geïnterviewden zich over het feit dat alleen Digit, en niet andere onderdelen van de politie op zo'n manier onderworpen worden aan het toezicht van de Inspectie. De Inspectie 'kijkt over de schouder mee, en dat werkt niet prettig'. Daarnaast zou de Inspectie meer uit mogen gaan van vertrouwen, zo blijkt uit het verslag van het gesprek met een andere geïnterviewde:

> *'Gevoelsmatig vindt geïnterviewde het toezicht lastig. Dat heeft (...) te maken met het* [door de geïnterviewde ervaren] *uitgangspunt dat Digit onbetrouwbaar zou zijn. De aanwezigheid van de Inspectie wekt de schijn van wantrouwen. Maar iedereen die bij Digit werkt, werkt met een bepaalde integriteit. Er zijn natuurlijk bij de politie zat voorbeelden dat dit niet altijd goed gaat, maar toch.'*

Ondanks kritische geluiden vanuit Digit, wordt door beide actoren verteld dat Digit haar medewerking verleent aan de Inspectie. Er is toegang tot gegevens waardoor de Inspectie vindt dat zij effectief toezicht kan uitvoeren. Ondanks de bereidheid om mee

[119] In het derde Verslag komt dit punt wel weer aan de orde (Inspectie JenV, 2022, p. 25).

te willen werken, wordt ook verteld dat het Digit niet altijd lukt om (tijdig) informatie te verschaffen. Dat geldt vooral voor de maatwerkinzetten die er in het begin waren. De Inspectie had in die gevallen behoefte aan meer informatie over hoe er gewerkt was. Naast dat in het verleden niet altijd de benodigde informatie is aangeleverd, is gedurende de afgelopen jaren het een en ander veranderd in de samenwerkingsrelatie tussen beide partijen. De verhouding lijkt enigszins stroever geworden te zijn.

### *5.3.7 Reactie op Verslagen*

**Aanpassingen Digit**

In haar brieven en Verslagen noemt de Inspectie verschillende punten die wat haar betreft verbetering behoeven. Een aantal ervan zijn in het voorgaande de revue gepasseerd (denk aan het kwaliteitssysteem). De bevindingen van de Inspectie worden binnen Digit besproken. In een deel van de verbeterpunten kan Digit zich goed vinden. Dat geldt bijvoorbeeld voor het vastleggen van informatie (journaliseren en verbaliseren). Digit is met die punten aan de slag gegaan. Zo is er een extra dossiervormer gekomen die ervoor moet zorgen dat alle dossiers (op tijd) gereed zijn en is een inhaalslag gemaakt met het opstellen van processen-verbaal. Daarnaast heeft Digit ervoor gezorgd dat activiteiten, uitgevoerd met behulp van een commercieel middel, in dezelfde ruimte en direct na het uitvoeren ervan worden vastgelegd. Vanuit de Inspectie wordt aangegeven dat een deel van de punten die Digit zegt te hebben doorgevoerd niet hebben plaatsgevonden in het laatste verslagjaar. Daarom kan de Inspectie nog niet oordelen over de doorgevoerde aanpassingen.

Van een aantal verbeterpunten heeft Digit aangegeven dat zij zich er niet in kan vinden en/of dat zij niet van plan is om aan deze punten tegemoet te komen. Naast het minimaal verbaliseren (zie hoofdstuk 6) gaat het bijvoorbeeld om het 'uitgiftepunt', het registratieproces met behulp waarvan moet worden bijgehouden aan wie een technisch hulpmiddel verstrekt wordt. Digit stelt zich op het standpunt dat het niet realistisch is om zo'n uitgifteproces te implementeren, omdat zo'n proces vooral geschikt zou zijn voor de uitgifte van klassieke (fysieke) technische hulpmiddelen. De Inspectie merkt echter op dat het uitgifteproces een hoofdeis is uit het Besluit en dat Digit 'een heel end zou kunnen komen met betrekking tot de naleving ervan'. Volgens één van de geïnterviewden betrokken bij het toezichtsproces is rondom het gebruik van een commercieel middel een procedure te bedenken waarmee digitaal toegang kan worden verschaft die ook weer kan worden ingetrokken op een bepaald moment. Zo'n proces zou gedeeltelijk al bestaan, omdat de teamleider beslist wie toegang tot het middel krijgt. Alle leden van het inzetteam zijn op dit moment geautoriseerd om het middel te gebruiken. Dat zou volgens deze geïnterviewde anders kunnen worden georganiseerd. Toch vraagt deze geïnterviewde zich ook af wat een uitgifteproces voor een technisch hulpmiddel precies oplevert. Dat er een proces zou zijn waarin de toegang tot binnendringingssoftware wordt georganiseerd zou beter voorstelbaar zijn volgens deze geïnterviewde. Aan de toegang tot dit soort software kleven meer risico's. In het Besluit staat echter dat alleen een proces ingericht hoeft te worden voor het verstrekken van de toegang tot een technisch hulpmiddel. Voor fysieke hulpmiddelen is dat volgens deze geïnterviewde misschien relevant, omdat het bijhouden wie het middel uitgereikt heeft gekregen (en weer heeft geretourneerd) ervoor zorgt dat er minder makkelijk mee 'geknoeid' kan worden, maar dat is bij softwareachtige middelen minder gemakkelijk. Bovendien heb je zo'n middel ook 'niet in handen', zoals een baken. In dat kader kan het uitgifteproces worden gezien als 'onuitvoerbaar'. Deze geïnterviewde vertelt dat rondom het verschijnen van het eerste

Verslag overwogen is om iets te zeggen over deze onuitvoerbaarheid. Uiteindelijk is besloten om dat niet te doen. Het uitgifteproces is een wettelijke eis en de Inspectie achtte zichzelf niet in de positie om, kort nadat de wet in werking was getreden, in het Verslag op te nemen dat zij begrip had voor het feit dat de politie niet aan deze eis kon voldoen. Als de politie het echt zou willen, dan kan aan de eis voldaan worden, aldus deze geïnterviewde.[120]

**Kamerbrieven minister**

Na het eerste en het tweede Verslag heeft de toenmalig Minister van Justitie en Veiligheid aan de Tweede Kamer een brief (*Kamerstukken II* 2019/20, 29 628, nr. 970) geschreven met daarin een reactie op het Verslag. Over het eerste Verslag verscheen een aparte brief, de reactie op het tweede Verslag stond opgenomen in een zogenoemde verzamelbrief (Grapperhaus, 2021). In de eerste brief besteedt de minister aandacht aan de door de Inspectie geformuleerde verbeterpunten en wat de politie zal doen om aan die punten tegemoet te komen. Ook in de tweede brief gaat de minister in op een aantal punten die de Inspectie constateert. In tegenstelling tot bij de eerste brief wordt niet beschreven met welke verbeteringen Digit zal komen, maar worden de bevindingen genuanceerd en de werkwijze van Digit verdedigt. Zo wordt bijvoorbeeld benadrukt dat de servers en software van het commerciële middel in eigendom en beheer van de politie zijn en dat de politie de leverancier toegang moet verschaffen om het technisch beheer te kunnen doen (Grapperhaus, 2021). De Inspectie constateert dat de leverancier de server beheert en altijd toegang heeft tot de gebruikte software en gegevens die hiermee verzameld worden (Inspectie JenV, 2020, p. 19; 2021, p. 20). In de praktijk blijkt dat voor beide conclusies iets te zeggen is. De leverancier heeft toegang tot de server waarop het commerciële hulpmiddel draait en tot gegevens die daarmee verzameld worden. Eerder is al beschreven dat verteld wordt dat met de leverancier afspraken zijn gemaakt over de toegang tot die gegevens (niet toegestaan) en de server (toegestaan voor technisch beheer). Uiteindelijk komen de verzamelde gegevens binnen bij Digit op een *stand-alone* computer. Deze computer heeft géén toegang tot de servers van Digit, zo wordt vanuit Digit uitgelegd, en daardoor de commerciële leverancier dus ook niet. Vervolgens worden de gegevens overgezet naar de technische infrastructuur van Digit.
Verder uit de Inspectie in haar tweede Verslag haar zorgen over het feit dat een commercieel middel wordt gebruikt dat niet aan de eisen van het Besluit voldoet en daardoor een risico oplevert voor het verzamelde bewijs (Inspectie JenV, 2021, p. 20). In reactie daarop wordt door de minister aangegeven dat het uiteindelijk aan de zittingsrechter is om een oordeel te vellen over de integriteit, herleidbaarheid en betrouwbaarheid van bewijs (Grapperhaus, 2021). Daarnaast geeft de minister aan dat er inmiddels een intern kwaliteitssysteem bestaat, gericht op informatiebeveiliging voor het beheersen van veiligheidsrisico's, maar dat het niet mogelijk is om werkprocessen 'uitputtend' te beschrijven (Grapperhaus, 2021). De Inspectie constateert echter dat Digit na twee jaar niet beschikt over een 'goed functionerend intern kwaliteitssysteem' (Inspectie JenV, 2021, p. 21).

Vanuit de Inspectie wordt kritiek geuit op de reactie van de minister. De reacties zouden niet in overeenstemming zijn met hoe de Inspectie de werkwijze in de praktijk ziet en waarover de Inspectie het eens is met de teamleiding van Digit. Een geïnterviewde betrokken bij het toezichtsproces vraagt zich af of de toenmalig minister in zijn (laatste) brief niet te veel het standpunt van Digit (OM en politie) verwoordt.

[120] Ook uit het derde Verslag van de Inspectie blijkt dat er geen proces aanwezig is rondom onder andere de uitgifte en inname van technische hulpmiddelen, Begin 2022 is er wel een systeem gekomen waarmee de uitgifte van digitale sleutels kan worden geregeld en geregistreerd (Inspectie JenV, 2022, p. 24).

Volgens deze geïnterviewde doet een dergelijke beleidsreactie onrecht aan de integriteit van de Inspectie. Deze geïnterviewde beschrijft dat het toezicht dat de Inspectie uitvoert erg intensief is, zeker in vergelijking met het toezicht op de andere politietaken. Maar de intensiteit van dit toezicht is door de wetgever bepaald. Mocht dit intensieve toezicht uiteindelijk niet wenselijk zijn, dan is de Inspectie bereid om haar toezicht anders in te richten. Maar als het toezicht op deze manier wel de bedoeling is, dan verwacht deze geïnterviewde dat 'met respect inhoud moet worden gegeven aan de bevindingen van de Inspectie'.

### *5.3.8 Hoofdpunten*

- De Inspectie kijkt, in lijn met hoe hier in de wetsgeschiedenis over gesproken wordt, of de uitvoering verloopt volgens het wettelijk kader. Zij kijkt niet naar de uitvoerbaarheid van hetgeen in de wet geregeld is (vergelijkbaar met hoe de Keuringsdienst kijkt naar de door Digit ontwikkelde technische hulpmiddelen). Digit ervaar dit als lastig in verband met de ontwikkelfase waarin de uitvoering van de nieuwe bevoegdheid zich bevindt.
- De reikwijdte van het toezicht van de Inspectie is op dit moment onderwerp van gesprek, vooral ten aanzien van het handelen van het Openbaar Ministerie.
- De Inspectie is van oordeel dat zij nog géén goed systeemtoezicht kan uitoefenen, omdat Digit niet beschikt over een eigen kwaliteitssysteem. In de praktijk bestaat onduidelijkheid over wat precies onder een kwaliteitssysteem moet worden verstaan.
- Digit is met een deel van de door de Inspectie geconstateerde punten aan de slag gegaan, maar zegt ook met een deel ervan niets te zullen kunnen doen, omdat het Besluit op een aantal punten niet goed uitvoerbaar zou zijn.
- De reactie van de minister op de Verslagen van de Inspectie werkt bij de Inspectie op sommige punten verbazing, omdat daaruit blijkt dat aan haar constateringen niet altijd gevolgtrekkingen worden verbonden.

## 5.4 Het Openbaar Ministerie

### *5.4.1 Digit-OM*

Het Openbaar Ministerie is één à twee dagen aanwezig bij de politie en wekelijks voeren beide overleg over de stand van zaken met betrekking tot de op dat moment lopende inzetten. Vanuit Digit-OM wordt aangegeven dat dat een bewuste keuze is geweest om op zo'n manier betrokken te zijn bij de uitvoering van de bevoegdheid. Ook wordt uitgelegd dat de toetsing van Digit plaatsvindt aan de hand van het gegeven juridisch kader (wetsteksten en toelichtingen daarop) en de daarop gebaseerde kaders waarin Digit-OM (in overleg met de jurist van team Digit), al dan niet op papier, de juridische wereld heeft geprobeerd te vertalen naar een technische wereld en andersom. Deze opgestelde kaders zijn voorgelegd aan de rechercheofficier van het Landelijk Parket. Naast de kaders specifiek gericht op de hackbevoegdheid hanteert Digit-OM de algemene kaders die gelden voor de opsporing, voortvloeiend uit het Wetboek van Strafvordering waarin is vastgelegd dat de officier van justitie het gezag over de opsporing voert. Deze kaders staan (deels intern) onder meer vastgelegd in aanwijzingen, instructies, memo's, factsheets en notities. Sommige ervan (aanwijzingen en instructies) zijn afkomstig van het College van Procureurs-generaal en/of de vergadering van rechercheofficieren.

De door Digit gestelde kaders hebben betrekking op verschillende aspecten van de inzet, zoals het binnendringen, kwetsbaarheden en het onderscheid tussen een technisch hulpmiddel en een handmatige inzet. Met die kaders in het achterhoofd voert Digit-OM haar gezag uit, beantwoordt zij vragen (bijvoorbeeld over het melden van kwetsbaarheden) en grijpt zij in waar nodig (denk aan het zonder toestemming openzetten van een microfoon). Als Digit een inzet gestart heeft, laat Digit-OM zich tussentijds bijpraten wat er precies in een zaak speelt. Het kan zijn dat Digit tegen iets aanloopt tijdens een inzet 'waar het tactisch team iets mee moet' waardoor het nodig kan zijn dat Digit-OM en de zaaksofficier overleg hebben wat er op dat gebied wel en niet kan.

### *5.4.2 Tactisch OM*

De zaaksofficier van justitie is verantwoordelijk voor de wijze waarop het tactisch onderzoek verloopt. Gedurende een inzet wordt de zaaksofficier vooral geïnformeerd over de voortgang van de inzet. Daarbij worden vragen beantwoord als: lukt het om binnen te kunnen dringen? Worden gegevens binnengehaald? Eén van de geïnterviewden spreekt over 'resultaatcontact'. Een ander vertelt:

> *'Wij horen alleen maar: het is gelukt of het is niet gelukt. Als ik verdere vragen ga stellen dan krijg ik ook vaak te horen van: nee maar dat moeten we allemaal niet willen weten. Ik heb contact met het tactisch team. Tactisch team krijgt alleen maar input van Digit, maar krijgt geen details. Dus dat is prima. Want wij willen alleen weten: lukt het of lukt het niet.'*

Ook bij andere middelen zou het zo gaan. Wanneer fysiek een microfoon is geplaatst hoeft een zaaksofficier niet te weten waar die hangt, maar alleen of hij hangt en of de microfoon het doet.
Wat betreft de controle van het tactisch politieteam vertelt één van de geïnterviewden dat de mate waarin een tactisch politieteam gecontroleerd wordt afhankelijk is van de bekendheid van de officier van justitie met dat team. Aan sommige teams is een 'eigen' officier van justitie verbonden. Een andere geïnterviewde legt uit niet naast de rechercheurs te gaan staan, maar eens in de paar dagen geïnformeerd te willen worden.

Eerder kwam al naar voren dat een hack geen 'rustig bezit' is voor een officier van justitie, omdat gedurende een inzet van Digit continu meegedacht moet worden vanuit de tactische kant. Denk onder andere aan de eerder besproken verificatiemomenten en het bepalen wanneer de microfoon kan worden aangezet. Eén van de geïnterviewden die betrokken is bij een opsporingsonderzoek waarin Digit een inzet deed, vertelt meer betrokken te zijn geweest dan bij een inzet van andere bevoegdheden. Dat had vooral te maken met de hoop dat de inzet van Digit 'net dat stukje' op zou leveren waarop in het tactisch onderzoek gewacht werd. Of 'net die extra kans' om in het onderzoek tot een bepaalde ontdekking te komen. Tijdens deze inzet kwamen uit de gegevens verzameld door Digit locaties van ontmoetingen naar voren waarover het tactisch team moest nadenken of ze daarbij aanwezig wilden zijn. Dat vergde afstemming op korte termijn om te bepalen wat de volgende stap in het onderzoek zou zijn. Daarnaast moest nagedacht worden welke informatie, uit de grote bulk aan gegevens die de inzet van Digit opleverde, wel en niet relevant was.

### *5.4.3 Hoofdpunten*

- Digit-OM vervult gedurende de inzet voor alle betrokkenen de rol van vraagbaak en kijkt mee met de inzetten aan de Digit-politiekant. Indien nodig grijpt zij in.
- De zaaksofficier van justitie wordt vooral op de hoogte gehouden of de hackbevoegdheid resultaten oplevert. Daar waar nodig gaat ze na of op basis van informatie die beschikbaar komt, gehandeld moet worden.

## 5.5 Verlenging inzet bevoegdheid

### *5.5.1 Samenvatting wettelijk kader*

Bij de beslissing omtrent een verlenging zijn dezelfde actoren betrokken die toetsen of een inzet überhaupt mag plaatsvinden binnen een opsporingsonderzoek. Het bevel kan, na een machtiging van de rechter-commissaris, met vier weken (steeds opnieuw) worden verlengd (art 126nba, lid 3 en lid 4 Sv). Indien sprake is van spoed kan verlenging en of wijziging van het bevel mondeling worden afgegeven waarna het binnen drie dagen op schrift moet worden gesteld (artikel 126nba, lid 5 Sv).

### *5.5.2 Verlenging in de praktijk*

Zodra de looptijd van een bevel eindigt (doorgaans na vier weken, een enkele keer na twee weken (bij OVC)) buigt de zaaksofficier van justitie zich over de vraag of de inzet van de bevoegdheid verlengd dient te worden. In vier van de geselecteerde inzetten is sprake geweest van ten minste één verlenging voor ten minste één geautomatiseerd werk en bij drie van de inzetten is besloten geen aanvraag te doen voor een verlenging (zie tabel 5.1).

**Tabel 5.1 Verlengingen**

| Geselecteerde inzet | Verlenging | Aantal verlengingen |
|---|---|---|
| 1 | Nee (voor beide geautomatiseerde werken) | 0 |
| 2 | Nee | 0 |
| 3 | Ja (beide bevelen) | ≤3 (126nba en 126m)<br>>3 (126nba en 126l) |
| 4 | Nee | 0 |
| 5 | Bevel 1 (subA en subD): Ja<br>Bevel 2 (subE): Nee | 1 (subA tm subD)<br>0 (subE) |
| 6 | Ja (voor alle geautomatiseerde werken) | >3 (geldt voor alle geautomatiseerde werken) |
| 7 | Ja (voor beide geautomatiseerde werken) | ≤3 (geldt voor beide geautomatiseerde werken) |

Er worden verschillende argumenten naar voren gebracht waarom een inzet verlengd wordt en voor een verlenging van één inzet kunnen verschillende argumenten tegelijkertijd een rol spelen. Doorgaans worden deze beschreven in het aanvraag verlengingsproces-verbaal en de vordering tot machtiging gericht aan de rechter-commissaris. Een eerste argument is dat na de eerste inzet behoefte is aan

aanvullende gegevens. Bij één van de inzetten werd het bijvoorbeeld nodig geacht om vanwege de complexiteit van het systeem meer data te vergaren met betrekking tot de *command and control* server van het botnet. Daarnaast was meer tijd nodig om het ontoegankelijk maken van de server mogelijk te maken. Bij deze inzet speelde nog een ander argument een rol, namelijk het risico verkleinen dat de politie ontdekt zou worden doordat opnieuw binnengedrongen zou moeten worden in het geautomatiseerde werk. Een ander voorbeeld van een inzet waarbij behoefte was aan meer gegevens betreft een inzet die meer dan een jaar geduurd heeft. In deze zaak was de verwachting dat door verlenging van de inzet onder andere meer inzicht zou kunnen worden verkregen in de samenstelling van een criminele organisatie en informatie over ontmoetingen en locaties. Met die laatste informatie konden andere -- (bijzondere) opsporingsbevoegdheden gerichter worden ingezet. Het verzamelen van meer gegevens werd in dit opsporingsonderzoek nodig geacht, omdat de criminele organisatie haar werkwijze breed aan het uitbreiden zou zijn op een manier waarop uiteindelijk het zicht op de activiteiten verloren zou worden. Een inzet gedurende een periode van meer dan een jaar kwam overigens vooral voor vlak na inwerkingtreding van de wet. Inmiddels is intern binnen Digit afgesproken dat een inzet in principe maximaal twee keer verlengd wordt. Op die manier kunnen meerdere tactische teams tegelijkertijd worden bediend.
Een tweede argument om te verlengen is dat het soms technisch niet tijdig lukt om een inzet voor elkaar te krijgen. Bij één van de geselecteerde inzetten was dat één van de redenen om het bevel te willen verlengen. Bij deze inzet is nog een ander argument gebruikt voor verlenging. Dit argument geldt overigens voor een tweede geautomatiseerde werk dat werd onderzocht. Door het gebruik van TOR (en de daaraan gekoppelde versleuteling) waren andere (bijzondere) opsporingsbevoegdheden nog steeds niet geschikt om inzicht te krijgen in 'criminele handelingen van de verdachte' en de infrastructuur van een marktplaats op het *darkweb*.
Een beperkte privacyinbreuk is een derde argument dat is genoemd om de inzet te verlengen. Dit argument komt zowel naar voren bij de hiervoor beschreven inzet als bij de inzet die meer dan een jaar duurde. In dat laatste geval werd aangegeven dat met de nieuwe bevoegdheid 'gericht' kan worden gewerkt. Daardoor zou minder sprake zijn van het maken van een inbreuk op de privacy van derden zoals dat wel het geval kan zijn bij een 'open OVC'. Bij een open OVC wordt afluisterapparatuur in een open ruimte geplaatst, bijvoorbeeld een café. Inherent aan zo'n ruimte is dat er derden aanwezig kunnen zijn die géén onderwerp van onderzoek zijn in het opsporingsonderzoek en waarvan dus ook gesprekken kunnen worden opgenomen. Bij deze inzet werd nog een argument gebruikt om te verlengen, namelijk een beperktere belasting voor buitenlandse opsporingsactiviteiten (deze inzet vond gedeeltelijk in het buitenland plaats).
Zoals aangegeven worden niet alle inzetten verlengd. Doorgaans vindt geen verlenging plaats op het moment dat een inzet onvoldoende resultaat oplevert, bijvoorbeeld omdat blijkt dat een verdachte niet of nauwelijks gebruik maakt van het geautomatiseerde werk waarop binnengedrongen is. Daarnaast, en dat geldt voor één van de geselecteerde inzetten, kan de omgeving waarin de verdachte zijn handelingen verricht *offline* gaan waardoor handelingen niet langer zichtbaar zijn voor de politie. Bij deze inzet speelde nog een ander argument een rol om de inzet te stoppen. Eén van de geïnterviewden vertelt dat de verdachte in deze zaak ook nog verdachte was in een ander (internationaal) onderzoek. In dat laatste onderzoek waren meer aanknopingspunten om de verdachte mogelijk veroordeeld te krijgen. Een inzet wordt ook niet meer verlengd op het moment dat het tactisch onderzoek 'geklapt' is en de verdachten worden aangehouden.

Bij het traject om een inzet te verlengen zijn dezelfde actoren betrokken die zich buigen over de vraag of de bevoegdheid überhaupt in een opsporingsonderzoek kan en mag worden ingezet. De rechter-commissaris dient doorgaans elke vier weken een nieuwe machtiging af te geven. De betrokkenheid van de rechter-commissaris gedurende de looptijd van het bevel verschilt. Twee geïnterviewden vertellen dat zij als rechter-commissaris zich gedurende de looptijd van het bevel niet bemoeien met de uitvoering van het bevel. Eén van hen legt uit dat het wel voor kan komen dat een voorwaardelijke machtiging wordt afgegeven (en dit geldt niet alleen voor verlengingen), bijvoorbeeld als nog onduidelijk is of een technisch hulpmiddel wordt ingezet.
Naast de rechter-commissaris velt de CTC een oordeel over een mogelijke verlenging. In de begintijd van de inzet van de bevoegdheid diende dat steeds te gebeuren vlak voordat de looptijd van het bevel beëindigd was. Dat bleek in de praktijk niet goed werkbaar, omdat de CTC met enige regelmaat een beslissing moest nemen over de verlenging van een inzet waarbij het nog niet gelukt was om binnen te dringen. Om tijd te besparen is afgesproken dat Digit voor het binnendringen langer de tijd krijgt, bijvoorbeeld twee maanden, en dat binnen vier weken na het binnendringen een mogelijke verlenging moet worden voorgelegd.
In principe komen de CTC en de rechter-commissaris tot eenzelfde oordeel. Verteld wordt dat het bij een verlenging wel eens voorgekomen is dat de CTC anders (negatief) besloot dan de rechter-commissaris (positief). Dat kon gebeuren vanwege de door de CTC langer toegestane looptijd. Voor deze inzet is er een bevel beëindiging 126nba gekomen.

