
PROCES-VERBAAL VAN BEVINDINGEN

Proces-verbaalnummer:
Documentcode:
Onderzoek:

Betreft: aanvullende waarborgen ex artikel 21 lid 4 Bogw
Parketnummer:
RC-Nummer:

PROCES-VERBAAL

<Ik/Wij>, <naam1/nummer1>, officier van justitie, en <naam2/nummer2>, officier van justitie, verklaren het volgende:

Op <datum> werd onder <mijn/onze> leiding een opsporingsonderzoek gestart onder de naam <naam onderzoek>. In dit onderzoek is/zijn (een) bevel(en) ex artikel <126nba/126uba/126zpa> Sv afgegeven.

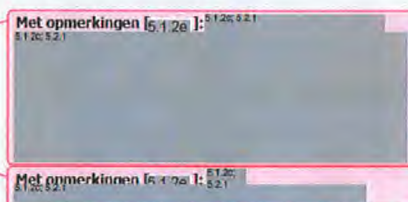
In dit/deze bevel(en) is ex artikel 21 lid 2 van het Besluit onderzoek in een geautomatiseerd werk (Bogw) bepaald dat een niet gekeurd technisch hulpmiddel werd gebruikt.

De uitvoering van dit/deze bevel(en) is gedaan door een technisch team van politie. Dit technisch team werkt onder gezag van een andere officier van justitie. Door deze officier van justitie is – ex artikel 21 lid 4 –beslist dat de aard van het technische hulpmiddel zich verzet tegen keuring na afloop van het gebruik. Keuring is om die reden achterwege gebleven. Daarvan is een apart proces-verbaal opgemaakt.

Daarnaast is door het technisch team van politie in proces-verbaal de werking en functionele specificaties van het technisch hulpmiddel nader beschreven. De door het technisch team getroffen waarborgen blijken daaruit.

Door <mij/ons> zijn de volgende aanvullende waarborgen getroffen:

<VERWIJDER DE OPMERKINGEN EN NIET BRUIKBARE TEKSTBLOKKEN>
5.1.2c; 5.2.1



5.1.2c; 5.2.1

Met opmerkingen [5.1.2c; 5.2.1]

Met opmerkingen [5.1.2c; 5.2.1]

Met opmerkingen [5.1.2c; 5.2.1]

Met opmerkingen [5.1.2c; 5.2.1]

Met opmerkingen [5.1.2c; 5.2.1]

Met opmerkingen [5.1.2c; 5.2.1]

Met opmerkingen [5.1.2c; 5.2.1]

Met opmerkingen [5.1.2c; 5.2.1]

Met opmerkingen [5.1.2c; 5.2.1]

5.1.2c; 5.2.1

Met opmerkingen [5.1.2a; 1; 5.1.2c; 5.2.1]

Met opmerkingen [5.1.2a; 1; 5.1.2c; 5.2.1]

Met opmerkingen [5.1.2a; 1; 5.1.2c; 5.2.1]

Met opmerkingen [5.1.2a; 1; 5.1.2c; 5.2.1]

Met opmerkingen [5.1.2a; 1; 5.1.2c; 5.2.1]

Met opmerkingen [5.1.2a; 1; 5.1.2c; 5.2.1]

Met opmerkingen [5.1.2a; 1; 5.1.2c; 5.2.1]

Met opmerkingen [5.1.2a; 1; 5.1.2c; 5.2.1]

5.1.2c; 5.2.1

Met onnervinnen [5.1.2c; 5.2.1]

Waarvan door <mij/ons> is opgemaakt dit proces-verbaal, dat <ik sloot / wij sloten> en <ondertekende/ondertekenden> op <datum> te <locatie LP/AP>.

<naam/nummer> op <ambtseed/ambtsbelofte>

<naam/nummer> op <ambtseed/ambtsbelofte>

PROCES-VERBAAL VAN BEVINDINGEN

Proces-verbaalnummer:

Documentcode:

Onderzoek:

Betreft: aanvullende waarborgen ex artikel 21 lid 4 Bogw

Parketnummer:

RC-Nummer:

PROCES-VERBAAL

<Ik/Wij>, <naam1/nummer1>, officier van justitie, en <naam2/nummer2>, officier van justitie, verklaren het volgende:

Op <datum> werd onder <mijn/ons> leiding een opsporingsonderzoek gestart onder de naam <naam onderzoek>. In dit onderzoek is/zijn (een) bevel(en) ex artikel <126nba/126uba/126zpa> Sv afgegeven.

In dit/deze bevel(en) is ex artikel 21 lid 2 van het Besluit onderzoek in een geautomatiseerd werk (Bogw) bepaald dat een niet gekeurd technisch hulpmiddel werd gebruikt.

De uitvoering van dit/deze bevel(en) is gedaan door een technisch team van politie. Dit technisch team werkt onder gezag van een andere officier van justitie. Door deze officier van justitie is – ex artikel 21 lid 4 –beslist dat de aard van het technische hulpmiddel zich verzet tegen keuring na afloop van het gebruik. Keuring is om die reden achterwege gebleven. Daarvan is een apart proces-verbaal opgemaakt.

Daarnaast is door het technisch team van politie in proces-verbaal de werking en functionele specificaties van het technisch hulpmiddel nader beschreven. De door het technisch team getroffen waarborgen blijken daaruit.

Voor de door <mij/ons> getroffen aanvullende waarborgen en de resultaten daarvan verwijs ik naar proces-verbaal/processen-verbaal <naam, documentcode> van <datum>.

Waarvan door <mij/ons> is opgemaakt dit proces-verbaal, dat <ik sloot / wij sloten> en <ondertekende/ondertekenden> op <datum> te <locatie LP/FP/AP>.

<naam/nummer> op <ambtseed/ambtsbelofte>

PROCES-VERBAAL VAN BEVINDINGEN

Betreft: beslissing ex artikel 21 lid 4 Bogw
Parketnummer:
Geautomatiseerd werk:
Onderzoek:

PROCES-VERBAAL

Ik, 5.1.2e , officier van justitie, verklaar het volgende:

In het opsporingsonderzoek <NAAM> is op <datum> een bevel ex artikel 126nba/uba/zpa Sv afgegeven ten aanzien van <omschrijving GW>. Dit geautomatiseerde werk is in gebruik bij <naam>.

In dit bevel is ex artikel 21 lid 2 van het Besluit onderzoek in een geautomatiseerd werk (Bogw) bepaald dat een niet gekeurd technisch hulpmiddel werd gebruikt.

De uitvoering van dit bevel (en eventuele verlengingen daarvan) is gedaan door een technisch team van politie. Dit technisch team werkt onder mijn gezag.

Door mij is – ex artikel 21 lid 4 Bogw – beslist dat de aard van het gebruikte technische hulpmiddel zich verzet tegen keuring. Keuring is om die reden achterwege gebleven.

Ik heb het technisch team van politie, dat is belast met de uitvoering van het/de genoemde bevel(en), daarom aanvullende waarborgen laten treffen om de betrouwbaarheid, integriteit en herleidbaarheid van de met het technisch hulpmiddel vastgelegde gegevens te garanderen.

Door het technisch team zijn in proces-verbaal de werking en functionele specificaties van het technisch hulpmiddel nader beschreven. De door het technisch team getroffen waarborgen blijken daaruit. Ik verwijs daarvoor naar proces-verbaal <naam, documentcode> van <datum>. Een verdergaande of gedetailleerdere omschrijven van het gebruikte technisch hulpmiddel is in verband met zwaarwegende opsporingsbelangen niet mogelijk.

Naast het voorgaande heeft ook officier van justitie, onder wiens gezag het tactische opsporingsteam werkt, aanvullende waarborgen laten treffen. Daarvan is/wordt een apart proces-verbaal opgemaakt.

Waarvan door mij is opgemaakt dit proces-verbaal, dat ik sloot en ondertekende op <datum> te Driebergen.

5.1.2e op ambtsbelofte

Notitie | Besluit voor de inzet TH

Landelijk Parket - DIGIT

Hoe verhoudt artikel 126nba lid 1 sub b Sv zich tot de artikelen 126l en 126m Sv?

1. Inleiding

Inzet van de hackbevoegdheid ex artikel 126nba, 126uba en/of 126zpa Sv¹ is voor wat betreft de uitvoering op grond van het eerste lid op twee manieren mogelijk: (1) er kan handmatig onderzoek worden gedaan, of (2) er kan onderzoek worden gedaan met behulp van een technisch hulpmiddel.

Een van de onderzoeksmogelijkheden onder artikel 126nba Sv is de uitvoering van een OVC- of tapbevel ex de artikelen 126l en 126m Sv.²

De ervaring leert dat vertrouwelijke - of telecommunicatie ook handmatig kan worden geregistreerd.^{5.1.2c}

In de artikelen 126l en 126m Sv staat echter specifiek dat deze communicatie moet worden opgenomen met een technisch hulpmiddel. In combinatie met artikel 126ee Sv en het Besluit technische hulpmiddelen moet gesproken worden van een verplichting.

Om die reden rijst de vraag hoe artikel 126nba zich verhoudt met de artikelen 126l en 126m Sv. Kan de uitvoering van een bevel 126l of 126m Sv op grond van artikel 126nba Sv ook handmatig worden uitgevoerd? Of dient er altijd een technisch hulpmiddel te worden ingezet? En zo ja, gelden voor dit technisch hulpmiddel dan de eisen van de artikelen 126l en 126m Sv; 126ee Sv jo. het Besluit technische hulpmiddelen strafvordering (hierna: Bths) of die van artikel 126nba Sv; het Besluit onderzoek in een geautomatiseerd werk (hierna: Bowg)?

2. Ter uitvoering van een bevel als bedoeld in de artikelen 126l of 126m Sv

Artikel 126nba Sv bepaalt dat er kan worden binnengedrongen in een geautomatiseerd werk en, al dan niet met een technisch hulpmiddel, onderzoek kan worden gedaan met het oog op de uitvoering van een bevel als bedoeld in de artikelen 126l of 126m.

¹ Ten behoeve van de leesbaarheid zal voortaan alleen worden verwezen naar art. 126nba Sv.

² Dan wel een tapbevel als bedoeld in art. 126t en 126zf Sv en de OVC-bevel als bedoeld in art. 126s en 126zg Sv. Ten behoeve van de leesbaarheid wordt steeds verwezen naar art. 126l en 126m Sv.

Artikel 126l Sv bepaalt dat er vertrouwelijke communicatie kan worden opgenomen met een technisch hulpmiddel.

Artikel 126m Sv bepaalt dat met een technisch hulpmiddel niet voor publiek bestemde communicatie, die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst, kan worden opgenomen.

Gezien de bewoordingen van artikel 126l en 126m Sv rijst de vraag of met de zinsnede van artikel 126nba lid 1 sub b Sv - “ter uitvoering van een bevel” – moet worden voldaan aan alle eisen die in respectievelijk artikel 126l en 126m Sv worden gesteld (dat wil zeggen het opnemen van communicatie met behulp van een technisch hulpmiddel) of dat die uitvoering slechts ziet op het opnemen van vertrouwelijke – dan wel niet voor publiek bestemde communicatie. En indien de communicatie moet worden opgenomen met een technisch hulpmiddel is de vraag welk besluit daar dan op van toepassing is.

Er lijken drie interpretaties mogelijk:

1. Het opnemen van de telecommunicatie en/of vertrouwelijke communicatie kan handmatig plaatsvinden. Artikel 126nba Sv is te zien als een specialis van artikelen 126l en 126m Sv.
2. Er moet een technisch hulpmiddel worden ingezet. De keuringseisen van artikelen 126l en 126m Sv en dus artikel 126ee en het Bths gelden onverkort.
3. Er moet een technisch hulpmiddel worden ingezet. De keuringseisen van artikel 126nba Sv en dus het Bogw zijn van toepassing.

Allereerst zal ik ingaan op de vraag of er gebruik moet worden gemaakt van een technisch hulpmiddel. En indien die vraag bevestigend wordt beantwoord of dat technisch hulpmiddel dan moet voldoen aan de eisen zoals bedoeld in het Bths of aan de eisen zoals bedoeld in het Bogw.

(Al dan niet) met een technisch hulpmiddel?

Ten aanzien van de vraag welke eisen die in art. 126m en 126l Sv worden gesteld van toepassing zijn bij een gecombineerde toepassing met art. 126nba Sv staat in de Memorie van Toelichting (hierna: MvT) ten aanzien van het opnemen van telecommunicatie:

(...) De in dit artikel opgenomen vereisten voor het opnemen van communicatie zijn onverkort van toepassing wanneer in het kader van een onderzoek in een geautomatiseerd werk wordt overgegaan tot het opnemen van communicatie. Er is een afzonderlijk bevel van de officier van justitie vereist. Hiervoor is een afzonderlijke schriftelijke machtiging van de rechter-commissaris vereist (artikelen 126m, 126s en 126zg, vijfde lid, Sv). Het Besluit technische hulpmiddelen strafvordering zal worden aangepast aan het opnemen van telecommunicatie in het kader van een onderzoek in een geautomatiseerd werk. Uitsluitend de opsporingsambtenaren die door de korpschef zijn aangewezen en die ter zake deskundig zijn, zullen met de uitvoering van een

dergelijk bevel kunnen worden belast. Ook zullen regels worden gesteld over het technische hulpmiddel dat hierbij kan worden gebruikt.³

En daarnaast staat er ten aanzien van communicatie zoals bedoeld in art. 126m en 126l Sv:

Tot slot wordt opgemerkt dat, voor zover het doel van het onderzoek is gelegen in het ontoegankelijk maken van gegevens (artikel 126cc, vijfde en zesde lid Sv), het aftappen en opnemen van communicatie of het opnemen van vertrouwelijke communicatie (artikelen 126l, 126m, 126s, 126t, 126zf, 126zg Sv) en de stelselmatige observatie (artikelen 126g, 126o, 126zd Sv), de bepalingen over de inzet van deze bijzondere opsporingsbevoegdheden van toepassing zijn. Hieruit volgt dat de wettelijke voorwaarden waaronder deze bevoegdheden kunnen worden ingezet onverminderd gelden.⁴

Op grond van bovenstaande kan worden geconcludeerd dat het opnemen van communicatie ter uitvoering van een bevel ex art. 126m of 126l Sv met een technisch hulpmiddel moet plaatsvinden.⁵

Besluit technische hulpmiddelen strafvordering vs. Besluit onderzoek in een geautomatiseerd werk

Dan is vervolgens de vraag of het technisch hulpmiddel dat wordt gebruikt ten behoeve van de uitvoering van het bevel ex art. 126m of 126l Sv dient te voldoen aan de eisen die worden gesteld in het Bths of aan de eisen van het Bogw.

In de MvT wordt tot uitdrukking gebracht dat de uitgangspunten in het Bths als basis dienen voor de inzet van een technisch hulpmiddelen onder artikel 126nba Sv, maar dat dit verder wordt geregeld/aangevuld in de maatregel van bestuur. Daarmee lijkt expliciet tot uitdrukking gebracht te worden dat het Bths in beginsel ook geldt bij de inzet van artikel 126nba Sv, maar dat er bij inzet onder artikel 126nba Sv een eigen (aanvullende) regeling is.

In de Nota van Toelichting (hierna: NvT) op het Bogw geautomatiseerd werk staat echter:

Het verrichten van onderzoekshandelingen in een geautomatiseerd werk kan plaatsvinden met het oog op bestaande bijzondere opsporingsbevoegdheden. Het betreft de stelselmatige observatie, het opnemen van communicatie of van vertrouwelijke communicatie (artikelen 126g, 126o, 126zd, eerste lid, onder a, 126l, 126m, 126s, 126t of 126zg Sv). Het Besluit technische hulpmiddelen strafvordering stelt eisen aan de traditionele technische hulpmiddelen die daarbij worden ingezet, zoals een camera of een richtmicrofoon. Op grond van de wet wordt het mogelijk om deze bevoegdheden uit te oefenen nadat op afstand heimelijk is binnengedrongen in een geautomatiseerd werk. In het onderhavige besluit worden eisen gesteld aan technische

³ Kamerstukken II 2015/16, 34372, nr.3, p. 24

⁴ Kamerstukken II 2015/16, 34372, nr.3, p. 31 en 103.

⁵ Zo ook Onderzoek in een geautomatiseerd werk (Eindrapportage Procureur-Generaal bij de Hoge Raad over de toepassing van opsporingsbevoegdheden als bedoeld in de artikelen 126nba lid 1, 126uba lid 1 en 126zpa lid 1 van het Wetboek van Strafvordering door het Openbaar Ministerie), bijlage bij Kamerstukken II 2022/23, 29279, nr. 744, p. 103.

hulpmiddelen die worden gebruikt bij de inzet van de bestaande bijzondere opsporingsbevoegdheden in het kader van een onderzoek in een geautomatiseerd werk. Alsdan gelden specifieke eisen voor de inzet van een technisch hulpmiddel, die zijn toegesneden op het gebruik in een digitale omgeving. Hieruit vloeit voort dat niet voldaan hoeft te worden aan de eisen van het Besluit technische hulpmiddelen strafvordering wat betreft de eisen met betrekking tot de traditionele technische hulpmiddelen.⁶

Gelet op hetgeen in de NvT op het Bogw staat dient het technisch hulpmiddel te voldoen aan de eisen zoals bedoeld in het Bogw en niet (tevens) aan de eisen van het Bths.

Conclusie

In geval van een combibeverl ex art. 126nba jo. 126m en/of 126l Sv dient er gebruik te worden gemaakt van een technisch hulpmiddel. Dit technisch hulpmiddel moet voldoen aan de eisen zoals omschreven in het Bogw.

26 oktober 2022

LP DIGIT - ^{5.1.2}
a

	Toegezonden	Afgerond
LP Digit	26-10-2022	16-12-2022
Afgestemd LE Digit	16-12-2022	

⁶ Staatsblad 2018 340, p. 19.

Notitie | Technisch hulpmiddel Besluit technische hulpmiddelen strafvordering vs. Besluit onderzoek in een geautomatiseerd werk

Landelijk Parket - DIGIT

1. Inleiding

Bij een inzet ex art. 126nba jo. 126m en/of 126l Sv¹ moet gebruik worden gemaakt van een technisch hulpmiddel dat voldoet aan de eisen zoals omschreven in het Besluit onderzoek in een geautomatiseerd werk (hierna: Bogw).² In deze notitie ga ik in op de vraag of een technisch hulpmiddel, zoals bijvoorbeeld een keylogger, dat in een eerder stadium al is goedgekeurd onder het regime van het Besluit technische hulpmiddelen strafvordering (hierna: Bths) ook een technisch hulpmiddel zou kunnen zijn in de zin van het Bogw.

2. Definitie technisch hulpmiddel

In art. 126ee Sv is bepaald dat er bij AMvB regels gesteld kunnen worden over de eisen waaraan een technisch hulpmiddel moet voldoen en hoe daarmee gewerkt kan worden. Het gaat dan om de wijze waarop de opslag, verstrekking, plaatsing en verwijdering van een technisch hulpmiddel plaats moet vinden, de technische eisen waaraan het hulpmiddel moet voldoen, de controle op de naleving van die technische eisen, de instellingen die de registratie van signalen aan een technische bewerking onderwerpen en de wijze waarop die technische bewerking plaatsvindt.

Die regels zijn terug te vinden in respectievelijk het Bths en het Bogw.

Bogw

Art. 1 onder f Bogw geeft de volgende definitie van een technisch hulpmiddel: een softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel.

Bths

Het Bths verwijst voor de definitie van een technisch hulpmiddel naar art. 126ee, onderdeel a Sv.³ Daarin staat benoemd dat er bij AMvB regels worden gesteld over technische hulpmiddelen als bedoeld in art. 126g, 126l, 126m en 126nba Sv. In de betreffende artikelen wordt het doel benoemd van het technisch hulpmiddel, namelijk het stelselmatig observeren of het opnemen van vertrouwelijke dan wel telecommunicatie zonder medewerking van de betrokken aanbieder.

De nota van toelichting voegt daar nog aan toe dat het besluit gericht is op technische

¹ Ten behoeve van de leesbaarheid zal steeds alleen worden verwezen naar de betreffende bevoegdheid in titel IVa. Tenzij anders vermeld is dit echter ook van toepassing op de soortgelijke bepalingen in titel V en VB.

² Zie voor meer informatie de notitie 20221026 Besluit vs. Besluit.

³ Zie art. 1 onder a Bths.

hulpmiddelen die signalen registreren en op een gegevensdrager vastleggen. Een technisch hulpmiddel kan samengesteld zijn uit verschillende componenten. Technische hulpmiddelen die alleen signalen detecteren, maar niet registreren, vallen buiten de reikwijdte van het besluit.⁴ Zowel hardware- als softwarematige technische hulpmiddelen lijken tot de mogelijkheden te behoren.⁵

De voorganger van het Bths, het Besluit technische hulpmiddelen bijzondere opsporingsbevoegdheden⁶ geeft in art. 1 onder b de volgende omschrijving van een technisch hulpmiddel: een configuratie van componenten die signalen detecteert, deze transporteert, hun registratie activeert en de signalen activeert. In de nota van toelichting staat dat in veel gevallen de genoemde functionaliteiten van het technisch hulpmiddel niet in één apparaat verenigd zullen zijn, maar dat het is opgebouwd uit diverse apparaten die met elkaar verbonden zijn.⁷

Tussenconclusie

De definitie van een technisch hulpmiddel in de zin van het Bths is ruimer dan die van het Bogw, maar sluit niet uit dat een technisch hulpmiddel in de zin van het Bths tevens een technisch hulpmiddel in de zin van het Bogw zou kunnen zijn.

3. Technische eisen

Op grond van art. 126ee onder b Sv kunnen bij AMvB regels gesteld worden omtrent de technische eisen waaraan de technische hulpmiddelen moeten voldoen, onder meer met het oog op de onschendbaarheid van de vastgelegde waarnemingen, of in geval van de hackbevoegdheid, de vastgelegde gegevens, en met het oog op voorkomen van misbruik door derden.

Om zeker te zijn dat een technisch hulpmiddel aan de eisen voldoet, moet het worden gekeurd. Uit het keuringsrapport dat wordt opgesteld blijkt dat is voldaan aan de eisen zoals omschreven in artt. 10 t/m 14 Bths.⁸ Voor het Bogw geldt dat een technisch hulpmiddel uitsluitend goed wordt gekeurd indien aan de eisen die worden gesteld in artt. 8 t/m 13 Bogw wordt voldaan.

Hieronder volgt een vergelijking van deze eisen om te kijken of ze elkaar al dan niet uitsluiten.

Gerichte werking, detectie en registratie

Art. 8 Bogw bepaalt dat een technisch hulpmiddel zodanig moet zijn ingericht dat de werking ervan kan worden beperkt tot de in het bevel vermelden functionaliteit(en). Daarnaast mag een technisch hulpmiddel – op grond van art. 9 Bogw – uitsluitend

⁴ Staatsblad 2006, 524, p. 14-15.

⁵ Zie ook Uit CTRL+ALT+DEL: De keuring van technische hulpmiddelen, C.M. Taylor Parkins-Ozepius, D.A. Wendt en D.A.G. van Toor, Platform Modernisering Strafvordering 2022, nr. 4, p. 3 en ECLI:NL:GHAMS:2018:4620.

⁶ Het Besluit technische hulpmiddelen bijzondere opsporingsbevoegdheden was van toepassing van 1-2-2000 tot 1-1-2007.

⁷ Staatsblad 1999, 547, p. 8-9.

⁸ Vgl. art. 18 Bths.

gegevens detecteren en registreren ten behoeve van die functionaliteit(en) in het bevel.⁹ In geval van het opnemen van telecommunicatie mag uitsluitend die communicatie worden gedetecteerd en geregistreerd die plaatsvindt met gebruikmaking van één of meer identificerende kenmerken van het geautomatiseerde werk van de individuele gebruiker(s) op wie het bevel betrekking heeft.¹⁰

Art. 11 Bths bevat ten aanzien van het opnemen van telecommunicatie een soortgelijke eis, namelijk dat het technisch hulpmiddel slechts communicatie mag opnemen die plaatsvindt met gebruikmaking van één of meer nummers van de individuele gebruiker(s) op wie het bevel tot het opnemen van de communicatie is gericht.

Daarnaast moet op grond van art. 14 lid 4 Bths door de opsporingsambtenaar, indien het technisch hulpmiddel bestaat uit een component die selecteert welke gegevens worden opgeslagen, worden vastgelegd welk selectie criterium is gehanteerd.

Tussenconclusie

Indien een technisch hulpmiddel in de zin van het Bths zo ingericht kan worden dat het alleen die gegevens detecteert en registreert waar het bevel art. 126nba Sv op ziet, sluiten deze eisen elkaar niet uit.

Betrouwbaarheid en integriteit

Art. 10 lid 1 Bogw bepaalt dat de gegevens die worden geregistreerd met een technisch hulpmiddel op zodanige wijze geregistreerd worden dat de inhoud van de gegevens identiek is aan de inhoud van de gedetecteerde gegevens. Lid 2 voegt daar aan toe dat het technisch hulpmiddel beveiligd moet zijn tegen wijziging van de werking daarvan, wijziging van de gegevens zelf en tegen kennisneming van de gegevens door onbevoegden.

De evenknie van dit artikel in het Bths is art. 14. Op grond van lid 1 moet de inhoud van de gedetecteerde signalen identiek zijn aan de op de gegevensdrager opgeslagen signalen. Lid 2 bepaalt dat de signalen die zijn opgeslagen niet bewerkt mogen worden. Voorts dienen bij de opslag van signalen maatregelen te worden genomen om manipulatie van de opgeslagen signalen te voorkomen of achteraf vast te kunnen stellen of manipulatie heeft plaatsgevonden (lid 3).

Tot slot moet als een opsporingsambtenaar niet voortdurend aanwezig is bij een inzet, het technisch hulpmiddel zodanig worden beveiligd dat technische veranderingen achteraf zoveel mogelijk vast te stellen zijn (art. 12).

Tussenconclusie

Het Bogw lijkt op dit punt iets strenger te zijn dan het Bths, maar deze eisen sluiten elkaar niet uit.

Herleidbaarheid

Op grond van art. 11 Bogw moet een geregistreerd gegeven worden voorzien van een uniek gegeven door het technisch hulpmiddel. Een soortgelijke bepaling kent het Bths niet.

Tussenconclusie

⁹ Vgl. art. 9 lid 1 Bogw.

¹⁰ Vgl. art. 9 lid 1 en 2 Bogw.

Ondanks dat het Bogw hier een eis stelt die het Bths niet kent, sluit deze eis niet uit dat een technisch hulpmiddel in de zin van het Bths tevens een technisch hulpmiddel in de zin van het Bogw zou kunnen zijn.

Datum en tijd

Een technisch hulpmiddel moet blijkens art. 12 Bogw de geregistreeerde gegevens voorzien van de datum en tijd waarop de registratie plaatsvindt. In art. 10 Bths is bepaald dat een technisch hulpmiddel de datum en tijd waarop signalen worden gedetecteerd automatisch en doorlopend op de gegevensdrager vast moet leggen.

Tussenconclusie

De bepalingen gaan uit van een ander moment van vastleggen, namelijk op het moment van registratie en het moment van detectie. Indien deze momenten samenvallen, sluiten ze elkaar niet uit. Vindt de registratie op een ander moment plaats dan dient aanvullend de detectie te worden vastgelegd.

Transport

Krachtens art. 13 Bogw moet het technisch hulpmiddel de geregistreeerde gegevens automatisch naar een technische infrastructuur transporteren. Tijdens het transport moeten de geregistreeerde gegevens door het technisch hulpmiddel worden beveiligd tegen wijziging en kennisneming door onbevoegden.

Op grond van art. 13 Bths moet het transport van het signaal dusdanig worden beveiligd dat manipulatie van de signalen wordt voorkomen of achteraf is vast te stellen.

Tussenconclusie

Hoewel de bepalingen van het Bogw strenger zijn dan die van het Bths, sluiten ze elkaar niet uit.

Keuringsdienst:

Op grond van art. 16 Bogw wijst de Minister een onderdeel van de Landelijke Eenheid aan als keuringsdienst. Door de Minister is in eerste instantie TNO aangewezen als keuringsdienst. Sinds 2021 verzorgt de keuringsdienst van de Landelijke Eenheid de keuringen.¹¹

In art. 22 Bths staat nog beschreven dat de voor dat besluit aangewezen keuringsdienst de keuringsdienst van de dienst Specialistische recherche toepassingen van de Landelijke Eenheid is.¹² De dienst Specialistische recherche toepassingen is de oude naam van een dienstonderdeel van de Landelijke Eenheid.

Er is bij de Landelijke Eenheid op dit moment één keuringsdienst die zo wel de technische hulpmiddelen onder het Bogw als onder het Bths keurt.

Tussenconclusie

De keuringen worden uitgevoerd door dezelfde instantie.

¹¹ Vgl. Regeling eisen keuringsdienst technisch hulpmiddel en Inspectie Justitie en Veiligheid, Verslag toezicht wettelijke hackbevoegdheid politie 2021, Den Haag: Ministerie van Justitie en Veiligheid 2022, p. 15.

¹² Art. 1 Aanwijzingsbesluit keuringsdienst technische hulpmiddelen strafvordering.

Conclusie

Uit het voorgaande volgt dat het Bogw in vergelijking met het Bths op sommige punten meer eisen stelt aan technische hulpmiddelen. Het valt niet uit te sluiten dat een onder het Bths goedgekeurd softwarematig technisch hulpmiddel kan worden ingezet als technisch hulpmiddel in de zin van het Bogw. Er zal echter wel aan de andere eisen van het Bogw voldaan moeten worden om het middel te laten voldoen voor een inzet op grond van art. 126nba Sv.

Het verdient daarbij aanbeveling, indien het onderzoeksbelang dringend vordert dat een (nog) niet gekeurd technisch hulpmiddel in de zin van art. 21 lid 2 Bogw wordt ingezet, op voorhand aanvullende waarborgen conform art. 21 lid 4 Bogw te treffen teneinde de betrouwbaarheid, integriteit en herleidbaarheid van de met het technisch hulpmiddel vastgelegde gegevens te garanderen.

04-08-2023

LP DIGIT – ^{5.1.2}_e

	Toegezonden	Afgerond
LP DIGIT	04-08-2023	20-03-2024
LE DIGIT	20-03-2024	
Rechercheovj LP	20-03-2024	

Aanvullende waarborgen bij inzet ex art. 126nba Sv j° art. 21 lid 4 Bogw

Landelijk Parket - DIGIT

Bij de inzet van artikel 126nba Sv zal soms gebruik gemaakt worden van een technisch hulpmiddel dat voorafgaand aan de inzet niet gekeurd is en zich naar zijn aard verzet tegen keuring. In dat geval moet de officier van justitie ex art 21 lid 4 Besluit onderzoek in een geautomatiseerd werk (Bogw) in de processtukken laten vermelden welke *aanvullende waarborgen* hij heeft getroffen.

Deze waarborgen zien er op om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te garanderen.¹

In de toelichting op het Bogw geeft de wetgever enkele suggesties voor *aanvullende waarborgen*:

“Als keuring van een hulpmiddel geheel achterwege blijft of als onderzoekshandelingen worden verricht zonder gebruik van een technisch hulpmiddel dan vermeldt de officier in de processtukken welke aanvullende waarborgen zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te garanderen (artikel 21, vierde en vijfde lid). **Hierbij kan worden gedacht aan een uitgebreide omschrijving van de functionele specificaties van op maat gemaakt technische hulpmiddel, het voegen van een digitale kopie van de software en de broncode bij het proces-verbaal, het vooraf en achteraf maken van een forensische kopie of het audiovisueel vastleggen van de uitvoering van de onderzoekshandelingen.** De aanvullende procedurele eisen van de officier van justitie kunnen de rechtmatigheid van de inzet waarborgen en voorkomen dat er twijfel ontstaat over de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens.”

Een deel van de *aanvullende waarborgen* zal DIGIT proberen te treffen. Deze kunnen bestaan uit:

5.1.2c



¹ Deze aanvullende waarborgen zijn iets anders dan de procedurele waarborgen die ex art. 21 lid 5 Bogw worden getroffen bij een handmatige inzet.

Naast de *aanvullende waarborgen* die DIGIT mogelijk treft, zullen er door het tactisch team en de zaaksofficier van justitie handelingen moeten worden verricht. Dit geldt met name in de gevallen waarin de software en broncode niet kunnen worden prijsgegeven en evenmin de functionele specificaties kunnen worden omschreven.

Deze *aanvullende waarborgen* zien vooral op het verifiëren van met de inzet ex art. 126nba Sv verkregen gegevens. De gegevens die zijn verkregen met de inzet ex 126nba Sv moeten worden vergeleken met informatie die op andere manier is gegenereerd of verkregen.

Voor de toetsing door de Centrale Toetsingscommissie (CTC) moet een plan van aanpak voor de te treffen *aanvullende waarborgen* worden opgesteld. Een dergelijk plan van aanpak moet inzichtelijk maken hoe het tactisch team en de zaaksofficier van justitie van plan zijn *aanvullende waarborgen* te treffen en daarop te sturen.

Sturing aanvullende waarborgen

1. Zorg dat het treffen van *aanvullende waarborgen* voor, tijdens en na een inzet een vast onderwerp is op de agenda van het overleg tussen de zaaksofficier en de (politie) teamleiding van een onderzoek.
2. Maak een vast lid van het tactisch team verantwoordelijk voor de coördinatie van het treffen van *aanvullende waarborgen*. Deze coördinator doet dit voor, tijdens en na een inzet, totdat de zaaksofficier en de (politie) teamleiding zich er van hebben vergewist dat de *aanvullende waarborgen* afdoende zijn.

Door te zorgen dat de *aanvullende waarborgen* ■■■■ vast onderwerp van overleg is en op het treffen er van door een coördinator wordt toegezien, wordt voorkomen dat in de hectiek en drukte van een opsporingsonderzoek voldoende aandacht is voor dit cruciale stuk bij het gebruik van een niet vooraf goedgekeurd technisch hulpmiddel.

Aanvullende waarborgen

5.1.2c



5.1.2c



In de bijlage staan een aantal suggesties voor het treffen van aanvullende waarborgen. Dit zijn aanvullingen op de 3 hier boven beschreven punten.

19 augustus 2021

LP Digit - 5.1.2e

	Toegezonden	Afgerond	Aangevuld	Aangevuld
LP DIGIT	22-06-2020	18-08-2020	19-08-2021	26-07-2024
Afgestemd LX DIGIT	22-06-2020	07-07-2020	05-01-2021	26-07-2024

5.1.2c







5.1.2c



5.1.2c



5.1.2c



5.1.2c



—

—

Aanbiedingsbrief Reflectiekamer

Datum reflectie:	12 september 2019
Onderzoek:	Artikel 126nba Sv inzet van een niet-gekeurd TH
Officier:	5.1.2e
Contactgegevens:	5.1.2e@om.nl 06-5.1.2e

Geachte Reflectiekamer,

Hierbij verzoek ik u om een advies aangaande 5.1.2c

bij de inzet van de bevoegdheid ex artikel 126nba Sv (het heimelijk van afstand binnendringen van een geautomatiseerd werk).

Graag wil ik u, ten behoeve van een handelingsperspectief bij onderzoeken die zich aanmelden voor de inzet van de bevoegdheid, voorleggen of (en zo ja, onder welke voorwaarden) commerciële software mag worden ingezet lopende de keuring van het daarbij geleverd technische hulpmiddel.

5.1.2c

Echter, vanwege de (politieke) gevoeligheden omtrent het gebruik van commerciële software, de verwachte uitkomst van de eerste keuring (die mondeling nader toegelicht zal/kan worden) en een aantal aanvullende eisen dat geldt bij de inzet van een dergelijk commercieel middel, leg ik deze variant graag specifiek aan u voor.

Hieronder ga ik in op de achtergrond van de gevoeligheden omtrent commerciële software. Vervolgens zal ik het reguliere toetsingskader schetsen voor de inzet van commerciële software (uitgaande van een *goedgekeurd* technisch hulpmiddel). In het derde deel wordt ingegaan op de keuring van het meegeleverde technisch hulpmiddel, waarna wordt afgesloten met een samenvatting met een aantal scenario's.

Vanwege de afscherming van het middel worden de mogelijkheden die commerciële software biedt, de kansen die daarmee voor de opsporing ontstaan niet in deze aanbiedingsbrief verwerkt, maar graag tijdens de mondelinge behandeling nader toegelicht. Dit geldt eveneens voor de stand van zaken omtrent de keuring.

