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)

Samenvatting

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)

Samenvatting

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.

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.

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