### *5.5.3 Hoofdpunten*

- Het grootste deel van de inzetten is verlengd. Vaak is aanvullende informatie in het opsporingsonderzoek benodigd. Inmiddels is binnen Digit de afspraak gemaakt dat inzetten niet voor langere tijd verlengd kunnen worden (in principe maximaal twee keer).
- Een inzet wordt niet verlengd wanneer een zaak 'geklapt' is, het geautomatiseerde werk niet in gebruik blijkt bij de verdachte, of dat het onderzoek te weinig informatie oplevert.
- Bij de beslissing of een inzet verlengd wordt, zijn dezelfde actoren betrokken die zich bezighouden met de vraag of een inzet überhaupt binnen een opsporingsonderzoek mag plaatsvinden, inclusief het daarbij behorende tijdpad.
- De CTC bouwt inmiddels in haar advies een langere periode in (bijvoorbeeld twee maanden) waarin geprobeerd kan worden een geautomatiseerd werk binnen te komen. Daartoe is besloten, omdat anders te snel weer besloten moest worden over een verlenging.

# 6 Afronden inzet en vervolgstappen

## 6.1 Inleiding

In dit hoofdstuk staat de afronding van de inzet van de bevoegdheid centraal en de vervolgstappen die daarna genomen worden (deelvraag 5). Na een samenvatting van het wettelijk kader richt de aandacht zich op de activiteiten die Digit onderneemt, waaronder de verwijdering van een technisch hulpmiddel en de omgang met gegevens (de overdracht ervan, geheimhoudersgegevens, vernietiging en dossiervorming). Daarna wordt aandacht besteed aan de opbrengst voor het tactisch onderzoek en de notificatieplicht. Het hoofdstuk besluit met een kleine paragraaf over de toetsing door een zittingsrechter.

## 6.2 Samenvatting wettelijk kader

Als het doel van een onderzoek in een geautomatiseerd werk is bereikt, of de geldigheidsduur van het bevel is verlopen, wordt een inzet beëindigd. Indien gebruik is gemaakt van een technisch hulpmiddel, dan moet dit zoveel als mogelijk verwijderd worden, zodat de server van de politie geen gegevens meer kan ontvangen (artikel 25 lid 1 Bogw; *Kamerstukken II* 2015/16, 34372, 3, p. 36). Het is de bedoeling dat het technisch team de resultaten van het onderzoek overdraagt aan het tactisch team (artikel 29 lid 1 Bogw). Mocht het binnen de reikwijdte van het bevel passen en in het kader van het opsporingsonderzoek nodig zijn, dan filtert het technisch team de gegevens (Besluit onderzoek in een geautomatiseerd werk, p. 17).
Voor geheimhoudersgegevens gelden de reeds bestaande wettelijke kaders zoals vastgelegd in artikel 126aa Sv. Het streven is om de handelingen die Digit verricht 'zo spoedig' mogelijk vast te leggen in een proces-verbaal (*Kamerstukken II* 2016/17, 34 372, nr. 3, p. 78). In verband met de afscherming van onderzoeksmethoden kan gekozen worden voor een verantwoording die minder gedetailleerd is. Het is aan de officier van justitie om hier een oordeel over te vellen (Besluit onderzoek in een geautomatiseerd werk, p. 22).
In aansluiting op de regeling voor de notificatie van bijzondere opsporingsbevoegdheden (artikel 126bb Sv) is er de verplichting om betrokkenen op de hoogte te brengen dat de bevoegdheid is ingezet. Dit betekent dat degene wiens geautomatiseerde werk is binnengedrongen in kennis moet worden gesteld dat een inzet heeft plaatsgevonden (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 40). Ook wanneer een geautomatiseerd werk in het buitenland wordt binnengedrongen is in principe notificatie vereist (*Kamerstukken II* 2016/17, 34 372, nr. 6). Notificatie is niet nodig als het proces-verbaal van de toepassing van de bevoegdheid is toegevoegd aan de processtukken (*Kamerstukken II* 2016/17, 34 372, nr. 6).

Wat betreft de vernietiging van gegevens gelden verschillende regimes. Met betrekking tot de gegevens op de technische infrastructuur hangt de bewaartermijn af van het doel waarvoor de gegevens verzameld zijn.
Op het moment dat gegevens niet langer nodig zijn voor het doel van het onderzoek, mogen zij maximaal een halfjaar worden bewaard om te bekijken of zij aanleiding geven tot een nieuw onderzoek of een nieuwe verwerking. Hoe lang een periode duurt totdat gegevens niet meer nodig zijn, is niet exact vastgelegd. Indien een zaak niet wordt ingezonden aan het Openbaar Ministerie, mogen gegevens bewaard blijven tot

het moment waarop de feiten die in het onderzoek centraal staan, zijn verjaard (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 22-23). Daarna mogen gegevens nog vijf jaar worden bewaard ten behoeve van de afhandeling van eventuele klachten en of verantwoording van onderzoeksactiviteiten die hebben plaatsgevonden. Na die vijf jaar dienen gegevens gearchiveerd of vernietigd te worden (Besluit onderzoek in een geautomatiseerd werk, 2018, p. 23).[121]
Voor het verwijderen van gegevens van 'onschuldige derden' gelden verschillende verwijderingsregimes, afhankelijk van de onderzoekshandeling die is uitgevoerd (*Kamerstukken II* 2018/19, 34 372, nr. 29, p. 14).

## 6.3 Afronding inzet

### *6.3.1 Verwijderen technisch hulpmiddel & evaluatie*

Een inzet wordt beëindigd als een bevel is uitgevoerd of anders uiterlijk op de laatste dag van de looptijd van het bevel. Een geïnterviewde opsporingsfunctionaris vertelt dat het 'altijd weer een verrassing is wanneer een zaak eindigt'. Het tactisch opsporingsonderzoek loopt door tijdens een inzet van Digit en (ook) daarin zijn voortdurend nieuwe ontwikkelingen. Soms wordt het werk van Digit ingehaald door die ontwikkelingen waardoor een zaak in één klap stopt of juist in een stroomversnelling komt.
Op het moment dat een inzet stopt, moet het technisch hulpmiddel van het geautomatiseerde werk worden verwijderd (artikel 25 Bogw, lid 1). Eén van de geïnterviewden werkzaam bij Digit vertelt dat het verwijderen van het commerciële hulpmiddel relatief eenvoudig gaat. Het verwijderen van dit middel lukt echter niet altijd direct. Als het op een later moment is gelukt om het technisch hulpmiddel te verwijderen, krijgt Digit-politie een bevestiging. Overigens is het nooit volledig uit te sluiten dat na verwijdering sporen achterblijven van het technisch hulpmiddel, zo legt deze geïnterviewde uit. De achtergebleven resten zouden doorgaans minimaal zijn. Wanneer dat niet het geval is, wordt met de Digit-officier van justitie gekeken wat mogelijke consequenties zijn voor het geautomatiseerde werk. Verder vertellen enkele geïnterviewden dat het bij één inzet niet gelukt is om het technisch hulpmiddel te verwijderen. Daarvan is een apart proces-verbaal opgemaakt. Het gaat hierbij om een eigen door Digit ontwikkeld hulpmiddel. Eén van hen legt uit dat bij deze betreffende inzet het bevel 'vrij plotseling stopte' waardoor er geen tijd meer was om het hulpmiddel te verwijderen. Deze geïnterviewde merkt op dat van deze ervaring is geleerd. Inmiddels wordt een automatische verwijderingsoptie ingebouwd. Indien een technisch hulpmiddel niet volledig kan worden verwijderd, probeert Digit de verbinding tussen het geautomatiseerde werk en Digit te verbreken.
Binnen Digit-politie is de werkafspraak gemaakt dat de operationeel coördinatoren een eindvermelding maken in het journaal waarin de laatste stand van zaken wordt beschreven. Ook dienen daarin de gemaakte eindafspraken met het tactisch politieteam en/of de zaaksofficier te worden opgenomen. Soms wordt na afloop van de inzet nog een eindgesprek gevoerd met het tactisch team. Het doel van zo'n eindgesprek is het evalueren van de inzet en eventuele afstemming over de beschrijving van de inzet in het procesdossier. Hoewel het streven was en is om dit na

[121] De officier van justitie houdt gegevens beschikbaar voor het onderzoek die verkregen zijn door observatie, het opnemen van vertrouwelijke communicatie en het opnemen van telecommunicatie met een technisch hulpmiddel en die niet bij de processtukken zijn gevoegd. Twee maanden na het beëindigen van het onderzoek en het op de hoogte stellen van betrokkenen dat bevoegdheden zijn ingezet, vernietigt de officier van justitie de processen-verbaal en andere voorwerpen (Besluit onderzoek in een geautomatiseerd werk, 2018), p 23.

elke inzet te doen, komt het er in de praktijk niet altijd van door tijdgebrek. Wel probeert Digit-politie na elke inzet een terugkoppeling te krijgen van het tactisch team over wat de inzet heeft opgeleverd.

### *6.3.2 Overdracht gegevens aan het tactisch team*

In paragraaf 4.4.7 is reeds stilgestaan bij de overdracht van gegevens aan het tactisch team. Deze overdracht vindt niet alleen gedurende een inzet plaats, maar ook na afloop ervan. De gegevens die worden overgedragen zijn in principe ruwe data. Het Team Digitale Ondersteuning (TDO) van de betreffende eenheid zal, indien nodig, de digitale resultaten inzichtelijk maken voor het tactisch team. Wanneer het ter uitvoering van het bevel nodig is om de gegevens te filteren, draagt Digit-politie zorg voor de selectie van onderzoeksgegevens. Dat wordt gedaan om ervoor te zorgen dat binnen de categorieën van gegevens die in het bevel van de officier van justitie zijn opgenomen uitsluitend de gegevens ter beschikking komen van het tactisch team die van belang zijn voor het opsporingsonderzoek (intern document 1). De afweging welke gegevens met het tactisch team gedeeld moeten worden is, zoals eerder gezegd, in ontwikkeling. Eén van de geïnterviewden werkzaam bij Digit merkt op dat tijdens de overdracht van de gegevens weleens 'wat discussie is geweest over wat precies gedeeld kon worden'. Dat was naar aanleiding van een aanvullend verzoek van het tactisch team. De discussie kwam voort uit het feit dat het tactisch team om gegevens vroeg aan de hand waarvan mogelijk meer duidelijk zou kunnen worden over de aanwezigheid van Digit op het geautomatiseerde werk. Als oplossing is in deze casus gekozen om het verstrekken van een *image* (van de server) goed te keuren.

De inzet van de hackbevoegdheid levert in de meeste gevallen een grote hoeveelheid data op die nog geanalyseerd moet worden door het tactisch team. Dat is iets waarvan de zaaksofficieren zich niet altijd bewust waren. Het verwerken van die gegevens is arbeidsintensief en verhoudt zich niet altijd goed tot de inzet in een opsporingsonderzoek waarbij de wens bestaat om snel te kunnen handelen. Eén van de geïnterviewde zaaksofficieren zegt dat element in de toekomst wel mee te nemen wanneer de inzet van de bevoegdheid overwogen wordt:

> '*Ja toch wel scherp zijn in wat voor zaak je het* [de inzet van de hackbevoegdheid] *wil doen. Wat de meerwaarde is om het op dat moment allemaal binnen te gaan krijgen. En daar moet je toch wel heel goed over nadenken. Want de inzet die daar aan vast zit, is wel heel groot.'*

In het eerste deel van de evaluatie is slechts beperkt stilgestaan bij wat de toepassing van de bevoegdheid aan de tactische kant van een opsporingsonderzoek betekent. Dit onderwerp zal uitgebreider aandacht krijgen tijdens het tweede deel van de evaluatie.

**Omgang geheimhoudersgegevens[122]**
Gegevens worden alleen aan het tactisch team overgedragen als de verzamelde gegevens binnen het bevel vallen. Niet alle gegevens kunnen dus zomaar worden verstrekt aan het tactisch team. Dat geldt ook voor gegevens die betrekking hebben op geheimhouders zoals een advocaat. Op grond van artikel 126aa Sv moeten processen-verbaal of andere stukken die mededelingen bevatten die zijn gedaan door of aan een geheimhouder (geheimhoudersgegevens) worden vernietigd. In haar werkafspraken met het tactisch team beschrijft Digit-politie: 'door DIGIT wordt geen

[122] Voor een aantal beroepen zoals medische en juridische beroepen bestaat het verschoningsrecht. Gesprekken met deze geheimhouders mogen niet worden opgenomen.

onderzoek gedaan naar mogelijke aanwezigheid van geheimhoudersgegevens'. Het tactisch team moet daarom de vastgelegde en verstrekte informatie op gelijke wijze behandelen als bijvoorbeeld in beslag genomen goederen. Het tactisch team dient zelf een geheimhouderscheck uit te voeren en overeenkomstig de geheimhoudersprocedure te handelen' (intern document 1). 'Digit gaat die data niet uitpluizen', aldus één van de geïnterviewden vanuit Digit. Ook op OM-niveau zijn afspraken gemaakt over de procedure die doorlopen dient te worden (Intern document 11). Tijdens dit onderzoek is vanuit Digit aangegeven dat de wijze waarop met geheimhoudersgegevens omgegaan moet worden (vernietiging op basis van artikel 126aa Sv) in strijd is met artikel 28 van het Besluit waarin onder andere staat genoemd dat de inhoud van de op de technische infrastructuur vastgelegde gegevens in principe niet mag worden gewijzigd. Op het moment dat een deel van de gegevens uit een bestand verwijderd wordt, zal de integriteit van het bestand worden aangetast, aldus een geïnterviewde opsporingsfunctionaris. Dat dient volgens deze geïnterviewde, vooral op basis van de toelichting op artikel 28 van het Besluit, uitgesloten te worden. Deze geïnterviewde trekt een vergelijking met de tegengestelde veiligheidsvoorschriften in de kinderopvang:

> *'Dit is voor mij zo'n voorbeeld* [van de tegengestelde regels]*, en de beeldspraak zal ik vaker aan hebben gehaald. In de kinderopvang* [geldt:] *de GGD zegt, de deur moeten open staan zodat je kunt controleren dat jouw medewerker geen rare dingen met een kind doet. En de brandweer zegt die deur moet dicht, want* [dat] *is in het kader van die brandveiligheid vereist.'*

Vanwege de tegenstrijdigheid die voortkomt uit de bestaande regelingen, is besloten dat Digit géén geheimhoudersgegevens verwijdert, zoals artikel 126aa Sv voorschrijft. De Digit-officier van justitie heeft, 'gedekt door de landelijke vergadering van rechercheofficieren', deze 'niet als ideaal' bestempelde beslissing genomen.

**Vernietiging gegevens**

De Inspectie schrijft in haar Verslag over 2020 dat Digit nog niet uitgewerkt heeft 'hoe verwijdering, vernietiging en naleving van bewaartermijnen van vastgelegde gegevens in de praktijk moet worden uitgevoerd en wat dit betekent voor gegevens die op diverse plaatsen zijn vastgelegd' (Inspectie JenV, 2021, p. 18).[123] Dit geldt ook voor de vernietiging van gegevens na afloop van het verstrijken van termijnen. Eén van de geïnterviewden betrokken bij het toezicht vertelt dat een discussiepunt gaat over de vraag of het 'weggooien' van gegevens (bijvoorbeeld geheimhoudersgegevens) hetzelfde is als het 'wijzigen' van gegevens. Dat laatst mag volgens artikel 28 Bogw niet. Over het vernietigen van gegevens na afloop van een inzet merkt een andere geïnterviewde van Digit op dat Digit-politie met het bewaren en opslaan van gegevens werkt op zaaksniveau, terwijl de Wpg uitgaat van gegevens op persoonsniveau. Bij Digit levert dat verschil problemen op, omdat de gehele technische infrastructuur bij Digit erop gericht is gegevens op zaaksniveau te bewaren. Daardoor is het lastig om gegevens op persoonsniveau te verwijderen. Deze geïnterviewde vertelt dat op dit moment voor een oplossing is gekozen, vergelijkbaar met de wijze waarop met geheimhoudersgegevens wordt omgegaan. In plaats van verwijdering worden gegevens ontoegankelijk gemaakt voor de personen die aan een zaak gewerkt hebben. Volgens een geïnterviewde van de Inspectie zou het mogelijk moeten zijn om zowel

[123] In 2020 heeft de politie van de officier van justitie geen bevel ontvangen tot vernietiging of verwijdering van gegevens. In het derde Verslag constateert de Inspectie dat Digit een werkinstructie heeft opgesteld voor het verwijderen van bestanden in de technische infrastructuur. Een instructie die 'voldoende houvast' geeft. De instructie beschrijft alleen niet voldoende hoe alle te verwijderen bestanden te identificeren (Inspectie JenV, 2022, p. 33).

aan het Besluit als aan de Wpg te voldoen. Deze 'technische oplossingsrichtingen' zullen wel 'complex en tijdrovend' zijn. Deze geïnterviewde kan zich voorstellen dat er niet veel behoefte zal bestaan om hierin te investeren. In dat opzicht is het volgens deze geïnterviewde gemakkelijker om het Besluit te volgen en er vanuit te gaan dat gegevens niet mogen worden weggegooid.

### *6.3.3 Dossiervorming*

In de Verslagen van de Inspectie over de kalenderkaren 2019 en 2020 heeft de vastlegging en verslaglegging door Digit-politie nadrukkelijk aandacht gekregen (Inspectie JenV, 2020, 2021).[124] Geconstateerd werd onder andere dat de verslaglegging en verantwoording niet compleet waren en in sommige gevallen ontbraken. Omdat de Inspectie al uitgebreid op dit onderwerp is ingegaan, wordt dit onderwerp in dit rapport beperkt besproken.

In de eerste anderhalf jaar heeft het een tijd geduurd voordat de definitieve processen-verbaal gereed waren. Inmiddels wordt door Digit-politie en -OM wekelijks gemonitord wat de stand van zaken is met betrekking tot het op orde krijgen van officiële stukken zoals de definitieve processen-verbaal. Daarnaast is een extra dossiervormer aangesteld die – zeker in de begintijd – de taak had om ervoor te zorgen dat de dossiers op orde zouden komen. Tijdens de interviews zijn verschillende verklaringen genoemd waarom het op orde brengen van officiële stukken, zoals processen-verbaal, een tijd op zich heeft laten wachten. Eén daarvan gaat over de discussies die zijn gevoerd met betrekking tot de vraag welke informatie er wel en niet in het proces-verbaal moest worden opgenomen. Geprobeerd is om tot een standaard proces-verbaal te komen. Een opsporingsfunctionaris vertelt dat dat lastig was, bijvoorbeeld omdat Digit zowel standaardinzetten als maatwerkinzetten voor haar rekening neemt. Bij een standaardinzet moet bij het opstellen van een proces-verbaal met andere aspecten rekening worden gehouden dan bij een maatwerkinzet. Het was een 'ingewikkeld' proces om dat 'helder' te krijgen. Daarnaast hebben bij het vertraagd verbaliseren het weinig gebruiksvriendelijke interne journaliseersysteem een rol gespeeld, een gebrek aan overzicht welke processen-verbaal al wel en welke nog niet aanwezig waren en de 'waan van de dag'. Een andere geïnterviewde geeft aan dat vaak pas op verzoek van een tactisch team stukken werden verstrekt. Bovendien werden niet altijd definitieve stukken opgesteld, maar was er alleen een conceptversie van een proces-verbaal.

Het is de bedoeling dat de dossiervormer uiteindelijk een verzamelproces-verbaal opstelt voor de teamleider van Digit-politie. De inhoud van dit proces-verbaal wordt intern afgestemd met de jurist van Digit-politie en ondertekend door de teamleider van Digit-politie. Voor deze werkwijze is gekozen om zo veel mogelijk de afscherming van personen en methodieken te kunnen garanderen. Vanuit Digit-OM is als kader meegegeven dat medewerkers van Digit 'minimaal' moeten verbaliseren en 'maximaal' dienen te journaliseren. Bij het maken van een proces-verbaal moet 'niet te veel techniek en tactiek' prijsgegeven worden. Tegelijkertijd moeten er niet te veel vragen ontstaan over een proces-verbaal. Minimaal verbaliseren wordt belangrijk gevonden in verband met de afscherming van de opsporingsmethoden die worden gebruikt. Een 'slimme lezer' van een proces-verbaal zou, op basis van de informatie in het proces-verbaal, niet in staat moeten zijn zich te verdedigen tegen de technische hulpmiddelen die Digit inzet. Eén van de geïnterviewden merkt op dat het altijd zoeken is hoe open

[124] Ook in het derde Verslag is aandacht besteed aan de verslaglegging. De journalisering in 2021 is 'sterk verbeterd' ten opzichte van 2020 (Inspectie JenV, 2022, p. 27).

en transparant een rechter in te lichten over wat er is gedaan, zonder dat meteen alles prijsgegeven wordt over wat er kan en wat gedaan is. Het beperkt beschrijven van handelingen kan een zeker 'procesrisico' met zich meebrengen. Een dergelijk risico wordt bij de start van een inzet al besproken tussen Digit-OM en de zaaksofficier van justitie. De Inspectie heeft kritiek op de opdracht om minimaal te verbaliseren (Inspectie JenV, 2021, p. 12).

Het verzamelproces-verbaal (een samenvatting van de door Digit opgestelde verbalen) wordt door de dossiervormer via Digit-OM aan de zaaksofficier verstrekt en daarnaast gearchiveerd bij Digit-politie. De overige processen-verbaal die zijn opgemaakt voorafgaand aan en tijdens de inzet worden niet verstrekt aan het tactisch team maar door Digit-politie in een eigen beveiligde omgeving opgeslagen en daarnaast fysiek gedocumenteerd in een map.
Ook het tactisch team dient in de interne verslaglegging en in de processen-verbaal die het opstelt rekening te houden met het belang van de afscherming van de methodieken en medewerkers van Digit. Bijvoorbeeld door te verwijzen naar 'Digit' in plaats van naar individuele medewerkers. In de werkafspraken van Digit wordt ook benadrukt dat er in de op te stellen processen-verbaal en verlengingsaanvragen verwezen moet worden naar de resultaten van de door Digit uitgevoerde inzet, maar niet naar de werkwijze waarmee de gegevens zijn verzameld (intern document 1). Het nadrukkelijke verzoek is daarnaast in processen-verbaal niet de termen 'hacken' of 'hackbevoegdheid' te gebruiken. In de werkafspraken is ook opgenomen dat bij vragen over afscherming en gebruik van de resultaten van de inzet de zaaksofficier of het tactisch team contact dient op te nemen met Digit-politie en/of de Digit-officier.

### *6.3.4 Hoofdpunten*

- De verwijdering van een technisch hulpmiddel gebeurt doorgaans zo goed als volledig. Indien dat niet lukt, vindt overleg met de officier van justitie plaats en wordt een proces-verbaal opgemaakt.
- Rondom de verwijdering van gegevens inclusief geheimhoudersgegevens is er geen eenduidige regelgeving (het Besluit en artikel 126aa Sv spreken elkaar tegen). Digit-OM heeft daarom voor dit moment besloten dat geheimhoudersgegevens niet definitief verwijderd worden.
- Vanuit Digit-OM is wat betreft het verbaliseren het volgende kader meegegeven: minimaal verbaliseren (en maximaal journaliseren). Dit in verband met de afscherming van opsporingsmethoden.

## 6.4 Opbrengst tactisch onderzoek

Voor dit onderzoek zijn zeven inzetten diepgaander bestudeerd. Bij zes van deze zeven inzetten is het gelukt om binnen te dringen. Het in deze paragraaf geschetste beeld moet worden gezien als een eerste indicatie voor wat de bevoegdheid binnen een tactisch onderzoek kan opleveren. Dit onderwerp zal nader uitgewerkt worden in het tweede deel van de evaluatie.
De bevoegdheid heeft vooral sturingsinformatie opgeleverd, dat wil zeggen informatie die een tactisch onderzoek verdere richting kan geven. Bewijs verzamelen volgt dan vaak via andere wegen zoals één van de geïnterviewde zaaksofficieren uitlegt:

> '*We hebben een paar hele interessante documenten aangetroffen (…)* [en] *we hebben uiteindelijk ook die telefoons in beslag genomen. Dus het is niet dat we die*

*info alleen maar hebben vanuit de nba* [artikel 126nba Sv – de hackbevoegdheid]*, alleen hadden we hem wel op dat moment vanuit de nba. Dus daarom zeg ik, het helpt je met name om in de actualiteit te komen als sturingsinformatie, maar als je kijkt voor je bewijs, dat hebben we ook binnengehaald (…) via inbeslagnemen* [tijdens] *de actiedag.'*

De inzetten die zijn bestudeerd ten behoeve van dit onderzoek hebben niet in alle gevallen het gewenste resultaat opgeleverd. Soms omdat het binnendringen niet lukte, in andere gevallen werd wel binnengedrongen en werden gegevens veiliggesteld, maar werd niet de informatie aangetroffen waarnaar het tactisch team zocht. Dat kan bijvoorbeeld gebeuren wanneer een verdachte over meerdere telefoons beschikt, en niet het 'goede' toestel wordt gekozen. Eén van de geïnterviewden vertelt:

*'Nou ja het treurige is: (…) op het moment dat we bij de CTC zaten, was er eigenlijk de keuze tussen twee telefoons. Telefoon A en telefoon B. En wij hebben voor telefoon A gekozen, omdat dat… nou goed daar waren allerlei redenen voor… maar dat bleek tactisch de verkeerde keuze te zijn geweest. En dat heeft vertraging opgeleverd, want natuurlijk hadden we over kunnen stappen naar telefoon B, maar inmiddels waren we toch wel weer zo ver in het onderzoek dat dat eigenlijk geen toegevoegde waarde meer zou bieden. (…). Dus het is jammerlijk mislukt qua inzet laat ik het zo maar zeggen. Dus het heeft voor ons uiteindelijk niks opgeleverd.'*

Ook kan het zijn dat de verwachtingen van het tactisch team en Digit-politie niet overeenkomen. Tactische teams verwachten soms waardevollere informatie dan een inzet van Digit kan opleveren. Het binnendringen van apparaten levert zelden de 'smoking gun' op waarnaar een tactisch team zoekt, zo vertelt een geïnterviewde. Een ander legt uit dat de verwachtingen van de buitenwereld ten aanzien van de bevoegdheid wellicht wat hooggespannen zijn.