1. Achtergrond: de politieke gevoeligheden omtrent commerciële software

De bevoegdheid ex art. 126nba Sv is geïntroduceerd met de inwerkingtreding van de Wet computercriminaliteit III op 1 maart 2019. Met deze bevoegdheid kan heimelijk en op afstand een geautomatiseerd werk worden binnengedrongen en vervolgens aldaar onderzoek worden verricht.

Om binnen te dringen in een geautomatiseerd werk zijn er ruwweg drie opties: (1) door gebruikmaking van een 'sociale' kwetsbaarheid (phishing, shouldering, etc.); (2) door gebruikmaking van een bekende kwetsbaarheid in de hard- of software van het geautomatiseerde werk; of (3) door gebruikmaking van een (bij de fabrikant) onbekende kwetsbaarheid in de hard- of software van het geautomatiseerde werk.

Een belangrijk discussiepunt bij de totstandkoming van die wet was het gebruik door de politie van die laatste categorie, de onbekende kwetsbaarheden. En in het verlengde daarvan het aanschaffen van commerciële binnendringsoftware, die mogelijk/waarschijnlijk dergelijke onbekende kwetsbaarheden benut (maar waar geen zekerheid over is noch verkregen kan worden).

Bij de behandeling van het wetsvoorstel zijn de volgende twee bezwaren tegen het gebruik van commerciële software naar voren gebracht.

A. Door het aanschaffen van commerciële binnendringsoftware wordt de markt voor onbekende kwetsbaarheden gestimuleerd (waarbij door tegenstanders dus wordt uitgegaan van het gebruik van onbekende kwetsbaarheden in commerciële binnendringsoftware); en

B. Commerciële software van derden is onbetrouwbaar. Er zijn risico's op misbruik van het middel c.q. de gecreëerde toegang door de fabrikant en/of (een) derde(n).

Hieronder worden deze bezwaren nader toegelicht.

A. Stimuleren van de markt voor onbekende kwetsbaarheden

Het is evident dat kwetsbaarheden in hard- en software misbruikt (kunnen) worden door criminelen en statelijke actoren. En daarmee een risico opleveren voor de digitale veiligheid. De overheid wil daarom bevorderen dat deze kwetsbaarheden (zo snel mogelijk) gedicht worden en dus bekend worden bij de fabrikant.

Dit gegeven levert een spanningsveld op met de inzet van de bevoegdheid ex artikel 126nba Sv. Om deze bevoegdheid te kunnen inzetten kan het gebruik van onbekende kwetsbaarheden namelijk noodzakelijk zijn. Waarbij politie en justitie dus profiteren van het feit dat de fabrikant nog niet bekend is met de kwetsbaarheid, er nog niet 'gedicht' is (kunnen worden).

Deze in de wetsgeschiedenis aangeduid als perverse prikkel, is in de wet ondervangen door art. 126ffa Sv. Als de politie stuit op een onbekende kwetsbaarheid dan moet zij deze melden bij de fabrikant. Alleen met machtiging van de RC kan deze meldplicht worden uitgesteld.

Verder is tijdens de totstandkoming door de minister en staatssecretaris heel nadrukkelijk aangegeven dat de politie geen onbekende kwetsbaarheden mag inkopen. Erop stuiten mag, gebruiken met toepassing van 126ffa Sv ook, maar dus niet de markt op om hem aan te schaffen.

In dit verband heeft de aanschaf van commerciële binnendringsoftware extra aandacht gekregen in het debat.

Er zijn bedrijven die zich hebben toegelegd op het leveren van software waarmee 5.1.2c op afstand binnengedrongen kunnen worden en waarmee het noodzakelijke onderzoek kan worden verricht.

Alhoewel er verschillende voor de fabrikant bekende kwetsbaarheden in 5.1.2c (zullen) zitten, deze niet altijd even snel worden gedicht en gebruikers niet altijd even snel updates (waarmee bekende kwetsbaarheden worden gerepareerd) doorvoeren, wordt zeker niet uitgesloten dat deze bedrijven in hun software gebruik maken van onbekende kwetsbaarheden.

Vanwege de commerciële belangen worden deze onbekende kwetsbaarheden (uiteraard) niet gedeeld met een koper. Ook als de software eenmaal is aangeschaft kan niet worden achterhaald of de software gebruik maakt van bekende of onbekende kwetsbaarheden.

Met name D66 - uitgaande van een grote waarschijnlijkheid van het gebruik van onbekende kwetsbaarheden - bracht naar voren dat de aanschaf van dergelijke software bezwaarlijk is omdat daarmee de markt van onbekende kwetsbaarheden gelegitimeerd wordt. Hackers zouden zodoende geneigd kunnen zijn om ontdekte (onbekende) kwetsbaarheden te melden bij bedrijven die binnendringsoftware ontwikkelen in plaats van bij de fabrikanten van de software. En zodoende de kwetsbaarheden in stand houden.

Deze insteek is verder verdedigd door partijen zoals de SP, GroenLinks, PvdD, 50Plus, en organisaties zoals PrivacyFirst, Bits of Freedom en de Autoriteit Persoonsgegevens.

Met daar (in meer of mindere mate) tegenover CDA, VVD en PVDA, en ook het NCSC, het OM en politie. Deskundige Ronald Prins (oud directeur van Fox-IT en op dit moment lid van de Toetsingscommissie Inzet Bevoegdheden) verwoordde zijn kritiek als volgt:

Misschien is er in het vragenronde nog meer tijd voor, maar ik heb zojuist heel veel onzin gehoord over het gebruik van die kwetsbaarheden, bijvoorbeeld de conclusie dat het gebruik van kwetsbaarheden door de politie Nederland onveiliger maakt. Volgens mij is de realiteit dat die computers nu al onveilig zijn. Die kwetsbaarheden zitten erin. Het enkele feit dat de politie een van die kwetsbaarheden ontdekt, maakt Nederland echt niet onveiliger. Eerder zal de politie in staat zijn om die kwetsbaarheid in te zetten om criminelen te kunnen aanhouden en Nederland daarmee netto wel veiliger te maken.

Een motie van D66 in de Tweede Kamer om de inkoop van dergelijke software uit te sluiten kreeg de stemmen van SP (15 zetels), de PvdD (2), GroenLinks (4), een lid van de fractie van de PvdA (1), D66 (12), 50PLUS (2), Klein (1), de GroepKuzu/Öztürk (2) en Monasch (1), maar (daarmee) (ruim: 40 tegen 110) onvoldoende steun en werd verworpen.

Met de deelname van D66 aan het huidige kabinet is de aanschaf van commerciële binnendringsoftware in het Regeerakkoord 2017–2021 beperkt. De software kan slechts worden ingekocht in een specifieke zaak met als doel om het betreden van de markt van

dergelijke software tot een minimum te beperken. De politie kan dan bijvoorbeeld een softwarepakket aanschaffen en/of op basis van de aanschaf van een licentie of gebruiksrecht enkel voor die zaak de software inzetten.

B. De risico's bij gebruik van commerciële software

Bij aanvang van de discussie over commerciële software werden andere bezwaren naar voren gebracht. In de adviezen naar aanleiding van het concept wetsvoorstel en concept Memorie van Toelichting en het verslag (kamerstuk nr. 5) werd (enkel nog) gewezen op *de risico's* van het gebruik van commerciële software.

Onder verwijzing naar negatieve ervaringen / discussie in Duitsland¹ werd gesteld dat er een risico bestaat dat dergelijke software misbruikt kan worden. Ofwel door de fabrikant van die software zelf, door heimelijk (meer) data (ook) naar zichzelf toe te halen, ofwel doordat dergelijke software zelf lek kan zijn en zo misbruikt kan worden door derden.

In de Memorie van Toelichting en Nota naar aanleiding van het Verslag schoof de minister deze bezwaren terzijde. Immers:

Met de voorafgaande keuring van het technische hulpmiddel kan worden voorkomen dat softwareapplicaties worden ingezet die niet voldoen aan de daaraan te stellen eisen. De ervaringen met bepaalde softwareapplicaties in andere landen onderstrepen het belang van een zorgvuldige keuringcertificering. De keuringseisen worden uitgewerkt in het Besluit technische hulpmiddelen strafvordering.

2. Het reguliere toetsingskader voor de inzet van commerciële software (uitgaande van een goedgekeurd technisch hulpmiddel)

Bij de totstandkoming van de wet zijn bij de behandeling in de Eerste Kamer de voorwaarden voor de aanschaf en inzet van binnendringsoftware besproken.

In het Besluit onderzoek in een geautomatiseerd werk is aangegeven:

Bij het binnendringen in een geautomatiseerd werk kan gebruik worden gemaakt van verschillende technieken. Daarbij is het gebruik van commerciële binnendringsoftware van derden waarvan niet duidelijk is of deze van bekende of onbekende kwetsbaarheden gebruik maakt beperkt tot het uiterste geval. Deze software kan alleen worden gebruikt wanneer minder ingrijpende middelen zoals het gebruik van inloggegevens, social engineering of bekende kwetsbaarheden niet toereikend zijn om heimelijk toegang te verkrijgen tot een geautomatiseerd werk. De regering wil de markt voor onbekende kwetsbaarheden niet bevorderen, dat zou negatieve gevolgen voor de veiligheid van het internet kunnen hebben. Het Regeerakkoord 2017–2021 beperkt bovendien het betreden van de markt voor commerciële binnendringsoftware die

¹ Hierbij werd verwezen naar gebruik van af luistersoftware van het bedrijf Digitask die via internet makkelijk te hacken bleek te zijn, en die meer functionaliteiten kende dan was toegestaan in Duitsland. Ook werd verwezen naar de aanschaf van Finfisher, software van Gamma International dat zijn software ook zou leveren aan totalitaire regimes waar het ingezet zou worden tegen mensenrechten-activisten en politieke dissidenten.

mogelijk gebruik maakt van onbekende kwetsbaarheden. In plaats daarvan wil de regering meer inzetten op de eigen ontwikkeling van methoden voor het binnendringen, daartoe zal de ontwikkeling van passende producten binnen de politie worden gestimuleerd. De beperking in het Regeerakkoord van het gebruik van software van derden zal leiden tot een grotere belasting van het technisch team van de Landelijke Eenheid dat met de uitvoering is belast en dat zelf passende methoden moet ontdekken en ontwikkelen, vooral in zaken waarin inzet zonder de aanschaf van software nodig is. Bij de toedeling van de financiële middelen voor de uitvoering van de bevoegdheid zal hiermee rekening worden gehouden. Niettemin is het gebruik van software die mogelijk gebruik maakt van onbekende kwetsbaarheden soms onvermijdelijk om ernstige criminaliteit te kunnen bestrijden. De aanschaf van dergelijke binnendringsoftware is in het Regeerakkoord 2017–2021 beperkt en zal slechts worden ingekocht in een specifieke zaak. De politie kan dan bijvoorbeeld een softwarepakket aanschaffen en/of op basis van de aanschaf van een licentie of gebruiksrecht enkel voor die zaak de software inzetten. Als de officier van justitie bepaalt dat gebruik van binnendringsoftware van een externe leverancier noodzakelijk is, zal dit centraal in het OM worden getoetst alvorens in die specifieke zaak wordt overgaan tot aanschaf.

Voor het toetsingskader zijn hieruit twee punten (met name) relevant.

1. Commerciële binnendringsoftware is een uiterst middel;
2. Er kan per (specifieke) zaak een licentie worden aangeschaft.

Ad 1 Uiterst middel

In de Nota van Toelichting op het Besluit, maar ook eerder in de Nadere Memorie van Toelichting en de parlementaire behandeling wordt benadrukt dat het gebruik van commerciële binnendringsoftware een uiterst middel is.

Dit is echter, zo blijkt uit de betreffende passages, niet opgehangen aan de proportionaliteitstoets. Dat wil zeggen, de ernst van het feit is niet bepalend voor de vraag of commerciële binnendringsoftware gebruikt mag worden.

Het begrip uiterst middel ziet op de vraag of het binnendringen niet op een andere wijze kan plaatsvinden, door gebruik van een 'sociale' kwetsbaarheid of gebruik van bekende kwetsbaarheden. Niet op de bevoegdheid ex artikel 126nba SV, als 'opsporingsmiddel'.

Dit sluit overigens ook aan bij de wijze waarop het binnendringen wordt gezien: niet van invloed op de proportionaliteit, tenzij het de risico's voor het geautomatiseerde werk (en die van derden) betreft.

Ad 2 Licentievoorwaarde

In het regeerakkoord en het Besluit is de mogelijkheid geboden om software aan te schaffen en vervolgens per specifieke zaak licenties aan te schaffen.

De gedachte achter dit licentiemodel is dat door de aanschaf van de software vooraf het keuringsproces alvast kan worden ingezet. In de Nota van Toelichting op het Besluit wordt opgemerkt:

Dit is noodzakelijk omdat de keuring enige tijd in beslag kan nemen en na een besluit om dergelijke software te gebruiken om binnen te dringen, deze snel ingezet moet kunnen worden. Het gebruik van software op basis van een licentie biedt de mogelijkheid om een demonstratieversie van de software te keuren voordat de software in een specifieke zaak kan worden ingezet om binnen te dringen. Indien inzet om binnen te dringen aan de orde is, dient alsnog een aparte licentie daarvoor te worden aangeschaft.

In de praktijk betekent deze voorwaarde dat de inzet (zeer) kostbaar is en daarmee beperkt tot een gering aantal.

Bij de toegezegde evaluatie van de wet, na twee jaar, wordt onder andere onderzocht of deze beperking werkbaar is.

3. De keuring van commerciële software

Zoals al aangegeven gaat het in de onderhavige kwestie om commerciële software,

5.1.2c

De binnendringsoftware is in het Besluit en de toelichtingen daarop buiten de keuring gehouden. In het verslag van een schriftelijk overleg, naar aanleiding van het Besluit geeft de minister hiervoor de volgende reden:

Het doel van de keuring van technische hulpmiddelen die worden gebruikt voor het verrichten van onderzoekshandelingen is om te borgen dat de werking van een hulpmiddel dusdanig betrouwbaar is dat de hiermee verkregen onderzoeksgegevens, die kunnen dienen als bewijs in een strafzaak, betrouwbaar, integer en herleidbaar zijn. De wijze waarop het binnendringen in een geautomatiseerd werk plaatsvindt is niet van invloed op de betrouwbaarheid van de onderzoeksgegevens en maakt daarom geen onderdeel uit van het keuringsproces. De kwaliteit van het binnendringen in een geautomatiseerd wordt geborgd door dit handelen voor te behouden aan daartoe opgeleide deskundige opsporingsambtenaren van een technisch team. Het functioneren van de binnendringsoftware wordt in een testomgeving gecontroleerd. In de procedure rondom de inzet van de bevoegdheid wordt aandacht besteed aan de risico's voor het te onderzoeken geautomatiseerd werk, waaronder de schade voor derden.

In de Nadere Memorie van Antwoord zag deze controle ook nog specifiek op de zorgen die hierboven werden beschreven, over mogelijk misbruik:

In het geval binnendringsoftware wordt ingekocht wordt het functioneren bovendien in een testomgeving gecontroleerd. De software wordt gecontroleerd op bruikbaarheid, of de software niet onrechtmatig data verzamelt en of die software niet heimelijk communiceert met derden.

In de praktijk is deze controle overigens geen apart proces, maar wordt hier met de reguliere keuring in voorzien.

De voorschriften ten aanzien van de keuring zijn verder hetzelfde als bij een 'normaal' technisch hulpmiddel. Over deze reguliere keuring kan het volgende worden opgemerkt.

Hoofdregel: keuring

In de wetsgeschiedenis is een duidelijke voorkeur te lezen voor het gebruik van vooraf gekeurde technische hulpmiddelen. Deze voorkeur komt tot uitdrukking in (bijvoorbeeld) de volgende passages:

De softwareapplicaties die worden gebruikt voor het verrichten van onderzoekshandelingen (dus na het binnendringen) – ook wel aangeduid als technische hulpmiddelen – waarmee bewijs wordt vergaard, worden in beginsel voor de inzet gekeurd.

Omdat de betrouwbaarheid, integriteit en herleidbaarheid van gegevens cruciaal zijn voor het gebruik van de verkregen gegevens voor het bewijs in een strafzaak, geniet het gebruik van een vooraf gekeurd hulpmiddel sterk de voorkeur.

In de praktijk zal daarom niet lichtzinnig van het gebruik van een vooraf goedgekeurd hulpmiddel worden afgezien.

Uitzondering: keuring achteraf

Desalniettemin is er in de artikelen 15 en 21 van het Besluit de mogelijkheid gecreëerd om inzet zonder keuring mogelijk te maken.

In **artikel 15 (uitzonderingen op voorafgaande keuring en herkeuring)** wordt bepaald:

1. In afwijking van artikel 14, eerste en derde lid, kan een technisch hulpmiddel na afloop van het gebruik ervan worden gekeurd of kan na afloop van het gebruik herkeuring plaatsvinden indien de officier van justitie dit heeft bepaald overeenkomstig artikel 21, tweede lid.
2. In afwijking van het eerste lid kan keuring of herkeuring achteraf achterwege blijven, indien de officier van justitie dit heeft bepaald overeenkomstig artikel 21, vierde lid.

In **artikel 21 (uitvoering van een bevel)** wordt bepaald:

2. In afwijking van het eerste lid kan de officier van justitie bepalen dat, indien het onderzoeksbelang dit dringend vordert, een niet gekeurd technisch hulpmiddel wordt gebruikt. In dat geval vermeldt de officier van justitie in het bevel dat toepassing is gegeven aan artikel 21, tweede lid.
3. Indien ter uitvoering van een bevel gebruik wordt gemaakt van een niet gekeurd technisch hulpmiddel vermeldt de officier van justitie de uitkomst van de keuring of herkeuring na afloop van het gebruik in de processtukken.

In de Nota van Toelichting op het Besluit wordt de reden hiervoor gegeven:

Het advies van [Bits of Freedom] om de uitzonderingen omtrent het gebruik van niet dan wel achteraf goedgekeurde technische hulpmiddelen te beperken is niet overgenomen. Dit zou te belemmerend zijn voor de opsporingspraktijk. In de nota van toelichting zijn de uitzonderingsgevallen waarin keuring achterwege kan blijven verduidelijkt.

Een uitzondering op de hoofdregel is mogelijk *als het onderzoeksbelang dringend vordert* dat gebruik wordt gemaakt van een hulpmiddel dat zich naar zijn aard niet leent voor voorafgaande goedkeuring. Hierbij kan worden gedacht aan op maat gemaakte software, zoals een script dat is geschreven door een technisch team en dat «semi-handmatig» wordt ingezet. In dat geval vermeldt de officier van justitie in het bevel dat gebruik wordt gemaakt van een niet gekeurd hulpmiddel. Na afloop vindt alsnog keuring plaats, tenzij de aard van het hulpmiddel zich naar het oordeel van de officier hiertegen verzet.

Ook, zo blijkt uit de toelichting op artikel 21 lid 2, kan hierbij worden gedacht aan de situatie dat (her)keuring voorafgaand aan de inzet teveel tijd zou vergen. Het moet dan gaan om situaties waarin het belang van het onderzoek de inzet van het desbetreffende technische hulpmiddel dringend vordert. Bij deze afweging zal de officier van justitie in overleg met de keuringsinstantie (in het verslag "in overleg met de politie") nagaan of het beoogde technische hulpmiddel naar verwachting zal voldoen aan de in de artikel 8 tot en met 13 gestelde technische eisen.

Bij de mondelinge behandeling zal/kan door Digit een toelichting worden gegeven op de stand van zaken ten aanzien van de keuring, de verwachtingen en de (on)mogelijkheden van keuring achteraf.

4. Mag niet gekeurde commerciële software worden ingezet?

Samenvatting bezwaren

Hierboven is ingegaan op de bezwaren tegen het gebruik van commerciële software en de regels aangaande de keuring en inzet daarvan.

Uit de besproken wet- en regelgeving en kamerstukken kunnen de volgende drie bezwaren tegen het gebruik van ongekeurde commerciële (binnendring)software worden geformuleerd:

A. Risico's op misbruik.

Met een nog niet afgerond keuringsproces blijft de mogelijkheid van invloed van de fabrikant of van derden boven de markt hangen, kan dit risico niet (objectief) worden uitgesloten.

Anders dan bij het op andere wijze binnendringen, waaronder met gekeurde software, wordt hiermee naar mijn mening de inzet van commerciële software onderdeel van de proportionaliteitstoets.

B. Integriteit van het bewijs.

Zonder keuring kunnen er vragen ontstaan over de betrouwbaarheid van het bewijs.

C. Politieke gevoeligheid van het gebruik van niet gekeurde commerciële software

Naast het belang van integriteit heeft de keuring ook nog een ander doel, namelijk het voorkomen van risico's op misbruik. De minister heeft het belang van keuring ook in dat licht onderstreept.

De constructie van het licentiemodel is geïntroduceerd om keuring mogelijk te maken alvorens de software in te zetten.

De Inspectie Justitie en Veiligheid is belast met het toezicht over de inzet van de bevoegdheid ex art. 126nba Sv en brengt jaarlijks een verslag uit. Verder kan worden opgemerkt dat er over twee jaar een evaluatie van de wet wordt uitgevoerd door het WODC. Inzet van niet gekeurde commerciële software zal (ongetwijfeld) leiden tot discussie.

Conclusie

De vraag die ik graag aan de reflectiekamer wil voorleggen is of ondanks deze bezwaren inzet van niet gekeurde software (onder bepaalde voorwaarden) mogelijk is.

Ten aanzien van het bezwaar onder A – risico's op misbruik – kan worden opgemerkt dat deze risico's meegenomen kunnen/moeten worden bij de proportionaliteits- (en dus) subsidiariteitstoets. Er zouden hoge(re) eisen gesteld kunnen worden aan de aard van de verdenking en uitputting van andere onderzoeksmogelijkheden. Ook kan rekening worden gehouden met het subject, in het bijzonder de mogelijkheid van een bredere (politieke / statelijke) interesse in dat subject.

Het bezwaar onder B – integriteit van het bewijs – zou kunnen worden meegenomen bij de beoordeling van het doel van de inzet. Bij het lokaliseren van een verdachte, vergaren van sturingsinformatie of bij inschatting van de gevaarzetting kan beter rekening gehouden worden met eventuele tekortkomingen. Een mogelijkheid zou kunnen zijn om de niet gekeurde software niet in te zetten voor de vergaring van 'bewijs'.

Overigens kan worden opgemerkt dat er door Digit maatregelen kunnen worden getroffen om de integriteit zoveel mogelijk te waarborgen. En ook tactisch kan aanvullend onderzoek worden verricht om de verkregen informatie te verifiëren.

De vraag die (daarmee) meen ik (vooral) voorligt is of de inzet onder de bovengenoemde voorwaarden [een (zeer) ernstig feit waar in het onderzoek alle reële mogelijkheden zijn uitgeput, de rol/aard van het subject en het doel van de informatievergaring] politiek te verantwoorden is, bezwaar C kan worden gepasseerd. Zowel voor het OM / het College / de Minister als met het oog op de evaluatie waarin we duidelijk willen laten zien wat we aan middelen nodig hebben, wat we ermee kunnen bereiken waar andere middelen falen en dat we daarbij een goede afweging maken.

OPENBAAR MINISTERIE

Landelijk Parket

Datum 17 september 2019
 Onderwerp Reflectiekamer 126nba Sv
 Aanwezig 5.1.2e (voorzitter), 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e, 5.1.2e en 5.1.2e
 Opgemaakt door 5.1.2e

Verslag

Inleiding

De bevoegdheid ex art. 126nba Sv is geïntroduceerd met de inwerkingtreding van de Wet computercriminaliteit III (CCIII) op 1 maart 2019. Met deze bevoegdheid kan heimelijk en op afstand een geautomatiseerd werk worden binnengedrongen en vervolgens aldaar onderzoek worden verricht.

Om binnen te dringen in een geautomatiseerd werk zijn er ruwweg drie opties: door gebruikmaking van (1) een 'sociale' kwetsbaarheid; (2) een bekende kwetsbaarheid in de hard- of software van het geautomatiseerde werk; of (3) een (bij de fabrikant) onbekende kwetsbaarheid in de hard- of software van het geautomatiseerde werk.

Een belangrijk discussiepunt bij de totstandkoming van CCIII was het gebruik door de politie van die laatste categorie, de onbekende kwetsbaarheden. En in het verlengde daarvan het aanschaffen van commerciële binnendringsoftware, die mogelijk/waarschijnlijk dergelijke onbekende kwetsbaarheden benut (maar waar geen zekerheid over is noch verkregen kan worden).

In de wetsgeschiedenis is daarnaast een duidelijke voorkeur te lezen voor het gebruik van vooraf gekeurde technische hulpmiddelen. Artikelen 15 en 21 van het Besluit onderzoek in een geautomatiseerd werk (hierna: Besluit) maken de inzet zonder keuring – als uitzondering op de hoofdregel – wel mogelijk. Er moet sprake zijn van een dringend onderzoeksbelang en een hulpmiddel dat zich naar zijn aard niet leent voor voorafgaande goedkeuring of dat (her)keuring voorafgaand aan de inzet teveel tijd zou vergen.

Over twee jaar wordt CCIII geëvalueerd door het WODC. Inzet van niet gekeurde commerciële software zal ongetwijfeld leiden tot discussie. Het gebruik van deze software ligt politiek gevoelig. In de politieke discussie zijn verschillende bezwaren tegen het gebruik van (niet gekeurde) commerciële software naar voren gebracht: door het aanschaffen van commerciële binnendringsoftware wordt de markt voor onbekende kwetsbaarheden gestimuleerd en er zijn risico's op misbruik van het middel c.q. de gecreëerde toegang door de fabrikant en/of derden. Daarnaast kan de inzet van niet-gekeurde commerciële software leiden tot discussie over de

integriteit/betrouwbaarheid van het vergaarde bewijs. De aanschaf van commerciële binnendringsoftware is daarom in het Regeerakkoord 2017–2021 beperkt: de software kan slechts worden ingekocht in een specifieke zaak (bijvoorbeeld door middel van het zogenaamde 'licentiemodel'). Het team Digit beschikt op dit moment over commerciële software. Aanvankelijk was het idee om de normale keuringsprocedure te doorlopen en na goedkeuring het middel in te zetten. Verwacht werd dat het middel in september gekeurd zou zijn. Nu blijkt dat het nog zeker vijf maanden (en mogelijk nog langer) gaat duren voordat er een keuringsrapportage ligt. Digit heeft inmiddels de kennis en kunde om met het middel te werken (door leden van Digit is een opleiding gevolgd om te werken met de software). Er hebben zich ondertussen verschillende onderzoeken gemeld waarin het middel goede kansen biedt. De Digit-ovj en het team Digit zijn daarom op zoek naar een handelingsperspectief bij onderzoeken die zich aanmelden voor de inzet van 126nba Sv met niet gekeurde commerciële software. De reflectievraag is niet gekoppeld aan een specifieke zaak.

Vragen

Aan de reflectiekamer worden de volgende vragen voorgelegd:

- Kan, ondanks de bezwaren (risico op misbruik, integriteit van bewijs en politieke gevoeligheid), commerciële software worden ingezet t.b.v. artikel 126nba Sv, lopende de keuring van het daarbij geleverd technische hulpmiddel?
- Zo ja, onder welke voorwaarden?

Bespreking

In de bespreking van de reflectievragen zijn verschillende onderwerpen aan bod gekomen: het keuringsproces, regelgeving die niet aansluit op de praktijk, het soort zaken waarin het middel kan worden ingezet en de procesrisico's, het gegeven dat voorlopig enkel met niet gekeurde software kan worden gewerkt en de politieke gevoeligheden. Hieronder volgt een kort verslag van de discussie per onderwerp.

Het keuringsproces en –rapport

De ovj en leden van het team Digit geven een toelichting op het keuringsproces. De verwachte termijn van 4 weken voor keuring blijkt in de praktijk helemaal niet realistisch. Dit is het eerste externe middel dat door TNO gekeurd moet worden. Het is voor hen nieuw en het is ingewikkelde materie om te testen. Het blijkt dat de praktijk weerbarstiger is dan aanvankelijk voorzien bij het opstellen van het keuringsprotocol.

De keuring is een dynamisch proces; als TNO tegen bepaalde problemen of tekortkomingen aanloopt, wordt met de fabrikant gekeken welke aanpassingen in het middel mogelijk zijn. Ook kan daarbij worden gekeken welke alternatieve waarborgen het team Digit kan treffen bij de inzet van het middel.

In de keuringsrapportage zal worden aangegeven op welke (vooraf bepaalde) punten het middel wel/niet voldoet, het is dus geen kwestie van goed-/afgekeurd. Een uitkomst van het keuringsproces kan ook zijn dat keuren volgens dit protocol niet mogelijk is. Op dit moment valt nog niet te zeggen in hoeverre het middel goedgekeurd zal worden en/of op welke punten alternatieve waarborgen getroffen moeten worden. Door Digit wordt wel zoveel mogelijk geanticipeerd op mogelijke extra waarborgen. De fabrikant is welwillend om aanpassingen te doen, maar op een aantal punten zal het bedrijf mogelijk geen concessies willen doen. Een quickscan – een keuring op de meest belangrijke punten – zou behulpzaam kunnen zijn, maar TNO heeft aangegeven dat zij dit niet willen doen. Door de wetgever is aangegeven dat de (niet gekeurde) commerciële software in een testomgeving op eventuele lekken getest zou moeten worden. 5.1.1c; 5.1.2b

Daarmee kan niet worden getest of het middel lekt naar derden. Dit heeft volgens de Digit-ovj consequenties voor het soort zaken waarbij dit middel kan worden ingezet 5.1.2c

Voortschrijdend inzicht

Niet alleen het keuringsprotocol blijkt niet goed aan te sluiten op de praktijk. In de politieke discussies is steeds onderscheid gemaakt tussen de software die gebruikt wordt om binnen te dringen en de software die gebruikt wordt om in het geautomatiseerd werk onderzoek te verrichten en de aanwezige informatie veilig te stellen. Alleen voor de laatste categorie – het eigenlijke technische hulpmiddel – geldt de keuringseis. 5.1.2c

Het Besluit blijkt net als het keuringsprotocol te beperkend voor de praktijk. De discussie over de strenge eisen in het Besluit loopt al. Hoewel OM en politie betrokken waren bij de totstandkoming van deze regelgeving, is nu sprake van voortschrijdend inzicht. Het team Digit heeft recent gesproken met de minister van JenV en daarbij aangegeven dat zij vrezen dat door de strenge eisen geen enkel middel (goed)gekeurd kan worden.

Soort zaken en procesrisico's

De reflectiekamer vraagt in welke/wat voor soort zaken behoefte is aan de inzet van dit middel. 5.1.2c

Verslag

Datum 17 september 2019

Pagina 4/6

5.1.2c

In al deze gevallen gaat het, in beginsel, niet om bewijsvergaring. De reflectiekamer bespreekt uitgebreid of het middel alleen ingezet zou moeten worden voor het lokaliseren van een verdachte en/of verzamelen van sturingsinfo of dat het ook voor bewijsvergaring kan worden ingezet. De reflectiekamer geeft aan dat niet op voorhand moet worden uitgesloten dat het middel wordt ingezet om bewijs te vergaren. Uitsluiting van deze categorie zou betekenen dat OM en politie onnodig strengere eisen voor zichzelf stellen dan wet- en regelgeving. Bij gebruik voor bewijsvergaring moet het met het technisch hulpmiddel vergaarde bewijs wel op een andere wijze geverifieerd kunnen worden. Dit in verband met de betrouwbaarheid, integriteit en herleidbaarheid van de met het technisch hulpmiddel vastgelegde gegevens en het daarmee samenhangende procesrisico dat er meer moet worden prijsgegeven van het technisch hulpmiddel.

Dit prijsgeven is onmogelijk. 5.1.1c; 5.1.2b

Met een keuringsrapport kan het middel wel worden afgeschermd. In hoeverre de rechtbank, of verdediging, in een concrete zaak hier een punt van zal maken, is op voorhand niet in te schatten. In het uiterste geval zal het betekenen dat het OM een bevel van de rechtbank om een externe deskundige naar het technisch hulpmiddel te laten kijken, naast zich neerlegt.

Op dit procesrisico moet goed regie gevoerd worden, onder andere in de selectie van de zaak, verdachte en het doel. Als besloten wordt om de opbrengsten van de inzet van het niet gekeurde middel te gebruiken voor bewijs, moet dit risico goed besproken worden met de betreffende zaaksovj. Als het fout gaat, en de rechter beveelt een extern onderzoek, kan het grote consequenties voor de betreffende zaak hebben. De reflectiekamer acht het ook van belang dat de Digit-ovj de zaaksovj goed ondersteunt bij het beantwoorden van vragen over het middel tijdens de rechtsgang en het schrijven van het requisitoir.

Uitzondering op de regel

In het Besluit is aangegeven dat niet gekeurde middelen alleen in uitzonderlijke gevallen mogen worden ingezet. Op dit moment wordt echter alleen nog maar gewerkt met niet gekeurde (overheids-)middelen. Volgens Digit zal dit voorlopig – in deze beginfase – ook zo blijven. De reflectiekamer wijst er op dat het enkel inzetten in uitzonderlijke gevallen één van de concessies is die gedaan zijn in het politieke debat, om toch over dit middel te kunnen beschikken. Voorkomen moet worden dat de uitzondering de regel blijft en dat de niet gekeurde commerciële software veelvuldig wordt ingezet. Dit valt politiek gezien, ook met het oog op de

evaluatie, moeilijk uit te leggen. In de opstartfase is het nog goed te verantwoorden, maar gaandeweg zullen de argumenten steeds sterker moeten worden. Digit geeft aan dat het nu met name gaat om de periode tot de afronding van de keuringsrapportage. Dan ontstaat er een nieuwe situatie. Het zal daarbij gaan om enkele inzetten, in belangrijke zaken.

Politieke gevoelheden

In de bespreking wordt er op gewezen dat de politieke gevoeligheid zit op het binnendringen van een geautomatiseerd werk en daarbij gebruikmaken van onbekende kwetsbaarheden. Dit is een andere discussie dan de procesrisico's bij de inzet van niet gekeurde commerciële software, waarbij het m.n. om de integriteit van het bewijs gaat. De reflectiekamer merkt op dat dit niet het juiste gremium is voor een discussie over de politieke gevoelheden m.b.t. de inzet van niet gekeurde commerciële software. Dit zal op een hoger niveau moeten worden besproken.

Wel merkt de reflectiekamer op dat inzet in de juiste zaak/zaken de politieke weerstand kan doen afnemen. Hierbij wordt gewezen op onderzoeken naar grote subjecten, in een vermissingszaak (zoals Anne Faber) of bij een CTER-incident; zaken waarbij (vrijwel) niemand tegen de inzet van dit middel kan zijn. Het is achteraf juist een lastige boodschap dat een dergelijk middel, dat voorhanden was, in zo'n zaak niet is ingezet.

Advies/conclusie

De reflectiekamer constateert dat voorop staat dat de inzet van niet gekeurde commerciële software in beginsel rechtmatig is; het Besluit biedt hiervoor de ruimte. Het zou dan ook jammer zijn als die mogelijkheid niet wordt benut. De reflectiekamer acht het onwenselijk om de mogelijke inzet van deze optie – zonder dat dit uit de onderliggende wet- en regelgeving voortvloeit – aan de voorkant door politie en OM zelf wordt beperkt. De reflectiekamer is het met de Digit-ovj eens dat de procesrisico's beheersbaar zijn bij inzet in een zaak waar het gaat om het lokaliseren van een verdachte dan wel wanneer het vergaarde bewijs op een andere wijze kan worden geverifieerd. Hierop moet goed regie worden gevoerd. Het belangrijkste procesrisico is de kans dat het OM niet-ontvankelijk verklaard zal worden omdat het ingezette middel niet prijsgegeven zal worden. Aan de rechter zal goed moeten worden uitgelegd waarom gebruik is gemaakt van dit middel. Naast mogelijke procesrisico's moet ook rekening worden gehouden met de politieke discussie rondom de inzet van niet gekeurde commerciële software en de aanstaande evaluatie.

De reflectiekamer adviseert de Digit-ovj om een concrete zaak aan de CTC voor te

Verslag
Datum 17 september 2019
Pagina 6/6

leggen, zodat ook het College zich kan uitlaten over de toelaatbaarheid van het middel.¹ De Digit-ovj bespreekt met de recherche-ovj's van het LP welke zaak/zaken nu het meest gepast zijn voor deze inzet en hoe het proces in te richten. Aan het ministerie van JenV is al het signaal afgegeven dat de huidige regelgeving te beperkend is. Aangegeven wordt dat de druk op JenV om aanpassingen te krijgen vanuit het team Digit en het OM verder opgevoerd moet worden.