*'Dit is niet de kip met de gouden eieren, dit is een gewoon een kip en die legt scharreleieren en die heb je wel nodig, alleen je gaat niet met deze bevoegdheid die smoking gun vinden. Het is gewoon een volgend stuk gereedschap in je* toolbox*. En zo moet je hem dus ook behandelen. (…). Het heeft (…) soms bijna mythische proporties hoe in het politiek debat hierover gedacht werd. Dat is het uiteindelijk niet, dat blijkt het niet te zijn.'*

Ondanks dat de inzet van de hackbevoegdheid dus niet altijd het gewenste resultaat oplevert, is een aantal geïnterviewde tactisch officieren toch te spreken over de ervaring die zij hebben opgedaan met de hackbevoegdheid. Het niet slagen van een inzet binnen het ene opsporingsonderzoek is géén reden om de bevoegdheid een volgende keer niet weer in te willen zetten. Eén van hen zegt hierover:

*'Ik vond het team professioneel, ik vond de communicatie professioneel, ik vind de manier waarop we het binnen het OM hebben gedaan professioneel en het is ook gewoon een kwestie van… net als met OVC, de ene OVC plaats je in een rooster en* [dan] *hoor je alleen maar ruis en een volgende keer heb je het bewijs. En dan denk ik ja… zo sta ik niet in de beoordeling van zo'n middel* [dat ik het om die reden een volgende keer niet meer in wil zetten]*. Dus nee, we hebben hem heel recent weer overwogen.'*

### 6.4.1 *Hoofdpunt*

- De resultaten van de bevoegdheid lijken vooralsnog vooral als sturingsinformatie te worden gebruikt.

## 6.5 Notificatieplicht

De notificatieplicht met betrekking tot de hackbevoegdheid is de verantwoordelijkheid van de zaaksofficier van justitie. Bij de inzetten die door een zittingsrechter behandeld worden, zo vertelt één van de geïnterviewde zaaksofficieren, wordt een toelichting in het 'BOB-dossier', waarin de gebruikte methodieken worden toegelicht, gezien als notificatie. Deze geïnterviewde vertelt daarbij de keuze te hebben hoe uitgebreid de toelichting is. Op het moment dat een ingezette bevoegdheid leidt tot bewijs zal meer toelichting moeten worden gegeven. Anders volstaat 'een mededeling in het relaas' met daarin ook een vermelding van het ingezette artikel.
Het is bij Digit-OM niet exact bekend hoeveel inzetten er tot en met maart 2021 zijn geweest waarin de (voormalig) verdachte op enig moment genotificeerd diende te worden. Ook is niet bekend in hoeveel zaken deze notificatie inmiddels heeft plaatsgevonden.
In de voor dit onderzoek geselecteerde inzetten waarvan de zaak niet door een zittingsrechter zal worden behandeld (drie in het totaal, zie volgende paragraaf) zijn de verdachten (nog) niet genotificeerd.[125] Uitstel is bijvoorbeeld mogelijk wanneer nog andere opsporingsonderzoeken lopen die door de notificatie 'stuk' worden gemaakt. In één van deze zaken was er gedurende het onderzoek geen verdachte waardoor notificatie niet kon plaatsvinden. Wel is in deze zaak de 'fingerprint' van de code gepubliceerd. In de tweede zaak, waarin de inzet van Digit voor de (inmiddels niet-) verdachte vergaande consequenties had, lijkt deze persoon nog niet te zijn genotificeerd. Eén van de geïnterviewden vanuit Digit merkt op dat er nog een 'dreiging' zou zijn. Een andere geïnterviewde geeft aan niet zo goed te weten of notificatie heeft plaatsgevonden. Volgens deze geïnterviewde zou er geen bezwaar moeten zijn om de verdachte te notificeren. In een derde zaak heeft nog geen notificatie plaatsgevonden, omdat dat een onderzoeksbelang zou schaden.

### 6.5.1 *Hoofdpunt*

- De notificatieplicht is de verantwoordelijkheid van de zaaksofficier van justitie. Nog niet in elke zaak heeft notificatie plaatsgevonden, vooral omdat dat een opsporingsbelang zou kunnen schaden.

## 6.6 Toetsing zittingsrechter

Voor zover bekend zijn er nog geen zaken inhoudelijk door een zittingsrechter behandeld waarin de hackbevoegdheid is ingezet. Derhalve is het, zoals al een aantal keer genoemd, niet mogelijk om in dit rapport aandacht te besteden aan de toetsing achteraf door een zittingsrechter en aan de waardering van de nieuwe bevoegdheid als bewijsmiddel (leveren de gegevens daadwerkelijk bewijs op in een strafzaak?). Dit thema wordt meegenomen in het tweede deel van de evaluatie. Wel is gedurende deze eerste evaluatie duidelijk geworden dat niet alle zaken waarbinnen Digit een inzet doet

[125] Dat lijkt niet uitsluitend te spelen bij de hackbevoegdheid, zie bijvoorbeeld het onderzoek naar de inzet van undercoverbevoegdheden (Kruisbergen et al., 2010).

en waarin het binnendringen gelukt is door een rechter behandeld zullen worden. Daarvoor zijn verschillende redenen. Bij één van de geselecteerde inzetten waren er geen verdachten in beeld. Er wordt uitgelegd dat het de vraag is of die ooit in beeld zullen komen. Het opsporingsonderzoek (en de inzet van Digit) hebben vooral geleid tot verstoring van criminele activiteiten. Bij twee andere inzetten kon onvoldoende bewijs worden verzameld om de verdachte voor de rechter te brengen. Bij één van die inzetten bleek dat de verdachte onschuldig was (niet door de inzet van de hackbevoegdheid) en bij een andere inzet leverde de inzet van Digit (en ook alle andere ingezette opsporingsmiddelen) onvoldoende bewijs op om de zaak inhoudelijk te laten behandelen. Bij een andere inzet, tot slot, degene waar het verkeerde toestel was gekozen, zal de zaak wel inhoudelijk behandeld worden, maar wordt geen bewijs aangedragen verzameld met behulp van de hackbevoegdheid.

Hoewel de zaken dus nog niet inhoudelijk behandeld zijn, denken zaaksofficieren van justitie wel na over de samenstelling van het procesdossier. Na afronding van de inzet is het aan de zaaksofficier om er voor te zorgen dat een definitief dossier wordt opgesteld. In dat kader moet nagedacht worden over de vraag hoe de gegevens die Digit verzameld heeft een plek krijgen. Eén van de geïnterviewde zaaksofficieren vertelt te worstelen met de vraag welke selectie van gegevens in het dossier opgenomen moet worden, bijvoorbeeld met WhatsApp gesprekken. Daar zit veel informatie tussen die niet interessant is. Tegelijkertijd zal het ook niet voldoende zijn om slechts enkele berichtjes te selecteren die interessant zijn voor het onderzoek. En hoe dient de vindplaats te worden vermeld als in het dossier wordt opgenomen dat uit WhatsApp verkeer blijkt dat de verdachte op een bepaald moment een ontmoeting heeft? Dat zijn vragen die in het kader van het opstellen van het einddossier beantwoord moeten worden. Soms kan ook besloten worden om in het dossier géén bewijs op te nemen dat verkregen is met de hackbevoegdheid, bijvoorbeeld als dezelfde informatie (of meer) ook uit een andere (bijzondere) opsporingsbevoegdheid naar voren komt, zoals een inbeslagname van een telefoon.

### *6.6.1 Hoofdpunt*

- Er is, voor zover bekend, nog geen zaak inhoudelijk behandeld door een zittingsrechter waarbij de hackbevoegdheid is ingezet. Bij een deel ervan zal dat ook nooit gebeuren.

# 7 Conclusie

## 7.1 Inleiding

Op 1 maart 2019 is de Wet Computercriminaliteit III in werking getreden. Met deze wet heeft de hackbevoegdheid een grondslag gekregen in het Wetboek van Strafvordering. In dit rapport is het proces geëvalueerd rondom de uitvoering van de hackbevoegdheid gedurende de eerste twee jaar na inwerkingtreding van de wet. De volgende onderzoekvraag stond daarbij centraal:

*Op welke wijze wordt uitvoering gegeven aan de hackbevoegdheid en welke eventuele knelpunten doen zich daarbij voor in de opsporingspraktijk?*

In dit concluderende hoofdstuk richt de aandacht zich op het beantwoorden van de hoofdvraag. Er is gekozen alleen in te gaan op de belangrijkste onderwerpen waarbinnen zich knelpunten voordoen. Allereerst wordt aandacht besteed aan de toetsing voorafgaand aan de inzet van de bevoegdheid, het binnendringen en de technische hulpmiddelen. Daarna richt de aandacht zich op de keuring van technische hulpmiddelen, inzetten met een buitenlandcomponent en functiescheiding. Afgesloten wordt met een vooruitblik naar deel 2 van de evaluatie.

## 7.2 Toetsing van de inzet: centrale rol Digit-OM

**Kernconclusie**
Aan de inzet van de bevoegdheid gaat een uitgebreid toetsingstraject vooraf door verschillende actoren. De technische toets vindt echter plaats bij een beperkt aantal personen. De rest van de actoren vaart op die deskundigheid.

Hoewel verschillende actoren betrokken zijn bij de toetsing van een inzet van de hackbevoegdheid, worden de technische aspecten van een inzet slechts door een beperkt aantal personen getoetst. Bij die toetsing is een zeer belangrijke rol weggelegd voor Digit-OM in overleg en samenspraak met Digit-politie.[126] Digit-OM is voor alle actoren vraagbaak en adviseur. Dat betekent dat Digit-OM een rol heeft bij de eerste selectie van inzetten en bij het ondersteunen van een tactisch team bij het opstellen van een aanvraagproces-verbaal. Ook licht Digit-OM de technische aspecten van een inzet toe aan actoren die zich bezighouden met de toetsing of de bevoegdheid überhaupt mag worden ingezet.
Er zijn tweede redenen waarom de technische aspecten van een inzet niet door alle betrokkenen bij het toetsingsproces gedetailleerd lijken te worden getoetst. De eerste is dat een zaaksofficier beperkt geïnformeerd wordt hoe een inzet (technisch) precies wordt uitgevoerd. Dat heeft te maken met de afscherming van de gehanteerde methodes. Een zaaksofficier krijgt alleen informatie over wat Digit nodig acht, mocht een zittingsrechter de zaak inhoudelijk behandelen. In dat opzicht moet de zaaksofficier erop vertrouwen dat Digit het goede doet. De tweede reden is dat het

[126] Bij de hackbevoegdheid is Digit (*Digital Intrusion Team*) een belangrijke speler. Digit zelf kent twee onderdelen: Digit-politie en Digit-OM. De uitvoering van de hackbevoegdheid is in handen van Digit-politie, ondergebracht bij de Landelijke Eenheid van de Nationale Politie. Digit-politie wordt aangestuurd door Digit-OM, ondergebracht bij het Landelijk Parket van het Openbaar Ministerie. Digit-OM bestaat uit één officier van justitie en één parketsecretaris.

volledig doorgronden van de technische finesses niet altijd aan de orde lijkt te zijn en niet haalbaar is. Digit-OM geeft op verzoek, maar ook op eigen initiatief, bij de Centrale ToetsingsCommissie (CTC) van het Openbaar Ministerie en bij de rechter-commissaris mondeling een toelichting op wat de inzet precies betekent, maar deze toelichting lijkt beperkt te worden tot de hoofdlijnen. Verder beschikt de CTC weliswaar over een haalbaarheidsonderzoek, maar daarin is het plan van aanpak met meer details over de werkwijze van Digit, niet opgenomen. Dit alles betekent dat een deel van die toetsing, vooral van de technische kant, zich beperkt tot een klein aantal personen. Digit-OM is zich bewust van deze prominente rol en weegt om die reden extra zorgvuldig wat wel en niet kan, bijvoorbeeld ten aanzien van de manier van binnendringen. Hierover vindt binnen het Openbaar Ministerie overleg plaats en dit wordt vastgelegd in interne documenten. Toch blijft staan dat de inzet van deze bevoegdheid zeer specialistische kennis vereist waarover maar weinig mensen beschikken. Omdat Digit-OM uit twee personen bestaat en de verantwoordelijkheid dus vooral op die schouders rust, maakt dat de positie van Digit-OM kwetsbaar. Een extra punt van aandacht is dat een deel van de technische details van een inzet hoogstwaarschijnlijk niet voorgelegd zullen worden aan een zittingsrechter. Dit komt deels omdat niet alle inzetten op zitting behandeld worden en deels omdat sommige informatie, bijvoorbeeld over het binnendringen, ook dan afgeschermd zal blijven.

## 7.3 Binnendringen in een geautomatiseerd werk

**Kernconclusie**

- Binnendringen kan niet altijd volledig op afstand, in tegenstelling tot wat de wetgever lijkt te hebben voorzien. Digit heeft daarom behoefte aan een (heimelijke) steunbevoegdheid die er momenteel niet is.
- De meldplicht ten aanzien van onbekende kwetsbaarheden geldt ook ten aanzien van kwetsbaarheden in geautomatiseerde werken die vrijwel alleen voor criminele doeleinden worden gebruikt. Dat is een knelpunt voor de opsporingsprakrijk, omdat personen met criminele intenties uiteindelijk op de hoogte moeten worden gebracht dat in hun systeem zich een kwetsbaarheid bevindt. Het is de vraag of dat werd bedoeld met het veiliger maken van computersystemen en het internet, een belangrijke reden waarom de meldplicht er is gekomen.
- Bij het grootste deel van de inzetten is, in tegenstelling tot de verwachting van de wetgever, gebruikgemaakt van een commercieel middel. Voor de opsporingspraktijk is de inzet van dat middel noodzakelijk. Zonder de inzet ervan zou het grootste deel van de inzetten op een telefoon niet mogelijk zijn geweest.
- De verplichting, voortvloeiend uit het Regeerakkoord, om bij een commercieel middel voor elke inzet een nieuwe licentie aan te schaffen, zorgt er hoogstwaarschijnlijk voor dat voor het gebruik ervan meer geld betaald wordt dan nodig is. Het is onwaarschijnlijk dat deze regeling voorkomt dat de markt van onbekende kwetsbaarheden gestimuleerd wordt.

### *7.3.1 Steunbevoegdheid*

In dit onderzoek is duidelijk geworden dat het voor het binnendringen soms nodig is om op locatie, in de buurt van het geautomatiseerde werk, aanwezig te zijn. De wetgever lijkt met deze optie geen rekening te hebben gehouden. Om toch op locatie aanwezig te kunnen zijn, moet Digit soms gebruikmaken van een (bijzondere)

opsporingsbevoegdheid. Van deze opsporingsbevoegdheid kan echter alleen gebruik worden gemaakt als die toevallig al door een tactisch team in het opsporingsonderzoek wordt ingezet. Deze afhankelijkheid van een tactisch team vormt voor Digit een knelpunt, omdat een tactisch team niet altijd van plan is zo'n bevoegdheid in te zetten. Daarom heeft Digit behoefte aan een steunbevoegdheid, vergelijkbaar met de wijze waarop dit geregeld is rondom het opnemen van vertrouwelijke communicatie (artikel 126l Sv). Daarnaast bestaat de wens vanuit Digit-OM om de inzet van deze steunbevoegdheid buiten het procesdossier te kunnen houden vanwege de afscherming van de gehanteerde methodes. Een argument dat door haar wordt aangevoerd waarom die afscherming niet problematisch zou moeten zijn, is dat met het binnendringen zelf géén bewijs wordt verzameld. Wel wordt om die reden gesuggereerd dat deze handelswijze door een rechter-commissaris getoetst zou moeten worden. Een dergelijke redenering stelt het opsporingsbelang voorop. Er zou daarentegen ook gesteld kunnen worden dat het binnendringen indirect bewijs kan opleveren, namelijk met behulp van onderzoekshandelingen die vervolgens worden verricht. Bovendien zou de stelling geponeerd kunnen worden dat, ook wat betreft het binnendringen, overwogen dient te worden of een inzet proportioneel is. Het gaat dan bijvoorbeeld om mogelijke ongewenste gevolgen die de wijze waarop een binnendringactie plaatsvindt, met zich mee brengt. Indien op geen enkele plek hierover verantwoording wordt afgelegd (de methode wordt immers afgeschermd) en feitelijk maar een beperkt aantal mensen een beslissing neemt over de wijze van binnendringen, is het de vraag of die beoordeling over de proportionaliteit op voldoende plekken wordt gemaakt.

### *7.3.2 Kwetsbaarheden en meldplicht*

Het gebruik van kwetsbaarheden[127] is doorgaans de manier waarop men een geautomatiseerd werk binnendringt. Kwetsbaarheden zijn zwakke plekken in hard- of software waardoor het voor derden mogelijk kan worden om op een geautomatiseerd werk binnen te komen. Om te kunnen binnendringen moeten kwetsbaarheden wel eerst gebruiksklaar gemaakt zijn. Rondom het gebruik van kwetsbaarheden zijn door verschillende partijen zorgen geuit, vooral omdat het bestaan en gebruik van deze kwetsbaarheden computersystemen onveiliger zou maken (zie bijlage 3). Vanuit het kabinet is de verwachting uitgesproken dat de politie vooral gebruik zou maken van bekende kwetsbaarheden, maar dat het gebruik van een onbekende kwetsbaarheid wordt gezien als 'een uiterste maar onmisbare optie voor de bestrijding van ernstige vormen van criminaliteit' (*Kamerstukken I* 2017/18, 34 372, G, p. 7). In verband met veiligheidsaspecten is (op indirecte wijze) een meldplicht afgesproken (voortkomend uit artikel 126ffa Sv waarin geregeld is dat het melden van een onbekende kwetsbaarheid uitgesteld mag worden, na een schriftelijke machtiging van een rechter-commissaris). Door een kwetsbaarheid te melden zou de (online) veiligheid verhoogd worden, omdat deze kwetsbaarheid niet langer misbruikt kan worden (ervan uitgaande dat de fabrikant de kwetsbaarheid verholpen heeft).
De meldplicht vormt voor Digit een knelpunt. In de eerste plaats omdat de meldplicht ook geldt voor kwetsbaarheden in systemen die specifiek gemaakt zijn voor en door personen met criminele intenties. Dat betekent dat deze personen uiteindelijk op de hoogte moeten worden gesteld dat in hun systeem, gebruikt voor criminele doeleinden, zich een kwetsbaarheid bevindt. Tot nu toe is één keer een machtiging gevorderd bij de rechter-commissaris om het melden van zo'n kwetsbaarheid uit te stellen. De rechter-commissaris heeft deze machtiging verleend, maar op een gegeven

[127] Vanwege de leesbaarheid wordt in dit hoofdstuk alleen nog onderscheid gemaakt tussen bekende en onbekende kwetsbaarheden. De onbekende kwetsbaarheden worden verder niet meer uitgesplitst.

moment zal de kwetsbaarheid toch gemeld moeten worden. Dit roept de vraag op in hoeverre het melden van dit soort kwetsbaarheden zorgt voor meer veiligheid. Het lijkt er eerder op dat personen met criminele intenties in dit soort gevallen juist de gelegenheid krijgen om hun afscherming beter op orde te brengen.
Ten tweede kan de meldplicht samenwerking met nationale, maar ook internationale partijen bemoeilijken. In sommige landen is het gebruik van een kwetsbaarheid staatsgeheim. Als Nederland met dat soort landen zou willen samenwerken, is dat problematisch omdat Nederland de verplichting heeft om hetgeen staatsgeheim is in het buitenland, in Nederland te melden. Het risico hiervan is dat die kwetsbaarheid niet langer bruikbaar is en samenwerking voor die landen onaantrekkelijk wordt.

### *7.3.3 Commerciële producten*

Hoewel het gebruik van een onbekende kwetsbaarheid werd gezien als 'uiterste optie', is duidelijk geworden dat Digit bij het overgrote deel van haar inzetten in de bestudeerde onderzoeksperiode gebruik heeft gemaakt van een commercieel product. Daarin zitten onbekende kwetsbaarheden verwerkt. Dat product wordt gebruikt voor standaardinzetten op een telefoon en met het product kan de politie zowel binnendringen als onderzoekshandelingen verrichten. Voor de opsporingspraktijk is dit product onmisbaar, omdat zij anders een groot deel van de inzetten (op een telefoon) niet kan doen. Hiervoor is een aantal redenen genoemd. De eerste is dat het zelf vinden van een onbekende kwetsbaarheid in een product, dat door nagenoeg alle Nederlanders wordt gebruikt, heel erg lastig is. Fabrikanten doen er bijvoorbeeld alles aan om hun product zo veilig mogelijk te maken en dus is er veel deskundige menskracht (en geld) nodig om deze kwetsbaarheden te vinden en gebruiksklaar te maken. Menskracht waarover Digit niet beschikt. De enige manier om enigszins in de buurt te komen bij wat een commerciële leverancier kan, is door op een veel grotere schaal (in elk geval Europees) aan de ontwikkeling van dit soort producten te werken. Dat is echter geen oplossing voor de nabije toekomst. Een andere reden is de meldplicht. Mocht het al lukken om zelf een onbekende kwetsbaarheid te vinden en gebruiksklaar te maken dan moet deze gemeld worden. Dat betekent dat die kwetsbaarheid, waarin veel tijd is gaan zitten om hem gebruiksklaar te maken, slechts een heel beperkt aantal keren kan worden gebruikt.
Uit het Regeerakkoord volgt dat het gebruik van een commercieel product dient te worden beperkt. Om de markt van onbekende kwetsbaarheden niet te stimuleren, dient per zaak een licentie te worden aangeschaft. Omdat dit product bij veel inzetten is gebruikt, wordt geschat dat deze afspraak ertoe heeft geleid dat inmiddels ruim twee keer de aanschafprijs voor het product betaald is. Ingeschat wordt dat het gaat om 'enkele miljoenen'. Gezien het relatief grote aantal inzetten waarin dit hulpmiddel wordt ingezet, is het onwaarschijnlijk dat het afgesproken licentiemodel ervoor zorgt dat de markt van onbekende kwetsbaarheden minder gestimuleerd wordt.

## 7.4 Technische hulpmiddelen

**Kernconclusie**
- Er bestaat discussie over de precieze invulling van de begrippen technisch hulpmiddel en handmatige inzet.
- Vanwege de lange ontwikkel- en keuringstijd, is slechts een klein aantal eigen technische hulpmiddelen ontwikkeld en die zijn beperkt ingezet.
- Technische hulpmiddelen zijn tot nu toe maatwerk. Digit zou graag werken met een aantal standaardcomponenten dat al gekeurd is. Dat is tot nu toe (nog) niet mogelijk gebleken.
- Digit overweegt steeds vaker een handmatige inzet. Dat betekent dat een werkwijze niet altijd volledig afgeschermd kan blijven. Dat wordt door Digit niet in alle gevallen als problematisch gezien.

Onderzoekshandelingen kunnen zowel met een technisch hulpmiddel als handmatig worden verricht. Een technisch hulpmiddel zorgt er kort gezegd voor dat data die relevant zijn voor een tactisch onderzoek (denk aan chatberichten, e-mails, geluidsbestanden), opgehaald worden bij de verdachte en worden opgeslagen in de digitale omgeving van Digit. Over de reikwijdte van het begrip technisch hulpmiddel bestaat discussie. De vraag of iets wel of géén technisch hulpmiddel is, is relevant omdat alleen een technisch hulpmiddel gekeurd dient te worden en Digit ziet de keuring als een groot knelpunt in de uitvoering (zie over de keuring zelf de volgende paragraaf). Digit stelt zich op het standpunt dat sprake is van een technisch hulpmiddel als drie processen (het detecteren, registreren, en transporteren van gegevens) volledig geautomatiseerd plaatsvinden. De Inspectie stelt, op basis van de toelichtende tekst in het Besluit, dat een script dat semi-handmatig wordt ingezet, ook een technisch hulpmiddel betreft. Wat semi-handmatig precies inhoudt, wordt in de wetstekst niet precies toegelicht.
Digit gebruikt twee soorten technische hulpmiddelen: commerciële producten en eigen door Digit-politie ontwikkelde hulpmiddelen. Slechts bij een klein aantal inzetten heeft Digit gebruik kunnen maken van een eigen ontwikkeld technisch hulpmiddel. Een belangrijke reden hiervoor is dat het veel tijd kost om een hulpmiddel te ontwikkelen èn uiteindelijk goedgekeurd te krijgen. Die lange doorlooptijd zorgt ervoor dat Digit slechts een klein aantal eigen ontwikkelde hulpmiddelen heeft kunnen gebruiken.
Tot nu toe is voor elke inzet een 'nieuw' technisch hulpmiddel ingezet, omdat een nieuwe inzet vaak vraagt om een aantal aanpassingen aan het technisch hulpmiddel. Bij Digit bestaat de wens om een aantal standaardcomponenten te ontwikkelen die in vrij korte tijd kunnen worden aangevuld, afhankelijk van de specifieke tactische onderzoekwensen bij een inzet. Er ontstaat dan een technisch hulpmiddel dat in een concrete zaak kan worden ingezet. Deze opzet is vooralsnog lastig gebleken, omdat bij de keuringen dit onderscheid niet wordt gemaakt en elk middel wordt gezien als een nieuw middel dat volledig gekeurd moet worden.
In de opsporingspraktijk wordt momenteel vaker dan in de begintijd overwogen een handmatige inzet te doen. Bij een handmatige inzet dient Digit haar werkwijze uitgebreider te verantwoorden, zodat op die manier met meer zekerheid kan worden gezegd dat met de werkwijze betrouwbare, integere en herleidbare gegevens zijn verzameld. Dat betekent wel dat de werkwijze niet volledig afgeschermd zal blijven. Niet in alle gevallen wordt dat door Digit als problematisch gezien.

## 7.5 Keuring van technische hulpmiddelen

**Kernconclusie**

- De keuring van technische hulpmiddelen moet ervoor zorgen dat gegevens die verzameld worden, betrouwbaar, integer en herleidbaar zijn. Voor Digit is het keuringsproces een groot knelpunt. Dat heeft te maken met het feit dat de twee belangrijkste actoren, Digit en de Keuringsdienst, vanuit een verschillend perspectief naar het keuringsproces kijken.
- Inzet van een vooraf goedgekeurd middel is in de praktijk nauwelijks haalbaar.
- Het grootste deel van de inzetten heeft plaatsgevonden met een commercieel hulpmiddel waarvan de Digit-officier van justitie besloten heeft dat de aard van het middel zich tot nu toe verzet tegen een keuring. Dit hulpmiddel zal hoogstwaarschijnlijk ook niet goedgekeurd kunnen worden.
- In de uitvoeringspraktijk wordt (ook) gebruikgemaakt van tactische aanvullende waarborgen. Deze maken geen onderdeel uit van het keuringsproces.

Gegevens die Digit met behulp van de hackbevoegdheid verzamelt, dienen betrouwbaar, herleidbaar en integer te zijn (vanwege de leesbaarheid wordt de opsomming hierna beperkt tot betrouwbaar). Een belangrijke waarborg om dit te realiseren is dat voorafgaand aan een inzet de Keuringsdienst een technisch hulpmiddel keurt. Voor Digit vormt de keuring een belangrijk knelpunt. Dat heeft te maken met het feit dat de twee betrokken actoren (Keuringsdienst en Digit) vanuit verschillende perspectieven naar het keuringsproces kijken. Deze perspectieven botsen in de uitvoeringspraktijk soms met elkaar.

### *7.5.1 Twee perspectieven*

Vanuit het perspectief van de Keuringsdienst staan vooral de regels uit het Besluit centraal en de daaruit voortvloeiende keuringseisen. Dat betekent onder andere dat een hulpmiddel, in lijn met het Besluit, alleen kan worden goedgekeurd als aan alle eisen wordt voldaan, al dan niet aangevuld met een aantal (extra) vervangende waarborgen. Op die manier kan met zekerheid worden gesteld dat de verzamelde gegevens betrouwbaar, integer en herleidbaar zijn. Dit perspectief botst soms met het perspectief van waaruit Digit het keuringsproces benadert. Binnen dit perspectief staan vooral de uitvoerbaarheid en de noodzakelijkheid van de regels uit het Besluit centraal en de daaruit voortvloeiende keuringseisen. Digit is kritisch ten opzichte van de keuring door de Keuringsdienst, omdat deze niet goed zou passen bij de hulpmiddelen die Digit ontwikkelt. De omgeving waarin deze middelen worden ingezet is namelijk niet volledig te controleren door Digit. Bovendien is inherent aan software, en dus aan de middelen die Digit gebruikt, dat met enige regelmaat een update plaatsvindt. Het is de vraag in hoeverre de Keuringsdienst daar rekening mee moet en kan houden, zeker wanneer een hulpmiddel vooraf goedgekeurd dient te worden. In de nota van toelichting op het Besluit staat beschreven dat dat in principe wel zou moeten.[128] Naast de uitvoerbaarheid wordt ook de noodzakelijkheid van de regels en eisen kritisch bekeken. In tegenstelling tot hoe de Keuringsdienst het keuringsproces bekijkt, is het volgens Digit niet nodig dat een technisch hulpmiddel aan alle keuringseisen voldoet. Daarom zou er, geredeneerd vanuit het perspectief van Digit, (meer) ruimte moeten zijn om rekening te kunnen houden met bewijswaardes en risicoanalyses. Rekening houden met bewijswaardes betekent dat het niet per se problematisch hoeft te zijn als

[128] De commissie Koops (2018) geeft een aantal overwegingen mee ten aanzien van de omgang met technische hulpmiddelen.

een hulpmiddel niet volledig is goedgekeurd. In de rechtszaal zou hier verantwoording over kunnen worden afgelegd. De consequentie hiervan is wel dat een opsporingsmethode niet meer volledig afgeschermd zal blijven. Vervolgens is het aan de rechter, eventueel na raadpleging van deskundigen, om het verzamelde bewijs op waarde te schatten. Dat vraagt wel dat een zaak waarin een inzet plaatsvond voor de rechter komt en dat een rechtbank over voldoende technische deskundigheid beschikt om deze inschatting te kunnen maken. Hoogstwaarschijnlijk zullen niet alle zaken inhoudelijk behandeld worden door een zittingsrechter. Daarnaast is het de vraag of de benodigde technische deskundigheid op dit moment voldoende aanwezig is. Verder betekent het meer centraal stellen van risicoanalyses dat veel meer uitgegaan zou moeten worden van de vraag wat het risico is als niet aan een bepaalde eis wordt voldaan, in plaats van dat het hulpmiddel voor goedkeuring aan die eis moet voldoen.

### *7.5.2 Moment van keuren en waarborgen*

In de afgelopen jaren is het Digit nauwelijks gelukt om een vooraf goedgekeurd technisch hulpmiddel in te zetten, vooral in verband met de (lange) ontwikkeltijd die hiermee gepaard gaat. Die ontwikkeltijd staat op gespannen voet met het dringende opsporingsbelang waarvan sprake moet zijn om de bevoegdheid in te mogen zetten. Het is dan ook de vraag of het altijd realistisch is om te eisen dat een vooraf goedgekeurd hulpmiddel dient te worden ingezet. In het Besluit is ook de mogelijkheid opengehouden om een hulpmiddel achteraf ter keuring aan te bieden of een keuring volledig achterwege te laten. Dat laatste zou een uitzondering moeten zijn. In de praktijk is dat niet het geval. De Digit-officier van justitie heeft geoordeeld dat de aard van een veelvuldig gebruikt commercieel hulpmiddel, waarvan de opsporingspraktijk de inzet ervan noodzakelijk acht, zich verzet tegen een keuring. Dat betekent dat aan één van de waarborgen, namelijk de keuring, bij een groot deel van de inzetten niet wordt voldaan. Wel is er in die gevallen aandacht voor het nemen van aanvullende technische en tactische waarborgen (zie volgende alinea). In de praktijk is gebleken dat dat middel hoogstwaarschijnlijk ook niet goedgekeurd kan worden. Het middel maakt namelijk gebruik van een server waartoe de leverancier toegang heeft. Weliswaar worden de verzamelde gegevens, zoals chatberichten van de verdachte, uiteindelijk op de server van Digit opgeslagen, maar dat neemt niet weg dat ook de leverancier gedurende het binnendringen en uitvoeren van onderzoekshandelingen (in theorie) toegang heeft tot de gegevens van een verdachte. Hoewel contractuele afspraken zijn gemaakt dat de leverancier deze gegevens niet mag inzien en alleen toegang mag hebben tot de server voor het onderhoud van zijn product, kan niet worden uitgesloten dat de leverancier ook op andere momenten zichzelf toegang verschaft tot de server. Alleen om die reden al kan een middel niet goedgekeurd worden. Vanuit Digit wordt beredeneerd dat een leverancier zich nooit op eigen initiatief toegang zal verschaffen tot de server om gegevens in te zien, omdat de kans op reputatieschade te groot is en de financiële risico's die dat met zich meebrengt te hoog. Toch betekent dit dat de betrouwbaarheid en de integriteit van de verzamelde gegevens in het gedrang kunnen komen.

Indien de Digit-officier besluit dat de aard van een technisch hulpmiddel zich verzet tegen een keuring, dan dienen waarborgen aanwezig te zijn om ervoor te zorgen dat het bewijs betrouwbaar is. In de toelichting op het Besluit blijkt dat het daarbij vooral kan gaan om technische waarborgen. Deze aanvullende waarborgen dient de officier van justitie te verantwoorden in het procesdossier. In de opsporingspraktijk wordt niet alleen gezorgd voor aanvullende technische waarborgen, maar ook voor aanvullende tactische waarborgen. Bij die laatste soort waarborgen gaat het om maatregelen die

het tactisch team neemt om gegevens verkregen met het niet gekeurde technisch hulpmiddel te kunnen verifiëren. In het Besluit wordt er geen rekening mee gehouden dat dat soort maatregelen genomen kan worden en in de praktijk ook genomen wordt. Dit roept de vraag op of het niet mogelijk is – voordat een zittingsrechter dat kan doen – met dit soort waarborgen rekening te houden bij een beoordeling van de betrouwbaarheid, herleidbaarheid en integriteit.

## 7.6 Toezicht door de Inspectie

**Kernconclusie**

- De Inspectie richt zich op de naleving van regels en niet op de uitvoerbaarheid van die regels. Digit ervaart dit als lastig, omdat een deel van de regels in haar ogen niet uitvoerbaar is en Digit dus nooit aan die regels zal (kunnen) voldoen.
- Het is onduidelijk wat de consequenties zijn als de Inspectie constateert dat de regels niet worden nageleefd.
- De reikwijdte van het toezicht door de Inspectie leidt tot discussie. Die discussie wordt voor een belangrijk deel veroorzaakt door het feit dat het werk van Digit-OM en Digit-politie onlosmakelijk met elkaar verbonden is.
- Het is voor de Inspectie niet goed mogelijk om systeemtoezicht uit te voeren, omdat Digit niet beschikt over een (volledig) eigen kwaliteitssysteem. In de praktijk bestaat onduidelijkheid over wat onder een kwaliteitssysteem moet worden verstaan.

In de uitvoeringspraktijk doet zich een aantal knelpunten voor waardoor het toezicht door de Inspectie niet zonder discussie verloopt. Naar aanleiding van de Verslagen van de Inspectie is Digit begonnen een aantal elementen binnen haar werkwijze te verbeteren. Toch heeft Digit besloten een aantal door de Inspectie gesignaleerde punten naast zich neer te leggen. Dat heeft te maken met het feit dat Digit deze punten binnen het Besluit niet goed uitvoerbaar vindt. De Inspectie richt zich echter op de wijze waarop Digit volgens het wettelijk kader zou moeten handelen, omdat het aan de wetgever is een oordeel te vellen over de uitvoerbaarheid van dat wettelijk kader (en of aanpassing nodig is). Geen oog voor de uitvoerbaarheid betekent dat de eisen uit het Besluit waarvan Digit besloten heeft dat zij daaraan niet zal (kunnen) voldoen, punten zullen zijn die de Inspectie zal blijven constateren en waarmee Digit op haar beurt niets zal doen. Een dergelijke patstelling roept de vraag op of de beoogde effecten van het toezicht behaald kunnen worden en wat de consequenties zijn als de Inspectie iets constateert en Digit besluit om daar verder niets mee te doen.

Het tweede knelpunt betreft de reikwijdte van het toezicht. De Inspectie houdt toezicht op het handelen van de politie en niet op dat van het Openbaar Ministerie. Het handelen van de Digit-officier en van Digit-politie is in de praktijk echter onlosmakelijk met elkaar verbonden en beide zijn daardoor lastig uit elkaar te trekken. Digit-OM stelt zich op het standpunt dat nagenoeg alle handelingen die Digit verricht onder het gezag van de officier van justitie plaatsvinden en dat om die reden de Inspectie niets over die handelingen te zeggen heeft. De Inspectie vindt dat zij daar wel degelijk toezicht op kan houden, omdat Digit-politie deze handelingen uitvoert en soms Digit-OM hierover adviseert. Bovendien zou de beperkte invulling van het toezicht, zoals Digit-OM het ziet, ervoor zorgen dat de Inspectie bijna nergens meer uitspraken over kan doen. Om die reden is het wenselijk dat er meer duidelijkheid komt over wie nu toezicht houdt en op welke onderwerpen de Inspectie toezicht houdt. Met deze gesprekken is reeds een begin gemaakt.

Een derde knelpunt gaat over de vraag wat nodig is om goed systeemtoezicht uit te kunnen voeren. In de wetsgeschiedenis wordt een globale definitie van systeemtoezicht gegeven, namelijk toezicht houden op het functioneren van het wettelijk systeem. Er wordt niet veel gezegd over *hoe* dat toezicht zou moeten plaatsvinden, behalve dat de Inspectie naar individuele zaken kan kijken. Juist de *hoe*-vraag levert in de uitvoeringspraktijk problemen op. De Inspectie wil zich bij haar toezicht kunnen baseren op interne kwaliteitssystemen van Digit. Dit is in lijn met de wijze waarop systeemtoezicht door de Inspectieraad gedefinieerd wordt (Inspectieraad, 2007, p. 4-5). Op het moment van schrijven van dit rapport is zo'n kwaliteitssysteem niet (volledig) aanwezig. Bovendien blijkt er onduidelijkheid te bestaan over de vraag wat een kwaliteitssysteem precies inhoudt. In de nabije toekomst zou het daarom goed zijn om te kijken naar wat in de praktijk georganiseerd moet worden om het systeemtoezicht van de grond te krijgen.

## 7.7 Inzetten met een internationale component

**Kernconclusie**
- De OM-aanwijzing (Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex. artikel 126nba Sv) richt zich op inzetten van Nederland op buitenlands grondgebied. In de OM-aanwijzing is niets geregeld voor inzetten op Nederlands grondgebied door het buitenland. Daardoor moeten ingewikkelde juridische constructies worden bedacht.

De OM-aanwijzing regelt inzetten die op verzoek van Nederland in het buitenland plaatsvinden. Voor inzetten door het buitenland in Nederland is echter niks geregeld. Voor de uitvoeringspraktijk is dat ingewikkeld, omdat in die gevallen complexe juridische constructies moeten worden bedacht waarbinnen verschillende rechtshulpverzoeken over en weer worden ingediend. Een ander meer praktisch punt is dat voor inzetten door het buitenland geen verlofprocedure is afgesproken, terwijl die voor andere bijzondere opsporingsbevoegdheden wel bestaat. Zo'n verlofprocedure houdt in dat, indien het buitenland een bijzondere opsporingsbevoegdheid in Nederland wil inzetten en daar toestemming voor is, de rechter-commissaris nog toestemming moet geven voor de daadwerkelijke overdracht van gegevens die met de bijzondere opsporingsbevoegdheid verzameld zijn. Dit is ter controle van een rechtmatige toepassing van de bevoegdheid.

## 7.8 Functiescheiding

**Kernconclusie**
- Strikte functiescheiding tussen het tactisch team en Digit-politie is wat betreft de uitvoering van de hackbevoegdheid een problematisch concept. Het technisch en het tactisch team hebben elkaar nodig om optimaal uitvoering te kunnen geven aan de hackbevoegdheid.

Uit de wetsgeschiedenis blijkt dat sprake dient te zijn van strikte functiescheiding. Die functiescheiding moet onder andere voorkomen dat Digit wordt beïnvloed als zij afwegingen maakt ten aanzien van de haalbaarheid van een inzet en de uitvoering ervan. In de praktijk vindt tussen Digit en het tactisch team regelmatig overleg en informatie-uitwisseling plaats, zowel voordat de bevoegdheid wordt ingezet als

gedurende de inzet. Juist voor een goede uitvoering, zo laat dit onderzoek zien, is Digit afhankelijk van de informatie van het tactisch team. Een inzet van Digit is minder goed uit te voeren zonder dat overleg. Daarom is functiescheiding in het licht van de hackbevoegdheid een problematisch concept.

## 7.9 Tot besluit

Dit eerste evaluatieonderzoek heeft zich vooral gericht op het proces rondom de uitvoering van de hackbevoegdheid door Digit. In tegenstelling tot de meer technische kant van een inzet, is minder aandacht besteed aan wat de inzet van deze nieuwe bevoegdheid praktisch betekent voor de tactische teams en welke meerwaarde de inzet kan hebben binnen een opsporingsonderzoek. Dat onderwerp zal uitgewerkt worden in het tweede deel van de evaluatie. Dan zal aandacht worden besteed aan tactische redenen om de bevoegdheid in te zetten (of er vanaf te zien), de samenwerking tussen Digit en het tactisch team en het soort gegevens dat het tactisch team ontvangt en de omgang hiermee. Hoe worden de gegevens verzameld met de hackbevoegdheid uiteindelijk gebruikt en waarom? In deel 2 van de evaluatie wordt verder beoogd meer aandacht te hebben voor zaken die een zittingsrechter inhoudelijk behandeld heeft en waarin gegevens inhoudelijk zijn gewogen. Indien voorhanden wordt in deze rechterlijke uitspraken wellicht meer duidelijk over de vragen en dilemma's die op basis van dit eerste onderzoek naar voren zijn gekomen. Daarnaast zal in het tweede deel van de evaluatie nader worden ingegaan op de andere onderdelen van de Wet CCIII.

Tijdens deze evaluatie is onder andere gekeken welke knelpunten zich voordoen bij de uitvoering van de hackbevoegdheid. Duidelijk is geworden dat de nieuwe bevoegdheid met veel verschillende waarborgen is omkleed. Die waarborgen zijn er niet voor niets. De bevoegdheid vormt een zeer ingrijpende inbreuk op het privéleven van mensen en mag om die reden niet zomaar worden ingezet. Dat neemt niet weg dat het wenselijk is om een aantal van die waarborgen en daaraan verwante onderwerpen nog eens nader onder de loep te nemen, omdat ze in dit onderzoek als knelpunt naar voren kwamen. Het gaat dan in ieder geval om: (1) de manier waarop kan worden binnengedrongen, (2) de inzet van commerciële middelen, (3) de meldplicht (4) het toezicht door de Inspectie en (5) de keuring van technische hulpmiddelen.
Ten eerste het binnendringen. Binnendringen dient heimelijk en op afstand plaats te vinden. De praktijk laat zien dat bij de uitvoering van de hackbevoegdheid de politie niet altijd volledig op afstand kan blijven. In dat soort situaties zou een steunbevoegdheid kunnen helpen bij de uitvoering van de bevoegdheid.
Ten tweede de inzet van commerciële middelen. Wanneer Digit gebruikmaakt van een commercieel middel, dient voor elke inzet een aparte licentie aangeschaft te worden. Omdat het middel veelvuldig is ingezet, leidt deze afspraak tot hoge kosten. Vanuit de opsporingspraktijk wordt aangegeven dat men niet zonder dit product kan. Als op eenzelfde manier met dit product gewerkt blijft worden, dan zou het goed zijn om de afspraak aparte licenties aan te schaffen tegen het licht te houden. Daarnaast is het nodig aandacht te hebben voor de wijze waarop met dit product herleidbare, betrouwbare en integere gegevensverzameling gewaarborgd kan worden, bijvoorbeeld middels technische en tactische waarborgen. Dat is van belang, omdat dit product onder het huidige keuringsregime niet goedgekeurd zal worden.
Ten derde de meldplicht. Vanuit veiligheidsoogpunt is (op indirecte wijze) een meldplicht ten aanzien van onbekende kwetsbaarheden in het leven geroepen. Deze meldplicht geldt voor alle onbekende kwetsbaarheden en dus ook voor

kwetsbaarheden in geautomatiseerde werken die voor en door personen met criminele intenties zijn ontwikkeld. Bovendien kan de meldplicht samenwerking bemoeilijken met zowel binnen- als buitenlandse partijen. Het is dan ook de vraag of de meldplicht zoals die nu geldt in alle gevallen veiligheidsbevorderend kan werken.
Ten vierde het toezicht door de Inspectie. Op dit moment is het voor de Inspectie niet goed mogelijk om, vanwege het ontbreken van een kwaliteitssysteem bij Digit, het door de wetgever gewenste systeemtoezicht te houden. Om die reden zou het goed zijn om te kijken naar wat in de praktijk georganiseerd zou moeten worden om het systeemtoezicht van de grond te krijgen. Daarnaast is het nodig meer duidelijkheid te krijgen over de wijze waarop het toezicht door de Inspectie tot haar recht kan komen en daarbij ook oog te hebben voor de uitvoerbaarheid van de bevoegdheid.
Tot slot de keuring. De keuring vormt voor Digit een groot knelpunt. Bovendien blijkt het lastig om een vooraf goedgekeurd hulpmiddel in te zetten. Daarom zou het goed zijn om met alle betrokken actoren *gezamenlijk* te kijken op welke manieren het beste een oordeel kan worden gegeven of gegevens op een betrouwbare, integere en herleidbare manier verzameld kunnen worden, ook wanneer gebruik wordt gemaakt van commerciële middelen. Het verzamelen van betrouwbare gegevens is per slot van rekening een belang dat *alle* actoren met elkaar delen.

# Summary

## The hacking power in practice

### An empirical study into the implementation of the hacking power (Sections 126nba, 126uba, 126zpa of the Dutch Code of Criminal Procedure)

The Computer Crime Act III (Wet Computercriminaliteit III; hereinafter the Act) came into force on 1 March 2019. The Act sets out a statutory basis for the 'hacking power' in the Dutch Code of Criminal Procedure (Wetboek van Strafvordering; Sections 126nba, 126uba and 126zpa Sv). The new investigative power allows law enforcement officials 'to access computerised systems remotely by stealth, under certain conditions, that are used by suspects, with a view to certain investigative objectives in the area of the investigation of serious criminal offences'. After accessing a computerised system (such as a mobile phone or a server) the police may carry out a number of investigative activities, namely: A) establishing specific characteristics of the computerised system or of the users thereof, such as their identity or location, and documenting such details; B) executing an order to record confidential communications or wiretapping and recording communications; C) executing an order for systematic observation; D) documenting data stored in the computerised system; and E) making data content inaccessible. These activities may only be carried out by specially designated investigating officers who are part of a special team of the Central Unit (Landelijke Eenheid) of the Dutch national Police. The Computer Crime Act III also includes a number of grounds with regard to the use of the hacking power either under or pursuant to an Order in Council, as was the case in the Investigations into Computerised Systems Decree (Besluit onderzoek in een geautomatiseerd werk; hereinafter the Decree).
The current report consists of an evaluation of the process surrounding the implementation of the hacking power in the first two years after the Act came into force. Another report is to follow at the end of 2024, containing the second part of the evaluation, which will focus on the implementation of the Act in full. The principal question in this study was:

*How is the hacking power put into practice and are there any particular problems that arise in the application of the hacking power in the investigative practice?*

A combination of research methods was used to answer the research question, including document analysis, interviews and case review. This summary provides an outline of the key findings and conclusions, initially focusing on the process surrounding the execution of the hacking power. Next, a number of issues are highlighted in relation to which notable difficulties have arisen.
As a preface to all of this, it is vital to note that both technical and tactical actors are involved with the power and its implementation, the former represented by Digit (Digital Intrusion Team). Digit itself consists of two components: Digit (Police) and Digit (Public Prosecution Service). Implementation of the hacking power is in the hands of Digit (Police), part of the Central Unit of the Dutch national police. Digit (police) is managed and led by Digit (Public Prosecution Service), which is part of the National Public Prosecutors' Office of the Public Prosecution Service. Any intervention

with the hacking power by Digit (hereinafter: intervention) takes place within an ongoing criminal investigation, which is carried out by a tactical police team (such as a team of the district criminal investigation team or
the National High Tech Crime Unit) under the authority of the Public Prosecutor handling the case. This Public Prosecutor bears ultimate responsibility for the criminal investigation in which Digit carries out an intervention, and he/she is accountable to the court when the case is heard by a judge in a trial court.

## Hacking power implementation process

*Intake and assessment*

The encryption of data has emerged in this study as a key reason as to why tactical investigation teams want to make use of the hacking power. Many other (special) investigative powers have often already been deployed and have not led to the desired information. If a tactical team is considering an intervention, it will consult Digit. Not every request, however, will lead to the use of the hacking power. Over the past two years, the majority of requests submitted to Digit (over two-thirds) were not actioned, due to both technical and tactical concerns.
Whenever a tactical team submits a request this is followed by an extensive intake process. This process consists of two procedures that partly take place sequently and partly take place simultaneously: an operational process and procedure for the legal assessment of the intervention. Within the operational process, Digit reviews whether an intervention is technically and tactically feasible. If this is the case, the tactical team will begin working on a (draft) application proposal for the use of the power, with Digit (Public Prosecution Service) monitoring the drafting process. Digit (Police) focuses on making an assessment of the technical feasibility of an intervention and of any potential risks or difficulties.
In addition to the operational process, an extensive, legal assessment procedure is carried out prior to the actual use of the hacking power. The proposed use of the power is discussed inter alia within the Central Assessment Committee (Centrale Toetsingscommissie, CTC) – an internal advisory body within the Public Prosecution Service. During the CTC meeting, attention is devoted both to the tactical relevance of the intervention using the power in the criminal investigation (by the Public Prosecutor handling the case) and the technical side (if necessary, clarified by Digit (Public Prosecution Service)). The CTC issues a positive recommendation in respect of the vast majority of requests. Ultimately, authorisation must be obtained from the Examining Magistrate on the basis of which the Public Prosecutor handling the case will issue an order to Digit (Police). During the assessment process outlined above, Digit (Public Prosecution Service), in consultation with Digit (Police), plays a key role in respect of all the various players involved, both as a source of information and adviser. This applies especially to the technical aspects of any intervention. The remainder of the actors involved rely on this expertise, and the fact that this responsibility rests on the shoulders of one or two persons makes the position of Digit (Public Prosecution Service) vulnerable.