¹ Ondertussen heeft het College de inzet van niet gekeurde commerciële software in een concrete zaak goedgekeurd.

Notitie m.b.t. de beslissing dat TH ^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Wettelijk kader

Per 1 maart 2019 is de Wet computercriminaliteit III (CCIII) in werking getreden. Deze wet creëert in artikel 126nba Sv de nieuwe bijzondere opsporingsbevoegdheid om heimelijk en op afstand binnen te dringen in een geautomatiseerd werk en daar onderzoekshandelingen te verrichten.¹

In art. 126nba lid 1 Sv is bepaald dat bij het doen van onderzoek in een binnengedrongen geautomatiseerd werk gebruik kan worden gemaakt van een technisch hulpmiddel (TH). Deze mogelijkheid is nader uitgewerkt in het Besluit onderzoek in een geautomatiseerd werk (Bogw).² In het Bogw wordt een TH omschreven als “softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel”.³

Het in het Bogw geformuleerde uitgangspunt voor het gebruik van TH's is dat er wordt gewerkt met een vooraf goedgekeurd TH (art. 14 en 21 lid 1 Bogw). Indien het onderzoek het dringend vordert, kan de OvJ bepalen dat gewerkt wordt met een niet gekeurd TH (art. 21 lid 2 Bogw). Die beslissing wordt ook opgenomen in het bevel. Het niet gekeurde TH wordt na afloop van de inzet alsnog gekeurd en de resultaten daarvan worden aan het procesdossier toegevoegd (art. 21 lid 3 Bogw).

De OvJ kan echter ook bevelen dat een ingezet TH, dat vooraf niet gekeurd is, überhaupt niet wordt gekeurd. Dit kan indien “de aard” van het TH zich, naar het oordeel van de OvJ, tegen keuring verzet (art. 21 lid 4 Bogw). In de toelichting op het Bogw is hierover het volgende opgemerkt:

“In uitzonderingsgevallen kan de keuring van een technisch hulpmiddel geheel achterwege blijven, namelijk indien de aard van het technische hulpmiddel zich naar het oordeel van de officier van justitie daartegen verzet (artikel 21, vierde lid). Van deze uitzondering zal in de praktijk niet lichtzinnig gebruik worden gemaakt. Hierbij kan worden gedacht aan de situatie van een speciaal op maat gemaakt technisch hulpmiddel. Wanneer het technische hulpmiddel specifiek is aangepast aan de omgeving waarin de inzet heeft plaatsgevonden, kan het problematisch zijn om bij een keuring dezelfde situatie na te bootsen. Met name bij op maat gemaakte software die tijdens het verrichten van onderzoekshandelingen nog moet worden aangepast aan de omstandigheden, kan het onuitvoerbaar zijn om de omstandigheden waarbinnen de inzet plaats heeft gevonden te reproduceren en het ingezette technische hulpmiddel daarop te keuren.”⁴

2. Technisch hulpmiddel ^{5.1.2c}

5.1.2c

[Redacted content]

¹ Computercriminaliteit III, *Stb.* 2018, 322.

² Besluit onderzoek in een geautomatiseerd werk, *Stb.* 2018, 340.

³ Artikel 1 sub f Bogw.

⁴ Bogw, p. 45.

5.1.2c



3. Ervaring met TH ^{5.1.2c} in concrete opsporingsonderzoeken

5.1.2c



5.1.2c



5.1.2c

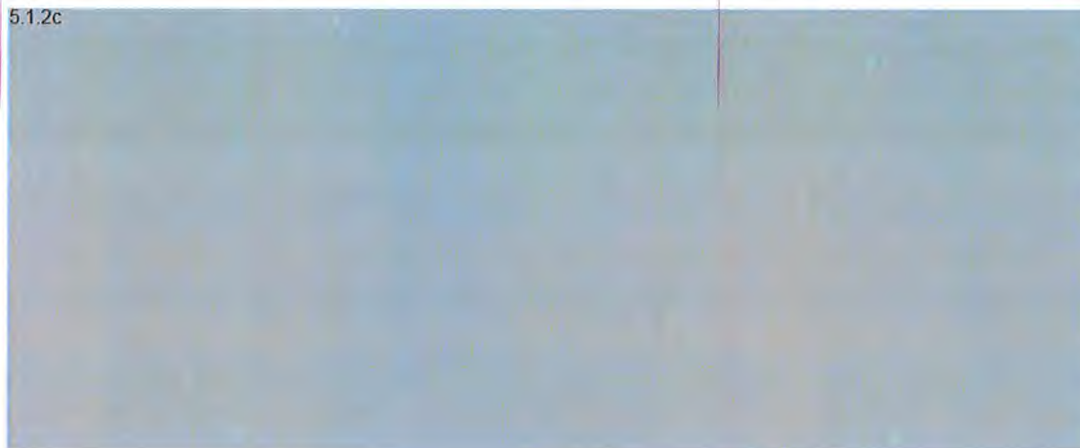


Uit de voorgaande beschrijving van TH **5.1.2c** volgt dat de aard van TH **5.1.2c** zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH **5.1.2c** zich hoogst waarschijnlijk tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat de keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁸ De praktijk op dit moment is echter dat de keuringsdienst de termijn van 4 weken niet haalt. De keuringen die thans verricht zijn, ongeacht het oordeel van de keuringsdienst, hebben meerdere maanden geduurd.

5.1.2c



Op dit moment heeft DIGIT LE geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. DIGIT LE is ook niet bekend met de beschikbaarheid van dergelijke middelen.

⁸ 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, Stcrt. nr. 10713.

⁹ TH **5.1.2c** was voorafgaand aan de Reflectiekamer van september 2019 reeds aangeschaft. De eerste inzet ervan is pas gedaan na die Reflectiekamer.

4. Conclusie

Gelet op het voorgaande komt de landelijk DIGIT OvJ tot de volgende oordelen:

1. De aard van TH ^{5.1.2c} dat is ingezet in ^{5.1.2c} verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH ^{5.1.2c} zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.
3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. DIGIT LE en DIGIT LP zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

5. Tot slot

Het voorgaande is in juli 2020 besproken in een Reflectiekamer van het Landelijk Parket. De landelijk DIGIT OvJ heeft daarin zijn voorgenomen besluit ex artikel 21 lid 4 Bogw voorgelegd en toegelicht. De Reflectiekamer heeft zich verenigd met het voorgenomen besluit. Deze notitie is de schriftelijke beschrijving daarvan.

5 oktober 2020

DIGIT LP ^{5.1.2e}

	Toegezonden	Afgerond
LP DIGIT	07-07-2020	08-09-2020
Afgestemd LE DIGIT	07-07-2020	08-09-2020
Afgestemd reflectiekamer LP	08-09-2020	25-09-2020
Afgestemd hoofdovj LP	05-10-2020	

Bijlage 1

5.1.2c



OPENBAAR MINISTERIE

Landelijk Parket

Postbus 395, 3000 AJ Rotterdam

College van Procureurs-Generaal

d.t.v. 5.1.2e

Posthumalaan 74

3072 AG Rotterdam

T +31 88 699 23 00

www.om.nl

Uitsluitend per mail verzonden

Datum 22 oktober 2020
Onderdeel Bureau Recherche
Ons kenmerk LP\20\003809
Contactpersoon 5.1.2e
Doorkiesnummer(s) +31 6 5.1.2e
E-mail 5.1.2e @om.nl
Bijlage(n) Besluit ex. artikel 21, vierde lid, Bogw, TH 5.1.2c
Onderwerp Aanbieding en toelichting van oordeel technisch
hulpmiddel t.b.v. inzet art. 126nba Sv.

Bij beantwoording de datum en
ons kenmerk vermelden.

Geacht college,

Hierbij ontvangt u ter kennisgeving een algemene toelichting en het bijbehorende oordeel van de landelijk officier van justitie voor digital intrusion (**DIGIT**) over de mogelijkheid tot keuring van het technisch hulpmiddel 5.1.2c dat tot op heden in 5.1.2c is ingezet (hierna: "**het oordeel**").

Gelet op potentiële politieke gevoeligheden van dit oordeel hecht ik er aan om de motivatie, met een nadere toelichting, bij u aan te bieden. Hieronder zal ik eerst kort het relevante wettelijk kader schetsen, waarna ik het oordeel van de DIGIT OvJ zal toelichten. Tot slot zal ik ingaan op de implicaties van het oordeel voor de betrokken strafzaken.

1. Wettelijk kader

Per 1 maart 2019 is de Wet computercriminaliteit III (**CCIII**) in werking getreden. Deze wet introduceert in artikel 126nba Sv. de zogenaamde "hackbevoegdheid", waarmee heimelijk en op afstand een geautomatiseerd werk kan worden binnengedrongen. Vervolgens kunnen daarin onderzoekshandelingen worden verricht.

Voor het verrichten van deze onderzoekshandelingen kan door de politie gebruik worden gemaakt van een technisch hulpmiddel. In het Besluit onderzoek in een

geautomatiseerd werk (hierna: "**Bogw**") zijn nadere eisen gesteld aan deze technisch hulpmiddelen en is er een keuringsproces beschreven. Specifieke technische keuringseisen zijn uitgewerkt in een (niet openbaar) keuringsprotocol.

In de parlementaire behandeling van CCIII is destijds een onderscheid gemaakt tussen 'binnendringsoftware', waarmee toegang tot een geautomatiseerd werk wordt verkregen, en het technisch hulpmiddel waarmee daarna onderzoekshandelingen worden verricht. Alleen het technisch hulpmiddel is keuringsplichtig.

Uit de parlementaire behandeling van CCIII en (de nota van toelichting bij) het Bogw volgt dat de wetgever als uitgangspunt heeft gehanteerd dat bij het inzetten van de hackbevoegdheid een vooraf goedgekeurd technisch hulpmiddel wordt gebruikt.¹ Van dit uitgangspunt kan bij uitzondering worden afgeweken.

Deze uitzonderingen zijn neergelegd in artikel 21, tweede en vierde lid, van het Bogw, waarbij lid 2 de mogelijkheid biedt om een niet vooraf goedgekeurd technisch hulpmiddel in te zetten. Lid 4 biedt vervolgens de mogelijkheid om die keuring achterwege te laten als de "aard van het middel" zich daar tegen verzet.

In het bijgevoegde oordeel van de landelijk DIGIT officier van mijn parket wordt van die laatste uitzondering (art. 21, lid 4, Bogw) gebruik gemaakt, omdat de aard van het onderhavige technische hulpmiddel zich daar naar zijn oordeel tegen verzet. Hieronder volgt een korte toelichting op dat oordeel.

2. Toelichting op het oordeel

Vooraf moet worden benadrukt dat het hier een oordeel betreft over een specifiek technisch hulpmiddel en geen (algemeen) soort of type technisch hulpmiddel. Dat betekent dat voor toekomstige technische hulpmiddelen, die niet (conform uitgangspunt van de wetgever) voorafgaand aan inzet zijn gekeurd, telkens een nieuw oordeel zal moeten worden gevormd.

In het onderhavige oordeel van de DIGIT officier worden enkele specifieke kernmerken van het technisch hulpmiddel beschreven, die ertoe leiden dat het middel naar zijn aard niet te keuren is. Daarbij wordt geen aandacht besteed aan het feit of het technisch hulpmiddel door de politie is vervaardigd of is gekocht van een bedrijf. Dat feit kan namelijk niet van invloed zijn op het oordeel of "de

¹ De Minister van JenV heeft dit in zijn beleidsreactie (d.d. 20 augustus 2020) op het eerste verslag van de Inspectie JenV over de uitvoering van de hackbevoegdheid door de politie nogmaals benadrukt (<https://www.rijksoverheid.nl/documenten/kamerstukken/2020/08/20/tk-reactie-verslag-ijenv-op-het-heimelijk-en-op-afstand-binnendringen-in-een-geautomatiseerd-werk>)

aard" van het hulpmiddel zodanig is dat er geen keuring kan plaatsvinden.
Kortom: de aard van het middel bestaat los van de vervaardiger van dat middel.

Het is niettemin voor de politiek-bestuurlijke context van de evaluatie van de hackbevoegdheid (voorzien 2 jaar na inwerkingtreding, d.w.z. per 1-3-2021) wel van belang om aan u mede te delen dat er in het onderhavige oordeel sprake is van een commercieel technisch hulpmiddel. Het gebruik van commerciële software was in de parlementaire behandeling van CCIII een gevoelig onderwerp.

De twee grootste zorgpunten waren:

- 1) het eventuele gebruik van onbekende kwetsbaarheden (zero-days), d.w.z. veiligheidslekken in de software die ook voor de producent nog niet bekend zijn, in de binnendringsoftware, en;
- 2) de mogelijke heimelijke toegang tot onderzoeksinformatie door de softwareleverancier.

5.1.2c



3. Implicaties voor de strafzaken

Indien de DIGIT OvJ besluit dat een technisch hulpmiddel naar zijn aard niet te keuren is, dan volgt uit artikel 21, vierde lid, Bogw dat daarvan in de processtukken melding wordt gemaakt. De DIGIT OvJ zal van deze beslissing een proces-verbaal opmaken en dat kan worden gevoegd in het procesdossier. Tevens wordt in de processtukken beschreven welke aanvullende waarborgen er zijn getroffen om de "betrouwbaarheid, integriteit en herleidbaarheid" van de met het technisch hulpmiddel vastgelegde gegevens te garanderen."

In de nota van toelichting bij het Bogw wordt hierover het volgende opgemerkt:

"Hierbij kan worden gedacht aan een uitgebreide omschrijving van de functionele specificaties van op maat gemaakt technische hulpmiddel, het voegen van een digitale kopie van de software en de broncode bij het proces-verbaal, het vooraf en achteraf maken van een forensische kopie of het audiovisueel vastleggen van de uitvoering van de onderzoekshandelingen." (pagina 45, NvT Bogw).

Met de betrokken zaaks OvJ's is voorafgaand aan de inzet steeds besproken dat het in te zetten technisch hulpmiddel niet gekeurd was en dat de mogelijkheid

zich kon voordoen dat beslist zou worden dat keuring achterwege zou blijven. De betrokken zaaks OvJ's is daarom verzocht om daar bij de inzet rekening mee te houden. Hen is gevraagd om in afstemming met het tactisch team op voorhand, tijdens en na de inzet waarborgen te treffen ter verificatie van de met het technisch hulpmiddel vastgelegde gegevens.

De DIGIT OvJ heeft inmiddels een set aan aanvullende waarborgen beschreven die voor dit specifieke technische hulpmiddel te treffen zijn en waarmee aan de eisen van betrouwbaarheid, integriteit en herleidbaarheid kan worden voldaan. Deze worden door het technisch team (dat de hackbevoegdheid uitvoert) en door het tactisch team getroffen. De uitwerking van deze aanvullende waarborgen is beschreven in een handreiking en aan de betrokken zaaks OvJ's verstrekt.

De DIGIT OvJ ondersteunt de zaaks OvJ's bij het verantwoorden van deze beslissing en de beschrijving van de aanvullende waarborgen in het dossier. Indien bij de behandeling ter terechtzitting vragen over de inzet worden gesteld zal de DIGIT OvJ ondersteunen bij de beantwoording daarvan.

Tot slot dient te worden opgemerkt dat de bewijsconstructies in de verschillende strafzaken hoogstwaarschijnlijk niet uitsluitend zullen bestaan uit gegevens die zijn verkregen met de inzet van het technisch hulpmiddel (met kenmerk ^{5.1.2c}), dat naar zijn aard niet te keuren blijkt.

5.1.2c

4. Conclusie

Het voorgaande leidt tot de conclusie dat:

- het wettelijk kader en de lagere regelgeving die zien op de inzet en keuring van technische hulpmiddelen expliciet voorziet in het gebruiken van een niet vooraf goedgekeurd technisch hulpmiddel, ook als dat door een commerciële partij is ontwikkeld;
- er een expliciete grondslag is in het Bogw voor de officier van justitie om eigenstandig te oordelen dat een dergelijk technisch hulpmiddel naar zijn aard niet te keuren is;
- indien daarvan sprake is hiervan melding wordt gemaakt in de processtukken en aanvullende waarborgen zijn en/of worden getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de (met het technisch hulpmiddel) vastgelegde gegevens te garanderen;
- dit per technisch hulpmiddel een nieuw oordeel vergt van de officier, waarbij het feit dat het middel van een commerciële partij komt niets zegt over de aard van het middel;

Datum 22 oktober 2020
Ons kenmerk LP\20\003809
Pagina 5/5

- niettegenstaande deze expliciete wettelijke grondslag de wetgever heeft beoogd dat dit een uitzonderingssituatie zou betreffen;
- de opsporingspraktijk echter wordt geconfronteerd met een werkelijkheid waarbij deze uitzondering gebruikt moet worden;
- daarmee politiek-bestuurlijke risico's ontstaan die kunnen leiden tot een verdere beperking van de inzet van commerciële technische hulpmiddelen na de evaluatie van de hackbevoegdheid in 2021;
- deze risico's geïnformeerd en beargumenteerd worden genomen.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoofachtend

5.1.2e

mr. J.J.A. Lucas
Hoofdofficier van justitie

Voorzitter College van procureurs-generaal

Postbus 20305, 2500 EH Den Haag

Minister van Justitie en Veiligheid
d.t.v. 5.1.2e (BD/DJOA/JBOZ)
Postbus 20301
2500 EH 'S-GRAVENHAGE

Prins Clauslaan 16
2595 AJ Den Haag
T +31 88 699 11 00
www.om.nl

GEHEIM

Datum 8 december 2020
Onderdeel Bestuurlijke en Juridische Zaken
Ons kenmerk PaG/BJZ/54358
Contactpersoon 5.1.2e
Doorkiesnummer(s) 088 - 5.1.2e
Onderwerp Technisch hulpmiddel in de zin van art. 126nba Sv

Bij beantwoording de datum en
ons kenmerk vermelden.

Geachte heer Grapperhaus,

Met het oog op het AO cybercriminaliteit op 9 december a.s., bericht ik u op basis van de informatie van de hoofdofficier van justitie van het Landelijk Parket, het volgende over het technisch hulpmiddel dat wordt gebruikt bij de inzet van de bevoegdheid ex artikel 126nba Sv.

Technische hulpmiddel in de zin van art. 126nba Sv

Per 1 maart 2019 is de Wet Computercriminaliteit III (hierna: CCIII) in werking getreden. Deze wet introduceert in artikel 126nba Sv de zogenoemde 'hackbevoegdheid' waarmee heimelijk en op afstand een geautomatiseerd werk kan worden binnengedrongen. Vervolgens kunnen daarin onderzoekshandelingen worden verricht.

Voor het verrichten van deze onderzoekshandelingen kan door de politie gebruik worden gemaakt van een technisch hulpmiddel. Het Besluit onderzoek in een geautomatiseerd werk (hierna: Bogw) stelt nadere eisen aan een technisch hulpmiddel en bevat een keuringsproces.

Keuringsplicht en uitzonderingen op die plicht

In de parlementaire behandeling van de CCIII is destijds onderscheid gemaakt tussen 'binnendringsoftware', waarmee toegang tot een geautomatiseerd werk wordt verkregen, en het technisch hulpmiddel waarmee vervolgens

onderzoekshandelingen kunnen worden verricht. Alleen het technisch hulpmiddel is keuringsplichtig.

Uitgangspunt is volgens de wetgever dat bij het inzetten van de hackbevoegdheid een vooraf goedgekeurd technisch hulpmiddel wordt gebruikt. Van dit uitgangspunt kan in uitzonderingsgevallen worden afgeweken.

Deze uitzonderingen zijn neergelegd in artikel 21, tweede en vierde lid, van het Bogw, waarbij het tweede lid de mogelijkheid biedt om een niet vooraf goedgekeurd technisch hulpmiddel in te zetten. Het vierde lid biedt de mogelijkheid om keuring van het middel achterwege te laten wanneer 'de aard van het middel' zich daartegen verzet.

Deze uitzonderingsgrond doet zich momenteel voor bij het gebruik van het technisch hulpmiddel in het kader van de toepassing van artikel 126nba Sv. Het gaat hierbij om een specifiek technisch hulpmiddel en niet om een (algemeen) soort of type technisch hulpmiddel. Toekomstige technische hulpmiddelen zullen opnieuw worden beoordeeld.

Het middel is na uitvoerige interne reflectie op grond van artikel 21 Bogw, ingezet in 5.1.2c. Het middel was voorafgaand aan de inzet niet gekeurd omdat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat van dit middel gebruik werd gemaakt.

Aard van het middel verzet zich tegen keuring

5.1.2c



5.1.2c



Implicaties voor de strafzaken

Wanneer een technisch hulpmiddel naar zijn aard niet te keuren is, wordt daarvan melding gemaakt in de processtukken (art. 21, vierde lid, Bogw). De betreffende officier van justitie zal van deze beslissing een proces-verbaal opmaken dat kan worden toegevoegd aan het dossier. Ook wordt in de processtukken beschreven welke aanvullende waarborgen er zijn getroffen om de betrouwbaarheid, integriteit en herleidbaarheid van de met het technisch hulpmiddel vastgelegde gegevens te garanderen.

5.1.2c

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hooachtend.
5.1.2e
het College van procureurs-generaal,
5.1.2e

G.W.A. van der Burg
5.1.2e

Beslissing dat TH^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel^{5.1.2c}

Op 5 oktober 2020 is door de landelijk DIGIT officier van justitie beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH^{5.1.2c}) zich verzette tegen keuring. TH^{5.1.2c} is na deze beslissing – met toepassing van art. 21 lid 2 Bogw – ingezet in een aantal (nieuwe) opsporingsonderzoeken.² TH^{5.1.2c} is niet vooraf aan inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 5 oktober 2020 golden ten aanzien van de aard van TH^{5.1.2c} gelden op dit moment onverkort.

5.1.2c



5.1.2c



5.1.2c

Uit de voorgaande beschrijving van TH ^{5.1.2c} volgt dat de aard van TH ^{5.1.2c} zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH ^{5.1.2c} zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat de keuringsdienst de keuring van een TH binnen 4 weken uitvoert.³ Hoewel de keuringsdienst ten opzicht van 5 oktober 2020 wel met iets meer snelheid keuringen van technische hulpmiddelen verricht, wordt deze termijn nog niet gehaald.

5.1.2c

Op dit moment heeft DIGIT LE geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. DIGIT LE is ook niet bekend met de beschikbaarheid van dergelijke middelen.

2. Conclusie

Gelet op het voorgaande komt de landelijk DIGIT OvJ tot de volgende oordelen:

1. De aard van TH ^{5.1.2c} (dat sinds 5 oktober 2020 is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH ^{5.1.2c} zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.

³ 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, Stcrt. nr. 10713.

3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. DIGIT LE en DIGIT LP zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

13 april 2021

DIGIT LP - 5.1.2e

	Toegezonden	Afgerond
LP DIGIT	07-04-2021	13-04-2021
Ter informatie LE DIGIT	07-04-2021	13-04-2021
Ter informatie recherche OvJ LP	07-04-2021	n.v.t.

Bijlage 1

5.1.2c



Beslissing dat TH^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel^{5.1.2c}

Op 5 oktober 2020 en 7 april 2021 is door de landelijk DIGIT officier van justitie beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH^{5.1.2c}) zich verzette tegen keuring. TH^{5.1.2c} is na deze beslissing - met toepassing van art. 21 lid 2 Bogw - ingezet in een aantal (nieuwe) opsporingsonderzoeken.² TH^{5.1.2c} is niet vooraf aan inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was - conform het bepaalde in art. 21 lid 2 Bogw - dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 5 oktober 2020 golden ten aanzien van de aard van TH^{5.1.2c} gelden op dit moment onverkort.



5.1.2c

5.1.2c

Uit de voorgaande beschrijving van TH **5.1.2c** volgt dat de aard van TH **5.1.2c** zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH **5.1.2c** zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat de keuringsdienst de keuring van een TH binnen 4 weken uitvoert.³ Hoewel de keuringsdienst inmiddels wel met iets meer snelheid keuringen van technische hulpmiddelen verricht, wordt deze termijn nog niet altijd gehaald.

5.1.2c

Op dit moment heeft DIGIT LE geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. DIGIT LE is ook niet bekend met de beschikbaarheid van dergelijke middelen.

2. Conclusie

Gelet op het voorgaande komt de landelijk DIGIT OvJ tot de volgende oordelen:

1. De aard van TH **5.1.2c** (dat sinds 7 april 2021 is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH **5.1.2c** zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.
3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever

³ 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, Stcrt. nr. 10713.

met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.

4. DIGIT LE en DIGIT LP zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

5 juli 2021

DIGIT LP - 5.1.2e

	Toegezonden	Afgerond
LP DIGIT	05-07-2021	05-07-2021
Ter informatie LE DIGIT	05-07-2021	n.v.t.
Ter informatie recherche OvJ LP	05-07-2021	n.v.t.

Bijlage 1

5.1.2c



Beslissing dat TH ^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel ^{5.1.2c}

Op 5 oktober 2020, 7 april 2021 en 5 juli 2021 is door de landelijk DIGIT officier van justitie beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH ^{5.1.2c}) zich verzette tegen keuring. TH ^{5.1.2c} is na deze beslissing – het toepassing van art. 21 lid 2 Bogw – gezet in een aantal (nieuwe) opsporingsonderzoeken.² TH ^{5.1.2c} is niet vooraf aan inzet in deze opsporingsonderzoeken gekeurd. Dereden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH ^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 5 oktober 2020 golden ten aanzien van de aard van TH ^{5.1.2c} gelden op dit moment onverkort.



^{5.1.2c}

5.1.2c

Uit de voorgaande beschrijving van TH **5.1.2c** volgt dat de aard van TH **5.1.2c** zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH **5.1.2c** zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat de keuringsdienst de keuring van een TH binnen 4 weken uitvoert.³ Hoewel de keuringsdienst inmiddels wel met iets meer snelheid keuringen van technische hulpmiddelen verricht, wordt deze termijn nog niet gehaald.

5.1.2c

Op dit moment heeft DIGIT LE geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. DIGIT LE is ook niet bekend met de beschikbaarheid van dergelijke middelen.

2. Conclusie

Gelet op het voorgaande komt de landelijk DIGIT OvJ tot de volgende oordelen:

1. De aard van TH **5.1.2c** (dat sinds 5 juli 2021 is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH **5.1.2c** zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.
3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever

³ 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, Stcrt. nr. 10713.

met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.

4. DIGIT LE en DIGIT LP zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

29 september 2021

DIGIT LP – 5.1.2e

	Toegezonden
LP DIGIT	29-09-2021
Ter informatie LE DIGIT	29-09-2021
Ter informatie recherche OvJ LP	29-09-2021

Bijlage 1

5.1.2c



Beslissing dat TH^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel^{5.1.2c}

Op 5 oktober 2020, 7 april 2021, 5 juli 2021 en 29 september 2021 is door de landelijk DIGIT officier van justitie beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH^{5.1.2c}) zich verzette tegen keuring. TH^{5.1.2c} is na deze beslissing – met toepassing van art. 21 lid 2 Bogw – ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH^{5.1.2c} is niet vooraf aan inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 5 oktober 2020 golden ten aanzien van de aard van TH^{5.1.2c} gelden op dit moment onverkort.

5.1.2c



5.1.2c



5.1.2c

Uit de voorgaande beschrijving van TH **5.1.2c** volgt dat de aard van TH **5.1.2c** zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH **5.1.2c** zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat de keuringsdienst de keuring van een TH binnen 4 weken uitvoert.³ Hoewel de keuringsdienst inmiddels wel met iets meer snelheid keuringen van technische hulpmiddelen verricht, wordt deze termijn nog niet gehaald.

5.1.2c

Op dit moment heeft DIGIT LE geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. DIGIT LE is ook niet bekend met de beschikbaarheid van dergelijke middelen.

2. Conclusie

Gelet op het voorgaande komt de landelijk DIGIT OvJ tot de volgende oordelen:

1. De aard van TH **5.1.2c** (dat sinds 29 september 2021 is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH **5.1.2c** zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.

³ 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, Stcrt. nr. 10713.

3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. DIGIT LE en DIGIT LP zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

16 december 2021

DIGIT LP 5.1.2e

	Toegezonden
LP DIGIT	16-12-2021
Ter informatie LE DIGIT	16-12-2021
Ter informatie recherche OvJ LP	16-12-2021

Bijlage 1

5.1.2c



Beslissing dat TH^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel^{5.1.2c}

Op 5 oktober 2020, 7 april 2021, 5 juli 2021, 29 september 2021 en 16 december 2021 is door de landelijk DIGIT officier van justitie beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH^{5.1.2c}) zich verzette tegen keuring. TH^{5.1.2c} is na deze beslissing – net toepassing van art. 21 lid 2 Bogw – ingezet in een aantal (nieuwe) opsporingsonderzoeken.² TH^{5.1.2c} is niet vooraf aan inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 5 oktober 2020 golden ten aanzien van de aard van TH^{5.1.2c} gelden op dit moment onverkort.

5.1.2c



5.1.2c



5.1.2c

Uit de voorgaande beschrijving van TH **5.1.2c** volgt dat de aard van TH **5.1.2c** zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH **5.1.2c** zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat de keuringsdienst de keuring van een TH binnen 4 weken uitvoert.³ Hoewel de keuringsdienst inmiddels wel met iets meer snelheid keuringen van technische hulpmiddelen verricht, wordt deze termijn nog niet gehaald.

5.1.2c

Op dit moment heeft DIGIT LE geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. DIGIT LE is ook niet bekend met de beschikbaarheid van dergelijke middelen.

2. Conclusie

Gelet op het voorgaande komt de landelijk DIGIT OvJ tot de volgende oordelen:

1. De aard van TH **5.1.2c** (dat sinds 16 december 2021 is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH **5.1.2c** zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.

³ 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, Stcrt. nr. 10713.

3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. DIGIT LE en DIGIT LP zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

31 maart 2022

DIGIT LP - 5.1.2e

	Toegezonden
LP DIGIT	31-03-2022
Ter informatie LE DIGIT	31-03-2022
Ter informatie recherche OvJ LP	31-03-2022

Bijlage 1

5.1.2c



Beslissing dat TH^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel^{5.1.2c}

Sinds 5 oktober 2020 is door de landelijk DIGIT officier van justitie herhaaldelijk beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH^{5.1.2c}) zich verzette tegen keuring.² TH^{5.1.2c} is na deze beslissing niet toepassing van art. 21 lid 2 Bogw ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH^{5.1.2c} is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was conform het bepaalde in art. 21 lid 2 Bogw dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 5 oktober 2020 golden ten aanzien van de aard van TH^{5.1.2c} gelden op dit moment onverkort.



5.1.2c

² Na 5 oktober 2020 zijn dergelijke besluiten genomen op 7 april 2021, 5 juli 2021, 29 september 2021, 16 december 2022 en 31 maart 2022.

5.1.2c

5.1.2c

Uit de voorgaande beschrijving van TH **5.1.2c** volgt dat de aard van TH **5.1.2c** zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH **5.1.2c** zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁴ Voor de keuringsdienst van de Landelijke Eenheid geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt noch door de keuringsdienst van de Landelijke Eenheid, noch door een aangewezen keuringsdienst niet gehaald.

5.1.2c

Op dit moment heeft DIGIT LE geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. DIGIT LE is ook niet bekend met de beschikbaarheid van dergelijke middelen.

2. Conclusie

Gelet op het voorgaande komt de landelijk DIGIT OvJ tot de volgende oordelen:

1. De aard van TH **5.1.2c** (dat sinds 31 maart 2022 is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH **5.1.2c** zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.

⁴ 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, Stcrt. nr. 10713.

3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. DIGIT LE en DIGIT LP zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

4 juli 2022

DIGIT LP - 5.1.2e

	Toegezonden
LP DIGIT	04-07-2022
Ter informatie LE DIGIT	04-07-2022
Ter informatie recherche OvJ LP	04-07-2022
Ter informatie hoofd OvJ LP	04-07-2022

Bijlage 1

5.1.2c



Beslissing dat TH^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel^{5.1.2c}

Sinds 5 oktober 2020 is door de landelijk DIGIT officier van justitie herhaaldelijk beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH^{5.1.2c}) zich verzette tegen keuring.² TH^{5.1.2c} is na deze beslissing - met toepassing van art. 21 lid 2 Bogw - ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH^{5.1.2c} is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was - conform het bepaalde in art. 21 lid 2 Bogw - dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 5 oktober 2020 golden ten aanzien van de aard van TH^{5.1.2c} gelden op dit moment onverkort.



5.1.2c

² Na 5 oktober 2020 zijn dergelijke besluiten genomen op 7 april 2021, 5 juli 2021, 29 september 2021, 16 december 2022, 31 maart 2022 en 4 juli 2022.

5.1.2c

5.1.2c

Uit de voorgaande beschrijving van TH **5.1.2c** volgt dat de aard van TH **5.1.2c** zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH **5.1.2c** zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁴ Voor de keuringsdienst van de Landelijke Eenheid geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt noch door de keuringsdienst van de Landelijke Eenheid, noch door een aangewezen keuringsdienst gehaald.

5.1.2c

Op dit moment heeft DIGIT LE geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. DIGIT LE is ook niet bekend met de beschikbaarheid van dergelijke middelen.

2. Conclusie

Gelet op het voorgaande komt de landelijk DIGIT OvJ tot de volgende oordelen:

1. De aard van TH **5.1.2c** (dat sinds 30 juni 2022 is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH **5.1.2c** zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.

⁴ 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, Stcrt. nr. 10713.

3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. DIGIT LE en DIGIT LP zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

26 september 2022

DIGIT LP - 5.1.2e

	Toegezonden
LP DIGIT	26-9-2022
Ter informatie LE DIGIT	26-9-2022
Ter informatie recherche OvJ LP	26-9-2022
Ter informatie hoofd OvJ LP	26-9-2022

Bijlage 1

5.1.2c



Beslissing dat TH^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel^{5.1.2c}

Sinds 5 oktober 2020 is door de landelijk DIGIT officier van justitie herhaaldelijk beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH^{5.1.2c}) zich verzette tegen keuring.² TH^{5.1.2c} is na deze beslissing - met toepassing van art. 21 lid 2 Bogw - ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH^{5.1.2c} is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was - conform het bepaalde in art. 21 lid 2 Bogw - dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 5 oktober 2020 golden ten aanzien van de aard van TH^{5.1.2c} gelden op dit moment onverkort.

5.1.2c



5.1.2c

² Na 5 oktober 2020 zijn dergelijke besluiten genomen op 7 april 2021, 5 juli 2021, 29 september 2021, 16 december 2022, 31 maart 2022, 4 juli 2022 en 26 september 2022.

5.1.2c

5.1.2c

Uit de voorgaande beschrijving van TH **5.1.2c** volgt dat de aard van TH **5.1.2c** zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH **5.1.2c** zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁴ Voor de keuringsdienst van de Landelijke Eenheid geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt noch door de keuringsdienst van de Landelijke Eenheid, noch door een aangewezen keuringsdienst niet gehaald.

5.1.2c

Op dit moment heeft DIGIT LE geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. DIGIT LE is ook niet bekend met de beschikbaarheid van dergelijke middelen.

2. Conclusie

Gelet op het voorgaande komt de landelijk DIGIT OvJ tot de volgende oordelen:

1. De aard van TH **5.1.2c** (dat sinds 13 september 2022 is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH **5.1.2c** zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.

⁴ 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, Stcrt. nr. 10713.

3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. DIGIT LE en DIGIT LP zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

17 januari 2023

DIGIT LP - 5.1.2e

	Toegezonden
LP DIGIT	17-1-2023
Ter informatie LE DIGIT	17-1-2023
Ter informatie recherche OvJ LP	17-1-2023
Ter informatie hoofd OvJ LP	17-1-2023

Bijlage 1

5.1/2c



Beslissing dat TH^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel^{5.1.2c}

Sinds 5 oktober 2020 is door de landelijk DIGIT officier van justitie herhaaldelijk beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH^{5.1.2c}) zich verzette tegen keuring.² TH^{5.1.2c} is na deze beslissing - met toepassing van art. 21 lid 2 Bogw - ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH^{5.1.2c} is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was - conform het bepaalde in art. 21 lid 2 Bogw - dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 5 oktober 2020 golden ten aanzien van de aard van TH^{5.1.2c} gelden op dit moment onverkort.

5.1.2c



5.1.2c

² Na 5 oktober 2020 zijn dergelijke besluiten genomen op 7 april 2021, 5 juli 2021, 29 september 2021, 16 december 2022, 31 maart 2022, 4 juli 2022, 26 september 2022 en 17 januari 2023.

5.1.2c

5.1.2c

Uit de voorgaande beschrijving van TH **5.1.2c** volgt dat de aard van TH **5.1.2c** zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH **5.1.2c** zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁴ Voor de keuringsdienst van de Landelijke Eenheid geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt noch door de keuringsdienst van de Landelijke Eenheid, noch door een aangewezen keuringsdienst gehaald.

5.1.2c

Op dit moment heeft DIGIT LE geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. DIGIT LE is ook niet bekend met de beschikbaarheid van dergelijke middelen.

2. Conclusie

Gelet op het voorgaande komt de landelijk DIGIT OvJ tot de volgende oordelen:

1. De aard van TH **5.1.2c** (dat sinds 13 september 2022 is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH **5.1.2c** zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.

⁴ 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, Stcrt. nr. 10713.

3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. DIGIT LE en DIGIT LP zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

20 maart 2023

DIGIT LP - 5.1.2e

	Toegezonden
LP DIGIT	20-3-2023
Ter informatie LE DIGIT	20-3-2023
Ter informatie recherche OvJ LP	20-3-2023
Ter informatie hoofd OvJ LP	20-3-2023

Bijlage 1

5.1.2c



Beslissing dat TH ^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel ^{5.1.2c}

Sinds 5 oktober 2020 is door de landelijk DIGIT officier van justitie herhaaldelijk beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH ^{5.1.2c}) zich verzette tegen keuring.² TH ^{5.1.2c} is na deze beslissing – met toepassing van art. 21 lid 2 Bogw – ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH ^{5.1.2c} is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH ^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 5 oktober 2020 golden ten aanzien van de aard van TH ^{5.1.2c} gelden op dit moment onverkort.



^{5.1.2c}

² Na 5 oktober 2020 zijn dergelijke besluiten genomen op 7 april 2021, 5 juli 2021, 29 september 2021, 16 december 2022, 31 maart 2022, 4 juli 2022, 26 september 2022, 17 januari 2023 en 20 maart 2023.

^{5.1.2c}

5.1.2c

Uit de voorgaande beschrijving van TH **5.1.2c** volgt dat de aard van TH **5.1.2c** zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH **5.1.2c** zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁴ Voor de keuringsdienst van de Landelijke Eenheid geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt noch door de keuringsdienst van de Landelijke Eenheid, noch door een aangewezen keuringsdienst niet gehaald.

5.1.2c

Op dit moment heeft DIGIT LE geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. DIGIT LE is ook niet bekend met de beschikbaarheid van dergelijke middelen.

2. Conclusie

Gelet op het voorgaande komt de landelijk DIGIT OvJ tot de volgende oordelen:

1. De aard van TH **5.1.2c** (dat sinds 13 september 2022 is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH **5.1.2c** zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.

⁴ 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, Stcrt. nr. 10713.

3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. DIGIT LE en DIGIT LP zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

20 juli 2023

DIGIT LP 5.1.2e

	Toegezonden
LP DIGIT	20-07-2023
Ter informatie LE DIGIT	20-07-2023
Ter informatie recherche OvJ LP	20-07-2023
Ter informatie hoofd OvJ LP	20-07-2023

Bijlage 1

5.1.2c



Beslissing dat TH ^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel ^{5.1.2c}

Sinds 5 oktober 2020 is door de landelijk DIGIT officier van justitie herhaaldelijk beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH ^{5.1.2c} zich verzette tegen keuring.² TH ^{5.1.2c} is na deze beslissing – met toepassing van art. 21 lid 2 Bogw – ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH ^{5.1.2c} is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH ^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 5 oktober 2020 golden ten aanzien van de aard van TH ^{5.1.2c} gelden op dit moment onverkort.



^{5.1.2c}

² Na 5 oktober 2020 zijn dergelijke besluiten genomen op 7 april 2021, 5 juli 2021, 29 september 2021, 16 december 2022, 31 maart 2022, 4 juli 2022, 26 september 2022, 17 januari 2023, 20 maart 2023 en 20 juli 2023.

^{5.1.2c}

5.1.2c



Uit de voorgaande beschrijving van TH 5.1.2c volgt dat de aard van TH 5.1.2c zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH 5.1.2c zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁴ Voor de keuringsdienst van de Landelijke Eenheid geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt noch door de keuringsdienst van de Landelijke Eenheid, noch door een aangewezen keuringsdienst niet gehaald.

5.1.2c



Op dit moment heeft DIGIT LE geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. DIGIT LE is ook niet bekend met de beschikbaarheid van dergelijke middelen.

⁴ 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, Stcrt. nr. 10713.

2. Conclusie

Gelet op het voorgaande komt de landelijk DIGIT OvJ tot de volgende oordelen:

1. De aard van TH 5.1.2c (dat sinds de vorige beslissing ex art. 21 lid 4 Bogw is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH 5.1.2c zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.
3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. DIGIT LE en DIGIT LP zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

6 november 2023

DIGIT LP – 5.1.2e

	Toegezonden
LP DIGIT	6-11-2023
Ter informatie LE DIGIT	6-11-2023
Ter informatie recherche OvJ LP	6-11-2023
Ter informatie hoofd OvJ LP	6-11-2023

Bijlage 1

5.1.2c



Beslissing dat TH ^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel ^{5.1.2c}

Sinds 5 oktober 2020 is door de landelijk DIGIT officier van justitie herhaaldelijk beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH ^{5.1.2c} zich verzette tegen keuring.² TH ^{5.1.2c} is na deze beslissing – met toepassing van art. 21 lid 2 Bogw – ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH ^{5.1.2c} is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH ^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 5 oktober 2020 golden ten aanzien van de aard van TH ^{5.1.2c} gelden op dit moment onverkort.



^{5.1.2c}

² Na 5 oktober 2020 zijn dergelijke besluiten genomen op 7 april 2021, 5 juli 2021, 29 september 2021, 16 december 2022, 31 maart 2022, 4 juli 2022, 26 september 2022, 17 januari 2023, 20 maart 2023, 20 juli 2023 en 6 november 2023.

5.1.2c

Uit de voorgaande beschrijving van TH 5.1.2c volgt dat de aard van TH 5.1.2c zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH 5.1.2c zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁴ Voor de keuringsdienst van de Landelijke Eenheid geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt noch door de keuringsdienst van de Landelijke Eenheid, noch door een aangewezen keuringsdienst niet gehaald.

5.1.2c

Op dit moment heeft DIGIT LE geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. DIGIT LE is ook niet bekend met de beschikbaarheid van dergelijke middelen.

⁴ 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, Stcrt. nr. 10713.

2. Conclusie

Gelet op het voorgaande komt de landelijk DIGIT OvJ tot de volgende oordelen:

1. De aard van TH 5.1.2c (dat sinds de vorige beslissing ex art. 21 lid 4 Bogw is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH 5.1.2c zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.
3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. DIGIT LE en DIGIT LP zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

4 januari 2024

DIGIT LP – 5.1.2e

	Toegezonden
LP DIGIT	04- 01 -2024
Ter informatie LE DIGIT	04- 01 -2024
Ter informatie recherche OvJ LP	04- 01 -2024
Ter informatie hoofd OvJ LP	04- 01 -2024

Bijlage 1

5.1.2c



Beslissing dat TH ^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel ^{5.1.2c}

Sinds 5 oktober 2020 is door de landelijk officier van justitie voor Digital Intrusion herhaaldelijk beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH ^{5.1.2c} zich verzette tegen keuring.² TH ^{5.1.2c} is na deze beslissing – met toepassing van art. 21 lid 2 Bogw – ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH ^{5.1.2c} is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH ^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 5 oktober 2020 golden ten aanzien van de aard van TH ^{5.1.2c} gelden op dit moment onverkort.



^{5.1.2c}

² Na 5 oktober 2020 zijn dergelijke besluiten genomen op 7 april 2021, 5 juli 2021, 29 september 2021, 16 december 2022, 31 maart 2022, 4 juli 2022, 26 september 2022, 17 januari 2023, 20 maart 2023, 20 juli 2023, 6 november 2023 en 4 januari 2024.

^{5.1.2c}

5.1.2c

Uit de voorgaande beschrijving van TH 5.1.2c volgt dat de aard van TH 5.1.2c zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH 5.1.2c zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁴ Voor de keuringsdienst van de Eenheid landelijke expertise en operaties (LX) geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt door de keuringsdienst van de LX of een aangewezen keuringsdienst niet gehaald.

5.1.2c

Op dit moment heeft LX DIGIT geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. LX DIGIT is ook niet bekend met de beschikbaarheid van dergelijke middelen.

⁴ 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, Stcrt. nr. 10713.

2. Conclusie

Gelet op het voorgaande komt de landelijk DIGIT OvJ tot de volgende oordelen:

1. De aard van TH 5.1.2c (dat sinds de vorige beslissing ex art. 21 lid 4 Bogw is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH 5.1.2c zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.
3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. LX DIGIT en LP DIGIT zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

24 april 2024

LP DIGIT – 5.1.2e

	Toegezonden
LP DIGIT	29-04-2024
Ter informatie LX DIGIT	29-04-2024
Ter informatie recherche OvJ LP	29-04-2024
Ter informatie hoofd OvJ LP	29-04-2024

Bijlage 1

5.1.2c



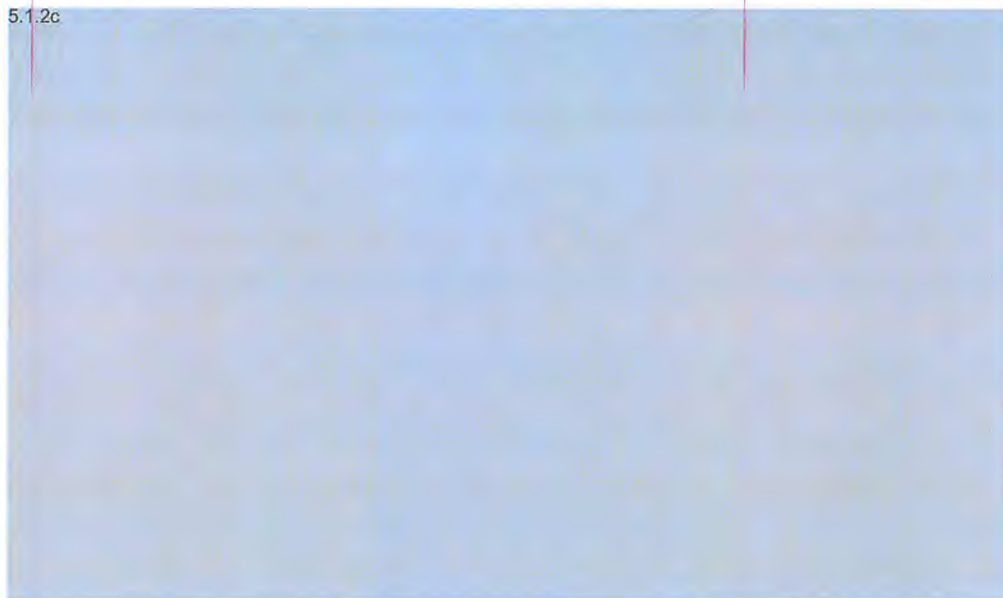
Beslissing dat TH ^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel ^{5.1.2c}

Sinds 5 oktober 2020 is door de landelijk officier van justitie voor Digital Intrusion herhaaldelijk beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH ^{5.1.2c} zich verzette tegen keuring.² TH ^{5.1.2c} is na deze beslissing – met toepassing van art. 21 lid 2 Bogw – ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH ^{5.1.2c} is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH ^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 5 oktober 2020 golden ten aanzien van de aard van TH ^{5.1.2c} gelden op dit moment onverkort.



5.1.2c

² Na 5 oktober 2020 zijn dergelijke besluiten genomen op 7 april 2021, 5 juli 2021, 29 september 2021, 16 december 2022, 31 maart 2022, 4 juli 2022, 26 september 2022, 17 januari 2023, 20 maart 2023, 20 juli 2023, 6 november 2023, 4 januari 2024 en 24 april 2024.

5.1.2c

5.1.2c

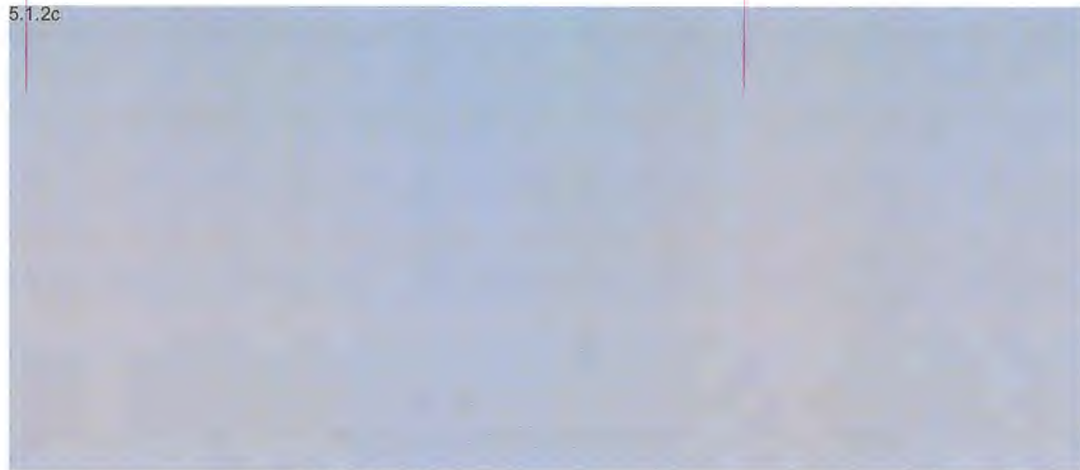


Uit de voorgaande beschrijving van TH 5.1.2c volgt dat de aard van TH 5.1.2c zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH 5.1.2c zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁴ Voor de keuringsdienst van de Eenheid landelijke expertise en operaties (LX) geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt door de keuringsdienst van de LX of een aangewezen keuringsdienst niet gehaald.

5.1.2c



Op dit moment heeft LX DIGIT geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. LX DIGIT is ook niet bekend met de beschikbaarheid van dergelijke middelen.

⁴ 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, Stcrt. nr. 10713.

2. Conclusie

Gelet op het voorgaande komt de landelijk officier van justitie voor Digital Intrusion tot de volgende oordelen:

1. De aard van TH 5.1.2c (dat sinds de vorige beslissing ex art. 21 lid 4 Bogw is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH 5.1.2c zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.
3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. LX DIGIT en LP DIGIT zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

10 juli 2024

LP DIGIT – 5.1.2e

	Toegezonden
LP DIGIT	10- 07 -2024
Ter informatie LX DIGIT	10- 07 -2024
Ter informatie recherche OvJ LP	10- 07 -2024
Ter informatie hoofd OvJ LP	10- 07 -2024

Bijlage 1

5.1.2c



Beslissing dat TH ^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel ^{5.1.2c}

Sinds 5 oktober 2020 is door de landelijk officier van justitie voor Digital Intrusion herhaaldelijk beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH ^{5.1.2c} zich verzette tegen keuring.² TH ^{5.1.2c} is na deze beslissing – met toepassing van art. 21 lid 2 Bogw – ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH ^{5.1.2c} is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH ^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 5 oktober 2020 golden ten aanzien van de aard van TH ^{5.1.2c} gelden op dit moment onverkort.



^{5.1.2c}

² Na 5 oktober 2020 zijn dergelijke besluiten genomen op 7 april 2021, 5 juli 2021, 29 september 2021, 16 december 2022, 31 maart 2022, 4 juli 2022, 26 september 2022, 17 januari 2023, 20 maart 2023, 20 juli 2023, 6 november 2023, 4 januari 2024, 24 april 2024 en 10 juli 2024.

^{5.1.2c}

5.1.2c



Uit de voorgaande beschrijving van TH 5.1.2c volgt dat de aard van TH 5.1.2c zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH 5.1.2c zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁴ Voor de keuringsdienst van de Eenheid landelijke expertise en operaties (LX) geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt door de keuringsdienst van de LX of een aangewezen keuringsdienst niet gehaald.

5.1.2c



Op dit moment heeft LX DIGIT geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. LX DIGIT is ook niet bekend met de beschikbaarheid van dergelijke middelen.

⁴ 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, Stcrt. nr. 10713.

2. Conclusie

Gelet op het voorgaande komt de landelijk officier van justitie voor Digital Intrusion tot de volgende oordelen:

1. De aard van TH 5.1.2c (dat sinds de vorige beslissing ex art. 21 lid 4 Bogw is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH 5.1.2c zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.
3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. LX DIGIT en LP DIGIT zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

24 februari 2025

LP DIGIT – 5.1.2e

	Toegezonden
LP DIGIT	24-02-2025
Ter informatie LX DIGIT	24-02-2025
Ter informatie recherche OvJ LP	24-02-2025
Ter informatie hoofd OvJ LP	24-02-2025

Bijlage 1

5.1.2c



Beslissing dat TH ^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel ^{5.1.2c}

Sinds 5 oktober 2020 is door de landelijk officier van justitie voor Digital Intrusion herhaaldelijk beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH ^{5.1.2c} zich verzette tegen keuring.² TH ^{5.1.2c} is na deze beslissing – met toepassing van art. 21 lid 2 Bogw – ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH ^{5.1.2c} is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH ^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 5 oktober 2020 golden ten aanzien van de aard van TH ^{5.1.2c} gelden op dit moment onverkort.



^{5.1.2c}

² Na 5 oktober 2020 zijn dergelijke besluiten genomen op 7 april 2021, 5 juli 2021, 29 september 2021, 16 december 2022, 31 maart 2022, 4 juli 2022, 26 september 2022, 17 januari 2023, 20 maart 2023, 20 juli 2023, 6 november 2023, 4 januari 2024, 24 april 2024 en 10 juli 2024 en 24 februari 2025.

^{5.1.2c}

5.1.2c

Uit de voorgaande beschrijving van TH 5.1.2c volgt dat de aard van TH 5.1.2c zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH 5.1.2c zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁴ Voor de keuringsdienst van de Eenheid landelijke expertise en operaties (LX) geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt door de keuringsdienst van de LX of een aangewezen keuringsdienst niet gehaald.

5.1.2c

Op dit moment heeft LX DIGIT geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. LX DIGIT is ook niet bekend met de beschikbaarheid van dergelijke middelen.

⁴ 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, Stcrt. nr. 10713.

2. Conclusie

Gelet op het voorgaande komt de landelijk officier van justitie voor Digital Intrusion tot de volgende oordelen:

1. De aard van TH 5.1.2c (dat sinds de vorige beslissing ex art. 21 lid 4 Bogw is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH 5.1.2c zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.
3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. LX DIGIT en LP DIGIT zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

13 mei 2025

LP DIGIT – 5.1.2e

	Toegezonden
LP DIGIT	13-05-2025
Ter informatie LX DIGIT	13-05-2025
Ter informatie recherche OvJ LP	13-05-2025
Ter informatie hoofd OvJ LP	13-05-2025

Bijlage 1

5.1.2c



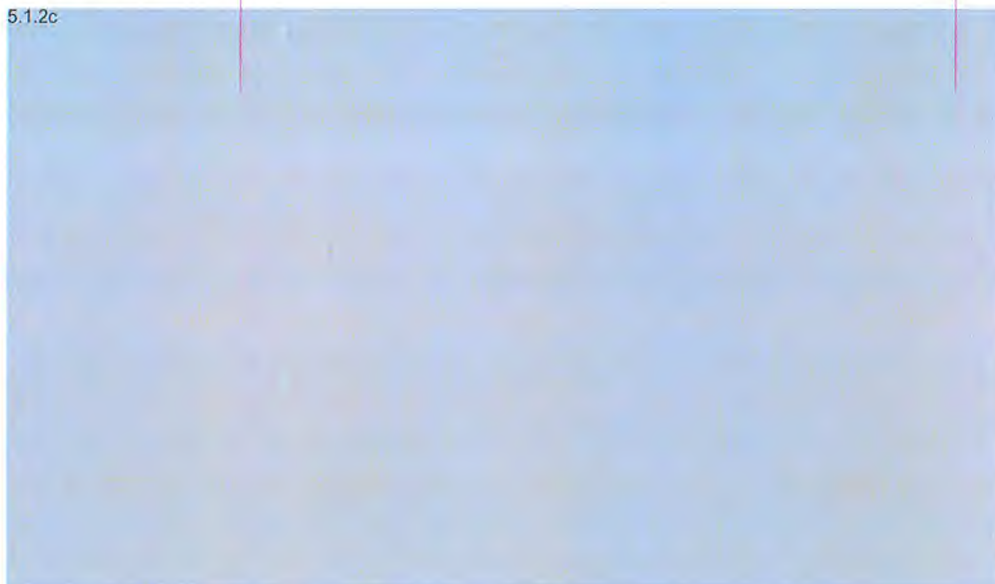
Beslissing dat TH ^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel ^{5.1.2c}

Sinds 5 oktober 2020 is door de landelijk officier van justitie voor Digital Intrusion herhaaldelijk beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH ^{5.1.2c} zich verzette tegen keuring.² TH ^{5.1.2c} is na deze beslissing – met toepassing van art. 21 lid 2 Bogw – ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH ^{5.1.2c} is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH ^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 5 oktober 2020 golden ten aanzien van de aard van TH ^{5.1.2c} gelden op dit moment onverkort.



^{5.1.2c}

² Na 5 oktober 2020 zijn dergelijke besluiten genomen op 7 april 2021, 5 juli 2021, 29 september 2021, 16 december 2022, 31 maart 2022, 4 juli 2022, 26 september 2022, 17 januari 2023, 20 maart 2023, 20 juli 2023, 6 november 2023, 4 januari

^{5.1.2c}

5.1.2c

Uit de voorgaande beschrijving van TH 5.1.2c volgt dat de aard van TH 5.1.2c zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH 5.1.2c zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁴ Voor de keuringsdienst van de Eenheid landelijke expertise en operaties (LX) geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt door de keuringsdienst van de LX of een aangewezen keuringsdienst niet gehaald.

5.1.2c

Op dit moment heeft LX DIGIT geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. LX DIGIT is ook niet bekend met de beschikbaarheid van dergelijke middelen.

⁴ 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, Stcrt. nr. 10713.

2. Conclusie

Gelet op het voorgaande komt de landelijk officier van justitie voor Digital Intrusion tot de volgende oordelen:

1. De aard van TH 5.1.2c (dat sinds de vorige beslissing ex art. 21 lid 4 Bogw is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH 5.1.2c zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.
3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. LX DIGIT en LP DIGIT zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

9 juli 2025

LP DIGIT – 5.1.2e

	Toegezonden
LP DIGIT	09-07-2025
Ter informatie LX DIGIT	09-07-2025
Ter informatie recherche OvJ LP	09-07-2025
Ter informatie hoofd OvJ LP	09-07-2025

Bijlage 1

5.1.2c



Onderzoek XX - inzet 126nba en achterwege blijven keuring technisch hulpmiddel

Beste XXX,

In onderzoek YYY is gebruik gemaakt van de bevoegdheid ex artikel 126nba Sv. Daarbij is een niet gekeurd technisch hulpmiddel ingezet. Inmiddels heb ik beslist dat de aard van het gebruikte technische hulpmiddel zich verzet tegen keuring achteraf. Dat heeft tot gevolg dat op grond van het Besluit onderzoek in een geautomatiseerd werk (verder: Bogw) door de officier van justitie in de processtukken moet worden vermeld welke aanvullende waarborgen zijn getroffen.

Een deel van deze waarborgen wordt door DIGIT getroffen. Daarnaast moeten binnen het tactische onderzoek echter ook waarborgen worden getroffen. Over het treffen van deze aanvullende waarborgen hebben we het daarom eerder gehad.

Bij deze mail voeg ik 2 format processen verbaal die je kan/jullie kunnen gebruiken voor de verantwoording van de getroffen aanvullende waarborgen; één voor de situatie dat de inzet van DIGIT bij heeft gedragen aan het bewijs en één voor de situatie dat dat niet het geval is. Het eerste format PV houdt sterk verband met de "Handreiking waarborgen 21 lid 4 Bogw". Dat stuk voeg ik daarom ook bij deze mail.

Ik heb DIGIT gevraagd een proces-verbaal op te maken met een beschrijving van de werking en functionele specificaties van het technisch hulpmiddel. De door het technisch team getroffen waarborgen blijken daaruit. Zodra dit stuk klaar is, zal ik dat toe sturen. Daarnaast zal ik proces-verbaal opmaken over de beslissing tot achterwege laten van de keuring. Dat stuur ik gelijktijdig met het proces-verbaal van DIGIT toe.

Als je/jullie vragen hebben of overleg over het voorgaande willen, let me know. 5.1.2e en ik helpen graag waar dat mogelijk is.

Met vriendelijke groet,

5.1.2e
Officier van Justitie

Openbaar Ministerie
Landelijk Parket
5.1.2e
Posthumalaan 74, 3072 AG Rotterdam
Postbus 395, 3000 AJ Rotterdam
06 - 5.1.2e
5.1.2e@om.nl
www.om.nl

Onderzoek XX - PV's achterwege blijven keuring technisch hulpmiddel

Ha XX,

Bijgevoegd is het PV over de beslissing om het in onderzoek XX ingezette technische hulpmiddel niet te laten keuren. Tevens voeg ik een PV bij waarin DIGIT beschrijft welke aanvullende waarborgen zij hebben getroffen. DIGIT zal deze stukken richting het politieteam sturen.

Als jullie vragen hebben, let me know.

Met vriendelijke groet,

5.1.2e

Officier van Justitie

To-do-list en checklist beslissing 21 lid 4 Bogw

1. 5.1.2c 
2. Besluit 21 lid 4 Bogw nemen
 - Ronde de eerste van elke 4^e, 7^e, 10^e en 1^e maand
3. Besluit 21 lid 4 Bogw schriftelijk vastleggen.
 - 2022XXXX Beslissing ex 21 lid 4 Bogw tav TH XX
4. Besluit 21 lid 4 Bogw mailen aan:
 - a. zaaksOvJ
 - mail FORMAT: mail aan zaaksofficier over besluit 21 lid 4 Bogw
 - Bijlagen:
 1. 20201016 PV bevindingen ex 21 lid 4 Bogw - geen bewijs ZAAKSOVJ
 2. 20201016 PV bevindingen ex 21 lid 4 Bogw - wel bewijs ZAAKSOVJ
 3. 20201016 Toelichting 21 lid 4 Bogw tbv zaaksOVJ
 4. 20210106 Handreiking waarborgen 21 lid 4 BOGW
 - b. Hoofdofficier LP, recherche officieren LP en teamleider team 2 LP
 - Bijlage:
 1. 2022XXXX Beslissing ex 21 lid 4 Bogw tav TH XX
 - c. Teamleider en jurist DIGIT
 - Bijlage:
 1. 2022XXXX Beslissing ex 21 lid 4 Bogw tav TH XX
5. Concept PV maken van besluit en door technisch team getroffen aanvullende waarborgen
 - FORMAT: 20201016 PV bevindingen besluit ex 21 lid 4 Bogw DIGIT LP
6. Concept PV mailen aan dossiervormers DIGIT
7. Na afronding PV's door DIGIT, de PV's mailen aan zaaksOvJ
 - 20210700 FORMAT mail aan zaaksofficier over PV's 21 lid 4 Bogw
 - Bijlage:
 1. 2021XXXX PV's XX

Notitie m.b.t. de beslissing dat TH 5.1.2c naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Wettelijk kader

Per 1 maart 2019 is de Wet computercriminaliteit III (CCIII) in werking getreden. Deze wet creëert in artikel 126nba Sv de nieuwe bijzondere opsporingsbevoegdheid om heimelijk en op afstand binnen te dringen in een geautomatiseerd werk en daar onderzoekshandelingen te verrichten.¹

In art. 126nba lid 1 Sv is bepaald dat bij het doen van onderzoek in een binnengedrongen geautomatiseerd werk gebruik kan worden gemaakt van een technisch hulpmiddel (TH). Deze mogelijkheid is nader uitgewerkt in het Besluit onderzoek in een geautomatiseerd werk (Bogw).² In het Bogw wordt een TH omschreven als "softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel".³

Het in het Bogw geformuleerde uitgangspunt voor het gebruik van TH's is dat er wordt gewerkt met een vooraf goedgekeurd TH (art. 14 en 21 lid 1 Bogw). Indien het onderzoek het dringend vordert, kan de OvJ bepalen dat gewerkt wordt met een niet goedgekeurd TH (art. 21 lid 2 Bogw). Die beslissing wordt ook opgenomen in het bevel. Het niet goedgekeurde TH wordt na afloop van de inzet alsnog goedgekeurd en de resultaten daarvan worden aan het procesdossier toegevoegd (art. 21 lid 3 Bogw).

De OvJ kan echter ook bevelen dat een ingezet TH, dat vooraf niet goedgekeurd is, überhaupt niet wordt goedgekeurd. Dit kan indien "de aard" van het TH zich, naar het oordeel van de OvJ, tegen keuring verzet (art. 21 lid 4 Bogw). In de toelichting op het Bogw is hierover het volgende opgemerkt:

"In uitzonderingsgevallen kan de keuring van een technisch hulpmiddel geheel achterwege blijven, namelijk indien de aard van het technische hulpmiddel zich naar het oordeel van de officier van justitie daartegen verzet (artikel 21, vierde lid). Van deze uitzondering zal in de praktijk niet lichtzinnig gebruik worden gemaakt. Hierbij kan worden gedacht aan de situatie van een speciaal op maat gemaakt technisch hulpmiddel. Wanneer het technische hulpmiddel specifiek is aangepast aan de omgeving waarin de inzet heeft plaatsgevonden, kan het problematisch zijn om bij een keuring dezelfde situatie na te bootsen. Met name bij op maat gemaakte software die tijdens het verrichten van onderzoekshandelingen nog moet worden aangepast aan de omstandigheden, kan het onuitvoerbaar zijn om de omstandigheden waarbinnen de inzet plaats heeft gevonden te reproduceren en het ingezette technische hulpmiddel daarop te keuren."⁴

¹ Computercriminaliteit III, *Stb.* 2018, 322.

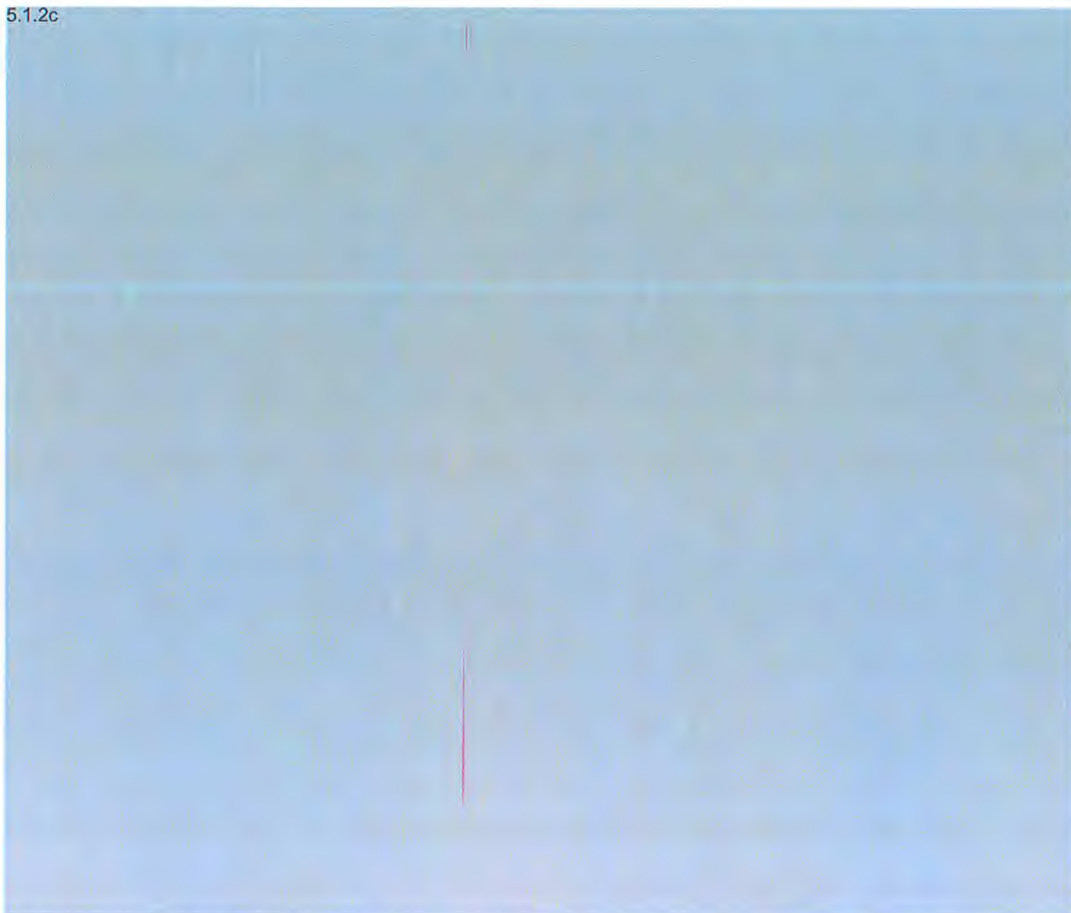
² Besluit onderzoek in een geautomatiseerd werk, *Stb.* 2018, 340.

³ Artikel 1 sub f Bogw.

⁴ Bogw, p. 45.

2. Technisch hulpmiddel 5.1.2c

5.1.2c



3. Ervaring met TH 5.1.2c in concrete opsporingsonderzoeken

5.1.2c



5.1.2c



5.1.2c



Uit de voorgaande beschrijving van TH 5.1.2c volgt dat de aard van TH 5.1.2c zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH 5.1.2c zich hoogst waarschijnlijk tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁸ Voor de keuringsdienst van de Landelijke Eenheid geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt niet gehaald door de keuringsdienst van de Landelijke Eenheid of een aangewezen keuringsdienst. 5.1.2c

5.1.2c



⁸ 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, Stcrt. nr. 10713.

Op dit moment heeft LE DIGIT geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. LE DIGIT is ook niet bekend met de beschikbaarheid van dergelijke middelen.

4. Conclusie

Gelet op het voorgaande komt de landelijk DIGIT OvJ tot de volgende oordelen:

1. De aard van TH 5.1.2c dat is ingezet in 11 opsporingsonderzoeken verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH 5.1.2c zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.
3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. LE DIGIT en LP DIGIT zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

5. Tot slot

Het voorgaande is in lijn met de besluitvorming ten aanzien van een ander TH dat door LE DIGIT in gebruik is. Die besluitvorming is in juli 2020 besproken in een Reflectiekamer van het Landelijk Parket. De landelijk DIGIT OvJ heeft daarin zijn voorgenomen besluit ex artikel 21 lid 4 Bogw ten aanzien van dat TH voorgelegd en toegelicht. De Reflectiekamer heeft zich verenigd met het voorgenomen besluit.

4 januari 2024

LP DIGIT – 5.1.2c

	Toegezonden
LP DIGIT	04- 01 -2024
Ter informatie LE DIGIT	04- 01 -2024
Ter informatie recherche OvJ LP	04- 01 -2024
Ter informatie hoofd OvJ LP	04- 01 -2024

|

|

|

|

Bijlage 1

5.1.2c



Beslissing dat TH ^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel ^{5.1.2c}

Op 4 januari 2024 is door de landelijk officier van justitie voor Digital Intrusion beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH ^{5.1.2c} zich verzette tegen keuring. TH ^{5.1.2c} is na deze beslissing – met toepassing van art. 21 lid 2 Bogw – ingezet in een aantal (nieuwe) opsporingsonderzoeken.² TH ^{5.1.2c} is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH ^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 4 januari 2024 golden ten aanzien van de aard van TH ^{5.1.2c} gelden op dit moment onverkort.

^{5.1.2c}



^{5.1.2c}



5.1.2c



Uit de voorgaande beschrijving van TH 5.1.2c volgt dat de aard van TH 5.1.2c zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH 5.1.2c zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.³ Voor de keuringsdienst van de Eenheid landelijke expertise en operaties (LX) geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt niet gehaald door de keuringsdienst van de LX of een aangewezen keuringsdienst. 5.1.2c



5.1.2c



Op dit moment heeft LX DIGIT geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. LX DIGIT is ook niet bekend met de beschikbaarheid van dergelijke middelen.