*Use of the hacking power*

Once an order has been issued, Digit begins working on the application of the hacking power. Between March 2019 and March 2021, orders were issued in 26 criminal investigations, which means that a minority of requests from tactical teams was

granted. Contrary to what the name computer crime suggests, over the past two years the hacking power has mainly been used in criminal investigations into more serious forms of traditional crime such as (attempted) murder, cases involving narcotics, falsification of documents, money laundering, sexual offences, terrorism and membership of a criminal organisation. Only one intervention is related to cybercrime in the narrow sense.

Interventions by Digit can also be extended, which applied for the majority of interventions. The tactical team will often require additional information based on the data that has already been collected. An agreement has now been reached with Digit that interventions can, in principle, only be extended up to a maximum of two times four weeks). An intervention is not extended, for example if a suspect is arrested or if the investigation yields too little information. The same parties that tackle the question of whether an intervention may take place within a criminal investigation at all, including the corresponding timeline, are also involved in deciding whether or not an intervention is to be extended.

Digit has attempted to gain access and/or has succeeded in gaining access to six types of computerised systems, which are phone, phone in combination with another computerised system, server, router, laptop and wireless access point. During the research, phones in particular have been the subject of investigation. In the meantime, a more or less standard method, using a commercial tool, has been developed for these types of interventions (hereinafter: 'standard interventions'). For other interventions (hereinafter: 'customised interventions'), Digit considers how best it can gain access and carry out its investigative activities on a case-by-case basis. These customised types of interventions are more labour intensive for Digit. Furthermore, a computerised system to which access is gained is usually limited to one or two devices.
After access has been gained, Digit carries out a number of investigative activities, laid down in sub A to E (see above). Standard interventions will often entail the selection of a combination of investigative activities: establishing specific characteristics (sub A), recording confidential communications or wiretapping (sub B), systematic observation (sub C), and documenting data stored in the computerised system (sub D). This combination is regarded as a logical choice, given that a phone contains a great deal of information about a suspect's activities – both past and present. In the case of customised interventions, the investigative activities to be carried out are less obvious. In the case of these interventions, the choice seems primarily to be made in favour of establishing specific characteristics (sub A) and the documenting of data (sub D), occasionally accompanied by rendering data inaccessible at a later stage (sub E).

Digit carries out investigative activities both using technical tools as well as manually. A technological tool, in short, ensures that data that is relevant in the context of a tactical investigation (such as chat messages, emails, audio files) can be retrieved from the suspect's device and stored in Digit's digital environment. Cases in which no technical tool is used are referred to as analogue/manual interventions. In line with the legal framework, any technical tools developed by Digit are approved by the Inspection Service (Keuringsdienst), which is part of the Central Unit (Landelijke Eenheid) of the Dutch national Police. The Inspection Service assesses these technical tools based on an inspection protocol. The inspection protocol is based on a number of sections set out in the Decree that aim to ensure that any technical tool is able to collect data in a reliable, honest and traceable manner. In this way, for example, it can be asserted with a greater degree of certainty that the collected data actually

originated from the computerised system of a suspect. Approval of a technical tool by the Inspection Service means that, should a trial court deal with the facts of the case, no clarification need be given as to the precise functioning of the tool, meaning that the investigate methods used can be protected. In the case of manual intervention, clarification must be provided of the working method applied.

The approval of a technical tool is a critical guarantee for the monitoring of the use of the power, which equally applies to the monitoring carried out by the Inspectorate of Justice and Security (Inspectie Justitie en Veiligheid; hereinafter referred to as the Inspectorate). Since the entry into force of the Act, the Inspectorate has been conducting monitoring of the implementation of the hacking power. The monitoring should be system monitoring which means that the Inspectorate monitors the functioning of the legal system. This form of monitoring came about due to the fact that during the legislative process there were concerns about the fact that not all cases in which the hacking power is used would be presented before a trial court. In addition, there were questions about the court's technical expertise.

*Completing intervention and gains*

An intervention will be terminated once an order has been executed, or otherwise, on the last day of the duration of the order at the latest. After completing an intervention, the technical tool is generally removed entirely (as comprehensively as possible), after which the collected data is transferred to the tactical team. Upon transferring any data, Digit will in principle not verify whether any data that is subject to a professional duty of confidentiality (geheimhoudersgegevens) is present: this responsibility rests with the tactical team. This type of data relates inter alia to communications between the suspect and their legal counsel. Pursuant to Section 126aa of the Dutch Code of Criminal Procedure this type of data should be destroyed. However, Digit has indicated that there currently is no unambiguous set of regulations on how to handle information subject to a professional duty of confidentiality. The destruction of such data under Section 126aa of the Dutch Code of Criminal Procedure is ostensibly contrary to Section 28 of the Decree, which, inter alia, states that the content of the data recorded on the technical infrastructure may in principle not be altered. Removal of part of the data from a file would alter and therefore affect the integrity of that file. On the basis of the Explanatory Memorandum to the Decree this must be ruled out. Up to the present Digit (Public Prosecution Service) has therefore decided that data subject to a duty of confidentiality will not be permanently deleted.
Digit (police) drafts a number of official police reports every time the hacking power is used and the organisation has in recent months been working on getting its house in order in this regard. In terms of reporting, Digit (Public Prosecution Service) has provided a framework for minimal reporting in connection with the protecting of investigative methods. Based on the information in the official report, any 'smart reader' of the report should not be able to defend him or herself against the technical tools used by Digit. Furthermore, Digit (police) must keep detailed records of its activities in its own internal systems ('maximum journalisation').

A limited number of interventions with the hacking power have been examined in greater depth for the purposes of this study, which shows that so far the power mainly yields information that guides the investigation. Contrary to some expectations, the collected data has not yet yielded the definite proof within a criminal investigation. Furthermore, according to the information available, to date a trial court has not yet heard the facts and substance of any case in which the hacking power was used. In

some cases, this will never take place, for example, due to there being no suspect in a given case or because the power (alongside other powers) has not provided sufficient incriminating evidence. As a result, no statements (as yet) can be made regarding the value of the new power as a type of evidence: does the data collected by means of the hacking power contribute to the evidence in a criminal case?

The foregoing outlines the process surrounding the implementation of the hacking power. A number of obstacles and difficulties that have arisen in investigative practice have already emerged. A number of issues will be outlined in greater detail in the following sections, given that difficulties have (likewise) arisen in those areas.

## Gaining access

The aim is for the hacking power to be used covertly and remotely. In practice, it is sometimes necessary to be present on location in the vicinity of the computerised system in order to penetrate and gain access. The legislator does not appear to have taken this option into account. In order to be able to get close to a computerised system, Digit occasionally will have to make use of a (special) investigative power, which can only be used if it already happens to have been used by a tactical team within the same investigation as the use of the hacking power is intended. This dependence on the tactical team always constitutes an obstacle to Digit, given that tactical teams may not always intend to use such a power. For that reason, Digit requires a support power, comparable to the way in which this is regulated with regard to the recording of confidential communications (Section 126l Dutch Code of Criminal Procedure). In addition, Digit (Public Prosecution Service) wishes to be able to keep the use of this support power out of the case file in connection with the protection of the methods used. The question, subsequently, is to what extent this covert aspect can still be used to assess whether an intervention is proportionate or not, for example, in connection with any adverse effects of an operation to gain access. If there is no accountability whatsoever (given that the method is protected) and in fact only a limited number of people are involved in the decision-making regarding the method of gaining access, this raises the question whether that assessment of proportionality is being carried out by a sufficient number of officials.

*Vulnerabilities and reporting obligation*

In order to gain access to computerised systems, Digit makes use of the vulnerabilities of computerised systems. Vulnerabilities are weaknesses in hardware or software that make it possible for third parties to gain access to a computerised system. In order to do so, these vulnerabilities must be rendered ready to be exploited. There are three types of vulnerabilities: known, known-unknown vulnerabilities and unknown-unknown vulnerabilities. A known vulnerability is a vulnerability that is already known to a given manufacturer of a product (e.g. a phone). These types of vulnerabilities are published in various places on the internet and manufacturers of the relevant products regularly develop updates to address the vulnerabilities that are known to them. As long as the manufacturer does not make an update available or a customer does not install the update, the police are able to make use of the vulnerability. An unknown vulnerability (both known-unknown and unknown-unknown) is a vulnerability about which information has not yet been disseminated on the internet and therefore cannot be known a wider audience. Also there is no update available. Until the time of dissemination, however, this is known as a zero day. These types of vulnerabilities can

likewise be used to gain access to a computerised system. A known-unknown vulnerability is a vulnerability that is known to the investigative authorities, but which is not yet known to the manufacturer of the product, resulting in a lower probability that the manufacturer will fix the vulnerability. The police therefore are able to make use of the vulnerability (most likely for a longer period of time than in the case of a known vulnerability). An unknown-unknown vulnerability is a vulnerability that is likewise not known to the investigative authorities. These types of vulnerabilities may be found in products that law enforcement agencies purchase from commercial suppliers to gain access to IT-systems.
Concerns have been raised by various parties regarding the use of vulnerabilities, particularly due to the fact that the existence and use of these vulnerabilities would ostensibly make computer systems less secure. The government has expressed the expectation for the police to preferably make use of known vulnerabilities, while the use of unknown vulnerabilities is regarded as 'a last resort, but an indispensable option to tackle serious forms of crime' (*Parliamentary Papers I* 2017/18, 34 372, G, p. 7). In connection with concerns regarding security aspects, indirectly a reporting obligation has been agreed for unknown vulnerabilities (under Section 126ffa of the Dutch Code of Criminal Procedure, which states that reporting an unknown vulnerability may be postponed, after a written authorization from a examining magistrate). Reporting a vulnerability would ostensibly increase (online) security, given that this vulnerability would no longer be able to be exploited (assuming that the manufacturer has fixed the vulnerability). The reporting obligation does not apply to products purchased from a commercial supplier. A supplier of these types of products generally will not reveal any information regarding the composition of its product, meaning that the party who purchases the product is unaware of possible vulnerabilities used – as a result of which no notification can be made. So the reporting obligation only applies to known-unknown vulnerabilities.

Digit experiences the reporting obligation outlined in the above as a key obstacle. First and foremost, because the reporting obligation similarly also applies to vulnerabilities in systems that are specifically made for and by persons with criminal intentions. This means that these people must ultimately be informed that their system, which is used almost exclusively for criminal purposes, contains a vulnerability. This raises the question to what extent reporting such vulnerabilities increases the level of security. Rather, it seems that persons with criminal intentions in such cases are afforded the opportunity to improve their security. Secondly, the reporting obligation may also complicate cooperation with national as well as international parties, given that in certain countries the use of a vulnerability is considered state secrets. If the Dutch police wishes to cooperate with such countries, this would be problematic due to them being obliged to report on a state secret of a foreign country under Dutch law. The risk of such a scenario is that the relevant vulnerability would no longer be usable and cooperation would become very unappealing for those countries.

*Commercial tools*

Although the use of an unknown vulnerability was regarded as a 'last resort', Digit has made use of a commercial tool (and therefore most likely of unknown-unknown vulnerabilities) in the vast majority of its interventions. That tool is used for the standard interventions and the tool allows Digit (police) to both gain access and carry out investigative activities. The use of this tool is indispensable to Digit, given that it would otherwise not be able to carry out a large percentage of the interventions. A number of reasons have been cited for this. One of the reasons is that finding an

unknown vulnerability in a IT-system, which is used by almost all Dutch citizens, is very difficult; the reporting obligation is another reason. If it were even possible to locate an unknown vulnerability independently and render it ready to be used, it would have to be reported. This means that the vulnerability in question, which has taken up a lot of time to prepare for use, can only be used a very limited number of times.
It followed from the 2017-2021 Government Coalition Agreement that the use of a commercial tool must be limited in order not to encourage the market for unknown vulnerabilities. It was therefore agreed that a licence must be purchased for each individual case instead of a tool being purchased once, subsequently allowing it to be used for multiple interventions. Given that that tool in the investigative practice has been used for a large number of interventions, it is estimated that this agreement has led to more than twice the purchase price being paid to date – it is estimated that this is in the range of 'several millions' of euros. Given the relatively large number of interventions in which this tool is used, it is unlikely that the agreed licencing model has led to the market for unknown vulnerabilities being less stimulated.

### Technical tools

Digit makes use of two types of technical tools: commercial tools (as discussed in the above) and dedicated technical tools developed by Digit (Police). In addition, Digit has the option of taking a non-automated route (manual intervention).
There is a debate regarding the scope of the term technical tool (and the non-automated intervention), primarily between Digit and the Inspectorate. The question of whether something does or does not constitute a technical tool is relevant given that only a technical tool need be assessed and approved and Digit regards assessment as a major obstacle in respect of implementation (please see more information about the assessment itself in the next section). Digit was only able to use its own proprietary technical tools, developed in house, in a small number of interventions. A key reason for this is that developing a technical tool and ultimately getting it assessed and approved is a time-consuming process. This lengthy turnaround time means that Digit was only able to use a small number of technical tools developed in house.
Until now, a 'new' technical tool has been used for each intervention, due to the fact that a new intervention with the hacking power will often require a number of adaptations to the technical tool. There is a desire within Digit to develop a number of standard components that have already been assessed and approved in advance. These could then be supplemented in a relatively short period of time, depending on the needs of the investigation in relation to a specific intervention. This would lead to the creation of a technical tool, including already assessed and approved components, which could be used in a specific case. This approach has so far proved difficult, given that this distinction between new and already assessed components is not made during assessments and each tool is regarded as a new tool in itself that must be assessed in full, including the associated assessment periods.
In investigative practice, non-automated intervention is currently considered more often compared to the early days. In the case of non-automated intervention, Digit must justify its working method in greater detail in order to assert with greater certainty the reliability, integrity and traceability of the data that was collected using the method in question. This does, however, mean that the method will not remain completely protected. This is not regarded as problematic by Digit in all cases.

## Assessment of technical tools

Assessment of technical tools presents a major difficulty to Digit. This is related to the fact that the two parties involved (Inspection Service and Digit) regard the assessment process from two different perspectives, which in the case of practical implementation occasionally clash with one another. From the perspective of the Inspection Service the principal focus is on the rules set out by the Decree and on the assessment requirements arising therefrom. This means inter alia that, in line with the Decree, a tool can only be approved if all requirements are met – whether or not supplemented with a number of (additional) substitute safeguards. In this way the integrity, reliability and traceability of the collected data can be stated with one hundred percent certainty. This perspective occasionally clashes with the way in which Digit approaches the assessment process. This perspective focuses principally on the feasibility and the necessity of the rules of the Decree and the assessment requirements in the assessment resulting from the Decree. Digit is critical of the assessment carried out by the Inspection Service, given that it is considered poorly matched to the tools developed by Digit (police). The fact that updates are regularly implemented, for example, is inherent to software and therefore inherent to the resources used by Digit. This is different compared to more traditional technical tools such as GPS trackers, and the question therefore is to what extent the Inspection Service must and can take this into account. Particularly when a technical tool must be approved in advance – the latter resulting from the Explanatory Memorandum to the Decree.
In addition to feasibility, the necessity of the rules and requirements is also given critical consideration by Digit. Contrary to how the Inspection Service views the assessment process, Digit believes it is not necessary for a tool to meet all the assessment requirements. In Digit's opinion there should, be (greater) flexibility to take into account evidential value and risk assessments. Taking into account evidential value means that it is not necessarily a problem if a technical tool were not fully approved, as appropriate accountability would be able to be provided in court. The impact of this, however, would be that the investigative method would no longer remain fully protected. It would then be at the discretion of the court, potentially, to assess the value of the evidence collected. However, this would require that a case in which the hacking power is used is brought to court and that a court has sufficient technical expertise at its disposal to make this assessment. Most likely, a trial judge will deal with not all cases substantively. In addition, the question is whether there is sufficient availability of such expertise at this juncture. Furthermore, putting risk assessments front and centre means that the point of departure should be based far more on the issue of what the risk is if a certain requirement contained in the assessment protocol were not met, instead of the tool having to meet that requirement for approval.

*Assessment and safeguards*

In recent years, Digit has largely been unsuccessful in using a technical tool that received ex-ante approval, which is chiefly related to the (lengthy) development lead time involved. However, as previously stated, the Explanatory Memorandum to the Decree states that this is in principle mandatory. The development period is at odds with the urgent investigative interests that must exist in order to be able to make use of the power in the first place. It is therefore prudent to consider whether it is always realistic to require the use of an ex-ante approved tool. The Decree also keeps open the option of presenting an tool for assessment ex-post or to omit an assessment entirely – both should be an exception. In practice, this is not the case. The Public

Prosecutor for Digit has concluded that the nature of a widely used commercial tool has so far precluded assessment. This means that in the majority of cases one of the safeguards, an assessment by the Inspection Service, was not executed. Instead in those cases additional technical and tactical safeguards were implemented (please see more information in the next section). In practice, however, it has become apparent that this tool most likely cannot be approved either, given that the tool that Digit has purchased uses a server to which the supplier has access. Although it is true that the data collected, such as the suspect's chat messages, are ultimately stored on the Digit server, this does not alter the fact that the supplier (in theory) has access to the suspect's data during the period access is gained by the investigative authorities and the execution of the investigative activities. Although contractual agreements are in place to ensure that the supplier is prohibited from reviewing the data in question and may only have access to the server for tool maintenance purposes, it cannot be excluded that the supplier could also give itself access to the server at other times. For that reason alone, the tool cannot be approved. Digit argues that a supplier would never access the server to review the data on its own initiative, due to agreements that were made between Digit and a supplier. Violating these agreements would damage a supplier's reputation as well as the financial risks this would entail would be too high. Nevertheless, this does mean that the reliability and integrity of the collected data could be compromised.
If a tool were used, for which Digit (Public Prosecution Service) decides that its nature precludes assessment, then safeguards must be in place to ensure the integrity, reliability and traceability of the data obtained. The Explanatory Memorandum to the Decree shows that these can be technical safeguards. These additional safeguards must be justified in the case file by the Public Prosecution Service. In investigative practice, not only are additional technical safeguards put in place but additional tactical safeguards are likewise provided. The latter type of safeguards relates to measures taken by the tactical team to verify the collected data. The Decree does not take into account that such measures can be taken and similarly are already taken in practice. This raises the question of whether it is not possible for these types of safeguards to be taken into account – before a trial court can do so – when assessing the reliability, traceability and integrity of the collected data.

### Monitoring by the Inspectorate

As stated previously, the Inspectorate monitors the implementation of the hacking power. There are a number of barriers in practical implementation, which has led to monitoring by the Inspectorate taking place accompanied by a fair share of debate in practice. Following the Reports (Verslagen) issued by the Inspectorate, Digit (police) has begun to improve a number of elements within its approach. Nevertheless, Digit has decided to disregard a number of aspects identified by the Inspectorate, such as the registration process in relation to the issuing of technical tools. This is related to the fact that Digit does not consider these aspects to be properly feasible within the framework of the Decree. The Inspectorate, however, focusses on the way in which Digit should act in accordance with the legal framework, given that it is up to the legislator to assess the feasibility of that legal framework (and whether any amendment is necessary). Failure to take into account feasibility means that the requirements of the Decree that Digit has decided it will not (or cannot) meet will be aspects that the Inspectorate will continue to flag up and which Digit in turn will disregard. A stalemate of this nature raises the question of whether the intended effects of monitoring can be achieved in the current situation. And subsequently raises

questions regarding what the consequences may be if the Inspectorate identifies specific issues, which Digit then decides not to pursue.

The second obstacle relates to the scope of monitoring. The Inspectorate carries out oversight on the activities of the police rather than on those of the Public Prosecution Service. Within the current study it has become clear that, in practice, the actions of the Public Prosecutor and of those of the police are inextricably linked and that the two are therefore difficult to separate. Digit (Public Prosecution Service) takes the position that virtually all activities carried out by Digit take place under the authority of the Public Prosecution Service and that the Inspectorate therefore does not have a remit to comment on those activities. The Inspectorate believes that it is indeed entitled to supervise those activities, given that they are carried out by Digit (Police) and Digit (Police) occasionally advises Digit (Public Prosecution Service) on those actions. Moreover, the limited implementation of the supervisory remit, under the interpretation of Digit (Public Prosecution Service), would ostensibly lead to the Inspectorate being virtually unable to make statements about any aspects whatsoever. It is therefore necessary to provide clarity who should exercise monitoring over whom and which aspects should be subject to monitoring by the Inspectorate. This dialogue has started.
A third obstacle relates to the issue of what is needed to be able to perform effective system monitoring. The legislative history does not provide much information about how that system monitoring ought to take place, except that the Inspectorate is entitled to review individual cases. It is precisely the question of *how* that causes problems in practical implementation. The Inspectorate wishes to be able to base its monitoring on Digit's internal quality control systems, which is in line with the way in which system monitoring is defined by the Inspection Council. At the time this report was drafted, a quality control system was not in place. Furthermore, there appears to be a lack of clarity about what a quality control system entails exactly. In the near future, it would therefore be prudent to review what should be organised in practice in order to get the system monitoring off the ground.

### Interventions with an international component

A Public Prosecution Service Guideline (OM-aanwijzing; Guideline on the international aspects of the use of the power pursuant to Section 126nba of the Dutch Code of Criminal Procedure) regulates what action must be taken in the event data are located on foreign territory. During the period of the study, Digit was involved in a limited number of interventions with an international component, which related to interventions abroad carried out from the Netherlands and interventions in the Netherlands carried out from abroad.
As far as the standard interventions are concerned, in principle the agreement is that a phone from a Dutch suspect located on foreign territory may not be accessed. In the case of customised interventions, whether or not the power is used will depend on the relationship with the relevant country.
The Public Prosecution Service Guideline focuses on interventions with the power abroad, however is not always sufficient. This, for example, applies in cases where a wide range of different computerised systems are involved, such as in the case of a botnet. The Minister of Justice and Security is notified in cases where there is derogation from the Public Prosecution Service Guideline. Interventions involving an international component can be especially complicated politically.

Interventions in the Netherlands from abroad are currently not regulated, including in the Public Prosecution Service Guideline. This presents complications for practical implementation, given that in those cases, complex legal constructions must be devised within which various requests for mutual legal assistance are submitted back and forth. Another more practical issue is that no judicial oversight procedure has been agreed for foreign interventions, whereas such a procedure is in place for other special investigative powers. A judicial oversight procedure of this nature means that, if a foreign country wishes to make use of a special investigative power in the Netherlands and has been granted permission, the Examining Magistrate must grant permission for the actual transfer of data collected using the special investigative power. This is to verify the lawful application of the power.

## Separation of duties

The legislative history shows that a strict separation of duties and functions must be in place, which should inter alia prevent Digit (police) from being influenced by tactical teams when assessing the feasibility of an intervention and its execution. In practice, regular consultation takes place between the technical and tactical team as well as an exchange of information, both before the hacking power is used and during the intervention. This study shows that Digit is dependent on the information provided by the tactical team to ensure effective execution. Interventions by Digit are less easy to carry out without that consultation. That is why the separation of duties and functions is a problematic concept in light of the hacking power.

## In conclusion

This first evaluation study has focused primarily on the process surrounding the practical implementation of the hacking power. In contrast to the more technical side of an intervention, less attention has been devoted to what the use of this new power means in practice to the tactical teams requesting its implementation and what added value the intervention can have in a criminal investigation. This subject is aimed to be fleshed out in greater detail in the second part of the evaluation. Part 2 of the evaluation also aims to devote more attention to cases that have been heard substantively in a trial court and in which data has been considered substantively. If available, the judgments from the courts may clarify the questions and dilemmas that have emerged on the basis of this initial study. In addition, the second part of the evaluation will look in more detail at the other components of the CCIII Act.
However, on the basis of this initial evaluation, a number of problems have already been identified that clearly complicate the use of the power and which could already be addressed: 1) the way in which access can be gained, 2) the use of commercial tools, 3) the reporting obligation, 4) monitoring by the Inspectorate and 5) the assessment of technical tools.
Let us turn first and foremost to the aspect of gaining access to computerised systems. Access must be gained both covertly by stealth and remotely. However, in practice, it has been shown that when the hacking power is used the police cannot always remain completely at a distance. A support power could be beneficial in these types of situations where operating completely remotely is not possible.
Secondly, the use of commercial tools. Whenever Digit makes use of a commercial tool, a separate licence must be purchased for each individual intervention. Given that a tool is used on multiple occasion, this agreement leads to high costs being incurred.

Investigative practice has indicated that this tool is indispensable to operations. If this tool continues to be used in the same way, it would be prudent to review the agreement on the purchase of individual licences. In addition, attention must be paid how to guarantee the integrity, reliability and traceability of the collected data, for example by means of technical and tactical safeguards. This is important, because under the current inspection regime, this tool will not be approved by the Inspection Service (Keuringsdienst).
Thirdly, the reporting obligation. Indirectly a reporting obligation for unknown vulnerabilities was created from the point of view of security. This reporting obligation applies to all unknown vulnerabilities, including systems that have been developed for and by persons with criminal intentions. Moreover, the reporting obligation can make cooperation with both domestic and international parties more difficult. This therefore raises the question as to whether the reporting obligation as it currently applies can actually improve and advance security in all cases.
Fourthly, the monitoring by the Inspectorate. At the moment it is not possible for the Inspectorate to carry out the system monitoring desired by the legislator, due to the lack of a quality system at Digit. For that reason, it would be good to look at what should be organized in practice in order to get system monitoring off the ground. In addition, it is necessary to gain more clarity about the way in which the monitoring by the Inspectorate can come into its own, while also paying attention to the practical feasibility of the hacking power.
Finally, the assessment of technical tools. The inspection procedure presents a major difficulty to Digit (police). Moreover, it appears to be difficult to put an ex-ante approved tool into use. It would therefore be prudent to *jointly* review, with all relevant actors, the best ways to assess how the integrity, reliability and integrity can be guaranteed, also when using commercial tools. That is after all an interest shared by *each of the* actors involved.

# Literatuur


Algemene Inlichtingen- en Veiligheidsdienst (z.d.). *Beleid omgang onbekende kwetsbaarheden*. Geraadpleegd op 20 april 2022: www.aivd.nl/documenten/publicaties/2018/05/01/beleid-omgang-met-onbekende-kwetsbaarheden.

Anti Money Laundering Centre (2021). *Witwassen van omzet afkomstig uit PGP-telefoons*. Geraadpleegd op 20 april 2022: www.amlc.nl/witwassen-van-omzet-afkomstig-uit-pgp-telefoons/.

Baarda, B., Bakker, E., Fischer, T., Julsing, M., Peters, V., Van der Velden, T., & De Goede, M. (2013). *Basisboek kwalitatief onderzoek: Handleiding voor het opzetten en uitvoeren van kwalitatief onderzoek.* (Derde druk). Groningen: Noordhoff Uitgevers.

Braster, J.F.A. (2000). *De kern van casestudy's Cybercriminaliteit: Raad van Europa verstrekt zijn juridisch arsenaal*. Geraadpleegd op 20 april 2022:

Bruins Slot, H.G.J., & Yeşilgöz-Segerius, D. (2022). *Kamerbrief betreffende beantwoording vragen Omtzigt (Omtzigt) en Van Dijk (SP) inzake hetgebruik van hacksoftware, zoals Pegasus, in Nederland.* (d.d. 23 juni 2022.) Geraadpleegd op 28 juli 2022: Antwoord op vragen van de leden Omtzigt en Jasper van Dijk over het gebruik van hacksoftware, zoals Pegasus, in Nederland | Tweede Kamer der Staten-Generaal.

Commissie modernisering opsporingsonderzoek in het digitale tijdperk (2018). *Regulering van opsporingsbevoegdheden in een digitale omgeving*. Geraadpleegd op 28 juli 2022: Rapport Commissie Koops - Regulering van opsporingsbevoegdheden in een digitale omgeving | Kennisbank Openbaar Bestuur (kennisopenbaarbestuur.nl).

Custers, B. (2018). Nieuwe online opsporingsbevoegdheden en het recht op privacy: Een analyse van de wet computercriminaliteit III. *Justitiële verkenningen, 44*(5). 100-117.

Derechtspraak.nl. (z.d.). *Kenniscentrum Cybercrime*. Geraadpleegd op 21 april 2022: Kenniscentrum Cybercrime | Gerechtshof Den Haag | Rechtspraak.

Grapperhaus, F. (2021). *Verzamelbrief politie.* (d.d. 23 juni 2022.) Geraadpleegd op 28 juli 2022: tk-verzamelbrief-politie.pdf (overheid.nl).

Helderman, J.K., Honingh, M.E., & Thewissen, S. (2009). *Systeemtoezicht: Een onderzoek naar de condities en werking van systeemtoezicht in zes sectoren*. Nijmegen: Radboud Universiteit Nijmegen.

Hof Den Haag (2018). *ECLI:NL:GHDHA:2018:3529, Computerrecht 2019, nr. 54, m.n.t. J.J. Oerlemans.* Geraadpleegd op 20 juni 2022: hof-den-haag-19-december-2018-computerrecht-m.nt_.-j.j.-oerlemans.pdf (wordpress.com).

Hoge Raad. (2021). *ECLI:NL:PHR:2020:927*. Geraadpleegd op 21 april 2022: ECLI:NL:HR:2021:202, Hoge Raad, 19/05471 (rechtspraak.nl).

Hutjes, J.M., & Van Buuren, J.A. (1992). *De gevalsstudie: Strategie van kwalitatief onderzoek.* Meppel: Boom.

Inspectie JenV (Justitie en Veiligheid) (2020). *Verslag toezicht wettelijke hackbevoegdheid politie 2019: Verslag van het toezicht door de Inspectie Justitie en Veiligheid op de toepassing door de politie van de bevoegdheid op basis van de wet Computercriminaliteit III om in een geautomatiseerd werk binnen te dringen en onderzoek te doen*. Den Haag: Inspectie Justitie en Veiligheid.

Inspectie JenV (Justitie en Veiligheid) (2021). *Verslag toezicht wettelijke hackbevoegdheid politie 2020: Heeft de politie zich aan de regels gehouden bij het*

*toepassen van de bevoegdheid tot binnendringen in een geautomatiseerd werk?* Den Haag: Inspectie Justitie en Veiligheid.
Inspectie JenV (Justitie en Veiligheid) (2022). *Verslag toezicht wettelijke hackbevoegdheid politie 2021: Toezicht op de toepassing door de politie van de bevoegdheid tot het binnendringen en doen van onderzoek in een geautomatiseerd werk.* Den Haag: Inspectie Justitie en Veiligheid.
Inspectieraad (2007). *Werkprogramma Inspectieraad 2008: 'Meer effect, minder last'*. Geraadpleegd op 28 juli 2022: D53416E3.doc (officielebekendmakingen.nl).
Koops, B.J., & Oerlemans, J.J. (2019). Formeel strafrecht & ICT. In B.J. Koops & J.J. Oerlemans (Eds.), *Monografieën recht en informatietechnologie* (p. 117-208). Den-Haag: Sdu.
Kruisbergen, E.W., De Jong, D., & Kouwenberg, R.F. (2010). *Opsporen onder dekmantel*. Den Haag: Boom Juridische uitgevers. Onderzoek en beleid 282.
Kruisbergen, E.W., Roks, R.A., & Kleemans, E.R. (2019). *Georganiseerde criminaliteit in Nederland: daders, verwevenheid en opsporing – rapportage in het kader van de vijfde ronde van de monitor georganiseerde criminaliteit*. Den Haag: WODC. Cahier 2019-17.
Maesschalck, J. (2010). *Methodologische kwaliteit in het kwalitatief criminologisch onderzoek*. In T. Decorte & D. Zaitch (Eds.), *Kwalitatieve methoden en technieken in de criminologie* (p. 119-145). (Tweede druk). Leuven/Den Haag: Acco.
NCSC (National Cyber Security Center) (z.d.). *Beveiligingsadviezen*. Geraadpleegd op 16 december 2020: Beveiligingsadviezen | Actueel | Nationaal Cyber Security Centrum (ncsc.nl).
NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid) (2020). *Cybersecuritybeeld Nederland (CSBN) 2020.* Geraadpleegd op 29 juli 2022: Cybersecuritybeeld Nederland (CSBN) 2020 | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl).
Nederlands Forensisch Instituut (z.d.). *Vakbijlage waarschijnlijkheidstermen.* Geraadpleegd op 20 april 2022: www.forensischinstituut.nl/publicaties/publicaties/2017/10/18/vakbijlage-waarschijnlijkheidstermen.
Odinot, G., & De Jong, J.B.J. (2012). Wie belt er nou nog? De veranderende opbrengst van de telefoontap. *Justitiële verkenningen, 44*(3), 8-19.
Oerlemans, J.J. (2011). Hacken als opsporingsbevoegdheid. *Delikt en Delinkwent, 8*(62), 888-908.
Oerlemans, J.J. (2017). De wet computercriminaliteit III. Meer handhaving op het internet. *Strafblad,* 350-359.
Openbaar Ministerie (z.d.). *Instructie voor de inzet van de bevoegdheid ex artt. 126nba, 126uba, 126zpa, 126ffa Sv (2021I002)*. Geraadpleegd op 21 april 2022: Instructie voor de inzet van de bevoegdheid ex. artt. 126nba, 126uba, 126zpa en 126ffa Sv (2021I002) | Beleid en Straffen | Openbaar Ministerie (om.nl).
Perlroth, N. (2021). *This is how they tell me the world ends: The Cyber Weapons Arms Race.* London, Oxford: Bloomsbury.
Politie. (z.d.). *Open source intelligence*. Geraadpleegd op 20 april 2022: kombijde.politie.nl/vakgebieden/ict/open-source-intelligence. www.zoek.officielebekendmakingen.nl/stb-2006-524.html.
Prins, R. (2021). Ronald van der Knijff. (nr. 28) [Podcastaflevering]. In *Cyberhelden* Geraadpleegd op 20 april 2022: www.cyberhelden.nl/episodes/episode-28/.
Rautiainen, A., Urquía-Grande, E., & Muñoz-Colomina, C. (2019). *Measures for Police Performance in Spain and Finland*. In Farazmand. (Ed.), *Global Encyclopedia of Public Administration, Public Policy, and Governance* (Living Edition). Springer.

Rechtbank Den Haag (2021). *ECLI:NL:RBDHA:2021:6770*. Geraadpleegd op 20 april 2022: ECLI:NL:RBDHA:2021:6770, Rechtbank Den Haag, 09/837305-20 (rechtspraak.nl).
Rechtbank Den Haag (2021b). *ECLI:NL:RBDHA:2013:19764*. Geraadpleegd op 20 april 2022: ECLI:NL:RBDHA:2013:19764, Rechtbank Den Haag, 09/837305-20 (rechtspraak.nl).
Staatsblad, 2006, 524 (2006, 20 oktober). Besluit van 20 oktober 2006 tot vaststelling van het Besluit technische hulpmiddelen strafvordering. Geraadpleegd op 25 april 2022: Staatsblad 2006, 524 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl).
Tweede Kamer (z.d.). *Innovatiewet Strafvordering.* Geraadpleegd op 20 april 2022: Innovatiewet Strafvordering | Tweede Kamer der Staten-Generaal.
Van Berkel, J.J., Van Uden, A., De Poot, C.J., Van den Eeden, C.A.J. & Lankhaar, C.C. (2021). *Tweede monitorronde evaluatie ANPR-wetgeving 126jj Wetboek van Strafvordering: De wet 'vastleggen en bewaren van kentekengegevens door de politie' twee jaar in werking.* Den Haag: WODC.
Van den Eeden, C.A.J., Van Berkel, J.J., Lankhaar, C.C., & De Poot, C.J. (2021). *Opsporen, vervolgen en tegenhouden van cybercriminaliteit*. Den Haag: WODC. Cahier 2021-20.
Van der Waagen, W., & Bernaards, F. (2018). De 'non-human (f)actor' in cybercrime: Cybercriminele netwerken beschouwd vanuit het 'cyborg-crime'-perspectief. *Justitiële verkenningen, 44*(5), 54-67.

# Bijlage 1 Samenstelling begeleidingscommissie

**Voorzitter**

| | |
|---|---|
| mw. prof. mr. dr. M.F.H. (Marianne) Hirsch Ballin | Hoogleraar Straf- en Strafprocesrecht, Vrije Universiteit Amsterdam |

**Leden**

| | |
|---|---|
| mw. mr. dr. J.M. (Jacqueline) Bonnes | Senior Officier van justitie Cybercrime en Digitaal Bewijs, Openbaar Ministerie, Rotterdam |
| mw. mr. M. (Madiha) Malik[129] | Beleidsadviseur DGPenV, Ministerie van Justitie en Veiligheid |
| prof. mr. dr. J.J. (Jan-Jaap) Oerlemans | Bijzonder hoogleraar Inlichtingen en Recht, Universiteit Utrecht |
| prof. dr. W.P. (Wouter) Stol | Bijzonder hoogleraar Politiestudies, Open Universiteit; Lector Cybersafety NHL Stenden Hogeschool en de Politieacademie |

[129] Aanvankelijk was de heer J. Raeven van DGRR betrokken als lid van de begeleidingscommissie. Na de eerste bijeenkomst zijn zijn taken overgenomen door mw M. Malik van DGPenV.

# Bijlage 2 Interviews en dossieranalyse

## Interviews – Hoe?

*Topicgestuurde interviews*

Voor deze evaluatie is gebruikgemaakt van topicgestuurde interviews. Dat betekent dat bij elk interview een topiclijst beschikbaar was met daarop ook enkele voorbeeldvragen die aan de orde konden komen (Baarda et al., 2013; Hutjes & Van Buuren, 1992). De volgorde van de te bespreken topics en het aantal te stellen vragen lag van te voren niet vast. Dat had als voordeel dat gedurende het interview nader in kon worden gegaan op onderwerpen die door de geïnterviewde werden aangedragen en die voor de evaluatie interessant waren. Een ander voordeel van deze manier van werken was dat op onderwerpen in kon worden gegaan die van te voren door de onderzoekers niet voorzien waren, maar die wel belangrijk waren om de inzet van de bevoegdheid in de praktijk en eventuele knelpunten beter te kunnen begrijpen. Dat paste bij het open en kwalitatieve karakter van deze evaluatie. Voorbeelden van dit soort thema's waren het keuringsproces en de reikwijdte van het toezicht door de Inspectie Justitie en Veiligheid.
Bij het opstellen van de topics zijn de onderzoeksvragen leidend geweest. Zo is in elk interview gevraagd naar de inhoud van de verschillende onderdelen van de wet (indien uiteraard van toepassing). Afhankelijk van de geïnterviewde zijn accenten gelegd die voor de betreffende geïnterviewde relevant waren. Bij wetgevingsjuristen en beleidsmakers werd bijvoorbeeld expliciet gevraagd naar de verschillende fases van het wetgevingsproces, inclusief de belangrijkste discussiepunten. In de interviews met de uitvoerders van de wet is juist gesproken over het toepassen van de bevoegdheid in de praktijk en de verschillende knelpunten die zij tegenkwamen. Voor elk categorie geïnterviewden werd een op maat gemaakte topiclijst gebruikt passend bij zijn of haar functie.
De wijze waarop dit evaluatieonderzoek is aangepakt was deels een inductief proces. Dat betekent dat informatie die werd verzameld gedurende het onderzoeksproces tussentijds geanalyseerd werd en waar nodig als input diende voor de rest van de dataverzameling. De informatie afkomstig uit de analyse van Kamerstukken en eerdere interviews waren daarom een belangrijke bron voor de samenstelling van de topiclijsten.

Een deel van de interviews is opgenomen en getranscribeerd. Nadat het transcriberen was afgerond, is de geluidsopname van het gesprek vernietigd. De uitwerking van de getranscribeerde interviews is niet voorgelegd aan de geïnterviewden. Een ander deel van de interviews is op verzoek van Digit-politie, vanwege de vertrouwelijke aard van de informatie die werd gedeeld, niet opgenomen. Van die interviews zijn zo snel mogelijk na afloop van het interview gespreksverslagen gemaakt. Deze verslagen zijn vervolgens voorgelegd aan de geïnterviewden met de vraag of er feitelijke onjuistheden in stonden. Vervolgens zijn de gespreksverslagen met aanvullende suggesties bekeken en beoordeeld of de suggesties konden worden overgenomen. Suggesties die betrekking hadden op een inhoudelijke aanvulling of iets dat niet klopte zijn doorgaans overgenomen in rood zodat zij duidelijk te onderscheiden zouden zijn van het origineel. Wijzigingen die betrekking hadden op aspecten die niet op een bepaalde toon zouden zijn gezegd, zijn meestal niet verwerkt, behalve met de opmerking erbij, tussen haakjes, dat de geïnterviewde een bepaalde zin liever niet zo

zag. Zowel de versie met suggesties (vaak aangeven met wijzigingen bijhouden) als de versie die uiteindelijk in de analyse is meegenomen, is door de onderzoekers bewaard. In het uiteindelijke rapport zijn citaten gebruikt ter illustratie van de bevindingen. Daarbij is zo dicht mogelijk gebleven bij wat geïnterviewden hebben verteld. Hier en daar zijn woorden en zinnen weggelaten. Op die plekken is gewerkt met (…). Soms zijn woorden door de onderzoekers toegevoegd. Die woorden staan tussen […].

### Dossieranalyse - selectie van inzetten

Om ten behoeve van de dossieranalyse tot een definitieve selectie van inzetten te komen, is aan Digit-politie een lijst gevraagd met inzetten die plaatsvonden in de periode maart 2019 t/m maart 2021.[130] Vanuit Digit-politie is op verzoek van de onderzoekers een Excelbestand aangeleverd met daarin de volgende kenmerken: zaaksnaam, aanvragende eenheid, jaar van inzet, verdenking (globaal), onderzoekshandelingen die in bevel staan opgenomen, soort technisch hulpmiddel (commercieel, eigen, handmatig), soort geautomatiseerd werk, verlenging (ja/nee), locatie van het geautomatiseerde werk, inzet in Nederland (ja/nee), inzet in buitenland (ja/nee), inzet op verzoek van buitenland (ja/nee), binnendringen gelukt (ja/nee) en gegevensverzameling gelukt (ja/nee). Op basis van het excelbestand is een selecte steekproef getrokken.

In de periode maart 2019 t/m maart 2021 is voor 26 inzetten een eerste bevel afgegeven om op basis van artt. 126nba Sv of 126uba Sv of 126zpa de hackbevoegdheid in te zetten. Eén inzet viel bij voorbaat af om in de selectie opgenomen te worden. Hoewel de onderzoekers toegang konden krijgen tot het Digit-dossier van deze inzet, is besloten het betreffende Digit-dossier niet mee te nemen ten behoeve van de definitieve inzetselectie. Deze inzet is zo uniek dat het lastig was de inzet op een zodanige manier te beschrijven dat niet herleidbaar zou zijn binnen welk opsporingsonderzoek de inzet had plaatsgevonden. Mogelijk wordt deze inzet meegenomen tijdens het tweede deel van de evaluatie.

Van de 25 inzetten zijn uiteindelijk 7 inzetten geselecteerd. Dat ging als volgt. De 25 overgebleven inzetten zijn onderverdeeld in ‘volledig gelukt’ om binnen te komen, ‘deels gelukt/mislukt’ om binnen te komen en ‘volledig mislukt’ om binnen te komen. Of het daadwerkelijk gelukt is om data binnen te halen is niet apart meegewogen, omdat dit vaak samenhing met het feit of het gelukt was om binnen te dringen. Het onderscheid is gemaakt, omdat informatie over zowel gelukte als niet gelukte inzetten inzicht kon bieden in de uitvoering van de bevoegdheid en eventuele knelpunten (deelvragen 2 t/m 5).
Vervolgens is een verdeling gemaakt per geautomatiseerd werk dat is binnengedrongen. Omdat voor het eerste deel van de evaluatie de nadruk is gelegd op het Digit perspectief, is voor deze verdeling gekozen. Daarnaast is de manier waarop de onderzoekshandelingen zijn verricht (eigen technisch hulpmiddel, commercieel technisch hulpmiddel, handmatige inzet) meegenomen als criterium bij de selectie. Omdat beide met elkaar bleken samen te hangen, is het geautomatiseerde werk in de selectie leidend geweest, naast het eerder genoemde criterium of het wel of niet gelukt was om binnen te dringen. Verder is nog gekeken naar inzetten met een internationale component en is gekeken naar een spreiding van jaartallen waarin de

[130] Dit betreft de aan beide Kamers toegezegde termijn waarover de eerste evaluatie zal gaan.

inzet plaatsvond. Voor dat laatste is gekozen omdat voorstelbaar was dat in het begin op een andere manier werd gewerkt dan in een latere periode.
Om voor de selectie niet alleen afhankelijk te zijn van inzetten die de onderzoekers op verzoek door Digit werden aangedragen (op basis van de door de onderzoekers zojuist opgestelde criteria is gevraagd welke inzetten geschikt zouden zijn) heeft de selectie binnen elk categorie geautomatiseerd werk (soms) op basis van toeval plaatsgevonden. Dat betekent dat per geautomatiseerd werk een lijstje werd gemaakt met inzetten en dat steeds de tweede op de lijst werd gekozen. Indien er inhoudelijke redenen waren, is hiervan afgeweken.

### Selectie inzetten

Zeven inzetten zijn geselecteerd. Bij één inzet is het niet gelukt om binnen te dringen. In tabel B2.1 staat per geautomatiseerd werk weergegeven wat de motivatie was om de inzet te selecteren.

**Tabel B2.1 Overzicht selectie**

| Geautomatiseerd werk | Aantal | Geselecteerde inzet |
|---|---|---|
| Server | 1 | Twee inzetten betroffen een inzet op een server. We kozen niet op basis van toeval, maar volgden de suggestie van de politie, omdat die inzet een inzet betrof met een internationale component. |
| Laptop/modem | 1 | Bij twee inzetten kwamen deze geautomatiseerde werken terug. We kozen niet op basis van toeval, maar kozen voor de andere inzet, omdat bij deze inzet een extra functionaliteit toegevoegd was. |
| Telefoon | 2 | Binnen de telefooninzetten werd in principe op basis van toeval gekozen. Daarbij maakten we ook een uitzondering. Een zaak bleek een internationale component te hebben. Die inzet is geselecteerd. Daarnaast is een inzet op basis van toeval gekozen. |
| Telefoon (icm ander geautomatiseerd werk) | 3 | Voor de selectie van inzetten binnen deze categorie, is een tweedeling gemaakt wat betreft de wijze van binnendringen. Uit beide categorieën selecteerden we één inzet op basis van toeval. |

# Bijlage 3 Wetgevingstraject

In deze bijlage wordt kort ingegaan op een aantal inhoudelijke thema's dat gedurende het wetgevingstraject onderwerp van discussie is geweest. Bij deze inhoudelijke punten gaat het om punten naar voren gebracht door direct betrokkenen bij het wetgevingstraject. Soms hebben de discussies geleid tot aanpassingen aan wetsteksten. Per thema zal aandacht zijn voor de inhoud van de belangrijkste onderwerpen binnen deze discussies en tot welke verandering die hebben geleid. De belangrijkste veranderingen/discussiepunten staan steeds aan het begin van een paragraaf kort samengevat. Achtereenvolgens komen nut en noodzaak en de reikwijdte (zowel wat betreft misdrijven als wat betreft het soort geautomatiseerde werk) aan bod. Vervolgens wordt ingegaan op het binnendringen, vooral het gebruik van kwetsbaarheden, en het thema waarborgen voor controle. Tot slot worden de thema's buitenland en waarden en waarborgen nader besproken.

## Nut en noodzaak

**Wijzigingen gedurende wetgevingstraject**
- Geen belangrijke wijzigingen. Argument blijft dat bestaande bevoegdheden niet volstaan.
- Noodzaak kan niet cijfermatig worden onderbouwd, omdat cijfers niet worden bijgehouden.

Gedurende de wetsgeschiedenis worden vragen gesteld over de precieze noodzaak voor de nieuwe bevoegdheid (*Kamerstukken II* 2016/17, 34 372, nr. 6). Volgens de staatssecretaris kan de noodzaak van de nieuwe bevoegdheid gevonden worden in 'voortschrijdende techniek en het wijdverbreide gebruik van geautomatiseerde werken voor communicatie en de verwerking en opslag van gegevens'. Daardoor is het voor opsporingsinstanties steeds ingewikkelder om bestaande opsporingsbevoegdheden in te zetten (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 1-2). Meerdere partijen willen ten aanzien van gepleegde misdrijven weten of er misdrijven zijn (en hoeveel dan) die niet zijn opgelost, omdat er nog geen hackbevoegdheid was.[131] In de nota naar aanleiding van het verslag geeft de staatssecretaris voorbeelden van misdrijven waarbij er problemen zouden kunnen ontstaan/zich hebben voorgedaan in het opsporingsproces (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 15-16).[132]

[131] Zie o.a. *Kamerstukken II*, Handelingen 13 december 2016, nr. 34 en *Kamerstukken I* 2016/17, 34 372, B.
[132] Wel wordt verwezen naar meer algemene rapporten om de omvang van *cybercrime* en 'de onderkenning van de urgentie' te schetsen (*Kamerstukken I* 2016/17, 34 372, D, p. 1).

### Reikwijdte – misdrijven en geautomatiseerde werken

*Misdrijven*

**Wijzigingen gedurende wetgevingstraject**
- Het inzetten van subD (vastleggen gegevens) en subE (ontoegankelijk maken van gegevens) beperkt zich tot misdrijven waarvoor een maximale gevangenisstraf van acht jaar of meer kan worden opgelegd of misdrijven die bij AMvB zijn aangewezen.
- Een informele voorhang wordt toegezegd met betrekking tot de misdrijven die in de AMvB worden opgenomen.
- De lijst van misdrijven opgenomen in de AMvB wordt tot en met de behandeling van het eerste deel van de evaluatie van de wet niet gewijzigd.
- Artikel 200 Sr (wegmaken van bewijs) en artikel 161bis onder 1°, Sr. (opzettelijke vernieling van elektriciteitsnetwerken) worden geschrapt van de AMvB-lijst op advies van de Raad van State. Het argument hiervoor is dat voor deze misdrijven géén voorlopige hechtenis is toegestaan.