2. Conclusie

Gelet op het voorgaande komt de landelijk officier van justitie voor Digital Intrusion tot de volgende oordelen:

1. De aard van TH 5.1.2c (dat sinds de vorige beslissing ex art. 21 lid 4 Bogw is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.

³ 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, Stcrt. nr. 10713.

2. De aard van TH **5.1.2c** zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.
3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. LX DIGIT en LP DIGIT zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

29 april 2024

LP DIGIT – **5.1.2a**

	Toegezonden
LP DIGIT	29-04-2024
Ter informatie LX DIGIT	29-04-2024
Ter informatie recherche OvJ LP	29-04-2024
Ter informatie hoofd OvJ LP	29-04-2024

Bijlage 1

5.1.2c



Beslissing dat TH ^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel ^{5.1.2c}

Sinds 4 januari 2024 is door de landelijk officier van justitie voor Digital Intrusion tweemaal beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH ^{5.1.2c} zich verzette tegen keuring.² TH ^{5.1.2c} is na deze beslissing – met toepassing van art. 21 lid 2 Bogw – ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH ^{5.1.2c} is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH ^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 4 januari 2024 golden ten aanzien van de aard van TH ^{5.1.2c} gelden op dit moment onverkort.

^{5.1.2c}



^{5.1.2c}

² Na 4 januari 2024 is een dergelijke besluiten genomen op 29 april 2024.
^{5.1.2c}

5.1.2c

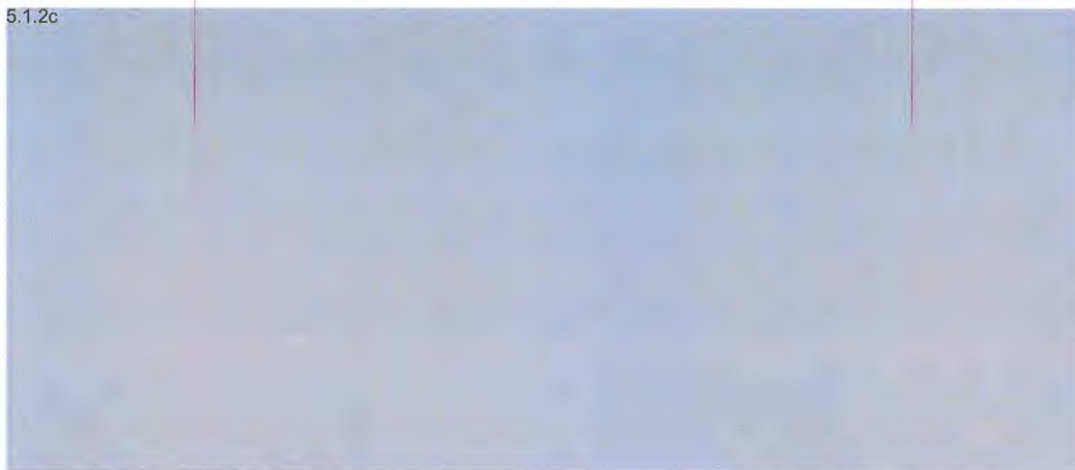


Uit de voorgaande beschrijving van TH 5.1.2c volgt dat de aard van TH 5.1.2c zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH 5.1.2c zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁴ Voor de keuringsdienst van de Eenheid landelijke expertise en operaties (LX) geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt niet gehaald door de keuringsdienst van de LX of een aangewezen keuringsdienst.

5.1.2c



Op dit moment heeft LX DIGIT geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. LX DIGIT is ook niet bekend met de beschikbaarheid van dergelijke middelen.

⁴ 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, Stcrt. nr. 10713.

2. Conclusie

Gelet op het voorgaande komt de landelijk officier van justitie voor Digital Intrusion tot de volgende oordelen:

1. De aard van TH 5.1.2c (dat sinds de vorige beslissing ex art. 21 lid 4 Bogw is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH 5.1.2c zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.
3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. LX DIGIT en LP DIGIT zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

16 juli 2024

LP DIGIT– 5.1.2e

	Toegezonden
LP DIGIT	16- 07 -2024
Ter informatie LX DIGIT	16- 07 -2024
Ter informatie recherche OvJ LP	16- 07 -2024
Ter informatie hoofd OvJ LP	16 07 -2024

Bijlage 1

5.1.2c



Beslissing dat TH ^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel ^{5.1.2c}

Sinds 4 januari 2024 is door de landelijk officier van justitie voor Digital Intrusion herhaaldelijk beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH ^{5.1.2c}) zich verzette tegen keuring.² TH ^{5.1.2c} is na deze beslissing – met toepassing van art. 21 lid 2 Bogw – ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH ^{5.1.2c} is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH ^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 4 januari 2024 golden ten aanzien van de aard van TH ^{5.1.2c} gelden op dit moment onverkort.

^{5.1.2c}



^{5.1.2c}

² Na 4 januari 2024 zijn dergelijke besluiten genomen op 29 april 2024 en 16 juli 2024.

^{5.1.2c}

5.1.2c



Uit de voorgaande beschrijving van TH 5.1.2c volgt dat de aard van TH 5.1.2c zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH 5.1.2c zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁴ Voor de keuringsdienst van de Eenheid landelijke expertise en operaties (LX) geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt niet gehaald door de keuringsdienst van de LX of een aangewezen keuringsdienst.

5.1.2c



Op dit moment heeft LX DIGIT geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. LX DIGIT is ook niet bekend met de beschikbaarheid van dergelijke middelen.

2. Conclusie

Gelet op het voorgaande komt de landelijk officier van justitie voor Digital Intrusion tot de volgende oordelen:

1. De aard van TH 5.1.2c (dat sinds de vorige beslissing ex art. 21 lid 4 Bogw is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.

⁴ 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, Stcrt. nr. 10713.

2. De aard van TH 5.1.2c zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.
3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. LX DIGIT en LP DIGIT zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

3 december 2024

LP DIGIT– 5.1.2e

	Toegezonden
LP DIGIT	03-12-2024
Ter informatie LX DIGIT	03-12-2024
Ter informatie recherche OvJ LP	03-12-2024
Ter informatie hoofd OvJ LP	03-12-2024

Bijlage 1

5.1.2c



Beslissing dat TH ^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel ^{5.1.2c}

Sinds 4 januari 2024 is door de landelijk officier van justitie voor Digital Intrusion herhaaldelijk beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH ^{5.1.2c} zich verzette tegen keuring.² TH ^{5.1.2c} is na deze beslissing – met toepassing van art. 21 lid 2 Bogw – ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH ^{5.1.2c} is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH ^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 4 januari 2024 golden ten aanzien van de aard van TH ^{5.1.2c} gelden op dit moment onverkort.



^{5.1.2c}

² Na 4 januari 2024 zijn dergelijke besluiten genomen op 29 april 2024, 16 juli 2024 en 3 december 2024.

^{5.1.2c}

5.1.2c



Uit de voorgaande beschrijving van TH 5.1.2c volgt dat de aard van TH 5.1.2c zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH 5.1.2c zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁴ Voor de keuringsdienst van de Eenheid landelijke expertise en operaties (LX) geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt niet gehaald door de keuringsdienst van de LX of een aangewezen keuringsdienst.

5.1.2c



Op dit moment heeft LX DIGIT geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. LX DIGIT is ook niet bekend met de beschikbaarheid van dergelijke middelen.

⁴ 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, Stcrt. nr. 10713.

2. Conclusie

Gelet op het voorgaande komt de landelijk officier van justitie voor Digital Intrusion tot de volgende oordelen:

1. De aard van TH 5.1.2c (dat sinds de vorige beslissing ex art. 21 lid 4 Bogw is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH 5.1.2c zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.
3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. LX DIGIT en LP DIGIT zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

24 februari 2025

LP DIGIT— 5.1.2e

	Toegezonden
LP DIGIT	24-02-2025
Ter informatie LX DIGIT	24-02-2025
Ter informatie recherche OvJ LP	24-02-2025
Ter informatie hoofd OvJ LP	24-02-2025

Bijlage 1

5.1.2c



Beslissing dat TH ^{5.1.2c} naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

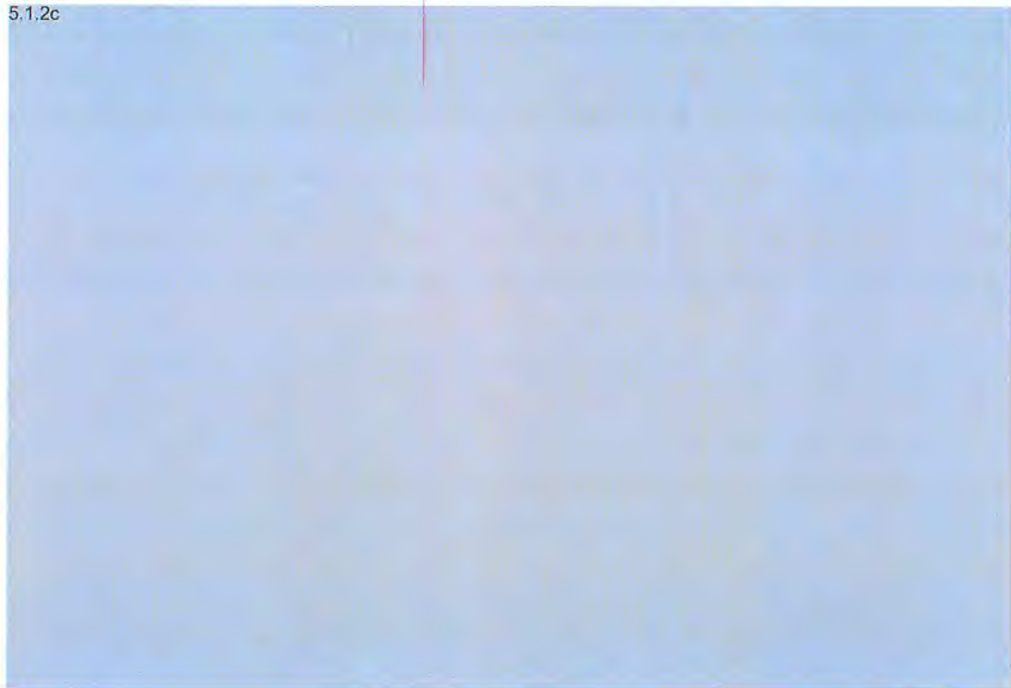
Landelijk Parket - DIGIT

1. Technisch hulpmiddel ^{5.1.2c}

Sinds 4 januari 2024 is door de landelijk officier van justitie voor Digital Intrusion herhaaldelijk beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH ^{5.1.2c}) zich verzette tegen keuring.² TH ^{5.1.2c} is na deze beslissing – met toepassing van art. 21 lid 2 Bogw – ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH ^{5.1.2c} is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH ^{5.1.2c} zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 4 januari 2024 golden ten aanzien van de aard van TH ^{5.1.2c} gelden op dit moment onverkort.

^{5.1.2c}



^{5.1.2c}

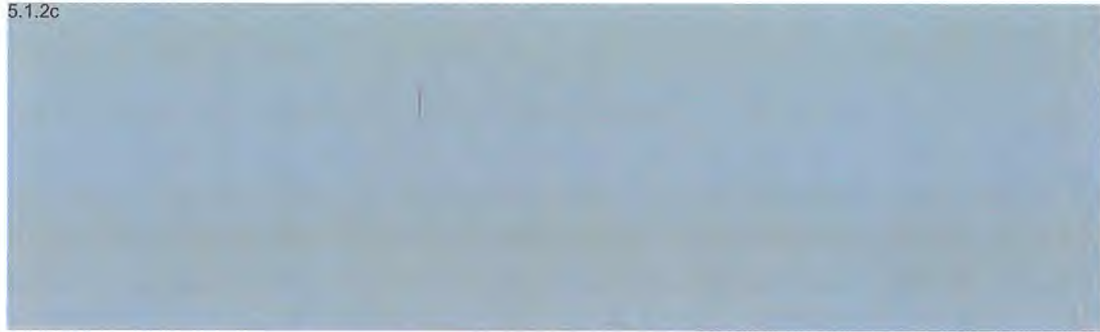


²

^{5.1.2c}



5.1.2c

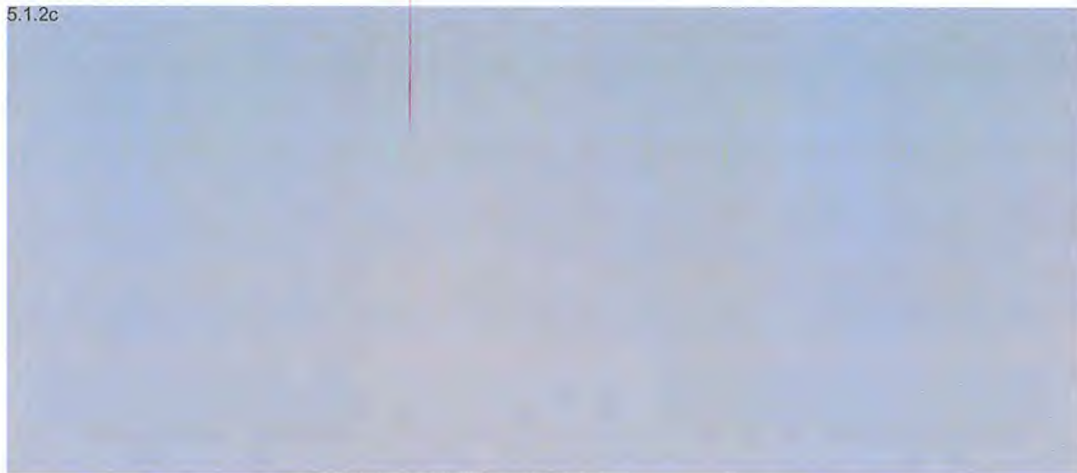


Uit de voorgaande beschrijving van TH 5.1.2c volgt dat de aard van TH 5.1.2c zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH 5.1.2c zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁴ Voor de keuringsdienst van de Eenheid landelijke expertise en operaties (LX) geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt niet gehaald door de keuringsdienst van de LX of een aangewezen keuringsdienst.

5.1.2c



Op dit moment heeft LX DIGIT geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. LX DIGIT is ook niet bekend met de beschikbaarheid van dergelijke middelen.

⁴ 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, Stcrt. nr. 10713.

2. Conclusie

Gelet op het voorgaande komt de landelijk officier van justitie voor Digital Intrusion tot de volgende oordelen:

1. De aard van TH 5.1.2c (dat sinds de vorige beslissing ex art. 21 lid 4 Bogw is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH 5.1.2c zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.
3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. LX DIGIT en LP DIGIT zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

13 mei 2025

LP DIGIT– 5.1.2c

	Toegezonden
LP DIGIT	13-5-2025
Ter informatie LX DIGIT	13-5-2025
Ter informatie recherche OvJ LP	13-5-2025
Ter informatie hoofd OvJ LP	13-5-2025

Bijlage 1

5.1.2c



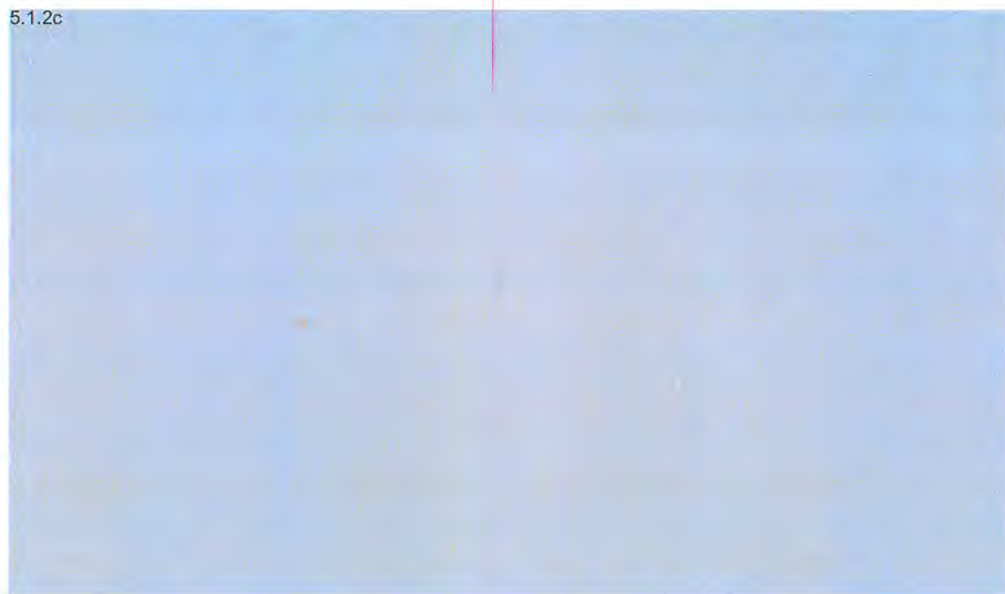
Beslissing dat TH 5.1.2c naar zijn aard niet te keuren is (ex 21 lid 4 Bogw)

Landelijk Parket - DIGIT

1. Technisch hulpmiddel 5.1.2c

Sinds 4 januari 2024 is door de landelijk officier van justitie voor Digital Intrusion herhaaldelijk beslist dat de aard van een technisch hulpmiddel (dat werd aangeduid als TH 5.1.2c) zich verzette tegen keuring.² TH 5.1.2c is na deze beslissing – met toepassing van art. 21 lid 2 Bogw – ingezet in een aantal (nieuwe) opsporingsonderzoeken.³ TH 5.1.2c is niet vooraf aan de inzet in deze opsporingsonderzoeken gekeurd. De reden hiervoor was – conform het bepaalde in art. 21 lid 2 Bogw – dat het onderzoeksbelang in deze opsporingsonderzoeken dringend vorderde dat een niet gekeurd TH werd gebruikt. Met TH 5.1.2c zijn in deze opsporingsonderzoeken, na advisering door de CTC en met toestemming van het College, onderzoekshandelingen in een geautomatiseerd werk verricht.

De overwegingen die op 4 januari 2024 golden ten aanzien van de aard van TH 5.1.2c gelden op dit moment onverkort.



5.1.2c

² Na 4 januari 2024 zijn dergelijke besluiten genomen op 29 april 2024, 16 juli 2024, 3 december 2024, 24 februari 2025 en

5.1.2c

5.1.2c

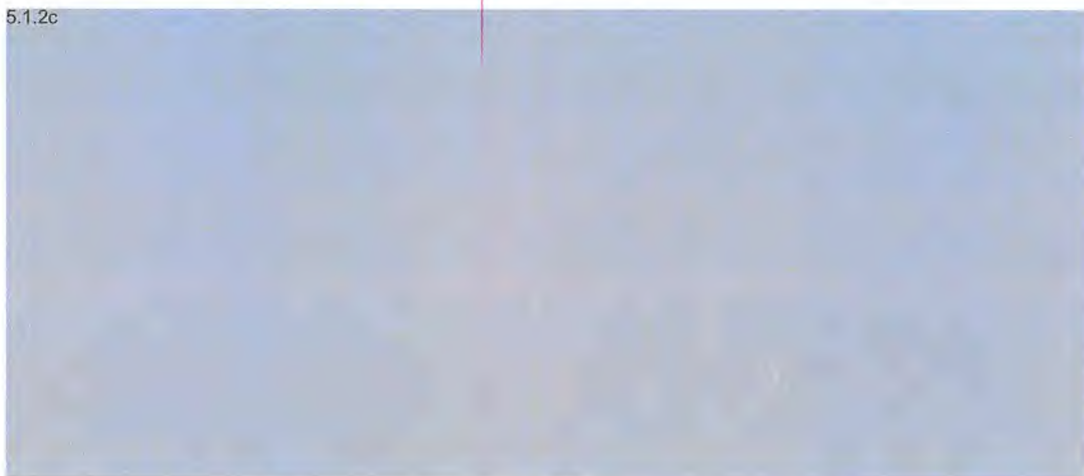


Uit de voorgaande beschrijving van TH 5.1.2c volgt dat de aard van TH 5.1.2c zich verzet tegen keuring.

Ook in toekomstige gevallen verzet de aard van het TH 5.1.2c zich hoogst waarschijnlijk nog steeds tegen keuring.

In artikel 6 van de Regeling eisen keuringsdienst technisch hulpmiddel is bepaald dat een aangewezen keuringsdienst de keuring van een TH binnen 4 weken uitvoert.⁴ Voor de keuringsdienst van de Eenheid landelijke expertise en operaties (LX) geldt geen termijn waarbinnen gekeurd moet zijn. De termijn van 28 dagen wordt niet gehaald door de keuringsdienst van de LX of een aangewezen keuringsdienst.

5.1.2c



Op dit moment heeft LX DIGIT geen beschikking over alternatieve TH's, met dezelfde noodzakelijke functionaliteiten, die een andere aard hebben en zich niet tegen keuring verzetten. LX DIGIT is ook niet bekend met de beschikbaarheid van dergelijke middelen.

⁴ 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, Stcrt. nr. 10713.

2. Conclusie

Gelet op het voorgaande komt de landelijk officier van justitie voor Digital Intrusion tot de volgende oordelen:

1. De aard van TH 5.1.2c (dat sinds de vorige beslissing ex art. 21 lid 4 Bogw is ingezet in opsporingsonderzoeken) verzet zich tegen keuring en zal daarom niet ter keuring worden aangeboden.
2. De aard van TH 5.1.2c zal zich ook in toekomstige onderzoeken hoogst waarschijnlijk verzetten tegen keuring vooraf en achteraf.
3. Gelet op het niet beschikbaar hebben van alternatieve TH's met dezelfde functionaliteiten, maar met een aard die zich niet tegen keuring verzet, en het beoogde doel van de wetgever met de bevoegdheid van art. 126nba (d.w.z. het bestrijden van ernstige vormen van computercriminaliteit of andere ernstige misdrijven), is het gebruikmaken van de uitzonderingsregel uit het Bogw te rechtvaardigen.
4. LX DIGIT en LP DIGIT zullen zich blijven inspannen om TH's met vergelijkbare functionaliteiten ter beschikking te krijgen en (vooraf) ter keuring aan te bieden.

9 juli 2025

LP DIGIT– 5.1.2e

	Toegezonden
LP DIGIT	09 - 07 - 2025
Ter informatie LX DIGIT	09 - 07 - 2025
Ter informatie recherche OvJ LP	09 - 07 - 2025
Ter informatie hoofd OvJ LP	09 - 07 - 2025

Bijlage 1

5.1.2c



Driebergen, 5 december 2019

AAN:

Departementaal vertrouwelijk / politie intern

De Inspectie Justitie en Veiligheid,

t.a.v. 5.1.2e

Hoofdinspecteur-directeur

Postbus 20301

2500 EH den Haag

Uw kenmerk: 2751664

Ons kenmerk:

Geachte 5.1.2e,

Op 19 november jl. ontving ik de resultaten van toezicht van de Inspectie op de eerste zaak van DIGIT. Graag maak ik van de gelegenheid gebruik om daarop te reageren.

DIGIT is sinds 1 maart 2019 operationeel na een lange periode van gedegen voorbereiding. De binnendringing bevoegdheid is een compleet nieuwe bevoegdheid waarin politie en bijzondere opsporingsdiensten nog geen ervaring hadden. Vanaf het moment van inwerkingtreding van de Wet CCIII en het operationeel worden van DIGIT is het opbouwen van praktijkervaring pas werkelijk begonnen. Vanwege de complexiteit van de materie en het innovatieve karakter is bewust gekozen voor een ontwikkelaanpak. Daarin is het door middel van praktijkervaring testen en toetsen, evalueren en zo nodig bijstellen van de aanpak het leidmotief. Vanzelfsprekend vormen de wettelijke eisen daarbij het kader.

We zien de feedback van de Inspectie graag vanuit dit leer- en ontwikkelperspectief. In uw brief zoomt u in op vier gebieden waarin u een aantal tekortkomingen signaleert, die zijn voorzien van 'noodzakelijke verbeteringen'. Hoewel ik er begrip voor heb dat de Inspectie als toezichtsorgaan deze onderdelen benoemt, had ik in uw rapportage graag meer balans gezien tussen verbeterpunten en de positieve aspecten die ook uit de inspecties naar voren zijn gekomen. In de gesprekken die wij met de Inspectie hadden was bij ons een evenwichtiger beeld ontstaan van sterke punten en gebieden voor verbetering.

Doordat de positieve aspecten in uw rapportage niet zijn belicht ontstaat een eenzijdig negatief beeld, wat naar mijn mening niet juist of op zijn minst onvolledig is. Ik zou het op prijs stellen als in toekomstige inspectierapporten meer balans is tussen kritiek/verbeterpunten en positieve punten. Constructieve feedback zal zeker helpen om de gewenste en deels noodzakelijke doorontwikkeling van DIGIT te bevorderen. Dan zal ik nu ingaan op de geconstateerde afwijkingen en verbeterpunten:

5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



Ik zou het dan ook op prijs stellen dat naar aanleiding van uw inspectierapport en deze brief, een vervolgesprek met u en de teamleiding van DIGIT wordt belegd waarin de teamleiding nader kan in gaan op de geconstateerde punten; de overeenkomsten en verschillen van inzicht; en de wijze waarop wij daaraan een vervolg geven.

Hoogachtend,

J.A. Van den Berg,
Chef Landelijke Eenheid



Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Dep. **VERTROUWELIJK**
Nationale politie
T.a.v. mevrouw J.A. van den Berg
Politiechef Landelijke Eenheid
Hoofdstraat 54
3972 LB Driebergen

**Inspectie Justitie en
Veiligheid**

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.inspectie-jenv.nl

contact

5.1.2e

Specialistisch inspecteur

5.1.2e

5.1.2e @inspectie-jenv.nl

Datum 29 april 2020
Onderwerp Bevindingen en aanbevelingen toezicht DIGIT zaken 2019

Ons kenmerk
2899539

*Bij beantwoording de datum
en ons kenmerk vermelden.
Wilt u slechts één zaak in uw
brief behandelen.*

Geachte mevrouw Van den Berg,

De Inspectie Justitie en Veiligheid (de Inspectie) houdt toezicht op de uitvoering van de bevoegdheid tot het binnendringen in een geautomatiseerd werk door de politie. Deze bevoegdheid is geïntroduceerd in het Wetboek van Strafvordering middels de Wet Computercriminaliteit III (Wet CCIII). Het Digital Intrusion Team (DIGIT) van uw eenheid heeft deze bevoegdheid uit de Wet CCIII in 2019 in acht zaken ingezet. Voor elk van deze zaken heeft de Inspectie onderzocht in welke mate de politie heeft gehandeld binnen de grenzen van het wettelijk kader.

Bevindingen inzet eerste zaak

Op 19 november 2019 heeft de Inspectie u per brief met kenmerk 2751664 de bevindingen en aanbevelingen van de Inspectie teruggekoppeld over het toezicht op de inzet van de bevoegdheid uit de Wet CCIII in de eerste zaak. Op 12 februari 2020 heeft de Inspectie uw schriftelijke reactie met kenmerk MS/JvdB/EvdW hierop ontvangen; dank daarvoor. In uw brief gaat u inhoudelijk in op de bevindingen en aanbevelingen van de Inspectie en verzoekt u een vervolgesprek te beleggen met de teamleiding van DIGIT. Op 18 februari 2020 heeft dit overleg plaatsgevonden. Naast de teamleiding van DIGIT en vertegenwoordigers van de Inspectie waren ook vertegenwoordigers van het Openbaar Ministerie hierbij aanwezig. In dit gesprek zijn naar aanleiding van uw brief standpunten toegelicht en opvattingen over de interpretatie van wet- en regelgeving gewisseld. De Inspectie heeft uw reactie uit de brief en de inzichten uit dit overleg meegenomen in het toezicht op de overige zaken waarin de bevoegdheid is ingezet.

Bevindingen en aanbevelingen inzetten zaken 2 tot en met 8

In deze brief geef ik u de bevindingen en aanbevelingen die de Inspectie naar aanleiding van haar toezicht heeft geformuleerd in de overige zeven zaken waarin DIGIT deze bevoegdheid in 2019 heeft ingezet. In deze brief brengt de Inspectie uitsluitend de afwijkingen van het wettelijk kader onder uw aandacht.

In verband met de vertrouwelijkheid zijn in deze brief geen zaaknamen opgenomen, maar wordt naar de zaken verwezen met een nummer. De relatie tussen zaaknamen en nummers is bekend bij de teamleiding van DIGIT.

Dep. **VERTROUWELIJK**

Pagina 1 van 7

Dep. VERTROUWELIJK

De Inspectie heeft haar belangrijkste bevindingen uit de zaken #2 tot en met #8 op 3 maart 2020 besproken met de teamleiding van DIGIT. Zij gaven aan dat geen van deze bevindingen hen onbekend voorkwam.

Bevindingen en aanbevelingen

Hieronder geeft de Inspectie haar bevindingen weer. De Inspectie heeft diverse afwijkingen en verbeterpunten geïdentificeerd, waarvan de acht belangrijkste hieronder zijn samengevat.

Inspectie Justitie en
Veiligheid
Inspectie VenJ

Datum
29 april 2020

Ons kenmerk
2899539

5.1.2c; 5.1.2i; 5.2.1



Dep. VERTROUWELIJK

Pagina 2 van 7

Dep. VERTROUWELIJK

5.1.2c; 5.1.2i; 5.2.1

Inspectie Justitie en
Veiligheid
Inspectie VenJ

Datum

29 april 2020

Ons kenmerk

2899539



Dep. VERTROUWELIJK

Pagina 3 van 7

Dep. VERTROUWELIJK

5.1.2c; 5.1.2i; 5.2.1

Inspectie Justitie en
Veiligheid
Inspectie VenJ

Datum
29 april 2020

Ons kenmerk
2899539

Dep. VERTROUWELIJK

Pagina 4 van 7

Dep. VERTROUWELIJK

5.1.2c; 5.1.2i; 5.2.1

Inspectie Justitie en
Veiligheid
Inspectie VenJ

Datum
29 april 2020

Ons kenmerk
2899539



Dep. VERTROUWELIJK

Pagina 5 van 7

Dep. VERTROUWELIJK

5.1.2c; 5.1.2i; 5.2.1



Inspectie Justitie en
Veiligheid
Inspectie VenJ

Datum
29 april 2020

Ons kenmerk
2899539

Dep. VERTROUWELIJK

Pagina 6 van 7

Dep. VERTROUWELIJK

5.1.2c; 5.1.2i; 5.2.1

Inspectie Justitie en
Veiligheid
Inspectie VenJ

Datum
29 april 2020

Ons kenmerk
2899539

Tot slot

De bevindingen zoals opgenomen in deze brief en in onze brief van 19 november 2019 betrekken wij bij het verslag van ons toezicht over 2019. Indien u in deze brief feitelijke onjuistheden in onze bevindingen signaleert of onze bevindingen anderszins voor u aanleiding geven hierop te reageren, zie ik uw reactie graag uiterlijk 15 mei 2020 tegemoet. Ik ben, indien u dat wenst, graag bereid u onze bevindingen mondeling nader toe te lichten.

Hoogachtend,
Inspecteur-generaal Inspectie Justitie en Veiligheid,
namens deze

5.1.2e

P.C.J. Neuteboom
Hoofdinspecteur-directeur

Dep. VERTROUWELIJK

Pagina 7 van 7

- Landelijke Eenheid



Adres Hoofdstraat 54
3972 LB Driebergen
Postadres 100
3970 AC Driebergen
Internet

Behandeld door 5.1.2e
Directe telefoon 088/5.1.2e
Directe fax
E-mail

Onderwerp Reactie 2^e brief toezichth. JV
Datum 18 mei 2020
Ons kenmerk
Uw kenmerk 2899539
Bijlage(n)

Departementaal vertrouwelijk / Politie
Confidentieel
De Inspectie Justitie en Veiligheid,
t.a.v. de heer dr. P.C.J. Neuteboom
Hoofdinspecteur-directeur
Postbus 20301
2500 EH Den Haag

Geachte heer Neuteboom,

Op 29 april 2020 heeft de Inspectie de bevindingen en resultaten van toezicht op de zaken 2 tot en met 8 van DIGIT toegestuurd. Graag maak ik van de gelegenheid gebruik om daarop te reageren. Eerst geef ik een algemene reactie, waarna ik puntsgewijs zal reageren op de door u genoemde acht afwijkingen en ontwikkelpunten.

U rapporteert uitsluitend over de geconstateerde afwijkingen van het wettelijk kader. Daarbij beperkt uw rapportage zich tot de constatering dat er een afwijking is, en gaat u niet in op de oorzaken of verklaringen van de afwijkingen. Hierdoor ontstaat naar mijn mening een eenzijdig en onevenwichtig beeld. Ik zou het op prijs stellen als er, in iedere geval in uw eerste openbare rapportage, meer aandacht wordt besteed aan verklaring van geconstateerde afwijkingen en wat er ter verdere ontwikkeling ondernomen is of wordt. Dit sluit aan bij de constatering van mijn vorige brief, waarin ik heb aangegeven dat wij een lerende organisatie willen zijn.

In uw rapportage worden de (werk)namen van technische hulpmiddelen (TH) met naam en toenaam genoemd. Deze namen zijn als *Politie Geheim* gerubriceerd en worden uitsluitend binnen het technisch team gehanteerd. Elke verwijzing naar de herkomst of werking van een TH in een niet-interne rapportage kan informatie verschaffen over de opsporingsmethodieken van DIGIT en dient daarom te allen tijde te worden vermeden. Ook het onderscheid tussen TH en commerciële binnendringsoftware is onwenselijk. Ik verzoek u daarom dit in uw rapportage aan te passen analoog aan de gehanteerde terminologie voor zaken.

5.1.2c; 5.1.2i; 5.2.1

Datum 18-05-2020
Blad 2 van 5

5.1.2c; 5.1.2i; 5.2.1



Datum 18-05-2020
Blad 3 van 5

5.1.2c; 5.1.2i; 5.2.1



Datum 18-05-2020
Blad 4 van 5

5.1.2c; 5.1.2i; 5.2.1



Datum 18-05-2020
Blad 5 van 5

5.1.2c; 5.1.2i; 5.2.1

Van de teamleiding van DIGIT heb ik vernomen dat er eind mei een overleg zal plaatsvinden met de Inspectie. Ik zou het op prijs stellen als tijdens dit overleg met u en de teamleiding van DIGIT wordt gesproken over de door de Inspectie benoemde ontwikkelpunten en de wijze waarop deze kunnen worden geïmplementeerd in de structurele werkwijze van DIGIT.

Hoochachtend.

5.1.2e

W.H. Woelders,
Plm Politiechef Landelijke Eenheid



Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Korpschef Nationale Politie
 Dhr. H.P. van Essen
 Postbus 17107
 2502 CC Den Haag

Inspectie Justitie en Veiligheid

Turfmarkt 147
 2511 DP Den Haag
 Postbus 20301
 2500 EH Den Haag
www.inspectie-jenv.nl

Contactpersoon

5.1.2e
 senior inspecteur

M 06 5.1.2e
 5.1.2e @inspectie-jenv.nl

Ons kenmerk
 2922044

Bijlagen
 1

*Bij beantwoording de datum
 en ons kenmerk vermelden.
 Wilt u slechts één zaak in uw
 brief behandelen.*

Datum 28 mei 2020
 Onderwerp Aanbieding concept verslag 2019 toezicht hackbevoegdheid politie
 t.b.v. wederhoor

Geachte heer Van Essen,

De Inspectie Justitie en Veiligheid (de Inspectie) heeft in 2019 onderzoek gedaan naar de toepassing van de zogenaamde hackbevoegdheid door de politie op basis van de Wet Computercriminaliteit III. Daartoe heeft de Inspectie in 2019 systematisch onderzoek uitgevoerd bij de politie. De bevindingen en conclusies van het onderzoek zijn beschreven in het bijgevoegde concept verslag toezicht hackbevoegdheid politie 2019.

Graag leg ik dit conceptverslag aan u voor om u in de gelegenheid te stellen eventuele feitelijke onjuistheden kenbaar te maken. Ik verzoek u uw reactie op te nemen in de bijgevoegde tabel. Uw reactie zie ik graag binnen twee weken, uiterlijk 15 juni 2020 tegemoet. De door u aangeleverde tabel wordt als bijlage aan het verslag toegevoegd, aangevuld met de reactie van de Inspectie op de door u genoemde punten.

Vervolgtraject

Nadat het verslag is vastgesteld, wordt u in de gelegenheid gesteld om tijdens een bestuurlijk gesprek een toelichting op het verslag te krijgen. Het verslag zal daarna aan de minister van Justitie en Veiligheid worden aangeboden. Uiterlijk zes weken na aanbieding aan de bewindspersoon wordt het verslag gepubliceerd op de website van de Inspectie.

Hoogachtend,
 Inspecteur-generaal Inspectie Justitie en Veiligheid,
 5.1.2e

P.C.J. Neuteboom
 Hoofdinspecteur Politie en Crisisbeheersing

Bijlage 1 Detailbevindingen toezicht hackbevoegdheid politie 2020

De Wet Computercriminaliteit III

De Wet CCIII verschaft de politie de bevoegdheid om onder strikte voorwaarden een geautomatiseerd werk (een apparaat zoals een laptop of smartphone) dat in gebruik is bij een verdachte heimelijk en op afstand binnen te dringen en hierin onderzoek te doen.¹ De bevoegdheid mag uitsluitend worden ingezet in geval van verdenking van een misdrijf dat een ernstige inbreuk op de rechtsorde oplevert, bij ernstige misdrijven in georganiseerd verband of bij aanwijzingen van een terroristisch misdrijf.²

Toezicht door de Inspectie Justitie en Veiligheid

De Inspectie JenV houdt toezicht op het functioneren van het wettelijk systeem rond het toepassen van de hackbevoegdheid door de politie.³ Toepassing van deze bevoegdheid vindt plaats binnen de grenzen van het bevel van de officier van justitie en de machtiging van de rechter-commissaris. De oordeelsvorming door de officier van justitie en de rechter-commissaris valt buiten de reikwijdte van het toezicht door de Inspectie JenV.

Het toezicht door de Inspectie JenV richt zich op de politie. Vooralsnog is uitvoering van de hackbevoegdheid centraal belegd bij één technisch team: het Digital Intrusion team (DIGIT) van de politie.

Aandachtsgebieden

In het wettelijk kader zijn regels opgenomen over het binnendringen en doen van onderzoek in een geautomatiseerd werk. Essentie van deze regels is te waarborgen dat het tijdens het onderzoek vergaarde bewijs betrouwbaar, integer en herleidbaar is. Concreet heeft het toezicht door de Inspectie betrekking op onder andere de volgende onderdelen:

- a) de voorbereidende activiteiten zoals het opstellen van een haalbaarheidsonderzoek en testen van het plan van aanpak;
- b) de organisatorische en personele aspecten waaronder het aanwijzen van opsporingsambtenaren, het instellen van een technisch team, vereiste screening, expertise en opleidingsniveaus;
- c) het keuringsproces en de uitgevoerde keuringen van technische hulpmiddelen door de keuringsdienst;
- d) het handelen van het technisch team binnen de kaders van het afgegeven bevel door de officier van justitie, inclusief eventuele aanvullende waarborgen en verantwoording daarover;
- e) de inzet (registratie, plaatsing, gebruik en verwijderen) van een technische hulpmiddel door het technisch team (kwaliteit en betrouwbaarheid);
- f) de vastlegging van gegevens over de toegang tot het technisch hulpmiddel, het functioneren van de technische infrastructuur en over de handelingen die worden verricht ter uitvoering van een bevel (logging) teneinde

¹ Daar waar de term "de bevoegdheid" of "hackbevoegdheid" wordt genoemd, wordt bedoeld op de bevoegdheid om een geautomatiseerd werk dat in gebruik is bij een verdachte heimelijk en op afstand binnen te dringen en hierin onderzoek te doen.

² Zie artt. 126nba, 126uba en 126zpa Wetboek van Strafvordering.

³ Zie art. 126nba, 7e lid, wetboek van Strafvordering en nota van toelichting bij het Besluit onderzoek in een geautomatiseerd werk dat op 9 oktober 2018 in het Staatsblad is gepubliceerd (Stb. 2018, nr. 340), p.23.

onregelmatigheden te kunnen vaststellen die van invloed zijn op de betrouwbaarheid en integriteit van de ter uitvoering van het bevel vastgelegde gegevens op een technische infrastructuur;

- g) de beveiliging van de logging (inzetlogging, systeemlogging en authenticatie en autorisatielogging);
- h) de beveiliging van de ter uitvoering van een bevel vergaarde gegevens die als bewijslast in een rechtszaak gebruikt kunnen worden (bewijslogging);
- i) de controle van logbestanden op onregelmatigheden en het melden van onregelmatigheden;
- j) het gebruik van de gegevens, inclusief de selectie, bewaring en vernietiging daarvan;
- k) de inzet van commerciële binnendringsoftware;
- l) Het gebruik van (onbekende) kwetsbaarheden en het melden daarvan.

De bovengenoemde onderdelen dienen ter verduidelijking van de reikwijdte van het toezicht. De Inspectie gaat in deze bijlage alleen in op de door haar geconstateerde (mogelijk) afwijkingen met betrekking tot bovengenoemde onderdelen, zonder risicoduiding en zonder in te gaan op oorzaken en (mogelijke) knelpunten in de regels en procedures. De structuur en volgorde van de hierboven genoemde onderdelen wordt niet strikt gevolgd in de volgende paragrafen.

5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2f; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2f; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1



5.1.2c; 5.1.2i; 5.2.1





Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Dep. VERTROUWELIJK / POLITIE INTERN
Nationale politie
T.a.v. mevrouw J.A. van den Berg
Politiechef Landelijke Eenheid
Hoofdstraat 54
3972 LB DRIEBERGEN

**Inspectie Justitie en
Veiligheid**

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.inspectie-jenv.nl

Contactpersoon

5.1.2e
coördinerend inspecteur

T 06 5.1.2e
5.1.2e@inspectie-jenv.nl

Ons kenmerk
3263694

Bijlagen
1

*Bij beantwoording de datum
en ons kenmerk vermelden.
Wilt u slechts één zaak in uw
brief behandelen.*

Datum 22 maart 2021
Onderwerp Bevindingen Inspectie toezicht op CCIII in 2020

Geachte mevrouw Van den Berg,

De Inspectie Justitie en Veiligheid (de Inspectie) houdt toezicht op de uitvoering van de bevoegdheid tot het heimelijk en op afstand binnendringen en doen van onderzoek in een geautomatiseerd werk door de politie. Deze bevoegdheid is geïntroduceerd in het Wetboek van Strafvordering middels de Wet Computercriminaliteit III (Wet CCIII) en wordt in de volksmond de 'hackbevoegdheid' genoemd.

Evenals in 2019, heeft de Inspectie ook in 2020 onderzoek verricht naar de toepassing van deze wettelijke hackbevoegdheid door de politie. In deze brief met bijlage informeert de Inspectie u over (mogelijke) afwijkingen van het wettelijk kader¹ en de afgegeven bevelen, zonder risicoduiding en zonder in te gaan op oorzaken en (mogelijke) knelpunten in dit wettelijk kader. In deze brief benoemt, concretiseert en illustreert de Inspectie haar bevindingen. De Inspectie legt middels deze brief haar bevindingen ter validatie voor, zodat u ons kunt wijzen op eventuele feitelijke onjuistheden hierin.

Deze bevindingen worden betrokken in het Verslag over 2020. Hierin geeft de Inspectie een conclusie en totaalbeeld van de door haar uitgevoerde activiteiten en bevindingen bij het toezicht op de toepassing van de wettelijke hackbevoegdheid door de politie in 2020. Nadat een conceptversie van het Verslag voor wederhoor is voorgelegd aan de korpschef, wordt het Verslag door de Inspectie vastgesteld en aangeboden aan de minister.

Reikwijdte en operationele afstemming van uitgevoerd toezicht in 2020

In 2020 heeft het Digital Intrusion Team (DIGIT) van uw eenheid de hackbevoegdheid in 14 zaken ingezet. Voor elk van deze zaken heeft de Inspectie onderzocht in welke mate de politie heeft gehandeld binnen de grenzen van het wettelijk kader en het bevel van de officier van justitie.

¹ Zoals vastgelegd in wet- en regelgeving en in verslagen van in parlementaire behandelingen.

Tevens heeft de Inspectie onderzoek verricht naar de keuring van technische hulpmiddelen zoals bedoeld in het Besluit onderzoek in een geautomatiseerd werk (hierna: Besluit of: Bogw).² De aangewezen keuringsdienst (TNO) heeft samen met de keuringsdienst van de Landelijke Eenheid in 2020 zes keuringen uitgevoerd van 3 verschillende technische hulpmiddelen.

De Inspectie heeft de bevindingen die betrekking hebben op DIGIT op 4 februari 2021 op hoofdlijnen besproken met de teamleiding van DIGIT. Daarnaast heeft ze op 11 januari 2021 met TNO en de keuringsdienst gesproken over de bevindingen die op hen betrekking hebben. Zowel de teamleiding van DIGIT als TNO en de keuringsdienst hebben aangegeven onze met hen gedeelde bevindingen te herkennen.

Toepassing hackbevoegdheid politie 2020 in aantallen

Onderwerp	Aantal
Totaal aantal zaken waarin de politie bevel(en) heeft gekregen tot inzet van de wettelijke hackbevoegdheid in 2020	14 ³
Zaken waarin bevel is gegeven voor de inzet van een vooraf goedgekeurd technisch hulpmiddel	1 van 14
Zaken waarin bevel is gegeven voor de inzet van een niet vooraf gekeurd technisch hulpmiddel	11 van 14
Zaken waarin bevel is gegeven voor het verrichten van onderzoekshandelingen zonder technisch hulpmiddel ⁴	3 van 14
Zaken waarin commerciële binnendringsoftware is ingezet	10 van 14
Zaken waarin door de politie aangetroffen onbekende kwetsbaarheden zijn gebruikt	0 van 14
Aantal goedgekeurde technische hulpmiddelen	2 van 3

Bevindingen Inspectie 2020

De Inspectie haalt in deze brief de hieronder genoemde hoofdthema's naar voren. De bijlage bij deze brief bevat een overzicht van alle (mogelijke) afwijkingen van het wettelijk kader.

Verrichte handelingen versus reikwijdte bevelen

In 2020 is de politie vier keer binnengedrongen in een geautomatiseerd werk waarvan het unieke kenmerk niet correspondeerde met het kenmerk dat was opgenomen in het bevel. Twee van deze vier afwijkingen zijn direct door de politie signaleerd. In deze gevallen heeft de politie niet actief onderzoekshandelingen verricht. In twee gevallen heeft de politie dit niet geconstateerd en heeft zij onderzoekshandelingen verricht en gegevens vastgelegd. Nadat de Inspectie de politie hierop heeft gewezen, is dit volgens DIGIT nader onderzocht en gemeld bij het tactisch team.

² Dit besluit is op 9 oktober 2018 in het Staatsblad gepubliceerd (Stb. 2018, nr. 340).

³ Waarvan in een van deze zaken het bevel tot inzet van de bevoegdheid reeds is ingegaan in 2019.

⁴ In één zaak kunnen zowel bevelen afgegeven zijn voor het verrichten van onderzoekshandelingen met als zonder technisch hulpmiddel.

Logging

Het Besluit schrijft voor dat elektronische verslaglegging plaatsvindt over de uitvoering van een bevel, ook wel logging genoemd. Op basis van deze logging dient te kunnen worden vastgesteld of gegevens die kunnen dienen als bewijs in een strafzaak, betrouwbaar en integer zijn. Ook de gegevens zelf die kunnen dienen als bewijs in een strafzaak vallen onder het begrip logging. Het Besluit stelt betrouwbaarheidseisen aan de inrichting en het gebruik van deze logging. De Inspectie stelt onder meer vast dat:⁵

- de logging van verrichte handelingen onvolledig is voor alle zaken waarin in 2020 onderzoekshandelingen zijn verricht;
- nog niet door de politie is uitgewerkt hoe per zaak invulling wordt gegeven aan de vereiste doorlopende en automatische vastlegging van gegevens in logbestanden;
- niet aantoonbaar is dat logging zodanig is ingericht dat onregelmatigheden vastgesteld kunnen worden.

Inzet commerciële binnendringsoftware en hieraan gekoppeld technisch hulpmiddel

In 2020 is in 10 zaken commerciële binnendringsoftware gebruikt in combinatie met een technisch hulpmiddel waarmee onderzoek is verricht. Dit technisch hulpmiddel was niet vooraf gekeurd. Op 5 oktober 2020 heeft het Openbaar Ministerie (OM) bepaald dat de aard van dit technisch hulpmiddel zich verzet tegen keuring.

De Inspectie stelt vast dat dit middel en de toepassing hiervan op de volgende punten afwijkt van het wettelijk kader:

- Het technisch hulpmiddel voldoet niet aan de technische eisen uit het Besluit;⁶
- De leverancier van het technisch hulpmiddel heeft toegang tot het technisch hulpmiddel en daarmee mogelijk toegang tot bewijslogging;
- Omdat de aard van dit technisch hulpmiddel zich volgens het OM verzet tegen keuring, moeten aanvullende waarborgen zijn getroffen in de zaken waarin dit is ingezet. Het is niet duidelijk welke aanvullende waarborgen in deze zaken zijn getroffen.
- De politie kan niet aantonen dat elke inzet van de binnendringsoftware vooraf op een zo representatief mogelijke testomgeving is gecontroleerd;
- Hergebruik van de licenties voor de binnendringsoftware is mogelijk.

Interne processen

De Inspectie stelt vast dat interne processen veelal nog niet op het niveau van volwassenheid zijn dat wordt verondersteld in het wettelijk kader. De Inspectie stelt onder meer vast dat de politie in 2020:

- niet alle vereiste documenten⁷ heeft opgesteld en in haar dossiers heeft opgenomen;
- niet beschikte over een goed functionerende interne controle op de naleving van het wettelijk kader.

⁵ Zie de bijlage bij deze brief voor het totaaloverzicht van vaststellingen.

⁶ Hoofdstuk 5 Bogw.

⁷ Zoals (definitieve versies van) aanwijzingsbesluiten, haalbaarheidsonderzoeken, plannen van aanpak en processen-verbaal.

Tot slot

Hierbij geef ik u de gelegenheid om eventuele feitelijke onjuistheden in deze brief en bijlage aan mij terug te geven. Ik zie uw schriftelijke reactie graag uiterlijk op 9 april 2021 tegemoet. Ik ben, indien u dat wenst, graag bereid onze bevindingen mondeling nader toe te lichten.

Hoogachtend,
Inspecteur-generaal Inspectie Justitie en Veiligheid,
namens deze,

5.1.2e

Hoofdinspecteur-directeur

Bijlage

- Bevindingen toezicht hackbevoegdheid politie 2020



Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Korpschef Nationale Politie
Dhr. H.P. van Essen
Postbus 17107
2502 CC Den Haag

**Inspectie Justitie en
Veiligheid**

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.inspectie-jenv.nl

Contactpersoon

5.1.2e
senior inspecteur

M 06 5.1.2e
5.1.2e @inspectie-jenv.nl

Ons kenmerk
3316913

Bijlagen
2

*Bij beantwoording de datum
en ons kenmerk vermelden
Wilt u slechts één zaak in uw
brief behandelen*

Datum 4 mei 2021

Onderwerp Aanbieding concept verslag 2020 toezicht hackbevoegdheid politie
t.b.v. wederhoor

Geachte heer Van Essen,

De Inspectie Justitie en Veiligheid (de Inspectie) houdt toezicht op de uitvoering van de bevoegdheid tot het heimelijk en op afstand binnendringen en doen van onderzoek in een geautomatiseerd werk door de politie. Deze bevoegdheid is in maart 2019 geïntroduceerd in het Wetboek van Strafvordering middels de Wet Computercriminaliteit III (Wet CCIII) en wordt in de volksmond de 'hackbevoegdheid' genoemd.

Evenals in 2019, heeft de Inspectie ook in 2020 systematisch onderzoek verricht naar de toepassing van deze wettelijke hackbevoegdheid door de politie. Op 22 maart 2021 is door mij een brief met daarin de gedetailleerde bevindingen van het uitgevoerde onderzoek ter validatie voorgelegd aan de politiefchef van de Landelijke Eenheid. Tot op heden heb ik daarop geen formele reactie mogen ontvangen. Informeel heeft de Inspectie via haar contactpersonen bij het met de uitvoering van de hackbevoegdheid belaste team vernomen dat deze detailbevindingen herkend worden. De detailbevindingen zijn door de Inspectie betrokken in het voorliggende conceptverslag over 2020.

In het bijgevoegde conceptverslag *toezicht wettelijke hackbevoegdheid politie 2020* geeft de Inspectie een totaalbeeld van de bevindingen en conclusies van het onderzoek.

Graag leg ik dit conceptverslag aan u voor om u in de gelegenheid te stellen eventuele feitelijke onjuistheden kenbaar te maken. Ik verzoek u uw reactie op te nemen in de bijgevoegde tabel (bijlage 2). Uw reactie zie ik graag binnen twee weken, uiterlijk 19 mei 2021 tegemoet. De door u aangeleverde tabel wordt als bijlage aan het verslag toegevoegd, aangevuld met de reactie van de Inspectie op de door u genoemde punten.

Voor de volledigheid wil ik u melden dat het bijgevoegde conceptverslag gelijktijdig door ons onderhands verstrekt zal worden aan onze contactpersonen bij DIGIT en de keuringdienst van de Landelijke Eenheid zodat zij hier direct kennis van kunnen nemen.

Vervolgtraject

Nadat het verslag is vastgesteld, wordt u in de gelegenheid gesteld om tijdens een bestuurlijk gesprek een toelichting op het verslag te krijgen. Het verslag zal aan de minister van Justitie en Veiligheid worden aangeboden. Uiterlijk zes weken na aanbidding aan de bewindspersoon wordt het verslag gepubliceerd op de website van de Inspectie.

Met vriendelijke groet,
Inspecteur-generaal Inspectie Justitie en Veiligheid,
namens deze,

5.1.2e

*Hoofdinspecteur-directeur***Inspectie Justitie en
Veiligheid****Datum**
4 mei 2021**Ons kenmerk**
3316913

Bijlage 1: Conceptverslag toezicht wettelijke hackbevoegdheid politie 2020
Bijlage 2: Hoor- en wederhoor tabel

Onderwerp
Wederhoor conceptverslag wet
CCIII

Inspectie Justitie en Veiligheid
t.a.v. mevrouw 5.1.2e ,
hoofdinspecteur Politie en Crisisbeheersing
Postbus 20301
2500 EH Den Haag

Organisatieonderdeel
Korpsstaf

Geachte mevrouw 5.1.2e ,

Behandeld door
5.1.2e

Bedankt voor de gelegenheid om te reageren op het conceptverslag *toezicht wettelijke hackbevoegdheid politie 2020*. We hebben het conceptverslag met interesse gelezen. In de bijlage van deze brief vindt u de ingevulde tabel voor hoor en wederhoor. Naar aanleiding van het concept verslag, zijn er enkele algemene overwegingen die wij (naast de tabel met wederhoor) aan u willen meegeven.

Telefoon

Rol van de Inspectie versus die van het Openbaar ministerie

E-mail
5.1.2e @politie.nl

Na invoering van de Wet Computercriminaliteit III hebben de (bijzondere) opsporingsdiensten de bevoegdheid gekregen om geautomatiseerde werken op afstand heimelijk binnen te kunnen dringen om daar onderzoek te doen. Deze bevoegdheid is nader uitgewerkt in het Besluit onderzoek in een geautomatiseerd werk (Bogw). De FIOD, KMar, politie en Bijzondere Opsporingsdiensten hebben deze bevoegdheid centraal belegd bij het Digital Intrusion Team (DIGIT).

Ons kenmerk
2021-0031564

Tijdens dit wetgevingstraject is er een theoretisch kader opgesteld dat niet altijd aansluit bij wat in de praktijk gevraagd wordt. Dat wekt geen bevreemding; de praktijk is zelden geheel te vatten in theoretische kaders. Dat dwingt de officier van justitie, die leiding geeft aan de onderzoeken bij DIGIT, dan ook om in gevallen te handelen in de geest van de huidige wet- en regelgeving en daarbij soms afwijkend van het theoretisch kader. Uiteraard gebeurt dit altijd in overeenstemming met de landelijke DIGIT officier.

Datum
26 mei 2021

Omdat de Inspectie (mogelijke) afwijkingen constateert zonder in te gaan op oorzaken en mogelijke knelpunten in het wettelijk kader, ontstaat er soms een onevenwichtig beeld. De geschetste situatie in het conceptverslag doet daarmee geen recht aan de juridische en technische complexiteit waarin DIGIT dagelijks opereert.

Bijlage(n)
1

Tevens oordeelt de Inspectie in haar conceptverslag over het inzetten van een niet vooraf gekeurd technisch hulpmiddel. Aan het besluit om een niet vooraf gekeurd technisch hulpmiddel in te zetten, gaat altijd de beoordeling van de officier van justitie vooraf of het middel voldoet aan de eisen die in het Bogw gesteld worden. De politie constateert dat er op het gebied van keuringen een verschil van inzicht bestaat tussen Inspectie en OM over wat wanneer gekeurd moet worden. De politie stelt voor dat Inspectie hierover in gesprek gaat met het OM.

Pagina
1

Ondersteun het lerend vermogen DIGIT

DIGIT is sinds twee jaar operationeel. Vanuit de gekozen ontwikkelaanpak stond het opbouwen van praktijkervaring in het eerste jaar centraal. In het tweede jaar heeft DIGIT zich ingespannen om het team verder uit te breiden en te professionaliseren met de ervaringen en inzichten die in het eerste jaar zijn opgedaan. Het team doet nog met grote regelmaat nieuwe inzichten op die van invloed zijn op de operationele werkwijze.

In het conceptverslag van de Inspectie wordt het spanningsveld zichtbaar tussen het beoordelingskader van de Inspectie (en de mate van volwassenheid die daarbij verwacht wordt) in relatie tot het relatief korte bestaan van DIGIT. Alhoewel DIGIT in 2020 diverse verbeteringen heeft doorgevoerd, beperkt de huidige capaciteit van DIGIT deels het verbeteringsproces. Om het lerend vermogen van DIGIT te ondersteunen, zouden diverse algemene conclusies en standpunten nader onderbouwd kunnen worden.

Bestuurlijk gesprek

Tot slot, net als vorig jaar is er de wens om te komen tot een bestuurlijk gesprek om te praten over de samenwerking tussen beide partijen en over hoe de Inspectie de rol van toezichthouder invult.

Hoogachtend,

5.1.2e ,
lid korpsleiding



Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Korpschef Nationale Politie
De heer H.P. van Essen
Postbus 17107
2502 CC DEN HAAG

**Inspectie Justitie en
Veiligheid**

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.inspectie-jenv.nl

Contactpersoon

5.1.2e
Senior Inspecteur

M 06 **5.1.2e**
5.1.2e @inspectie-jenv.nl

Ons kenmerk
3364303

Bijlagen
2

*Bij beantwoording de datum
en ons kenmerk vermelden.
Wilt u slechts één zaak in uw
brief behandelen.*

Datum 2 juni 2021

Onderwerp Aanbieding Verslag toezicht wettelijke hackbevoegdheid politie 2020

Geachte heer Van Essen,

De Inspectie Justitie en Veiligheid (de Inspectie) heeft, evenals in 2019, ook in 2020 onderzoek gedaan naar de toepassing van de hackbevoegdheid door de politie op basis van de Wet Computercriminaliteit III. Daartoe heeft de Inspectie in 2020 onderzoek uitgevoerd bij de politie. U bent in de wederhoorfase van het Verslag in de gelegenheid gesteld eventuele feitelijke onjuistheden kenbaar te maken, waar u ook gebruik van heeft gemaakt.

Het Verslag is inmiddels vastgesteld en aangeboden aan de minister van Justitie en Veiligheid. Graag bied ik u hierbij het Verslag aan. Ook heb ik onze reactie op uw wederhoorreactie bijgevoegd.

Vervolgtraject

Ik ben vanzelfsprekend bereid om het Verslag toe te lichten. Naar aanleiding van uw verzoek zal ik een afspraak maken voor een bestuurlijk gesprek via uw secretariaat. Het Verslag wordt samen met de wederhoortabel, conform de Aanwijzingen van de minister-president inzake rijksinspecties, uiterlijk zes weken na aanbieding aan de bewindspersoon gepubliceerd op de website van de Inspectie.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

5.1.2e

H.C.D. Korvinus
Inspecteur-generaal Inspectie Justitie en Veiligheid



Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Korpschef Nationale Politie
Dhr. H.P. van Essen
Postbus 17107
2502 CC Den Haag

**Inspectie Justitie en
Veiligheid**

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.inspectie-jenv.nl

Contactpersoon

5.1.2e

M 06 5.1.2e
5.1.2e @inspectie-jenv.nl

Projectnaam
Toezicht CCIII

Ons kenmerk
3909839

Bijlagen
2

*Bij beantwoording de datum
en ons kenmerk vermelden.
Wilt u slechts één zaak in uw
brief behandelen.*

Datum 15 maart 2022

Onderwerp Aanbieding conceptverslag toezicht wettelijke hackbevoegdheid politie
2021 t.b.v. wederhoor

Geachte heer Van Essen,

De Inspectie Justitie en Veiligheid (de Inspectie) houdt toezicht op de uitvoering van de bevoegdheid tot het heimelijk en op afstand binnendringen en doen van onderzoek in een geautomatiseerd werk door de politie. Deze bevoegdheid wordt in de media de 'hackbevoegdheid' genoemd.

De Inspectie heeft inmiddels voor de derde keer onderzoek verricht naar de toepassing van deze wettelijke hackbevoegdheid door de politie. In het bijgevoegde conceptverslag *toezicht wettelijke hackbevoegdheid politie 2021* geeft de Inspectie een totaalbeeld van de bevindingen en conclusies van het onderzoek. De Inspectie rapporteert in dit verslag over de periode 1 januari 2021 tot en met 31 december 2021.

Graag leg ik dit conceptverslag aan u voor om u in de gelegenheid te stellen eventuele feitelijke onjuistheden kenbaar te maken. Ik verzoek u uw reactie op te nemen in de bijgevoegde tabel (bijlage 2). Uw reactie zie ik graag binnen twee weken, uiterlijk 31 maart 2022 tegemoet. De door u aangeleverde tabel wordt als bijlage aan het verslag toegevoegd, aangevuld met de reactie van de Inspectie op de door u genoemde punten. Voor eventuele vragen kunt u contact opnemen met 5.1.2e. Contactgegevens zijn hierboven vermeld.

Voor de volledigheid wil ik u melden dat het bijgevoegde conceptverslag gelijktijdig door ons verstrekt zal worden aan onze contactpersonen bij DIGIT en de keuringdienst van de Landelijke Eenheid zodat zij hier direct kennis van kunnen nemen.

Vervolgtraject

Na ontvangst van de ingevulde wederhoortabel kan, indien u dit wenst, een bestuurlijk gesprek plaatsvinden waarin de inspecteur-generaal van de Inspectie het verslag nader toelicht. Ook uw reactie op het verslag kan in dit gesprek worden betrokken.

Na verwerking van uw wederhoorreactie wordt het verslag vastgesteld in het MT van de Inspectie. Vervolgens zal het verslag aan de minister van Justitie en

Veiligheid worden aangeboden. Uiterlijk zes weken na aanbieding aan de minister wordt het verslag gepubliceerd op de website van de Inspectie.

Met vriendelijke groet,

5.1.2e



H.C.D. Korvinus

Inspecteur-generaal Inspectie Justitie en Veiligheid

Bijlage 1: Conceptverslag toezicht wettelijke hackbevoegdheid politie 2021

Bijlage 2: Hoor- en wederhoor tabel

OPENBAAR MINISTERIE

Aan Gerrit van der Burg
Kopie aan 5.1.2e , 5.1.2e
Van 5.1.2e
Doorkiesnummer(s) 06 – 5.1.2e
Datum 2 mei 2022
Onderdeel B&S PaG
Onderwerp Bestuurlijk overleg aanbieding verslag toezicht
wettelijke hackbevoegdheid politie 2021

Memo

Dag Gerrit,

Hierbij een korte annotatie voor het bestuurlijk overleg van 4 mei over het verslag toezicht wettelijke bevoegdheid 2021. Het overleg is op verzoek van de inspectie ingepland. Er is geen agenda opgesteld.

Zowel 5.1.2e , 5.1.2e en ik zullen aansluiten bij het overleg. De anno is voor het grootste deel gebaseerd op een notitie van 5.1.2e die als landelijk officier voor Digital Intrusion (DIGIT) goed zicht heeft op de gang van zaken rondom dit thema.

Op pp. 4-7 van deze anno heb ik het verslag van het bestuurlijk overleg uit 2021 opgenomen. In de bijlagen van de mail zijn de uitnodiging, het verslag en de wederhoortabel te vinden.

Groet,

5.1.2e

1 Belangrijkste gesprekspunten

Vanuit de landelijk officier DIGIT worden onderstaande punten aangedragen voor het gesprek. Deze worden in de anno nader toegelicht.

1. Je kunt in het bestuurlijk overleg aangeven dat we blij zijn met de evenwichtigere wijze van verslaglegging.
2. Daarnaast kun je benoemen dat we tevreden zijn dat de wederzijdse inspanningen om te komen tot een heldere afbakening tussen taken/rollen. Dit heeft geleid tot een verslag waarin nagenoeg geen conflicterende situaties bestaan.

2 Aanleiding

Op 4 mei 2022 vindt er een bestuurlijk overleg plaats over het verslag van de Inspectie J&V m.b.t. inzet van de hackbevoegdheid (art. 126nba Sv) door de politie in 2021. Dit verslag ligt op dit moment bij het departement van J&V voor het voorbereiden van een beleidsreactie van de minister. Vanuit het departement plant men om de beleidsreactie en het verslag uiterlijk vrijdag 27 mei 2022 openbaar te maken.

Het LP (landelijk officier voor Digital Intrusion, senior adviseur en strategisch beleidsadviseur) hebben de politie van input voorzien voor de wederhoor tabel. Deze wordt samen met het verslag openbaar gemaakt.

Er zal vanuit het LP (in samenspraak met het PaG) en politie ook input worden geleverd aan het departement voor de (concept) beleidsreactie.

3 Korte reactie op het verslag

Het verslag van de inspectie over 2021 bevat geen onverwachte resultaten of conclusies. De landelijk officier DIGIT verwacht n.a.v. dit verslag geen problemen voor concrete onderzoeken / strafzaken.

Anders dan de voorgaande verslagen (over 2019 en 2020) hanteert de inspectie dit jaar een wijze van verslaglegging die een evenwichtiger beeld schetst van de manier waarop de politie uitvoering geeft aan de hackbevoegdheid. Er wordt niet enkel meer gekeken naar hetgeen niet volledig compliant is, maar er worden steeds inleidend daaraan zaken beschreven die wel al (deels) gerealiseerd zijn.

Het meest in het oog springende punt in dit verslag zijn de constatering en opmerkingen over het gebruik van commerciële software. Het College is over (de besluitvorming rond) de inzet van deze software in 2020 al geïnformeerd. Ik citeer uit het voorwoord, de resultaten en de conclusie van het verslag:

- *Op enkele onderwerpen, waaronder de inzet van commerciële binnendringsoftware en technische hulpmiddelen, signaleer ik spanning tussen de wettelijke kaders en de uitvoeringspraktijk. Het is van belang dat – mede in het licht van de evaluatie van de Wet CCIII – hier aandacht aan wordt besteed. Het WODC doet hier momenteel onderzoek naar. (p. 3 verslag toezicht, voorwoord)*
- *Net als in 2020 heeft de politie in het merendeel van de zaken gebruik gemaakt van commerciële software. Voor zowel de politie als de Inspectie is deze software een 'black box'. Het kenmerk van een 'black-box' is dat de resultaten zichtbaar zijn maar voor de gebruiker*

niet bekend is hoe de software precies werkt. Hoewel in een addendum bij het contract procedurele afspraken zijn gemaakt met de leverancier, is technisch niet afdwingbaar en controleerbaar wat de leverancier van deze software precies op welk moment doet. De leverancier kan daarbij mogelijk ook toegang verkrijgen tot de tijdens een inzet met deze software verkregen gegevens. De Inspectie heeft er begrip voor dat deze software in het belang van de opsporing wordt ingezet, maar signaleert dat hierdoor spanning ontstaat met het rechtskader. In het rechtskader is namelijk aangegeven dat de verkregen gegevens uitsluitend toegankelijk mogen zijn voor de door de korpschef aangewezen ambtenaren. Zie hoofdstuk A.4 voor de detailbevindingen (p.8, verslag toezicht, resultaten van het onderzoek).

- *Net als in 2020 heeft de politie in 2021 in het merendeel van de zaken commerciële software ingezet waarbij de leverancier toegang heeft, zonder dat dit technisch door de politie kan worden gecontroleerd en beperkt. Tegelijkertijd concludeert de Inspectie dat het gebruik van deze software spanning geeft met het rechtskader (p.8, verslag toezicht, conclusie).*

4 Toezicht Inspectie vs. gezag officier van justitie

In de verslagen over 2019 en 2020 kwam naar voren dat de inspectie op een aantal punten oordelen gaf die de besluitvorming van de officier van justitie betroffen. De inspectie trad daarmee buiten haar taak / opdracht bij het houden van toezicht. In het bestuurlijk gesprek tussen de inspecteur generaal van de inspectie en de voorzitter van het College van 21 juni 2021 (over toezicht jaar 2020) is op dat punt uitgebreid stilgestaan (zie OM verslag in bijlage – pp. 4-7).

De gesprekken tussen LP en de betrokken inspecteurs zijn na juni 2021 iets geïntensiveerd. De inspecteurs zijn nog meer meegenomen in de wijze waarop het OM functioneert en de manier waarop het OM als het gezag van de opsporing de (toezichthoudende) rol op de politie vorm geeft. Daarnaast is duidelijker vastgelegd welke kaders door de landelijk officier DIGIT aan de politie zijn gesteld.

De inspectie heeft in 2021 veel werk gestoken in het opstellen / formaliseren van een toetsingskader aan de hand waarvan ze hun toezicht uitvoeren. Ze hebben (concepten) van dit kader met het OM gedeeld en input gevraagd bij het opstellen om helder te krijgen hoe de afbakening tussen rollen er uit zou moeten zien. De definitieve versie van dit kader wordt op korte termijn met de politie besproken en daarna met OM gedeeld.

In het verslag over 2021 komt de afbakening tussen de rol van de inspectie en het Openbaar Ministerie (OM) duidelijker naar voren. Anders dan in het verslag over 2020 begeeft de inspectie zich nagenoeg niet meer op het terrein waarin het OM het gezag over de opsporing voert. Op twee punten waar het nog enigszins wringt (zie nrs. 11 en 17 in de wederhoortabel) heeft de inspectie hun verslag zodanig verduidelijkt of aangevuld dat het in optiek van de landelijk officier DIGIT acceptabel is.

Tot slot is het goed om te weten dat de het DIGIT team van de politie zich meer kan richten op de 'eigenlijke DIGIT-taken'. In voorgaande jaren dreigde die soms 'onder te sneeuwen' door de 'verantwoordingsdruk' vanuit de inspectie (vrij samengevat). De politie heeft zich daar zakelijker in opgesteld.

5 OM intern verslag bestuurlijk gesprek inspectie inzake de hackbevoegdheid

Deelnemers inspectie: Henk Korvinus, Angela van der Putten, 5.1.2e , 5.1.2e

Deelnemers OM: Gerrit van der Burg, 5.1.2e , 5.1.2e

Henk: Algemene introductie. Inspectie wil graag spreken over de lijn die wordt gezien. Inspectie kijkt naar de taakuitvoering van de politie en PG Hoge Raad naar die van het OM. Het inspectieverslag is een opmaat naar de evaluatie van de wet op de hackbevoegdheid. Deze wet is ingegeven door wantrouwen vanuit het parlement voor het toekennen van deze bevoegdheid. Het zou technisch neutraal moeten zijn, maar praktijk lijkt anders.

Gerrit: waardering voor het initiëren van dit overleg. Goed om nog eens te kijken waar inspectie en OM voor staan. Er is een trend waarneembaar dat politie en OM in de gezagsrol aan het zoeken zijn naar de invulling van de wet. Wat opvalt in het verslag is:

- Er wordt vooral benadrukt wat nog niet volledig geregeld is. Dingen die wel goed op stoom zijn worden weggelaten. Daar maakt het OM zich zorgen over. Door disbalans in wat wel/niet goed gaat wordt geen recht gedaan aan de inspanningen van de politie.
- Wat OM ook steeds in ogen houdt is dat het een nieuwe wet betreft waar in de uitvoering ook tegen allerlei elementen wordt aangelopen waar oplossingen voor moeten worden bedacht.
- Inspectie kan inderdaad niet naar het OM kijken, maar we zien dat er wel

tegenaan wordt geschurkt. Het is niet aan de inspectie om een uitspraak over de gezagsrol van het OM te doen. Er zijn verscheidene voorbeelden in het verslag waar dit uit blijkt. Daar kan ook afzonderlijk nog het gesprek over worden gevoerd.