Er is veel kritiek op de reikwijdte van de nieuwe bevoegdheid, bijvoorbeeld omdat het vereiste dat de bevoegdheid kan worden ingezet wanneer sprake is van een artikel 67 feit en een ernstige verstoring van de openbare orde, te ruim zou zijn.[133] Ook de Raad van State heeft bedenkingen bij de reikwijdte van de bevoegdheid. Niet voor alle onderzoekshandelingen vindt zij de geformuleerde criteria passend. Daarom acht zij differentiatie nodig en in haar advies richt zij zich op het vastleggen van gegevens (subD). Dat is in de ogen van de Raad van State te vergelijken met het heimelijk binnentreden van een woning om vertrouwelijke communicatie op te kunnen nemen. Daardoor zou sprake zijn van een meer ingrijpende inbreuk op de persoonlijke levenssfeer dan bij andere onderzoekshandelingen die in het wetsartikel genoemd worden. Het heimelijk binnentreden mag pas bij misdrijven waarbij een gevangenisstraf van acht jaar of meer is vereist (*Kamerstukken II* 2015/16, 34 372, nr. 4, p. 5). In de nota naar aanleiding van het verslag aan de Tweede Kamer wordt duidelijk dat de wet naar aanleiding van dit advies (deels) aangepast is. Voor het vastleggen van gegevens, maar ook voor het ontoegankelijk maken van gegevens is een misdrijf vereist 'dat een ernstige inbreuk op de rechtsorde oplevert en waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld'. Ook wordt aangegeven, en dit ligt niet in lijn met het advies van de Raad van State,[134] dat beide onderzoekshandelingen mogen worden uitgevoerd als sprake is van een misdrijf dat bij Algemene Maatregel van Bestuur (AMvB) is aangewezen (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 3-4). Deze misdrijven zullen in het Besluit onderzoek in een geautomatiseerd werk worden vastgelegd. Het voordeel van het vastleggen van een aantal misdrijven in een AMvB (in plaats van in de wet) is volgens de staatssecretaris dat 'flexibel ingespeeld kan worden op ontwikkelingen in de computercriminaliteit' (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 36). Ondanks de toevoeging van het achtjaarscriterium en de AMvB-lijst, blijven kritische geluiden bestaan ten aanzien van de reikwijdte van de nieuwe bevoegdheid.[135] Een groot deel van de zorg zit (gedurende het gehele wetgevingstraject) bij het feit dat de bevoegdheid kan worden ingezet voor misdrijven die bij Algemene Maatregel van Bestuur worden vastgelegd (*Kamerstukken I* 2018/19, 34 372, L, p. 7). E r is

[133] Advies Bits of Freedom. Advies Nederlandse orde van advocaten.
[134] Het belangrijkste argument hiervoor is dat alleen het 8-jaarscriterium te beperkend wordt geacht. (*Kamerstukken II* 2015/16, 34 372, nr. 4, p. 19).
[135] Bijvoorbeeld *Kamerstukken II*, Handelingen 13 december 2016, nr. 34, p. 15 & p. 17-18.

bijvoorbeeld zorg dat de staatssecretaris deze lijst met misdrijven mag wijzigen zonder dat controle door de Tweede Kamer plaatsvindt, omdat er geen 'voorhang' geregeld is. Sommige partijen suggereren dat in plaats van een AMvB-lijst, misdrijven wettelijk zouden moeten worden vastgelegd.[136] Op verschillende momenten in het wetgevingstraject wordt door de verantwoordelijk bewindspersoon (eerst de staatssecretaris Veiligheid en Justitie en later de Minister van Justitie en Veiligheid) uitgelegd dat hij zich niet wil beperken tot een aparte lijst van misdrijven. Ook wil hij het grootste deel van de AMvB-lijst niet wijzigen.[137] In reactie op de zorgen die bestaan over een beperkte invloed van de Kamer(s) op de misdrijven die uiteindelijk op de AMvB-lijst terecht komen, geeft de staatssecretaris aan dat er geen formele voorhangprocedure komt (zo'n procedure zou veel tijd in beslag nemen), maar dat de lijst aan beide Kamers bekend wordt gemaakt. Wel komt er een 'informele nahangprocedure'. Dat betekent dat de AMvB pas in werking zal treden nadat beide Kamers, indien zij dat nodig achten, zich uit hebben kunnen spreken over de proportionaliteit. Mochten er daarna nog wijzigingen komen, dan zal een 'informele voorhangprocedure' plaatsvinden (*Kamerstukken I*, Handelingen 19 juni 2018, nr. 34, p. 36).

*Geautomatiseerde werken*

**Wijzigingen gedurende wetgevingstraject**
- Op advies van de Raad van State wordt 'computergegevens' niet opgenomen in de nieuwe definitie van een geautomatiseerd werk.
- Er komt geen (beperkende) lijst van geautomatiseerde werken ten aanzien waarvan de politie de hackbevoegdheid mag inzetten.
- De minister zegt wel toe dat de politie niet zal binnendringen in geautomatiseerde werken die zich in het lichaam bevinden (bijvoorbeeld pacemakers).

Gedurende de wetsgeschiedenis zijn er vragen over de reikwijdte van het begrip geautomatiseerd werk. Vooral over de breedte van de definitie is discussie. Een aantal partijen wil graag weten welke geautomatiseerde werken wel en welke niet binnen de gehanteerde definitie vallen (*Kamerstukken II* 2015/16, 34 372, nr. 5, p. 7-8, 11). Soms wordt deze vraag gespecificeerd door concrete voorbeelden te noemen, zoals het binnendringen van elektronische '*connected cars' (Kamerstukken II* 2015/16, 34 372, nr. 5, p. 13). Ook wordt geopperd dat deze wet het mogelijk maakt pacemakers binnen te dringen (*Kamerstukken II* 2015/16, 34 372, nr. 5, p. 15). Vanwege de breedte van de definitie wensen sommige partijen dat de definitie van een geautomatiseerd werk ingekaderd wordt en/of een limitatieve opsomming wordt gegeven (bijvoorbeeld in een AMvB) van het soort geautomatiseerde werken dat de politie met deze nieuwe bevoegdheid mag binnendringen (*Kamerstukken II* 2015/16, 34 372, nr. 5, p. 12; *Kamerstukken II* 2016/17, 34 372, nr. 20; *Kamerstukken II*, Handelingen 13 december 2016, nr. 34, p. 18; *Kamerstukken I*, Handelingen 19 juni 2018, nr. 34, p. 12). De staatssecretaris wil aan dit verzoek echter geen gehoor geven. Ook komt er geen aparte lijst van geautomatiseerde werken die mag worden binnengedrongen (*Kamerstukken I* 2016/17, 34 372, D, p. 29). Argument hiervoor is onder andere dat op dit moment niet te voorspellen is wat in de (nabije) toekomst de

[136] Zie onder andere *Kamerstukken I* 2016/17, 34 372 & *Kamerstukken II* 2016/17, 34 372, nr. 21.
[137] Een uitzondering hierop vormen Artikel 200 wetboek van Sr (wegmaken van bewijs) en artikel 161bis onder 1°, Sr. (opzettelijke vernieling van elektriciteitsnetwerken). Deze worden, op advies van de Raad van State, geschrapt van de AMvB-lijst, omdat voor deze misdrijven geen voorlopige hechtenis is toegestaan. De minister legt uit dat een misdrijf waarvoor voorlopige hechtenis is toegestaan 'de ondergrens van de inzet van de bevoegdheid' is (*Kamerstukken* 2018/19, 34 372, L, p. 6).

technische mogelijkheden zijn om informatie te verkrijgen zodat gemakkelijk toegang kan worden verkregen tot de *cloud*diensten van een verdachte (*Kamerstukken II Handelingen* 13 december 2016, nr. 34, p. 43). Wel zegt de minister tijdens de plenaire behandeling van de wet in de Eerste Kamer uiteindelijk toe dat de bevoegdheid niet zal worden ingezet bij apparatuur die zich 'op enigerlei manier in het lichaam bevindt' (*Kamerstukken I*, Handelingen 19 juni 2018, nr. 34, p. 24) zoals een pacemaker.

### Binnendringen & het gebruik van kwetsbaarheden

**Wijzigingen gedurende wetgevingstraject**

- Informatie over de identificeerbaarheid van een geautomatiseerd werk moet worden opgenomen in het bevel (naar aanleiding van advies Raad van State).
- Nieuw wetsartikel met betrekking tot het uitstellen van het melden van een onbekende kwetsbaarheid (artikel 126ffa Sv.), toegevoegd naar aanleiding van een amendement in de Tweede Kamer.
- Gebruik van een commercieel product wordt beperkt (vastgelegd in het Regeerakkoord) en mag voor één opsporingsonderzoek worden gebruikt. Bij een nieuwe zaak moet een nieuwe licentie worden aangeschaft (*Kamerstukken I* 2017/18, 34 372, G, p. 11-12).
- De politie koopt zelf géén informatie in over onbekende kwetsbaarheden (*Kamerstukken I* 2016/17, 34 372, D, p. 19).
- De eigen ontwikkeling van binnendringingsproducten door de politie dient gestimuleerd te worden (Staatsblad 2018, 340, p. 15).

Gedurende het wetgevingstraject bestaan er zorgen over mogelijke risico's die kleven aan het inzetten van de nieuwe bevoegdheid. Naast economische risico's gaat het om veiligheidsrisico's. Zorgen met betrekking tot veiligheid hebben vooral betrekking op het binnendringen met behulp van kwetsbaarheden die de politie wil gebruiken. De vrees bestaat dat ook (onbevoegde) derden hiervan gebruik kunnen maken. Daardoor zouden onveilige situaties kunnen ontstaan in computersystemen. Een extra risico wordt vermeld bij de toegang tot organisaties binnen de vitale sector, denk aan de bancaire of zorgsector (*Kamerstukken II* 2015/16, 34 372, nr. 4). Omdat lang niet altijd duidelijk is wie de eigenaar is van het geautomatiseerde werk dat wordt binnengedrongen, beveelt de Raad van State aan om alleen binnen te dringen wanneer de identiteit van het geautomatiseerde werk bekend is of om beter te motiveren waarom zou moeten worden binnengedrongen als deze onbekend is. Ook adviseert zij om op te nemen dat voor de rechter-commissaris gemotiveerd dient te worden waarom het een aanvaardbaar risico is binnen te dringen, zonder dat de identiteit van het geautomatiseerde werk vaststaat (*Kamerstukken II* 2015/16, 34 372, nr. 4). Naar aanleiding van het advies van de Raad van State wordt vastgelegd dat in het bevel gegevens opgenomen dienen te worden met betrekking tot de identificeerbaarheid van het geautomatiseerde werk. Ook is aangegeven dat informatie met betrekking tot de identificeerbaarheid belangrijk is voor de rechter-commissaris (*Kamerstukken II* 2015/16, 34 372, nr. 4).

Een deel van de politieke partijen is gedurende het wetgevingstraject huiverig ten aanzien van het benutten van kwetsbaarheden. Sommige partijen zijn tegen het gebruik van alle soorten kwetsbaarheden (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34, o.a. p. 23; *Kamerstukken II* 2016/17, 34 372, nr. 8), bijvoorbeeld omdat een dergelijke werkwijze het opsporingsbelang laat prevaleren boven het verminderen

van het risico op cybercrime (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34). Voor andere partijen ligt het gebruik van kwetsbaarheden genuanceerder (*Kamerstukken II* 2015/16, 34 372, nr. 4; *Kamerstukken II* 2016/17, nr. 6; *Kamerstukken II*, Handelingen 13 december 2016, nr. 34, p. 33). Zij geven aan dat opsporingsinstanties hun werk moeten kunnen blijven doen (*Kamerstukken II* 2016/17, 34 372, nr. 6). Daarnaast zouden gebruikers van software zelf verantwoordelijk zijn om maatregelen te nemen die de kans verkleinen dat derden toegang krijgen tot hun systeem, bijvoorbeeld door bijtijds nieuwe updates te installeren (*Kamerstukken II* 2016/17, 34 372, nr. 6). Het gebruik van (onbekende) kwetsbaarheden zou ook voordelen hebben wat betreft veiligheid. De PvdA betoogt bijvoorbeeld dat kwetsbaarheden ('zwakheden') sowieso bestaan, of de politie er gebruik van maakt of niet. Het voordeel van het gebruik door de politie is dat deze de kwetsbaarheid kan melden. Bekende onbekende kwetsbaarheden kunnen op die manier een bekende kwetsbaarheid worden en worden opgelost (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34, p. 33), een redenering die ook de staatssecretaris op een later moment tijdens de behandeling van de wet in de Tweede Kamer naar voren brengt (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34, p. 36).

## Meldplicht

Om het gebruik van (bekende) onbekende kwetsbaarheden enigszins te reguleren wordt een amendement ingediend waarin het melden van een onbekende kwetsbaarheid in uitzonderlijke gevallen mag worden uitgesteld, onder andere wanneer sprake is van een 'zwaarwegend opsporingsbelang'. Een bevel tot uitstel kan worden gegeven na een machtiging van de rechter-commissaris (*Kamerstukken II* 2016/17, 34 372, nr. 14).
Gedurende het wetgevingstraject is er discussie of deze meldplicht al aanwezig is in de wet. Staatssecretaris Dijkhoff geeft aan dat er een meldplicht geldt voor onbekende kwetsbaarheden waar 'willens en wetens' (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34, p. 41) gebruik van wordt gemaakt. Deze verplichting staat volgens hem weliswaar niet in de wet, maar wel in de toelichting en in de eerdergenoemde brief over het gebruik van kwetsbaarheden.[138,139] De onbekende kwetsbaarheid zal gemeld worden bij de fabrikant van de hard- of software waarin deze kwetsbaarheid zich bevindt. Alleen het uitstellen van een melding wordt uiteindelijk opgenomen in de wet (artikel 126 ffa Sv).
In de Eerste Kamer wordt toegelicht dat de afweging om een melding uit te stellen op centraal niveau binnen het Openbaar Ministerie zal worden gemaakt, omdat een dergelijke beslissing 'het individuele opsporingsonderzoek overstijgt' (*Kamerstukken I* 2017–2018, 34 372, G, p. 4). De rechter-commissaris, die voor het nemen van zijn beslissing externe deskundigen kan raadplegen,[140] bepaalt de lengte van de periode dat het uitstel mag duren (*Kamerstukken I*, Handelingen 19 juni, nr. 34). Een rechter-commissaris kan het uitstel steeds met vier weken verlengen. Verder wordt besproken

[138] Eerder wordt aangegeven dat de regering, in het kader van digitale veiligheid en de vermindering van criminaliteit, door middel van beleid voor *resonsible disclosure* het melden van kwetsbaarheden stimuleert (*Kamerstukken II* 2016/17, 34 372, nr. 6).
[139] 'Kwetsbaarheden die in het kader van een opsporingsonderzoek aan het licht komen, en waarvan aannemelijk is dat ze nog onbekend zijn, worden in beginsel direct of zo spoedig mogelijk gemeld aan de fabrikant van de desbetreffende hardware of software' (*Kamerstukken II* 2016/17, 26 643, nr. 428, p. 4).
[140] Een aantal partijen heeft de wens uitgesproken om beslissingen over het niet melden van kwetsbaarheden over te laten aan een *review board*, naar Amerikaans voorbeeld. De regering is daar geen voorstander van. Zij vindt dat de ingebouwde waarborgen, zoals toetsing door een rechter-commissaris, voldoende zijn (*Kamerstukken I* 2017/18, 34 372, G).

dat een onbekende kwetsbaarheid in commerciële software alleen wordt gemeld, als de politie en of het Openbaar Ministerie daar kennis van nemen (*Kamerstukken I* 2016/17, 34 372, D, p. 22).

### Commerciële software

Een ander punt waarover discussie is gedurende het wetgevingstraject, is het aankopen en gebruikmaken van commerciële producten (waarin onbekende onbekende kwetsbaarheden verwerkt zitten). Critici vrezen dat deze producten gemakkelijk misbruikt zouden kunnen worden.[141] De staatssecretaris gaat hier deels in mee wanneer hij uitlegt dat het aankopen van software een 'ongemakkelijk hoekje is', omdat ook 'andere afnemers die minder fris zijn' gebruik kunnen maken van een softwareproduct dat door een bedrijf verkocht wordt (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34, p. 39-40). Een ander punt van kritiek is dat de politie gemakkelijk misbruik zou kunnen maken van de nieuwe bevoegdheid.[142] In de nota naar aanleiding van het verslag legt de staatssecretaris uit dat misbruik, in welke vorm dan ook, altijd mogelijk is, maar dat de nieuwe bevoegdheid wat dat betreft niet afwijkt van de bevoegdheden die behoren tot het 'analoge domein'. Ook daar kan misbruik van worden gemaakt (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 52). Ook wijst hij op het bestaan van verschillende waarborgen die ervoor zouden moeten zorgen dat de bevoegdheid op een goede manier wordt gebruikt. Het gaat onder andere om logging die het mogelijk moet maken om eventuele manipulaties te achterhalen (*Kamerstukken II* 2016/17, 34 372, nr. 6).[143]
Ondanks de kritiek mogen commerciële producten aangeschaft worden (*Kamerstukken I*, Handelingen 19 december 2018, nr. 34, p. 21). De staatssecretaris wil de mogelijkheid openhouden dat software kan worden ingekocht waarvan de precieze samenstelling onbekend is. Soms zal een fabrikant bekende kwetsbaarheden benutten en op het moment dat het inkopen van software te veel beperkt wordt, worden te veel opties uitgesloten die voor de politie heel nuttig zouden kunnen zijn (Kamerstukken II Handelingen 13 december 2016, nr. 34). In een memorie van antwoord aan de Eerste Kamer staat overigens beschreven dat de politie zelf geen informatie over onbekende kwetsbaarheden zal inkopen in het kader van de inzet van de nieuwe bevoegdheid (*Kamerstukken I* 2016/17, 34 372, D, p. 19). In het regeerakkoord 2017-2021 wordt de aanschaf van commerciële binnendringingssoftware beperkt: de software mag voor slechts één specifieke zaak worden aangekocht. Dat betekent dat het moet gaan om 'een specifiek onderzoek, specifieke gegevens en specifieke personen'. De regering wil niet 'de markt voor onbekende kwetsbaarheden bevorderen', omdat die de veiligheid van het internet negatief zouden kunnen beïnvloeden (*Kamerstukken I* 2017/18, 34 372, G, p. 11). Bij een nieuwe zaak zal eerst opnieuw de 'bruikbaarheid van minder ingrijpende middelen worden beoordeeld' voordat kan worden overgegaan tot de aankoop van een nieuwe licentie (*Kamerstukken I* 2017/18, 34 372, G, p. 11-12). Bij de evaluatie na twee jaar zal worden gekeken of het licentiemodel 'de effectiviteit van de wet belemmert of niet' (*Kamerstukken I*, Handelingen 19 december 2018, nr. 34, p. 8).

[141] Zie oa: *Kamerstukken II* 2016/17, 34 372, nr. 22; *Kamerstukken II Handelingen* 13 december 2016, nr. 34.
[142] Aanvullend advies BoF; *Kamerstukken I* 2018/19, 34 372, M, p. 3 (bij dat laatste gaat het overigens om het verrichten van onderzoekshandelingen).
[143] Andere waarborgen waaraan kan worden gedacht zijn: functiescheiding en screening van politieambtenaren (*Kamerstukken II* 2016/17, 34 372, nr. 6).

### Eigen ontwikkelde producten

Gedurende het wetgevingstraject wordt een aantal keer de vraag gesteld of de politie niet zelf software zou kunnen ontwikkelen.[144] De SP merkt in een debat in de Eerste Kamer op dat het wellicht goed zou zijn om de aanschaf van commerciële software uit te faseren en om de benodigde kennis 'zelf in huis te halen en ook in huis te houden' (*Kamerstukken I*, Handelingen 19 december 2018, nr. 34, p. 11). In het verslag van de Tweede Kamer over het schriftelijk overleg naar aanleiding van het Besluit bevestigt de regering een dergelijke werkwijze. Zij wil graag 'inzetten op de eigen ontwikkeling van methoden voor het binnendringen' door 'de ontwikkeling van passende producten binnen de politie' te stimuleren (*Kamerstukken II* 2018/19, 34 372, nr. 29, p. 9).[145] In een eerdere discussie in de Tweede Kamer blijkt dat daarmee niet bedoeld wordt dat de politie burgers zal vragen om kwetsbaarheden bij haar te melden, zodat de politie kan bekijken of deze nuttig kunnen zijn in opsporingsonderzoeken en ze daarna te melden zodat de kwetsbaarheden gedicht kunnen worden. Eenieder zou een onbekende kwetsbaarheid altijd direct bij het NCSC[146] moeten melden (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34, p. 42).

### Waarborgen voor controle

**Wijzigingen gedurende wetgevingstraject**

- De Inspectie Justitie en Veiligheid gaat het 'systeemtoezicht' voor haar rekening nemen. Systeemtoezicht betekent toezicht op het functioneren van het wettelijk systeem. Er komt geen nieuw toezichtsorgaan vergelijkbaar met de CTIVD die toezicht houdt op de Algemene Inlichtingen- en Veiligheidsdienst (AIVD).

De waarborgen voor controle rondom de bevoegdheid is een belangrijk discussiepunt gedurende het gehele wetgevingstraject. De Raad van State merkt op dat er een toezichthoudende instantie zou moeten komen die het 'structurele systeemtoezicht' op zich neemt. Systeemtoezicht betekent dat toegezien wordt op de 'rechtmatige uitoefening van opsporingsbevoegdheden, waarbij door middel van informatie- en communicatietechnologie naar gegevens wordt gezocht en/of deze worden verkregen'. Om het systeemtoezicht uit te kunnen voeren zullen individuele zaken kunnen worden ingezien, maar hoeft daarover géén oordeel uitgesproken te worden (zoals een rechter dat doet). In haar advies roept de Raad van State op tot een jaarlijkse openbare rapportage (*Kamerstukken II* 2015/16, 34 372, nr. 4, p. 19). Het extra toezicht is volgens de Raad van State allereerst nodig, omdat rechters waarschijnlijk niet (altijd) in staat zullen zijn om de wijze waarop het onderzoek heeft plaatsgevonden, goed te kunnen beoordelen. Een rechter krijgt weliswaar toegang tot logbestanden, maar de verwachting is dat hij deze, en dat geldt ook voor officieren van justitie en advocaten, niet zelfstandig, zonder hulp van een technisch deskundige, kan beoordelen. Een tweede argument is dat lang niet alle opsporingsonderzoeken aan een zittingsrechter worden voorgelegd. Het enige dat in het kader van toetsing dan nog rest is dat de betrokkene(-n) op de hoogte worden gebracht dat de bevoegdheid is ingezet. Op basis van eerder onderzoek naar het nakomen van de notificatieverplichting is de Raad van

144 Zie bijvoorbeeld: *Kamerstukken II*, Handelingen 13 december 2016, nr. 34.
145 Deze wens wordt in het Besluit bevestigd (Besluit onderzoek in een geautomatiseerd werk, p. 15).
146 Het NCSC heeft ook de taak om organisaties die behoren tot de 'vitale infrastructuur' op de hoogte te stellen van de aanwezigheid van een onbekende kwetsbaarheid, mits zij hier kennis over heeft (Besluit onderzoek in een geautomatiseerd werk, p. 31.).

State, maar ook de Tweede Kamer sceptisch over deze vorm van toezicht (*Kamerstukken II* 2015/16, 34 372, nr. 4). Het is in de praktijk mogelijk om van notificatie af te zien (*Kamerstukken I*, Handelingen 19 juni 2018, nr. 34).

Tijdens de behandeling van de wet in beide Kamers wordt duidelijk dat een deel van de Kamerleden het eens is met de oproep tot extra systeemtoezicht, inclusief de argumentatie die daaraan ten grondslag ligt. Gedegen systeemtoezicht zou onder andere het 'rechtsstatelijke gehalte van de toepassing van de dwangmiddelenbevoegdheid' ten goede komen. Bovendien is het een mooie aanvulling op de niet altijd toereikende kennis van opsporingsambtenaren en rechters die verondersteld wordt (*Kamerstukken II* 2015/16, 34 372, nr. 5). Voorstanders van extra systeemtoezicht pleiten voor de komst van een commissie vergelijkbaar met de Commissie van Toezicht op Inlichtingen en Veiligheidsdiensten (CTIVD). Deze houdt 'toezicht op de rechtmatigheid van het handelen van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen en Veiligheidsdienst (MIVD)'. Het kabinet is geen voorstander van het instellen van een (extra) toezichtscommissie. Een belangrijk argument hiervoor is dat voldoende waarborgen aanwezig worden geacht. Het kabinet wijst op de Inspectie Justitie Veiligheid die het systeemtoezicht voor haar rekening kan nemen. Zij houdt zowel toezicht op zaken die aan de rechter worden voorgelegd als op zaken waarbij dat niet gebeurt. Systeemtoezicht betekent dat de Inspectie toezicht houdt op het functioneren van het wettelijk systeem. De grenzen van het bevel en de machtiging vormen de reikwijdte van het toezicht. De oordeelsvorming van de rechter-commissaris en de officier van justitie vallen hier niet binnen (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 82).
Het naar voren schuiven van de Inspectie wordt in beide Kamers kritisch bekeken, onder andere omdat (nog steeds) het risico bestaat dat er onvoldoende toezicht is op zaken die niet aan de rechter worden voorgelegd (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34). Bovendien wordt de onafhankelijkheid van de Inspectie in twijfel getrokken en zijn er vragen over de (beperkte) bevoegdheden die zij tot haar beschikking heeft (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34). De Inspectie Justitie en Veiligheid kan bijvoorbeeld geen mensen onder ede horen (*Kamerstukken I*, Handelingen 19 juni 2018, nr. 34).