- Dat als eerste opmerkingen onder de waardering van het werk dat door de inspectie is verricht. Ook fijn dat de inspectie contact onderhoudt met de PG Hoge Raad.

5.1.2e De blik van de inspectie op de bedrijfsvoering van DIGIT stelt het OM in staat om e.e.a. aan te scherpen. Het is weliswaar zoeken waar de signalerende rol van de inspectie stopt en waar het OM verder gaat. De gezagsrol van het OM wordt nu in het rapport wel te nauw beschreven. Hierover zijn eerder gesprekken gevoerd tussen OM en inspectie en zal ook op worden doorgesproken. Het is vervelend voor dit politieteam als er twee toezichthouders zijn.

Henk: Het beeld van **5.1.2e** wordt herkent vanuit de wederhoortabel die door de politie is aangeleverd in reactie op het verslag. Inspectie probeert haar rol uit te voeren met de wet in de hand. Fijn dat inspectie en OM hier nader over kunnen doorspreken.

5.1.2e Focus van de inspectie ligt op de taakuitvoering, maar daar zit een grijs gebeid. Wat is echt de politie aan te rekenen en wat komt vanuit de gezagsrol van het OM. Het is belangrijk dat we elkaar daar in gaan vinden. We spreken ook met de PG hoge raad hoe ver we kunnen gaan.

Angela: de politie gaf ook expliciet aan dat de inspectie met het OM in gesprek moeten omdat zij zich tussen twee werelden in voelen.

5.1.2e Inspectie focust zich op de naleving van de wettelijke bepaling. Daarin wordt getracht objectief te kijken of de wettelijke bepaling al dan niet worden nageleefd. Ook wat betreft het technisch hulpmiddel zijn er een aantal regels. Dat zijn zaken waar de inspectie geen oordeel over heeft, maar er wordt wel geconstateerd dat er niet altijd wordt voldaan aan de onderliggende eisen. Een andere gevoeligheid is de betrouwbaarheid van het bewijs. Als de inspectie een risico ziet, moet dat worden benoemd. Dat is ook afgestemd met de PG Hoge Raad

Henk: Meer algemeen als de inspectie enig risico ziet bij de taakuitoefening van de politie, dan moeten daar iets over gemeld worden. De vervolgstappen daarop en gevolgen zijn aan andere partijen.

5.1.2e De beoordeling of iets en technisch hulpmiddel is valt volledig onder het OM. Daarmee ook onder het gezag van het OM. Daarin zit ingebakken dat de OvJ een oordeel geeft. Als het verslag daar op ziet, kun je je afvragen of de inspectie zich niet teveel op het terrein van het OM begeeft.

Gerrit: Goed dat er nader wordt doorgesproken over de rolafbakening. Het gezag van het OM heeft een smal en een breed kader. Het is van belang om vanuit dat kader naar de voorbeelden in het rapport te kijken.

Henk: Goed dat de politie constateert en dat betrokken partijen (OM en inspectie) (idealiter) overeenstemming bereiken over de rolafbakening. De inspectie zal dit ook in het contact met de PG Hoge Raad aanstippen. Als we zien dat de politie anders handelt dan de opdracht van het OM is, dan kunnen we stellen dat er enig risico ontstaat. Hoe daarmee verder te gaan is dan aan de OvJ.

Angela: Wij kijken er naar wat er in de wet staat.

Henk: Er is ook nog de evaluatie van het WODC. De diepere vraag aan de wetgever is 'weet je wel wat je vraagt van politie?'. In hoeverre bevat de vraag die voorligt daadwerkelijk de waarborgen waar de wetgever initieel zorgen over had.

5.1.2e Richting evaluatie zijn de twee verslagen natuurlijk heel waardevol. Daar is voor de inspectie wel een lastige positie. Vanuit OM is er de uitdaging om de wet nog nader in te vullen.

V.w.b. de signalering dat technische hulpmiddel niet goed is toegepast helpt het OM enerzijds. Anderzijds wordt er een zin aan toegevoegd waar de inspectie niet over kan oordelen. De opmerking dat er een consequentie is voor het bewijs past in optiek van het OM niet in het verslag. Dit kan er ook toe leiden dat de inspectie als getuige-deskundige worden gevraagd een oordeel te geven.

Het OM stelt voor dat inspectie stopt bij signalering en niet over gaat op oordeelsvorming.

Henk: De toelichting wordt door de inspectie als nuttig ervaren. De inspectie kijkt op basis van deze toelichting en 'horizonverbreding' naar de mogelijke consequenties van bepaalde zinsneden uit het rapport. De inspectie heeft uiteraard wel een onafhankelijke positie.

Gerrit: Een ander punt is dat wat het OM betreft de toonzetting kort door de bocht is geformuleerd. Al is er uiteraard ook begrip voor het referentiekader van de inspectie.

Angela: De inspectie weerspreekt dat de toon kort door de bocht is. Het eerste jaar is relatief coulant opgetreden. Er zijn een aantal zaken die in de ogen van de inspectie niet goed geregeld zijn.

5.1.2e In aanvulling daarop ziet de inspectie wel dat er goede richtingen zijn ingezet. Maar over 2020 zijn er weinig feiten die onderbouwd kunnen worden. De hoop is dat 2021 anders is, al wordt nu al geconstateerd dat de Logging niet helemaal op orde is. Het is wachten op concrete resultaten.

5.1.2e Er is een verschil in prioritering door OM en inspectie. Inspectie kijkt veelal naar de bedrijfsvoering. OM hecht grote waarde in welke mate DIGIT ondersteuning kan bieden en de opsporingsbevoegdheid kan inzetten. De progressie op dat vlak is gigantisch. Er is mogelijk daardoor minder progressie in de bedrijfsvoering. Dat is niet het primaat waar dit team voor op aarde is. De vragen vanuit tactische teams en vanuit zaaksofficieren wordt door de DIGIT OvJ gekanaliseerd. Het is ook aan het OM om de inspectie inzicht te geven in hetgeen er in opdracht van het gezag gebeurt en wat DIGIT zelf doet.

Gerrit: ook procedureel heeft het OM sterke eisen gesteld. Het is een ingewikkeld proces hoe je vooraf e.e.a. al kan inkleden. De wet had natuurlijk wel wat open eindjes. Daar wordt nog steeds invulling aan gegeven.

Henk: Het schrikbeeld van de kamer is dat de wet wat random en zomaar wordt ingezet. En het OM wil juist de wet graag inzetten wanneer echt nodig. We hebben dit jaar te weinig verbeteringen gezien. Ook in 2021 moet er echt wel even opgelet worden.



Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

Inspectie Justitie en
Veiligheid

Contactpersoon
contact@inspectie-jenv.nl

Datum
4 mei 2022

Projectnaam
CCIII

Notulist

5.1.2e

Gesprek op bestuurlijk niveau n.a.v. Verslag wettelijke
hackbevoegdheid 2021

Omschrijving	Gesprek op bestuurlijk niveau naar aanleiding van het Verslag van het toezicht door de Inspectie Justitie en Veiligheid op de toepassing door de politie in 2021 van de bevoegdheid op basis van de Wet Computercriminaliteit III om in een geautomatiseerd werk heimelijk en op afstand binnen te dringen en onderzoek te doen.
Vergaderdatum en -tijd	4 mei 2022, 16:00 uur
Vergaderplaats	WebEx
Aanwezig	Openbaar Ministerie: Gerrit van der Burg 5.1.2e 5.1.2e 5.1.2e Inspectie Justitie & Veiligheid: Henk Korvinus 5.1.2e

- Henk Korvinus licht het Verslag van de Inspectie kort toe. De Inspectie ziet verbetering in de wijze waarop de hackbevoegdheid is uitgeoefend door de politie. De Inspectie vraagt wel aandacht voor het organiseren van de kwaliteitsborging door de politie zelf. Als de politie haar interne kwaliteitsborging op dit onderwerp op orde heeft, kan de Inspectie het toezicht iets terughoudender uitvoeren.
- De politie onderkent in het bestuurlijk gesprek het belang en het positieve effect van het inrichten van eigen kwaliteitszorg. Problemen in de bezetting zijn er volgens de politie debet aan dat dit nog onvoldoende opgepakt is. De politie heeft aangegeven dat zij gaat bezien hoe aan de kwaliteitszorg bij de toepassing van de hackbevoegdheid de komende tijd invulling gegeven kan worden.
- Henk Korvinus legt uit dat de Inspectie zich geen oordeel aanmeet over het handelen door het OM. Als de politie in opdracht van het OM bepaalde handelingen uitvoert dan schrijven wij dat op en zetten dit af tegen de wettelijke voorschriften en rapporteren daar signalerend over. Deze formulering is ook met de AG van de Hoge Raad afgestemd. Door zo te formuleren wordt voorkomen dat de Inspectie oordeelsvormend spreekt over

het handelen van het OM. Henk geeft verder aan dat hij de indruk heeft dat het contact tussen de inspecteurs en 5.1.2e het afgelopen jaar is verbeterd, met meer wederzijds begrip voor elkaars rol.

- Gerrit van de Burg herkent zich in dit beeld. Het OM is blij met het evenwichtige en leesbare Verslag, waarvoor complimenten. Het Verslag biedt concrete handvatten voor de politie voor het doorvoeren van verbeteringen. 5.1.2e beaamt dit.
- Henk Korvinus geeft aan dat hij vanochtend van de pg-HR heeft vernomen dat het thematisch onderzoek dat de Hoge Raad uitvoert inzake de 'hackbevoegdheid' in de afrondende fase zit. De verwachting is dat dit rapport voor de zomer aan de minister aangeboden wordt.
- Gerrit van der Burg bericht over de voortgang van het onderzoek dat door het WODC wordt uitgevoerd. 5.1.2e vult aan dat het onderzoeksrapport van het WODC mogelijk half juni aangeboden wordt aan de minister. De rapporten van de Hoge Raad en het WODC worden dan mogelijk min of meer in dezelfde periode gepubliceerd.
- Gerrit van der Burg en Henk Korvinus spreken hun zorg uit over het verouderde beeld van opvattingen en opgenomen citaten van het OM en de Inspectie in het onderzoeksrapport van het WODC. Dit vraagt om alertheid dat het WODC ook het meest actuele beeld in haar onderzoek meeneemt.



Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

ONGERUBRICEERD

Aan de korpschef van de Nationale Politie,
de heer H.P. van Essen
Postbus 17107
2502 CC DEN HAAG

**Inspectie Justitie en
Veiligheid**

Hoge Nieuwstraat 8
2514 EL Den Haag
Postbus 20301
2500 EH Den Haag
www.inspectie-jenv.nl

Contactpersoon

5.1.2e
Senior Inspecteur

T 06 5.1.2e
5.1.2e@inspectie-jenv.nl

Projectnaam

Toezicht CCIH-
Hackbevoegdheid

Ons kenmerk
4654451

Uw kenmerk
-

Bijlagen

2

*Bij beantwoording de datum
en ons kenmerk vermelden.
Wilt u slechts één zaak in uw
brief behandelen.*

Datum 10 mei 2023

Onderwerp Aanbieding conceptverslag toezicht wettelijke hackbevoegdheid politie
2022 t.b.v. wederhoor

Geachte heer Van Essen,

De Inspectie Justitie en Veiligheid (de Inspectie) houdt toezicht op de uitvoering van de bevoegdheid tot het heimelijk en op afstand binnendringen en doen van onderzoek in een geautomatiseerd werk door de politie. Deze bevoegdheid wordt in de media de 'hackbevoegdheid' genoemd. De politie en de bijzondere opsporingsdiensten beschikken over deze hackbevoegdheid sinds de inwerkingtreding van de Wet computercriminaliteit III in maart 2019.

De Inspectie heeft, vanaf de inwerkingtreding van de Wet in 2019, voor het vierde opeenvolgende jaar onderzoek verricht naar de toepassing van deze wettelijke hackbevoegdheid door de politie. In het bijgevoegde conceptverslag *toezicht wettelijke hackbevoegdheid politie 2022* geeft de Inspectie een totaalbeeld van de bevindingen en conclusies van het onderzoek. De Inspectie rapporteert in dit verslag over de periode 1 januari 2022 tot en met 31 december 2022.

Graag leg ik dit conceptverslag aan u voor om u in de gelegenheid te stellen eventuele feitelijke onjuistheden kenbaar te maken. Ik verzoek u uw reactie op te nemen in de bijgevoegde tabel (bijlage 2). Uw reactie zie ik graag uiterlijk 26 mei 2023 tegemoet. De door u aangeleverde tabel wordt als bijlage aan het verslag toegevoegd, aangevuld met de reactie van de Inspectie op de door u genoemde punten. Voor eventuele vragen kunt u contact opnemen met 5.1.2e. Contactgegevens zijn hierboven vermeld.

Voor de volledigheid wil ik u melden dat het bijgevoegde conceptverslag gelijktijdig door ons verstrekt zal worden aan onze contactpersonen bij DIGIT en de keuringsdienst van de Landelijke Eenheid zodat zij hier direct kennis van kunnen nemen.

Vervolgtraject

Na ontvangst van de ingevulde wederhoortabel kan, indien u dit wenst, een bestuurlijk gesprek plaatsvinden waarin de inspecteur-generaal van de Inspectie het verslag nader toelicht. Ook uw reactie op het verslag kan in dit gesprek worden betrokken.

Na verwerking van uw wederhoorreactie wordt het verslag vastgesteld in het DT van de Inspectie. Vervolgens zal het verslag aan de minister van Justitie en Veiligheid worden aangeboden.

Hoogachtend,

5.1.2e



P.C.J. Neuteboom

Hoofdinspecteur-directeur Politie, Security en Crisisbeheersing

Bijlage(n)

- Conceptverslag Hackbevoegdheid 2022 versie t.b.v. hoor-wederhoor
- Tabel t.b.v. reactie hoor- en wederhoor

**Afzender**

Korpsleiding

Mr. 5.1.2e

Inspectie Justitie en Veiligheid
t.a.v. de heer P.C.J. Neuteboom
Postbus 20301
2500 EH Den Haag

Rubricering

Niet Vertrouwelijk

Datum	31 mei 2023	Behandeld door	Staf korpsleiding
Ons kenmerk	2023-0032642	Kopie aan	-
Uw kenmerk	4654451	Bijlage(n)	-

Onderwerp Wederhoor conceptverslag toezicht wettelijke hackbevoegdheid politie

Geachte heer Neuteboom,

Hartelijk dank voor de gelegenheid tot het geven van een reactie op het (concept)verslag toezicht wettelijke hackbevoegdheid politie 2022. Ik heb het verslag met veel interesse gelezen. In de bijlage van deze brief vindt u de ingevulde tabel voor hoor en wederhoor.

Sinds de start van het Digital Intrusion Team (DIGIT) heeft de politie het toezicht door de Inspectie van Justitie en Veiligheid (hierna: Inspectie) verwelkomd. Het nauwkeurige toezicht door de Inspectie heeft de politie geholpen om de operationalisering van de binnendringbevoegdheid te verscherpen en te versnellen. Daar spreekt de politie haar waardering voor uit.

Het huidig verslag en de voorgaande verslagen laten de spanning tussen de uitvoeringspraktijk en het wettelijk kader zien. De ervaringen van DIGIT in de afgelopen vier jaar hebben bewezen dat een gedetailleerd wettelijk kader in de praktijk moeizaam uitvoerbaar is. De politie heeft daar waar de praktijk en middelen het toelieten de rapporten van de Inspectie gebruikt om verbeteringen door te voeren. Vanwege deze beperkingen hebben de inspanningen helaas niet op alle punten geleid tot tevredenheid bij alle betrokken partijen. Ik ben het met de Inspectie eens dat het een taak van Minister is om te bepalen of en welke knelpunten worden weggelaten door aanpassingen in het wettelijk kader. Zolang het wettelijk kader ongewijzigd is, zullen de discrepanties tussen de praktijk en het wettelijk kader zoals de Inspectie dit signaleert bestaan.

Wetsevaluatie

Tijdens de totstandkoming van de bevoegdheid heeft de wetgever bepaald dat het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) na twee jaar een evaluatie uitvoert naar de uitvoeringspraktijk en de eventuele knelpunten die de politie ervaart bij het uitvoeren van de binnendringbevoegdheid. In september 2022 is dit rapport gepubliceerd. Ondanks dat de beleidsreactie van de minister van Justitie en Veiligheid nog niet bekend is, is het aannemelijk dat naar aanleiding van dit rapport de invulling van de binnendringbevoegdheid op onderdelen wezenlijk verandert. Aangezien het toezicht door de Inspectie een onderwerp was van het WODC-rapport, zal ook het onderwerp toezicht onderdeel zijn van de beleidsreactie van de Minister. De beleidsreactie heeft dus niet alleen gevolgen voor de inhoud van het toezicht maar mogelijk ook op de wijze van uitvoering van het toezicht. De beleidsreactie van de Minister is voor politie de basis voor de

Korpsleiding politie
Nieuwe Uitleg 1, 2514BP, Den Haag

31 mei 2023
2023-0032642

eventuele aanpassing van de uitvoering van de binnendringbevoegdheid. Het continueren van inspanningen om verbeteringen door te voeren zonder de beleidsreactie in acht te nemen, vind ik niet effectief. Na publicatie van de beleidsreactie nodig ik u uit om de gevolgen van de beleidsreactie te bespreken zodat er op een duurzame wijze invulling kan worden gegeven aan de toekomst van het toezicht op de binnendringbevoegdheid.

Bestuurlijk gesprek

Tot slot, net als vorig jaar ga ik graag in op uw uitnodiging tot een bestuurlijk gesprek over dit verslag.

Hoogachtend,

5.1.2e

lid korpsleiding

Bijlage: politie hoor en wederhoortabel



5.1.2f, 5.2.1



5.1.2i, 5.2.1



5.1.2; 5.2.1



5.1.2), 5.2.1



5.1.2i, 5.2.1



5.1.2i; 5.2.1



5.1.2i, 5.2.1



5.1.2i; 5.2.1



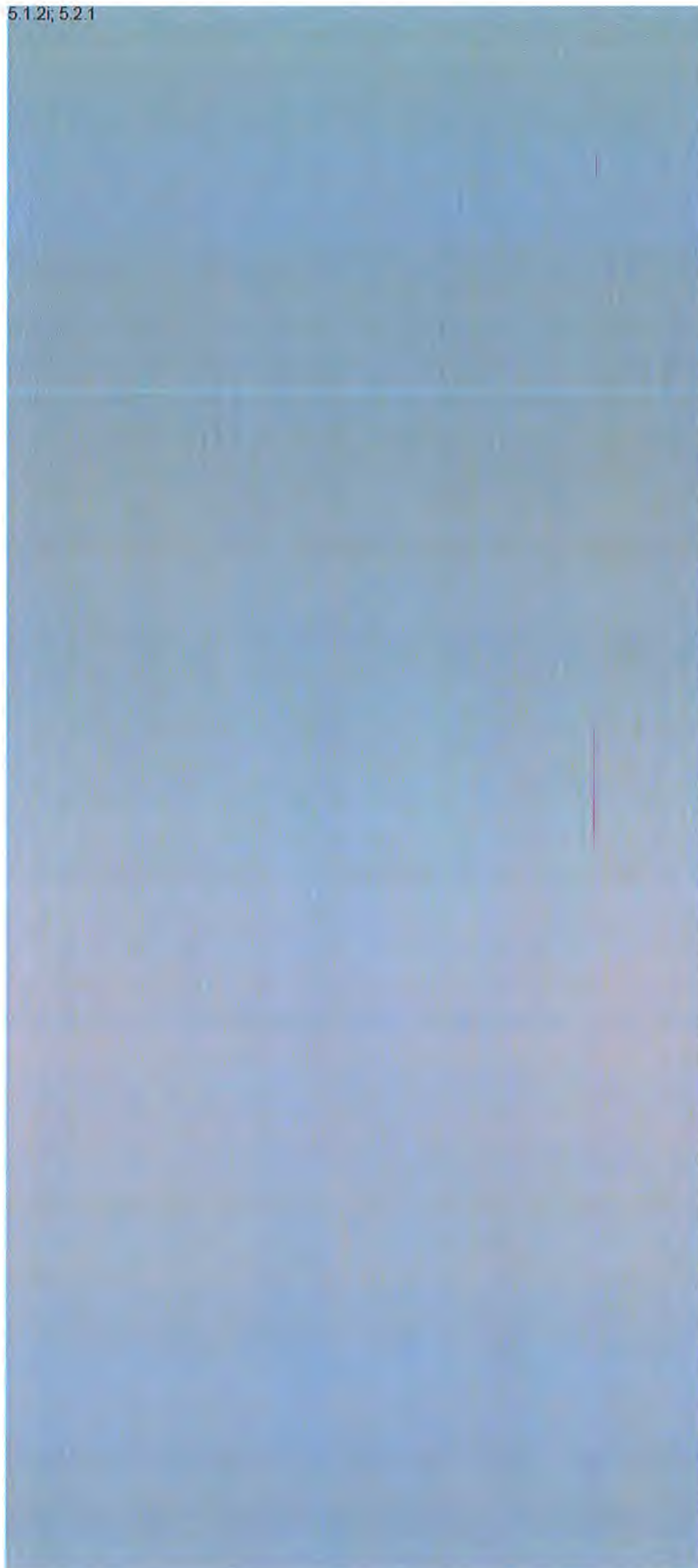
5.1.2i, 5.2.1



5.1.2], 5.2.1



5.1.2i, 5.2.1



Reactie op de wederhoor hackbevoegdheid 2022

OPENBAAR MINISTERIE

Aan 5.1.2e
Van 5.1.2e
Datum 20 september 2023
Onderdeel Landelijk Parket – DIGIT
Onderwerp Verslag Inspectie J&V m.b.t. inzet van de
hackbevoegdheid in 2022.

Memo

1 Aanleiding

Op 28 september 2023 vindt er een bestuurlijk overleg plaats over het verslag van de Inspectie J&V m.b.t. inzet van de hackbevoegdheid (art. 126nba Sv) door de politie in 2022. Dit verslag is op 31 augustus 2023 openbaar gemaakt. Bij dat verslag is een wederhoortabel gevoegd die de politie op een concept van het rapport heeft ingevuld. Sinds dit jaar maakt die tabel als bijlage onderdeel uit van het verslag. Vanuit het LP (landelijk officier voor Digital Intrusion, senior adviseur en strategisch beleidsadviseur) hebben we de politie van input voorzien bij deze wederhoor tabel.

Anders dan de voorgaande 3 jaar, vindt het bestuurlijk overleg dit jaar plaats na publicatie van het verslag.

Het departement van J&V heeft aangegeven de beleidsreactie op het verslag van de Inspectie te combineren met de beleidsreactie op de rapportages van het WODC en de PG bij de Hoge Raad over de hackbevoegdheid. De rapportages zijn in 2022 en 2023 gepubliceerd.

2 Korte algemene reactie op het verslag

Het verslag van de Inspectie over 2022 bevat geen onverwachte resultaten of conclusies. De Inspectie blijft dezelfde constatering doen over de politie die in eerdere verslagen ook staan beschreven. Daarin wordt de Inspectie iets scherper in de bewoording, omdat ze te weinig opvolging van haar bevindingen ervaart. Daarbij lijkt ook voor de Inspectie van belang welke (politieke) keuzes de minister van J&V zal maken n.a.v. eerder genoemde WODC en PG HR rapportages (zie p. 21 van het verslag en de daar verwoorde aanbeveling). De Inspectie richt haar toezicht daarom de komende tijd enkel op onderwerpen: de logging en handmatige verslaglegging, informatiebeveiliging, kwaliteitszorg en interne controle.

Net als het rapport over 2021 hanteert de Inspectie dit jaar een wijze van verslaglegging die een wat evenwichtiger beeld schetst van de manier waarop de politie uitvoering geeft aan de hackbevoegdheid. Er wordt niet enkel – zoals over

de jaren 2019 en 2020 het geval was – meer gekeken naar hetgeen niet volledig compliant is. Er worden ook zaken beschreven die wel al (deels) gerealiseerd zijn.

Twee punten die in het verslag relevant kunnen zijn voor concrete onderzoeken / strafzaken hebben betrekking op bevindingen ten aanzien van de juistheid van processen-verbaal en de omgang met gegevens van geheimhouders.

- Ten aanzien van de juistheid van processen-verbaal beschrijft de Inspectie op p. 20 dat de verslaglegging in het journaal niet altijd juist en volledig is en dit gevolgen heeft voor de juistheid van de opgemaakte processen-verbaal. Uit de nadere uitwerking van dit punt op p. 49 en 50 van het verslag volgt dat dit lijkt te zien op punten die geen betrekking hebben op elementen in de verbalen die de bewijswaarde van informatie in een strafzaak aantasten. Dat geldt ook voor de voorbeelden die de Inspectie van dit punt in mondeling overleg heeft gegeven.
- De Inspectie maakt in dit verslag ook een aantal (kritische) opmerkingen over de wijze waarop DIGIT omgaat met vergaarde gegevens waarin geheimhoudercommunicatie is opgenomen. Deze opmerkingen zijn in lijn met de constatering die op dit punt – op aandragen van DIGIT en ons – door het WODC en de PG HR zijn gedaan. In zoverre bevatten ze geen nieuwe informatie; rond de hackbevoegdheid zijn tegenstrijdige stukken regelgeving die vernietiging van data of een bewaarplicht voor data inhouden. Het is aan de wetgever hier een keuze in te maken.

In de wederhoortabel zijn op dit punt door de politie diverse opmerkingen gemaakt over de conceptversie van het verslag. Die punten hebben geleid tot diverse grotere aanpassingen in het gepubliceerde verslag. Die wijzigingen zijn niet (andermaal) voor wederhoor aan de politie voorgelegd of (al dan niet informeel) bij het OM op juistheid getoetst. Dat maakt dat het verslag nu – na de aanpassingen in verband met de wederhoor tabel – een beschrijving bevat die niet evident uitgaat van het juiste rechtskader rond dit soort gegevens; dat geldt voor passages over de toepasselijkheid van Besluit bewaren en vernietigen niet-gevoegde stukken met betrekking tot nummerherkenning en het kader rond selecteren van over te dragen gegevens.

Ik verwacht n.a.v. dit verslag voor concrete onderzoeken / strafzaken geen problemen rond de benoemde twee punten of anderszins.

3 Toezicht Inspectie vs. gezag officier van justitie

In de begin jaren van het toezicht door de Inspectie ontstond door de verslagen daarover spanning met de besluitvorming van de officier van justitie. Iets waar zij in hun toezichtsrol niet in mogen treden. Hier is in het bestuurlijk gesprek tussen de (toenmalig) inspecteur generaal van de Inspectie en de (toenmalig) voorzitter

van het College van 21 juni 2021 (over toezicht jaar 2020) uitgebreid bij stilgestaan.

Dat gesprek, de gesprekken die wij sindsdien voeren met de betrokken inspecteurs en de explicitering van kaders die wij als OM aan de politie stellen bij deze bevoegdheid, hebben er in geresulteerd dat in het verslag over 2021 en het huidige verslag over 2022 de afbakening van de rol van de Inspectie en die van het OM duidelijker naar voren. Net als vorig jaar zijn er – behoudens de 2 hier voor benoemde punten over geheimhouders – geen noemenswaardige punten waar de Inspectie over oordeelt die treden in de gezagsrol van het OM.

4 Slotsom

Ik denk dat het wenselijk is om in het bestuurlijk gesprek tussen de inspecteur-generaal en de voorzitter van het College te benoemen dat we blij zijn met de continuering van de wat evenwichtigere wijze van verslaglegging en de continuering van de wederzijdse inspanningen om te komen tot een heldere afbakening tussen taken/rollen.

Daarnaast lijkt het me nuttig om te benoemen dat het ons wenselijk voorkomt als de Inspectie onderwerpen uitdiept die raken aan punten die in grote mate onder de verantwoordelijkheid van het OM vallen – zoals de omgang met geheimhoudersgegevens – ze het OM daarin op voorhand consulteren om te toetsen of er op- of aanmerkingen zijn bij hetgeen de Inspectie beschrijft.

20 september 2023

5.1.2



Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

CONCEPT

Inspectie Justitie en
Veiligheid

Contactpersoon
contact@inspectie-jenv.nl

Datum
28 september 2023

Projectnaam
Toezicht hackbevoegdheid -
CCIII

Notulist

5.1.2e

Gesprek op bestuurlijk niveau OM-IJenV n.a.v. Verslag
wettelijke hackbevoegdheid 2022

Omschrijving	Gesprek op bestuurlijk niveau naar aanleiding van het Verslag van het toezicht door de Inspectie Justitie en Veiligheid op de toepassing door de politie in 2022 van de bevoegdheid op basis van de Wet Computercriminaliteit III om in een geautomatiseerd werk heimelijk en op afstand binnen te dringen en onderzoek te doen
Vergaderdatum en -tijd	28 september 2023, 10:30-11:15 uur
Vergaderplaats	Lange Voorhout 7, Den Haag
Aanwezig	Guus Schram (lid College van procureurs-generaal, OM) 5.1.2e (OVJ, Landelijk Parket, OM) 5.1.2e (Beleidsadviseur, Parket-Generaal, OM) Esther de Kleuver (Inspecteur-Generaal, IJenV) Peter Neuteboom (Hoofdinspecteur-directeur, IJenV) 5.1.2e (Inspecteur, IJenV)

- Esther geeft aan dat de Inspectie toeziet op de naleving van de regels bij de toepassing van de hackbevoegdheid door de politie, maar dat de Inspectie ook kijkt naar de spanning die dat oplevert bij de praktische uitvoerbaarheid. Esther licht vervolgens de hoofdconclusie van het verslag over 2022 kort toe.
- Het verslag legt volgens Guus de vinger op de zere plekken maar heeft ook aandacht voor wat er in gang is gezet.
- 5.1.2e beaamt dat het verslag net als vorig jaar meer in evenwicht en herkenbaar is.
- Wel is er volgens Guus een aantal punten waar het OM en de Inspectie in professionele zin langs elkaar schuren.
- Wat het volgens Guus ingewikkeld en complex maakt is de verhouding van het toezicht van de Inspectie op de politie enerzijds en de gezagsrelatie van het OM op de politie anderzijds. Daar waar de relatie met de PG-HR voor het OM, als de toezicht genietende organisatie, veel duidelijker is. Guus merkt op dat het in gezamenlijkheid zoeken is naar een werk- en omgangsmodus met behoud van en begrip voor elkaars rol. Guus voegt eraan toe dat door regelmatig overleg het wederzijds begrip en daarmee de verhouding tussen Inspectie en OM de laatste jaren verbeterd en goed is.
- Esther vult aan dat de Inspectie als vanzelfsprekend zich ervan bewust is dat zij geen toezicht houdt op het OM. Signalen en risico's kan de Inspectie wel

beschrijven. Bij de verwerking van de wederhoor is dat op een aantal punten door de Inspectie nog verduidelijkt.

- Guus en 5.1.2e wijzen op het onderwerp geheimhouders en de aanpassingen en opmerkingen die de Inspectie daarover in het verslag heeft gemaakt n.a.v. het hoor-en-wederhoor. Volgens 5.1.2e is er geen sprake van een feitelijke onjuistheid en zijn deze aanpassingen bijna spot-on, maar net ernaast.
- 5.1.2e geeft aan dat het had geholpen om dit in de rapportage scherper te beschrijven als het OM nog context aan de Inspectie had kunnen meegeven en de consequenties op dit onderwerp had kunnen toelichten.
- Guus begrijpt dat het OM geen formele partij is in de wederhoor die vanuit de Inspectie plaatsvindt met de politie als toezicht ondervindende organisatie.
- Guus geeft aan dat het OM op zoek is naar een passend moment en wijze om met de Inspectie in gesprek te komen en daarbij op bepaalde onderwerpen nog context ter overweging mee te geven. Dit maakt de rapportage van de Inspectie volgens Guus ook beter. Het gesprek zou dan plaats moeten kunnen vinden voordat het verslag definitief wordt.
- Peter geeft aan dat bezien wordt in welke fase het bestuurlijk gesprek gehouden wordt om de acceptatie van rapporten van de Inspectie bij de ontvangende partijen te bevorderen. De beweging is om dat moment naar voren te halen en niet pas op het moment dat een rapport al is vastgesteld. Dit mag echter niet leiden tot enige vorm van beïnvloeding en afbreuk doen aan de onafhankelijkheid van de Inspectie. Het voegen van de wederhoortabel en de vastlegging in de vorm van gespreksverslagen zorgen daarbij voor transparantie.
- Esther vult aan dat zij wil nadenken over of en hoe dit in de vorm van een bestuurlijk gesprek zou kunnen waarbij onafhankelijkheid vanzelfsprekend voorop staat.
- Esther geeft aan dat de Inspectie het belangrijk vindt dat de politie een aantal punten, waaronder de kwaliteitszorg, actief en met urgentie oppakt. Als dat goed gebeurt, kan het toezicht van de Inspectie meer op afstand plaatsvinden. Deze lijn is ook besproken met de korpsleiding van de politie en wordt daar herkend. Esther vraagt of het OM het belang van kwaliteitszorg bij de politie deelt. Het zou namelijk mooi zijn om daar gezamenlijk in op te trekken.
- 5.1.2e deelt dit. Volgens 5.1.2e is het goed om in het verslag van de Inspectie te lezen dat de politie t.o.v. eerdere jaren zelf gesignaleerd en onderkend heeft als iets niet goed gegaan is. 5.1.2e beaamt dat in het kader van de kwaliteitszorg hierin door de politie nog wel stappen gemaakt moeten en kunnen worden. Van constatering op een ad-hoc basis moet dit gebracht worden naar een meer systematische inrichting en daarmee robuust gemaakt worden. Hierbij moet volgens 5.1.2e wel gezocht worden naar een balans tussen de beschikbare capaciteit om dit te verbeteren en de operationele belangen om zaken te kunnen draaien. Niet elk onderwerp binnen de kwaliteitszorg heeft daarbij volgens 5.1.2e evenveel prioriteit. Het zou volgens 5.1.2e onderwerp van gesprek moeten zijn op een hoger dek binnen de politieorganisatie om hierin keuzen te maken. Het zou mooi zijn als de

Inspectie over kan gaan naar een meer meedenkende vorm van toezicht om de politie te helpen om de kwaliteitsslag te maken.

- Guus vult aan dat binnen de politie van alles gebeurt op het gebied van kwaliteit, maar dat dit niet altijd met elkaar samenhangt en vaak gedreven is vanuit incidenten.
- Peter geeft aan dat het onderwerp van kwaliteitszorg bij de politie voor het komende jaar op het toezichtsprogramma van de Inspectie staat. Peter is benieuwd naar de beelden van het OM op het onderwerp kwaliteitszorg en waar het meeste behoefte aan is. Peter gaat daarover graag met het OM in gesprek zodat de Inspectie dat bij de keuze kan meenemen.

Onderwerp
Reactie toetsingskader toezicht
hackbevoegdheid politie

Inspectie Justitie en Veiligheid
Mevr. 5.1.2e
Postbus 20301
2500 EH Den Haag

Organisatieonderdeel
Directie operatie

Geachte mevrouw 5.1.2e,

Behandeld door
5.1.2e

Ten eerste wil ik u dankzeggen voor de gelegenheid om te reageren op het *Toetsingskader toezicht hackbevoegdheid politie*. We hebben het herziende toetsingskader met interesse gelezen.

Functie
Adviseur

De politie waardeert dat de Inspectie Justitie en Veiligheid (hierna: de Inspectie) het toetsingskader zo transparant mogelijk heeft gemaakt door de context, duiding, en herkomst van alle onderdelen nader uit te schrijven. Inzicht in de wijze waarop de Inspectie toezicht houdt, draagt bij aan een constructieve relatie tussen het Digital Intrusion Team (DIGIT), de Keuringsdienst en de inspecteurs die belast zijn met het toezicht op de bevoegdheid tot het heimelijk en op afstand binnendringen en doen van onderzoek in een geautomatiseerd werk door de politie.