## Buitenland

**Wijzigingen gedurende wetgevingstraject**
- Naar aanleiding van het advies van de Raad van State dient in het bevel aandacht te zijn voor de locatie van het geautomatiseerde werk.
- Optreden in het buitenland wordt mogelijk, ondanks dat hiervoor (nog) geen internationaal rechterlijk kader bestaat. Regels met betrekking tot (mogelijk) optreden in het buitenland worden vastgelegd in een OM-aanwijzing in plaats van in een Algemene Maatregel van Bestuur.

Een belangrijk punt van zorg is dat de nieuwe bevoegdheid niet past binnen internationale wet- en regelgeving waardoor het risico bestaat dat het buitenland gemakkelijker in Nederland zal optreden (*Kamerstukken II* 2015/16, 34 372, nr. 5, p. 33), dat wil zeggen dat het buitenland het minder nauw neemt met het soevereiniteitsbeginsel.[147] De Raad van State is kritisch, omdat de kans bestaat dat opsporingshandelingen worden uitgevoerd 'buiten het territorium in Nederland, zonder

[147] Aanvullend advies Bits of Freedom, p.12.

dat hiervoor een grondslag in het volkenrecht bestaat'. Om die reden vindt zij het niet voldoende dat in de concept memorie van toelichting alleen wordt gesproken over 'voorzichtig optreden bij het zelfstandig optreden'. Zij zou graag zien dat die voorzichtigheid duidelijk naar voren komt in regelgeving (*Kamerstukken II* 2015/16, 34 372, nr. 4, p. 12). Naar aanleiding van het advies is het wetsvoorstel aangepast. In de reactie op het advies van de Raad van State staat beschreven dat in het bevel moet worden aangegeven dat, indien dit aan de orde is, de gegevens niet in Nederland staan opgeslagen. Daarnaast is de memorie van toelichting aangevuld. Een rechter-commissaris kan een bevel afgeven, ook als gegevens niet in Nederland zijn opgeslagen. Daarbij mag er vanuit worden gegaan dat de officier zich houdt aan de regels met betrekking tot internationale samenwerking. Ook is aandacht besteed aan de situatie dat de locatie pas later bekend wordt (*Kamerstukken II* 2015/16, 34 372, nr. 4).
Op meerdere momenten in het wetgevingstraject legt de regering uit dat zij zich bewust is van het feit dat de wet- en regelgeving op internationaal niveau nog niet op orde is. Het territorialiteitsbeginsel in cyberspace zou onder druk staan. Verschillende opsporingsdiensten in Europa zouden digitaal bewijs verzamelen op een manier die verder gaat dan is voorzien in het Cybercrimeverdrag uit 2001 (*Kamerstukken II* 2016/17, 34 372, nr. 6). Tijdens het debat in de Tweede Kamer zegt de staatssecretaris dat het volkenrecht en verschillende internationale verdragen de regels ten aanzien van internationale samenwerking bepalen. De verschillende multilaterale en bilaterale rechtshulpverdragen zullen volgens de staatssecretaris wel moeten worden aangepast 'om aan de eisen van de moderne tijd te kunnen voldoen' (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34, p. 45). Ook in de memorie van toelichting wordt al duidelijk dat een verdere ontwikkeling van het internationaalrechtelijk kader de voorkeur heeft, maar dat de ontwikkeling ervan 'een ideaal is dat slechts op langere termijn kan worden gerealiseerd' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 46).[148]
In de tussentijd zijn er, zoal blijkt uit diezelfde memorie van toelichting, twee opties. De eerste is dat geen onderzoek plaatsvindt als onbekend is waar gegevens zich bevinden. Dat zou betekenen dat het internet 'een vrijplaats is voor criminaliteit' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 46). Omdat dat onwenselijk wordt gevonden, is gekozen voor de tweede optie, namelijk het 'zelfstandig op een zorgvuldige wijze uitoefenen van rechtsmacht bij de bestrijding van computercriminaliteit waarbij zo veel mogelijk rekening wordt gehouden met verschillende belangen' (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 46). De te volgen werkwijze wordt uiteindelijk in een OM-aanwijzing beschreven in plaats van bij Algemene Maatregel van Bestuur zoals in de wet gesuggereerd wordt als mogelijkheid (*Kamerstukken II* 2016/17, 34 372, nr. 6). De staatsecretaris vindt dat een meer voor de hand liggende optie, omdat het opsporingsonderzoek wordt uitgevoerd onder verantwoordelijkheid van het Openbaar Ministerie. Via een beleidsregel van het ministerie zou 'de consistentie en de kwaliteit' van opsporingsonderzoeken worden bevorderd (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 96).

[148] Gedurende het wetgevingstraject wordt duidelijk welke initiatieven worden genomen op internationaal niveau (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 99-100).

## Waarden en waarborgen

**Wijzigingen gedurende wetgevingstraject**
- Er zijn veel vragen over inbreuken op de persoonlijke levenssfeer. Verschillende waarborgen, al dan niet gedurende het wetgevingstraject toegevoegd, moeten ertoe leiden dat de inzet van de bevoegdheid proportioneel en subsidiair is.

### Inbreuk op de persoonlijke levenssfeer

De impact van de hackbevoegdheid op de persoonlijke levenssfeer van burgers is een belangrijk punt van zorg dat gedurende het wetgevingstraject naar voren komt. Deze inbreuk zou te groot zijn. De Raad van State vindt om die reden dat meer differentiatie nodig is ten aanzien van situaties waarin de bevoegdheid wel en niet kan worden ingezet (*Kamerstukken II* 2015/16, 34 372, nr. 3). Ook anderen zijn van mening dat vanwege de privacyschending de bevoegdheid met extra waarborgen omkleed zou moeten worden (*Kamerstukken II* 2015/16, 34 372, nr. 5). Toch maakt niet iedereen zich zorgen over mogelijke inbreuken op de persoonlijke levenssfeer. De CDA-fractie van de Tweede Kamer is van mening dat opsporingsinstanties door de nieuwe bevoegdheid zorgvuldiger kunnen handelen dan in het verleden het geval was. Het binnendringen in een geautomatiseerd werk zorgt er volgens haar voor dat klassieke opsporingsmethoden, zoals een huiszoeking en een fysieke inbeslagname, waarmee (ook) inbreuk wordt gemaakt op verschillende grondrechten, niet meer hoeven worden ingezet (*Kamerstukken II* 2015/16, 34 372, nr. 5). Een standpunt waarin de regering zich kan vinden (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 3). Desalniettemin erkent de regering dat de nieuwe bevoegdheid een ‘ingrijpende aantasting van de persoonlijke levenssfeer vormt’. De aanpassing van het wetboek is echter noodzakelijk, omdat de huidige bevoegdheden niet meer volstaan. Gegevens staan bijvoorbeeld niet meer opgeslagen op een vaste locatie (zie hoofdstuk 2). Een dergelijke inbreuk wordt bovendien gerechtvaardigd geacht, omdat verschillende waarborgen zijn ingebouwd: voorafgaande toestemming van een rechter-commissaris, opname onder Titel IVA in het Wetboek[149] en differentiatie wat betreft het soort misdrijven waarvoor de verschillende onderzoekshandelingen die in de wet zijn opgenomen, kunnen worden ingezet.[150] Verder meldt de regering dat reeds bestaande bevoegdheden, zoals het in beslagnemen van gegevensdragers, ook een ‘ingrijpende inbreuk vormen op de persoonlijke levenssfeer van betrokkenen’ (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 4). Een ander punt tot slot dat een aantal keer terugkomt, is dat het recht op privacy belangrijk is maar niet absoluut. In bepaalde gevallen is het toegestaan (*Kamerstukken I* 2016/17, 34 372, D).

Een specifiek aandachtspunt van degenen die zich zorgen maken over het maken van een inbreuk op de persoonlijke levenssfeer heeft te maken met hoe om wordt gegaan met burgers die niet als verdachte zijn aangemerkt. Een deel van de betrokkenen bij het wetgevingstraject acht de kans groot dat, op het moment dat de politie een computer van een verdachte binnendringt en daarin verschillende onderzoekshandelingen verricht, inzicht kan worden verkregen in gegevens die niet

[149] In dit deel van het Wetboek zijn ‘bijzondere bevoegdheden tot opsporing van vermoedelijk begane strafbare feiten’ vastgelegd.

[150] Gedurende de behandeling van de wet in de Eerste Kamer worden deze waarborgen deels herhaald, maar worden ook nieuwe waarborgen genoemd. De minister noemt wettelijke voorwaarden (er geldt een zwaarder criterium als het gaat om gegevensovername) en procedurele voorwaarden, voorafgaand aan de inzet (toetsing door CTC) en gedurende de inzet (logging) (*Kamerstukken* I *Handelingen* 19 juni 2018, nr. 34).

direct toebehoren aan de verdachte. Gerefereerd wordt aan het creëren van een sleepnet waarin de omgeving van de verdachte meegetrokken wordt (*Kamerstukken II* 2015/16, 34 372, nr. 5). De staatssecretaris erkent dat niet kan worden uitgesloten dat de politie gegevens verzamelt van niet-verdachte burgers. Ook bij andere reeds bestaande opsporingsbevoegdheden, zoals het afluisteren van vertrouwelijke communicatie, kan dat aan de orde zijn. Rondom de bevoegdheid is echter een aantal waarborgen ingebouwd (bijvoorbeeld het geautomatiseerde werk moet in gebruik zijn bij de verdachte, een inzet kan niet plaatsvinden bij alle soorten misdrijven) waardoor een sleepnet niet voor de hand ligt. Mochten gegevens worden verzameld van niet-verdachte burgers, dan ligt het voor de hand dat die gegevens gewist worden,[151] aldus de staatssecretaris (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 27-28).

### Subsidiariteit en proportionaliteit

Voor de regering is helder dat de nieuwe bevoegdheid voldoet aan het 'noodzakelijkheidscriterium'. Bovendien is het dringend opsporingsbelang, en daarmee de proportionaliteit en de subsidiariteit, een belangrijk onderdeel van de afweging die de officier van justitie en rechter-commissaris voorafgaand aan de inzet maken. Bij elke inzet zullen zij beoordelen of de inzet proportioneel is in relatie tot 'de inbreuk op de persoonlijke levenssfeer, het risico op nevenschade en de ernst van het strafbare feit'. Ook kijken zij of het onderzoeksdoel niet met minder ingrijpende middelen bereikt kan worden (*Kamerstukken II* 2016/17, 34 372, nr. 6). Er zijn echter partijen die vrezen dat de veiligheid juist in het geding komt door deze nieuwe bevoegdheid. Dat zou vooral het geval zijn wanneer bij de inzet van de bevoegdheid gebruik wordt gemaakt van kwetsbaarheden die zich in software bevinden die (ook) door consumenten wordt gebruikt (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34).

Hoewel het kabinet overtuigd is van de noodzaak van de wet, bediscussiëren anderen de subsidiariteit en de proportionaliteit ervan. In het kader van subsidiariteit wordt bijvoorbeeld gevraagd welke 'leemte' deze nieuwe bevoegdheid opvult (*Kamerstukken II* 2016/17, 34 372, nr. 6, p. 31).[152] Ook wordt gevraagd waarom andere bevoegdheden, zoals de IP-tap, niet volstaan (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34) Er bestaat behoefte aan cijfermatige onderbouwing van het aantal zaken waarin de reeds bestaande bevoegdheden niet voldeden (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34, p. 28). De antwoorden van de staatssecretaris en de minister bevatten argumenten die onder andere in de memorie van toelichting naar voren komen. Zo is een IP-tap lastig in verband met het bestaan van hotspots (draadloze netwerken). Eén van de redenen hiervoor is dat een tapbevel per toegangspunt afgegeven wordt. Op het moment dat meerdere toegangspunten in het spel zijn, betekent dit dat meerdere taps moeten worden geplaatst (bij elke netwerk- en dienstenaanbieder een tap). Dat is praktisch niet goed werkbaar vanwege de grote hoeveelheid data die verzameld wordt. Hierdoor wordt het moeilijker om volledig zicht te krijgen op de communicatie van een verdachte (*Kamerstukken II* 2015/16, 34 372, nr. 3, p. 10). Met betrekking tot aantallen wordt duidelijk dat die niet gegeven kunnen worden.

[151] Wat betreft het verwijderen van gegevens, gelden verschillende verwijderingsregimes.
[152] In deze nota blijkt dat deze bevoegdheid in sommige gevallen geen oplossing biedt, namelijk wanneer verdachten geen communicatiesoftware gebruiken of technisch zo onderlegd zijn dat de politie geen toegang kan krijgen tot hun informatie.

Wat betreft subsidiariteit worden niet alleen vragen gesteld over bestaande bevoegdheden van de politie maar ook over die van de Inlichtingendiensten. Is het bijvoorbeeld nodig dat de politie, in het kader van terrorismebestrijding, een zelfde soort bevoegdheid krijgt als de Inlichtingendiensten en is er geen risico op 'versnippering' van taken, zo vragen D66 en de SP zich af? (*Kamerstukken I* 2016/17, 34 372, D, p. 15-16). De minister vindt een nieuwe bevoegdheid voor de politie nodig, omdat terrorismebestrijding volgens hem zowel betrekking heeft op het beschermen van de nationale veiligheid (het terrein van de Inlichtingendiensten) als op de bestrijding van criminaliteit (het terrein van politie en justitie). Ook over 'versnippering' maakt hij zich geen zorgen. De AIVD richt zich op 'het tijdig onderkennen' van mogelijke terroristische aanslagen, terwijl de politie en het Openbaar Ministerie zich bezighouden met het opsporen en vervolgen van terroristische misdrijven (*Kamerstukken I* 2016/17, 34 372, D, p. 15-16).

Met betrekking tot de proportionaliteit van deze nieuwe bevoegdheid worden onder andere zorgen geuit ten aanzien van het soort misdrijven waarvoor de bevoegdheid kan worden ingezet en de omvang van gegevens die verzameld wordt (*Kamerstukken I*, Handelingen 19 juni 2018, nr. 34, p. 3). Daarnaast bestaan vragen over mogelijke schade die aangericht kan worden als gevolg van het gebruik van kwetsbaarheden (*Kamerstukken II*, Handelingen 13 december 2016, nr. 34). D66 vraagt zich in de Tweede Kamer af in hoeverre het proportioneel is om gebruik te maken van technische kwetsbaarheden die door derden kunnen worden misbruikt. Ook wil zij weten welke mogelijkheden een leverancier van kwetsbaarheden nog heeft, als een onderzoeksteam gebruik maakt van de kwetsbaarheid? Kan de leverancier dan bijvoorbeeld nog updates uitvoeren en zelf controle krijgen over het geautomatiseerde werk waarin binnengedrongen wordt? (*Kamerstukken II* 2015/16, 34 372, nr. 5, p. 26). Ook de VVD heeft vragen over het gebruik van kwetsbaarheden en de schade die hierdoor veroorzaakt kan worden. Zij is benieuwd of het binnendringen bij vitale sectoren,[153] en de schade die hierdoor mogelijk veroorzaakt wordt (maatschappelijke ontwrichting of financieel), proportioneel is. De VVD zou graag zien er een norm komt 'die de proportionaliteit van de inzet van hacksoftware toetst voordat een geautomatiseerd werk wordt binnengedrongen' (*Kamerstukken II* 2016/17, 34 372, F, p. 4). In antwoord hierop geeft de minister aan dat het onwaarschijnlijk is dat binnengedrongen zal worden in een geautomatiseerd werk van een vitale sector.[154] Er zijn minder zware manieren om gegevens te verkrijgen, namelijk het zelf benaderen van deze organisaties met het verzoek de benodigde gegevens te overhandigen. In dat geval zou het verzoek de subsidiariteitstoets niet doorstaan. Toch kan ook niet helemaal worden uitgesloten dat binnendringen bij een organisatie uit de vitale sector niet voorkomt, bijvoorbeeld wanneer dienstverleners zelf zijn geïnfiltreerd. In dit soort unieke gevallen zal een verzoek de proportionaliteitstoets doorstaan en zal toestemming worden gegeven tot het binnendringen in het betreffende werk. De toetsing komt volgens de minister voor rekening voor de verschillende organisaties die hiertoe aangewezen zijn (*Kamerstukken I* 2017/18, 34 372, G, p. 9-10).

[153] Ook de Raad van State wijst op subsidiariteit in relatie tot het afsluiten van botnets en het toenemende risico dat daardoor op geautomatiseerde werken binnengedrongen wordt die een vitale functie hebben (*Kamerstukken II* 2015/16, 34 372, nr. 4).

[154] Dit geldt ook voor andere geautomatiseerde werken, zoals een pacemaker.

# Bijlage 4 Procedure toetsing voorafgaand aan de inzet

De formele procedure is dat de zaaksofficier van justitie zijn of haar voornemen om de inzet van de bevoegdheid ex artikel 126nba Sv te vorderen voorlegt aan de rechercheofficier van justitie en de hoofdofficier van justitie van zijn/haar parket. Als beiden instemmen, wordt de voorgenomen toepassing na een officieel verzoek van de hoofdofficier van justitie ter goedkeuring voorgelegd aan het College van PG's. Dit gebeurt door tussenkomst van en na advisering door de Centrale Toetsingscommissie (CTC; Openbaar Ministerie, z.d.). Op basis van het advies van de CTC beslist het College van PG's vervolgens over de inzet van de bevoegdheid. De CTC, onder voorzitterschap van de hoofdofficier van het Landelijk Parket, kent drie kamers. De CTC-kamers zijn samengesteld uit leden van het Openbaar Ministerie en de politie. Deze leden hebben veel ervaring op het gebied van de opsporing van zware criminaliteit.

Het College van PG's beslist, met inachtneming van het advies van de CTC, of de hackbevoegdheid mag worden ingezet. Het College informeert de CTC over zijn beslissing en de eventueel daarbij gestelde voorwaarden. De CTC stelt vervolgens de hoofdofficier van justitie van het aanvragende parket en de Digit-officier van justitie op de hoogte van die beslissing, met de eventueel daarbij gestelde voorwaarden. De CTC stuurt hen ook het schriftelijke advies toe.
De zaaksofficier is verantwoordelijk voor de voortgang van het opsporingsonderzoek en of die conform de besluitvorming door het College van PG's verloopt. De zaaksofficier van justitie informeert de Digit-officier van justitie hierover.
Indien voortzetting van de inzet van de bevoegdheid na het verstrijken van de door het College van PG's gegeven termijn wenselijk is, legt de betrokken hoofdofficier van justitie de zaak opnieuw ter toetsing voor aan de CTC, conform bovenstaande procedure.
In alle gevallen waarin het College toestemming heeft verleend, informeert de betrokken hoofdofficier van justitie, (uiterlijk) na afloop van de zaak in eerste aanleg, de CTC over het resultaat van de toegepaste opsporingsmethode(n) (Openbaar Ministerie, z.d.).

Voor de aanvraag van de hackbevoegdheid heeft het Openbaar Ministerie ook een spoedprocedure ingericht (Openbaar Ministerie, z.d.). Die schrijft voor dat 'in geval van dringende noodzakelijkheid' de zaaksofficier van justitie zich direct kan richten tot het secretariaat van de CTC. Daarvoor is toestemming van de hoofdofficier van justitie en instemming van de Digit-officier van justitie nodig. De zaaksofficier van justitie motiveert het spoedeisende karakter van de voorgenomen inzet en de termijn waarbinnen een beslissing van het College van PG's gewenst is. Indien de CTC van oordeel is dat sprake is van een dringende noodzakelijkheid, stuurt de zaaksofficier van justitie aan de CTC (minimaal) een beknopte notitie met een toelichting van het verzoek en de zaak. De CTC beoordeelt het verzoek vervolgens op dezelfde wijze als bij een reguliere toetsing en geeft het College van PG's (mondeling) advies. Het College van PG's neemt hierop (mondeling) een beslissing en informeert de CTC daarover. De CTC koppelt deze beslissing per ommegaande terug aan de zaaksofficier van justitie. Deze spoedprocedure vindt schriftelijk en niet telefonisch plaats. Alle betrokkenen leggen na toepassing van de spoedprocedure alsnog hun verzoek, advies en beslissing schriftelijk vast.

# Bijlage 5 Keuringsproces

Het keuringsproces bestaat uit een aantal stappen, namelijk de acceptatietest (intake), de keuring zelf (uitvoering) en het keuringsrapport (afronding).
Tijdens de acceptatietest bekijkt de Keuringsdienst of het technisch hulpmiddel keurbaar is. Dat doet zij op basis van een checklist met daarin informatie die zij nodig heeft om tot een oordeel te komen. In die checklist staat onder andere dat gekeken moet worden of de bijgevoegde documentatie, waarin Digit de werking van het hulpmiddel toelicht, op orde is. Een acceptatie zou in principe in een halve dag kunnen gebeuren.
Na de acceptatietest volgt de keuring. Tijdens de keuring wordt gewerkt met een testplan. Daarin zijn alle testen opgenomen die worden uitgevoerd. Deze testen zijn samengebracht in een keur*tool* die ontwikkeld is door TNO. Veel van de testen die worden uitgevoerd zijn standaard en worden bij elk hulpmiddel dat Digit ter keuring aanbiedt, doorlopen. Aanvullend kunnen er testen worden gedaan, specifiek toegespitst op het aangeboden hulpmiddel.
Het testplan kan gedurende de keuring worden aangepast, bijvoorbeeld als blijkt dat een bepaalde test niet geschikt is. Digit heeft geen inzicht in het testplan. Zij kent alleen het keuringsprotocol. Hoeveel testen worden afgenomen is afhankelijk van het hulpmiddel, maar het aantal varieert van ongeveer 50 tot ongeveer 80. Het uitvoeren van deze testen vindt plaats in een eigen omgeving van de Keuringsdienst die niet verbonden is met het internet.

Nadat de resultaten van de verschillende testen bekend zijn, stelt de Keuringsdienst een keuringsrapport op dat openbaar kan worden gemaakt. Dat rapport beslaat 1 A4 waarin staat aangegeven of het middel goed- of afgekeurd is. Naast het rapport ontvangt Digit een toelichting (niet openbaar) waarin per eis wordt aangegeven wat het oordeel was. Groen betekent goedgekeurd en rood betekent afgekeurd. Als een eis oranje kleurt, dan betekent dit dat Digit vervangende waarborgen moet nemen om ervoor te zorgen dat het hulpmiddel aan de eis voldoet. Een middel kan alleen worden goedgekeurd als *alle* zeventien eisen groen en/of oranje kleuren. Indien (minstens) één eis rood kleurt, wordt het middel niet goedgekeurd. Dat betekent dat op dat moment Digit het middel niet zonder meer kan inzetten.
Bij een keuringsrapport van een goedgekeurd middel voegt de Keuringsdienst een handleiding toe. Daarin staat beschreven hoe Digit het middel zou moeten gebruiken inclusief (eventueel) extra te nemen vervangende waarborgen. Een voorbeeld van zo'n vervangende waarborg is dat medewerkers van het inzetteam datum en tijd moeten controleren. Het zou niet voldoende zijn als alleen het systeem van Digit dat doet.
Vanuit Digit klinken kritische geluiden over de waarborgen (onder andere het aantal) die vanuit de Keuringsdienst worden aangedragen. Door die waarborgen verdwijnt een voordeel van een technisch hulpmiddel, namelijk dat een aantal handelingen sneller (want geautomatiseerd) kan plaatsvinden. Eén van de geïnterviewden legt uit dat eigenlijk dubbel werk moet worden gedaan. Volgens deze geïnterviewde wordt in de systemen van Digit *screen recording* en *key recording* bijgehouden. Daarnaast vindt (andere) logging plaats. Ondanks die maatregelen zou Digit bij elk bestand dat binnengehaald wordt de tijd moeten checken bij het geautomatiseerde werk van de verdachte en bij Digit zelf. Dat moet vervolgens in een proces-verbaal worden vastgelegd. De Inspectie Justitie en Veiligheid heeft in haar tweede verslag

geconstateerd dat logging en het maken van beeld- en schermopnames niet altijd op orde is (Inspectie JenV, 2021, p. 11).[155]

[155] In haar derde Verslag wordt geconstateerd dat de volledigheid van de vastgelegde beeldschermopnames in 2021 'sterk is verbeterd' (Inspectie JenV, 2022, p. 27). Ook stelt zij vast dat in het begin van 2021 de logging niet op orde was, In de loop van 2021 is dit verbeterd (Inspectie JenV, 2022, p. 31).

Het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) is het kennisinstituut voor het ministerie van Justitie en Veiligheid. Het WODC doet zelf onafhankelijk wetenschappelijk onderzoek of laat dit doen door erkende instituten en universiteiten, ter ondersteuning van beleid en uitvoering.

Meer informatie:

www.wodc.nl