Telefoon
-

E-mail
5.1.2e@politie.nl

In deze brief geeft eerst de onafhankelijke Keuringsdienst van de politie haar reactie op het deel van het toetsingskader dat gaat over het keuringsproces. Daarna volgt de algemene reactie vanuit de politie op het voorgelegde toetsingskader.

Ons kenmerk
2021-0060734

Uw kenmerk
3516573

In afschrift aan
-

Reactie vanuit de Keuringsdienst politie

Datum
13 oktober 2021

In algemene zin stelt de Keuringsdienst vast dat het toetsingskader accuraat en volledig zijn grondslag vindt in onderliggende wet- en regelgeving. Aanvullend daarop heeft de keuringsdienst enkele op- en/of aanmerkingen die wij hier onder artikelsgewijs zullen toelichten. Wij hebben ons hierbij beperkt tot het kader neergelegd in hoofdstuk 4 van het toetsingskader dat gaat over de keuring van technische hulpmiddelen.

Bijlage(n)
1

Pagina
1

- N12: In de toelichting bij deze eis wordt gesteld dat, omdat de LE niet beschikte over voldoende capaciteit en expertise, er gekozen is om een andere keuringsdienst aan te wijzen. Onze suggestie zou zijn om aan te vullen dat deze keuze is gemaakt in 2019, om de ruimte tot groei met het huidige tijdsframe te verduidelijken.
- N15: Gesteld wordt dat er van herkeuring sprake zal zijn als een middel (of onderdeel daarvan) zodanig wijzigt dat redelijkerwijs kan worden aangenomen dat de werking niet langer voldoet aan de gestelde eisen. Dit is correct, maar verdient naar mening van de keuringsdienst(en) enige aanvulling op twee aspecten. Ten eerste kunnen ook omgevingsfactoren zodanig wijzigen dat redelijkerwijs verwacht kan worden dat een middel niet meer voldoet aan de gestelde eisen. Denk hierbij aan veranderende omstandigheden in de 'stand der techniek', zoals bijvoorbeeld een encryptietechniek die niet meer veilig wordt geacht. Voorts wil de keuringsdienst opmerken dat het in de praktijk vrijwel onmogelijk is om met zekerheid vast te stellen dat een middel, na wijziging, nog voldoet aan de gestelde

Onderwerp
Reactie toetsingskader toezicht
hackbevoegdheid politie

Datum
13 oktober 2021

Pagina
2 van 3

eisen op basis van een inschatting of 'redelijke verwachting'. Er zal altijd in enige mate opnieuw gekeken moeten worden naar wijzigingen en het middel om deze verwachting te onderbouwen. Om deze reden heeft de keuringsdienst er voor gekozen om in vrijwel alle gevallen na wijziging van een technisch hulpmiddel voor te schrijven dat het middel in ieder geval in enige mate opnieuw bekeken zal moeten worden.

- N18: onder g) zie opmerking hierboven met betrekking tot aanvulling wijziging werking technisch hulpmiddel.

Algemene reactie

In het toetsingskader maakt de Inspectie een vertaalslag van wat wet- en regelgeving betekent voor het toezicht en de (voorgenomen) handelswijze van de politie bij de toepassing van de bevoegdheid. Daarbij duidt de Inspectie die wet- en regelgeving door te putten uit toelichtingen die zijn gegeven tijdens de parlementaire behandeling. Hoewel de politie begrijpt dat enige vorm van eigen interpretatie onvermijdelijk is bij het opstellen van een toetsingskader, constateert de politie dat de Inspectie de voorgeschreven wet- en regelgeving breed interpreteert en op onderdelen verder gaat dan de wetgever heeft bepaald. Dit is onder andere op de onderwerpen onbekende kwetsbaarheden en onregelmatigheden geconstateerd.

Daarnaast wil de politie graag aan de Inspectie meegeven dat deze toelichting(en) gelezen moeten worden in de context van het politieke debat dat in de periode 2015 tot 2019 werd gevoerd. De toelichting bevat een variëteit aan onderwerpen die veelal een reactie was op vragen tijdens een politiek debat en werd gevoerd door input van belangenorganisaties. De politie is van mening dat deze toelichting in dit licht en in de tijdsgeest van toen, moet worden gelezen. Het zwaartepunt van het toetsingskader moet bij de artikelen in het Wetboek van Strafvordering en het Besluit onderzoek in een geautomatiseerd werk (Bogw) liggen. De toelichting op die wet- en regelgeving kan niet 1 op 1 vertaald worden naar harde normen voor toezicht.

Bij het uitvoeren van de binnendringbevoegdheid gaat de politie in eerste instantie altijd uit van de vastgestelde wet- en regelgeving. DIGIT werkt zoveel mogelijk conform dit kader en de daarop gegeven toelichting. Daarbij opereert DIGIT onder het gezag van het Openbaar Ministerie. De DIGIT officier van justitie bepaalt de kaders waarbinnen het technisch team haar werkzaamheden verricht. Daarnaast wordt in concrete opsporingsonderzoeken door een officier van justitie een bevel afgegeven. Dit houdt in dat de werkwijze wordt ingevuld door de aanwijzingen en beslissingen die het OM neemt. Deze situatie zorgt bijna onvermijdelijk voor frictie, wanneer de Inspectie zich begeeft op onderdelen die (ook) aan het OM zijn voorbehouden.

In het verlengde van de brede vertaalslag constateert de politie dat de Inspectie zich op meerdere onderwerpen uitlaat over de wijze waarop processen ingericht dienen te worden die verder gaan dan een wettelijke verplichting. Dit geldt in het bijzonder voor de onderwerpen 'kwaliteitssysteem en interne controle' en 'gegevens vastgelegd in logbestanden'. Binnen de wettelijke kaders heeft de politie de vrijheid om haar eigen processen in te richten. Toetsingsnormen gerelateerd aan processen gaan voorbij aan deze autonomie. De politie verzoekt de Inspectie daarom terughoudend te zijn in het opleggen van toetsingskaders die raken aan de (vorm van) processen.

Het toetsingskader maakt duidelijk dat de Inspectie vraagt om gedetailleerde documentatie van hoe de politie invulling geeft aan de binnendringbevoegdheid. Vanwege de relatief nieuwe bevoegdheid worden nog regelmatig nieuwe inzichten opgedaan die van invloed zijn op de operationele werkwijze. Naar mening van de politie is het snel veranderend karakter van de operationele werkwijze een teken van een groot lerend vermogen van het team. Deze grilligheid knelt met het verlangen van de Inspectie dat het team alles aantoonbaar moet maken door alle facetten van de operatie

Onderwerp
Reactie toetsingskader toezicht
hackbevoegdheid politie

Datum
13 oktober 2021

Pagina
3 van 3

vast te leggen in gedetailleerde ontwerpdocumentatie en processen. Binnen de opsporing geldt dat een opsporingsambtenaar zijn onderzoekshandelingen waar nodig aantoonbaar maakt door processen-verbaal op ambtseed/ambtsbelofte op te stellen. Alles aantoonbaar vastleggen zoals de Inspectie verlangt om het toezicht te vereenvoudigen legt een onevenredig groot beslag op de capaciteit van een team dat nog volop in ontwikkeling is.

Tot slot

Ransomware is door de NCTV betiteld als risico voor de nationale veiligheid. De actualiteit maakt dat het bestrijden hiervan vraagt om inzet van alle mogelijkheden van de wet CCIII. Politie en partners, publiek en privaat, zien de uitoefening van de binnendringbevoegdheid ook als belangrijk middel in de aanpak. De voorgestelde brede interpretatie van wet- en regelgeving maakt de uitvoering en toetsing complex, en draagt daarmee niet bij aan de gewenste slagkracht van de operatie. De politie verzoekt de Inspectie dan ook zich te beperken tot een enge interpretatie van de Wet CCIII en het Bogw. Een toetsingskader met een brede interpretatie van de wet- en regelgeving kan resulteren in een wederkerend onevenwichtig beeld in de Inspectierapporten die de inspanningen van de politie geen recht doet.

In de bijlage van deze brief vindt u een tabel waarin bovenstaande constateringën geconcretiseerd zijn met voorbeelden uit het toetsingskader.

Mochten er naar aanleiding van deze brief extra toelichting gewenst zijn, dan licht de ik onze bevindingen graag verder toe in een gesprek.

Met vriendelijke groet

5.1.2e

lid korpsleiding

Nr.	Pagina	Betreffende tekst	Constatering politie	Reactie politie
1	5	Sub c, d en f	Mogelijke frictie tussen toezicht door de Inspectie en het gezag van het Openbaar Ministerie	De wijze waarop het is opgeschreven is te ruim. Bij de genoemde punten zitten diverse afwijkingen van het OM of valt binnen de oordeelsvorming van het OM.
2	13	Voor het ... testomgeving benodigd	Mogelijke frictie tussen toezicht door de Inspectie en het gezag van het Openbaar Ministerie	Hier kan mogelijk frictie ontstaan als het OM beslist dat er sprake is van een voldoende representatieve testomgeving terwijl de Inspectie een andere mening is toebedeeld.
3	15	Norm 11	Mogelijke frictie tussen toezicht door de Inspectie en het gezag van het Openbaar Ministerie	Deze norm houdt geen rekening met het scenario dat het OM oordeelt dat er geen sprake is van een onbekende kwetsbaarheid en geen uitstel vraagt bij de rechter-commissaris.
4	21	Deze in... het bevel	Mogelijke frictie tussen toezicht door de Inspectie en het gezag van het Openbaar Ministerie	De officier van justitie stelt ook kaders in diens rol als leider van het opsporingsonderzoek. Dit onderdeel in het toetsingskader houdt geen rekening met een mogelijke afwijking ingegeven door een beslissing van het OM.
5	21	Norm 22	Mogelijke frictie tussen toezicht door de Inspectie en het gezag van het Openbaar Ministerie	Het binnendringen in een geautomatiseerd werk door het technisch team wordt zoveel mogelijk uitgevoerd volgens het vooraf opgestelde plan van aanpak. Als leider van het opsporingsonderzoek kan de officier van justitie besluiten om het technisch team de opdracht te geven om af te wijken van het plan van aanpak.

6	24	Norm 28	Mogelijke frictie tussen toezicht door de Inspectie en het gezag van het Openbaar Ministerie	Het is de verantwoordelijkheid van het OM om de aanvullende (procedurele) waarborgen te vermelden in de processtukken. Het oordeel of deze aanvullende (procedurele) waarborgen afdoende zijn valt naar mening van de politie buiten de scope van het toezicht.
7	24	Norm 29	Mogelijke frictie tussen toezicht door de Inspectie en het gezag van het Openbaar Ministerie	De beslissing om een TH in te zetten dat niet is gekeurd, is voorbehouden aan de officier van justitie. Dat betekent ook dat het aan de officier van justitie is, om te bepalen of een TH in afdoende mate voldoet aan het Bgw. De politie licht de officier van justitie daartoe voor over het TH en de werking ervan. Op de voorgestelde manier bestaat het gevaar dat het toezicht van de Inspectie zich vormt naar een schaduw keuringsdienst
8	27	Hierbij is... staat bevinden	Mogelijke frictie tussen toezicht door de Inspectie en het gezag van het Openbaar Ministerie	Dit is primair een verantwoordelijkheid van het OM. Ook wat betreft de inspanning die van de politie wordt geleverd. Daarbij ligt hier een hybride rol voor het tactisch team en zaaks-OM. Deze inspanning ligt dus niet exclusief bij DIGIT.
9	12	Het onderzoek... geautomatiseerde werk	Frictie tussen toezicht door de Inspectie en het gezag van het Openbaar Ministerie	De politie is zich ervan bewust dat de genoemde werkwijze terug te vinden is in de toelichting. Echter, vanwege operationele redenen en het kunnen afschermen van de opsporingsmethode is door het OM bepaald dat hiervan afgeweken wordt.

10	29	Indien door ...ingevuld wordt	Brede interpretatie van het wettelijk kader	Hier mist de wettelijke grondslag dat een onderbouwing voor handmatig vastleggen verplicht aanwezig moet zijn.
11	29	Het is ...in logbestanden	Brede interpretatie van het wettelijk kader	Het vastleggen en verantwoorden van de wijze van doorlopende en automatische logging vanuit een ontwerp vloeien niet direct voort uit een wettelijke verplichting.
12	45	Hoofdstuk 14: kwaliteitssysteem en interne controle	Brede interpretatie van het wettelijk kader	De politie heeft vanzelfsprekend eigen verantwoordelijkheid bij de uitvoering. Echter, het intern kwaliteitssysteem wordt nu een doel op zichzelf terwijl een intern kwaliteitssysteem niet direct voortvloeit uit een wettelijke verplichting
13	12	Er wordt...technisch hulpmiddel	Brede interpretatie van het wettelijk kader: er wordt invulling gegeven aan de door de wetgever gestelde kaders	Binnen de wettelijke kaders heeft de politie de vrijheid om haar eigen processen in te richten. Toetsingsnormen/ gerelateerd aan processen gaan voorbij aan deze autonomie.
14	13	Voor het... vastgelegd zijn	Brede interpretatie van het wettelijk kader: er wordt invulling gegeven aan de door de wetgever gestelde kaders	Binnen de wettelijke kaders heeft de politie de vrijheid om haar eigen processen in te richten. De wijze waarop een proefopstelling wordt ingevuld en hoe de resultaten worden vastgelegd is de bevoegdheid van de politie.
15	15	Naar mening... van Strafvordering	Brede interpretatie van het wettelijk kader: er wordt invulling gegeven aan de door de wetgever gestelde kaders	De Inspectie heeft hier een bredere interpretatie dan vastgelegd in het wettelijk kader. 126ffa Wetboek van Strafvordering reguleert niet het gebruik van kwetsbaarheden die gebruikt kunnen worden voor onderzoekshandelingen.

16	26	Naar mening.. te verrichten		Brede interpretatie van het wettelijk kader: er wordt invulling gegeven aan de door de wetgever gestelde kaders	Wanneer deze inspanning verricht wordt moet worden laat het wettelijk kader in het midden. Binnen de wettelijke kaders heeft de politie de vrijheid om haar eigen processen in te richten.
17	34	Naar mening.. van beheersingsmaatregelen		Brede interpretatie van het wettelijk kader: er wordt invulling gegeven aan de door de wetgever gestelde kaders	Binnen de wettelijke kaders heeft de politie de vrijheid om haar eigen processen in te richten. De politie heeft de vrijheid om de wijze waarop het informatiebeveiligingsbeleid tot stand komt vorm te geven.
18	35	Norm 41 en Om onregelmatigheden... moeten worden		Brede interpretatie van het wettelijk kader: er wordt invulling gegeven aan de door de wetgever gestelde kaders	Binnen de wettelijke kaders heeft de politie de vrijheid om invulling te geven aan de wet- en regelgeving. Het uitputtend beschrijven van het begrip onregelmatigheid vloeit niet direct voort uit het wettelijk kader.
19	36	Norm 43		Brede interpretatie van het wettelijk kader: er wordt invulling gegeven aan de door de wetgever gestelde kaders	Binnen de wettelijke kaders heeft de politie de vrijheid om haar eigen processen in te richten. Hoe en wanneer er op onregelmatigheden wordt gecontroleerd valt binnen deze vrijheid.
20	12	De minister...technisch hulpmiddel		Andere interpretatie van de toelichting	Op p. 63 van nr 6. schrijft de minister: "het binnendringen omvat veelal het plaatsen en verwijderen..." p. 70 idem. Het woord 'veelal' wordt niet betrokken in de uitleg van de Inspectie. Door het woord veelal wel te betrekken in de interpretatie ontstaat er een genuanceerder beeld.
21	24	Er wordt.. de politie		Andere interpretatie van de toelichting	In dit deel van de tekst wordt verwezen naar voetnoot 141. Met betrekking tot de

				aangehaalde voetnoot: dit onderdeel wordt gezegd in de context van een vraag van D66 of er feitelijk sprake is van een botnet. Die nuancering ontbreekt hier.
22	25	Om het ... van buiten	Andere interpretatie van de toelichting	In de aangehaalde voetnoot schrijft de wetgever dat 100% zekerheid niet te geven is. Deze nuance ontbreekt in de gestelde norm.
23	27	Norm 23	Andere interpretatie van het wettelijk kader	De gestelde norm is niet in overeenstemming met de Aanwijzing internationale aspecten. Uit de aanwijzing blijkt dat de politie er vanuit mag gaan dat data in NL is, tenzij er indicaties zijn dat data buiten NL is.
24	8	Norm 2	Onduidelijke formulering	De norm specificeert niet of 'onderdeel van' een lid en/of deelnemer betreft
25	10	Norm 5	Onduidelijke formulering	De term strikte functiescheiding zal in de praktijk discussie opleveren.
26	14	Norm 9	Onduidelijke formulering	Politie stelt niet vast, maar voert een toets uit waarbij de leverancier wordt gevraagd niet te hebben geleverd aan landen waartegen vanuit de EO of de VN restrictieve sancties bestaan en wordt gecontroleerd of in het land waar de leverancier is gevestigd een exportcontrole regime bestaat waar mensenrechten een onderdeel is in de beoordeling voor het verstrekken van een exportvergunning. Zie beantwoording Kamervragen in voetnoot 73.

27	18	Deze verplicht... keuringsrapport vastgelegd	Onduidelijke formulering	De politie stelt voor om de term vervangende waarborgen te gebruiken i.p.v. vervangende procedurele waarborgen. De term vervangende procedurele waarborgen kan verwarrend zijn met de elders in het Bogw voorgeschreven procedurele waarborgen. Zodoende het voorstel om hier enkel te spreken van vervangende waarborgen.
28	11	Ook wordt... worden aangeschaft	Aanvulling	De voetnoot wijst naar p.16 van de NvT. De juiste verwijzing zou moeten zijn op p. 10 van nr. 29 (verslag van een schriftelijk overleg) in de wetsgeschiedenis.
29	39	Het proces-verbaal... van wetenschap	Aanvulling	Naaat de ambtseed is het ook mogelijk om een proces-verbaal op te maken op ambtsbelofte

Normenkader kwaliteitssysteem DIGIT

1. Normen die rechtstreeks voortvloeien uit wet-of regelgeving (zoals artikelen uit het Bogw of het Wetboek van Strafvordering).
2. Normen die zijn ontleend aan toezeggingen / uitspraken uit het parlementaire traject en/of aan toelichtingen (zoals MVT Wet CCIII, NvT Bogw).
3. Normen gebaseerd uit het toetsingskader van de Inspectie die de Inspectie heeft geformuleerd vanuit haar toezicht op de kwaliteit van de taakuitvoering.

Norm	Grondslag
1. Aanwijzing opsporingsambtenaren en uitvoering door technisch team	
N1	De opsporingsambtenaren die belast worden met het binnendringen en het uitvoeren van onderzoekshandelingen zijn daartoe door hun werkgever aangewezen. 1
N2	Het technisch team dat is belast met het binnendringen in een geautomatiseerd werk en het verrichten van onderzoekshandelingen is onderdeel van de Eenheid Landelijke Expertise en Operaties. 1
N3	Een opsporingsambtenaar wordt door (de ondergemandateerde van) de korpschef aangewezen als lid van een technisch team als de opsporingsambtenaar voldoet aan de vereiste (opleidings)kwalificaties. 1
N4	Een opsporingsambtenaar wordt door (de ondergemandateerde van) de korpschef op een incidentele basis aangewezen als deelnemer aan een technisch team voor de duur van de uitvoering van het bevel in een concrete zaak indien hij beschikt over specifieke kennis en vaardigheden, benodigd voor de uitvoering van dat bevel. 1 + 2
N5	Er is sprake van een functiescheiding tussen het technisch team en het tactisch team. Het technisch team wordt niet beïnvloed door het tactisch team ten aanzien van de haalbaarheid van de inzet, de uitvoering daarvan en de verwijdering van een technisch hulpmiddel. 2
2. Voorbereiding	
N6	2

	Het technisch team stelt op basis van de intakegegevens en overige relevante gegevens een advies inzet op, op basis waarvan de OvJ een inschatting van de beheersing en beperking van risico's voor het geautomatiseerde werk kan maken. Het advies inzet bestaat uit de volgende onderdelen: • Plan van aanpak voor de uitvoering van een onderzoek • De inschatting van de beheersing en beperking van risico's (deze risico's zijn breder dan de risico's dan alleen voor derden. Denk ook aan afbreukrisico, procesrisico, persrisico etc.) • Welk technisch hulpmiddel voor de uitvoering van het onderzoek wordt gebruikt • Welke bevelen nodig zijn • Indien nodig, welke software van derden moet worden aangeschaft	2
N7	Het technisch team stelt een plan van aanpak op voor het binnendringen in het geautomatiseerd werk en test dit in een proefopstelling.	
	3. Binnendringingssoftware	
N8	Er wordt alleen commerciële binnendringingssoftware aangeschaft van leveranciers die zijn gescreend door de AIVD. De politie vraagt bij aanschaf aan de leverancier of zij niet levert aan dubieuze regimes. De toets houdt in dat de leverancier verklaart niet te leveren aan landen waartegen restrictieve sancties bestaan vanuit de EU en/of VN. Tevens wordt gecontroleerd of in het land waar de leverancier is gevestigd, een exportcontrole regime bestaat waar mensenrechten een onderdeel is in de beoordeling voor het verstrekken van een exportvergunning. Per kwartaal wordt beoordeeld of deze situatie na aanschaf is gewijzigd.	2
N9	In het geval binnendringingssoftware wordt ingekocht, wordt het functioneren hiervan in een testomgeving gecontroleerd.	2
N10	Indien de politie beschikt over kennis van een mogelijke onbekende kwetsbaarheid, meldt de politie dit allereerst bij de officier van justitie. Indien het OM besluit om geen machtiging tot uitstel bij de rechtercommissaris aan te vragen dan wel deze machtiging wordt niet verleend, dan meldt de politie de kwetsbaarheid in beginsel direct of zo spoedig mogelijk, aan de producent van de desbetreffende hardware of software.	2
	4. Keuring technisch hulpmiddel	
N11	Een technisch hulpmiddel is door (de ondergemandateerde van) de korpschef ter (her)keuring aangeboden aan de keuringsdienst.	1

5. Uitvoering binnendringen en verrichten van onderzoekshandelingen		
N12	Het technisch team past de bevoegdheid tot het binnendringen en het verrichten van onderzoek in een geautomatiseerd werk toe conform door de officier van justitie afgegeven bevelen, aanwijzingen en instructies. Aanvullende toelichting: De typen aanwijzingen en instructies van de officier van justitie zijn uiteenlopend, deze kunnen bestaan uit schriftelijke en vastgestelde handelingskaders, ad-hoc aanwijzingen, mondelinge aanwijzingen etc. Afhankelijk van het type kan de wijze van vastlegging verschillen.	1
N13	Het binnendringen in het geautomatiseerde werk wordt door het technisch team uitgevoerd volgens het vooraf opgestelde plan van aanpak. Het plan van aanpak voor het binnendringen is een voorgenomen werkwijze waar het technisch team binnen de kaders van het bevel kan afwijken.	2
N14	Het binnendringen en het uitvoeren van (onderzoeks)handelingen is uitgevoerd door een lid of deelnemer van een technisch team.	1
N15	Een deelnemer aan een technisch team wordt gedurende de uitvoering van het bevel begeleid door een lid van een technisch team. Deze begeleiding wordt afgestemd op het kennisniveau van de betreffende deelnemer en de omstandigheden van de zaak. Aanvullende toelichting: de vorm van begeleiding kan variëren vanwege de omstandigheden. Denk hierbij aan de kennis, vaardigheden en ervaring van een deelnemer, de complexiteit van de handelingen en/of zaak en de vastgestelde risico's.	1
N16	Alleen de technische, daartoe aangewezen ambtenaren hebben toegang tot het systeem van waaruit het op afstand binnendringen van een geautomatiseerd werk wordt uitgevoerd.	2
N17	De politie treft procedurele waarborgen indien sprake is van een situatie zoals bedoeld in artikel 21 lid 5 Bgwg en verbaliseert dit.	2
5.1 Inzet technisch hulpmiddel		
N18	Een ingezet technisch hulpmiddel is - behoudens de situatie in artikel 21 lid 2 en 4 - goedgekeurd.	1

N19	De politie treft de vervangende waarborgen indien sprake is van een situatie zoals bedoeld in artikel 18 lid 3 sub e Bogw en verbaliseert dit.	2
N20	De politie treft aanvullende waarborgen indien sprake is van een situatie zoals bedoeld in artikel 21 lid 4 Bogw en verbaliseert dit.	2
N21	De politie biedt een technisch hulpmiddel achteraf ter keuring aan in het geval dat de officier van justitie bepaalt dat er een niet gekeurd technisch hulpmiddel is ingezet.	1
5.2 Verwijdering van een technisch hulpmiddel		
N22	Een technisch hulpmiddel wordt verwijderd uit een geautomatiseerd werk door een opsporingsambtenaar van een technisch team zodra het onderzoeksdoel is bereikt of uiterlijk zodra de periode, waarbinnen aan het bevel uitvoering moet worden gegeven, is verlopen.	1
N23	Indien een technisch hulpmiddel niet of niet volledig kan worden verwijderd uit een geautomatiseerd werk, beëindigt de met verwijdering belaste opsporingsambtenaar het transport van de door het technische hulpmiddel geregistreerde gegevens naar de technische infrastructuur.	1
N24	Indien de niet of niet volledige verwijdering van een technisch hulpmiddel risico's oplevert voor het functioneren van het geautomatiseerde werk waarin het is geplaatst, stelt de opsporingsambtenaar de officier van justitie hiervan in kennis en stelt hij informatie ter beschikking ten behoeve van de volledige verwijdering.	1
5.3 Communicatie met leverancier technisch hulpmiddel		
N25	Een technisch hulpmiddel is beveiligd tegen wijziging van de werking hiervan, tegen wijziging van de geregistreerde gegevens en tegen kennisneming van de geregistreerde gegevens door onbevoegden.	2
N26	De registratie van de beperkte en gecontroleerde toegangsverlening tot en uitgifte van technisch hulpmiddelen vindt centraal plaats door daartoe door de korpschef aangewezen ambtenaren.	1

6. Gegevens vastgelegd in logbestanden (logging)			
N27	Gedurende de uitvoering van een bevel zijn doorlopend en automatisch gegevens in logbestanden vastgelegd over: a) de handelingen die worden verricht ter uitvoering van een bevel; b) de toegang tot een technisch hulpmiddel; c) de gegevens die al dan niet met een technisch hulpmiddel op de technische infrastructuur worden vastgelegd ter uitvoering van een bevel; d) het functioneren van de technische infrastructuur.	1	
N28	Indien de gegevens niet automatisch in logbestanden kunnen worden vastgelegd legt een opsporingsambtenaar van een technisch team de handelingen handmatig vast.	1	
N29	Voor de vastlegging van gegevens in logbestanden zijn maatregelen getroffen om wijziging van de logbestanden of kennisneming hiervan door onbevoegden te voorkomen en achteraf te kunnen vaststellen of wijziging of kennisneming heeft plaatsgevonden.	1	
N30	Het loggingsproces is zo ingericht dat de loggingsinformatie tijdens de fase van bewijsvergaring functioneert en niet valt te manipuleren, te wijzigen of te verwijderen.	2	
7. Technische infrastructuur en bewijslogging			
N31	De vastlegging van de tijdens het onderzoek geregistreerde gegevens vindt plaats op een technische infrastructuur, waarbij het unieke kenmerk en de datum en tijd van vastlegging wordt geregistreerd.	1	
N32	De politie treft maatregelen om wijzigingen bij de vastgelegde gegevens of kennisneming van de vastgelegde gegevens hiervan door onbevoegden te voorkomen en achteraf te kunnen vaststellen of wijziging of kennisneming hiervan heeft plaatsgevonden.	1	
8. Onregelmatigheden			
N33		1	

N34	De logging is zodanig ingericht dat vastgesteld kan worden of onregelmatigheden plaatsvinden of hebben gevonden die van invloed zijn op de betrouwbaarheid en integriteit van de bewijslogging.	2
9. Proces-verbaal		
N35	De opsporingsambtenaar maakt proces-verbaal op van het plaatsen van een technisch hulpmiddel en eventuele onregelmatigheden daarbij. De opsporingsambtenaar maakt proces-verbaal op van het verrichten van onderzoekshandelingen en eventuele onregelmatigheden daarbij. De opsporingsambtenaar maakt proces-verbaal op na vaststelling van een onregelmatigheid die de betrouwbaarheid en integriteit van de bewijslogging heeft aangetast. De opsporingsambtenaar maakt proces-verbaal op van het verwijderen van een technisch hulpmiddel en eventuele niet of niet volledige verwijdering. De opsporingsambtenaar maakt proces-verbaal op van bewerkingen die hebben plaatsgevonden met betrekking tot de kopie van de vastgelegde gegevens. De opsporingsambtenaar maakt een proces-verbaal van vernietiging op nadat de gegevens zijn vernietigd op grond van een bevel vernietiging van de officier van justitie. Het opmaken van een proces-verbaal vindt ten spoedigste plaats.	1
10. Verstrekking en bewerking van vastgelegde gegevens		
N36	Alleen die gegevens die binnen de categorieën van gegevens in het bevel van de officier van justitie zijn opgenomen, worden door het technisch team verstrekt aan een opsporingsambtenaar die is belast met het opsporingsonderzoek.	2
N37	Bij de selectie van gegevens is gebruikgemaakt van een forensische kopie van de ter uitvoering van het bevel vastgelegde gegevens.	1 + 2

	Aanvullende toelichting: het uitgangspunt is dat het technisch team gebruikmaakt van een forensische kopie bij de uitvoering van het bevel. In de praktijk kunnen er situaties voordoen waarin het niet mogelijk is om een forensische kopie te maken maar alleen een logische kopie. In dit geval wordt dit door de opsporingsambtenaar gejournaliseerd.	
11. Bewaartermijn, verwijdering en vernietiging gegevens		
N38	De politie richt de werkprocessen, procedures en technische voorzieningen op een dusdanige wijze in en past deze zodanig toe dat gegevens tijdig, juist en volledig worden verwijderd en vernietigd. Ook geldt hierbij dat gegevens juist en volledig bewaard en toegankelijk zijn en blijven gedurende de periode dat dat vereist wordt.	3
12. Geheimhoudersgegevens		
N39	De politie heeft processen en maatregelen ingericht waardoor de mogelijkheid dat leden van het technisch team kennisnemen van geheimhoudersgegevens zoveel mogelijk wordt beperkt bij het uitvoeren van onderzoekshandelingen.	1
N40	De politie heeft processen en maatregelen ingericht zodat indien er sprake is van kennisname van geheimhoudersgegevens door leden van het technisch team, de kennis over de inhoud van geheimhoudersgegevens in een zaak niet verder wordt verspreid binnen DIGIT, het tactisch team en andere betrokkenen.	1
N41	De politie heeft processen en maatregelen ingericht zodat zodra er sprake is van kennisname van geheimhoudersgegevens door leden van het technisch team, dit onverwijld gemeld wordt aan de DIGIT officier van justitie en de DIGIT teamleiding of door de teamleiding aangewezen personen. De afhandeling van de kennisname van geheimhoudersgegevens geschiedt volgens de gegeven instructies van LP DIGIT.	1
N42	Bij toepassing van een (gecombineerd) bevel op grond van art. 126m, 126t of 126zg Sv wordt het opnemen van de communicatie onmiddellijk beëindigd, indien een nummer wordt herkend dat is aangemeld in overeenstemming met artikel 4a lid 2 van het Besluit bewaren en vernietigen niet-gevoegde stukken. Indien communicatie is opgenomen voordat het nummer is herkend, worden de voorwerpen die deze communicatie behelzen onmiddellijk langs geautomatiseerde weg vernietigd.	1

13. Informatiebeveiliging

N43	De systemen van de politie worden voortdurend beschermd en bewaakt tegen mogelijke aanvallen van buiten.	2
N44	De politie treft van passende technische en organisatorische maatregelen om een beveiligingsniveau te waarborgen dat op het risico is afgestemd. Door middel van periodieke controles ziet de politie toe of deze maatregelen juist zijn toegepast en vindt eventuele bijstelling plaats.	3

Handelingskader

Melden van onbekende kwetsbaarheden ex art.
126ffa Sv

OPENBAAR MINISTERIE

Landelijk Parket DIGIT

Datum 9 juli 2025

Auteur LP DIGIT – 5.1.2a en 5.1.2b

Inhoud

1	Inleiding	4
2	Parlementaire behandeling rondom onbekende kwetsbaarheden in het kader van de opsporing	6
3	Definitie van onbekende kwetsbaarheid	12
3.1	Definitie 'kwetsbaarheid in het kader van cybersecurity	12
3.2	Onbekende kwetsbaarheid ex art. 126ffa Sv	13
3.3	Wanneer is een kwetsbaarheid (on)bekend?	15
3.3.1	Bekendheid bij de producent v. bekendheid bij de gebruiker	16
3.4	Kwetsbaarheden die in het kader van een opsporingsonderzoek aan het licht komen	16
3.5	Specifieke situaties in het kader van definitie 'kwetsbaarheid'	18
3.5.1	Designkeuzes	18
3.5.2	Systeem ontbeert beveiligingseigenschappen	18
3.5.3	End-of-life	18
3.6	Samenvatting	19
4	Afwegingskader melden onbekende kwetsbaarheden	20
4.1	Zwaarwegend opsporingsbelang	21
4.2	Maatschappelijk belang	24
4.2.1	Inschatting maatschappelijk risico	25
4.2.2	De CVSS-score: de ernst van de kwetsbaarheid en potentiële impact van de onbekende kwetsbaarheid voor het systeem of het slachtoffer	25
4.2.3	De voetafdruk: de omvang van de kwetsbaarheid	26
4.2.4	Aanvullende informatie	27
4.3	Samenvatting toepassing afwegingskader	28
4.4	Ethische beoordeling	29
5	Moment en wijze van melden	30
5.1	Moment van melding	31
5.2	De relatieve competentie van de rechter-commissaris	31
5.3	Wijze van melding	32
5.4	Samenvatting	33

6	Bijzondere situaties	34
6.1	Commerciële binnendringsoftware	34
6.2	Onbekende kwetsbaarheden van (samenwerkings-)partners	35
6.3	Producten van antidemocratische landen	37
6.4	Producten van criminelen	38
6.5	Samenvatting	39
	BIJLAGE A	41
	Stappenplan handelingskader onbekende kwetsbaarheid	41
	BIJLAGE B	44
	Hoofdvragen onbekende kwetsbaarheid	44

1 Inleiding

Tijdens de parlementaire behandeling van artikel 126nba van het Wetboek van Strafvordering (Sv) is uitgebreid gedebatteerd over de noodzaak van de hackbevoegdheid, het gebruik van onbekende kwetsbaarheden daarbij en het maatschappelijk belang om veiligheid van het internet te waarborgen en de persoonlijke levenssfeer van gebruikers te beschermen. Bij het binnendringen¹ in een geautomatiseerd werk² door het technisch team van de politie kan gebruik worden gemaakt van verschillende technieken, zoals het gebruik van inloggegevens, *social engineering* of gebruik van bekende kwetsbaarheden. Bij het binnendringen kan ook gebruik worden gemaakt van onbekende kwetsbaarheden.³

De term onbekende kwetsbaarheid, ook bekend als 'zero-day vulnerability', is afkomstig uit de wereld van cybersecurity en computerwetenschappen. De term wordt daarbij op verschillende manieren toegepast.⁴ De strafvorderlijke definitie van een onbekende kwetsbaarheid is neergelegd in art. 126ffa lid 4 Sv.

¹ Voor de definitie van 'het binnendringen van een geautomatiseerd werk' heeft de wetgever tijdens de parlementaire behandeling veelal verwezen naar art. 138ab Sr. Deze strafbaarstelling van binnendringen in een geautomatiseerd werk heeft zijn oorsprong in het Cybercrimeverdrag en het Kaderbesluit over aanvallen op informatiesystemen. Beide bronnen hanteren de term 'toegang' tot een computersysteem of een onderdeel ervan, dan wel een informatiesysteem. In de toelichting op de wijziging van art. 138ab Sr spreekt de wetgever eveneens over 'toegang tot', waaruit zou kunnen worden afgeleid dat binnendringen en toegang hebben tot een systeem inwisselbaar zijn. In het kader van de 126nba Sv is daaraan toegevoegd dat het binnendringen op afstand en heimelijk gebeurt.

² De definitie van een geautomatiseerd werk is te vinden in art. 80sexies Sr: 'Een geautomatiseerd werk is een apparaat of een groep van onderling verbonden apparaten of samenhangende apparaten, waarvan er één of meer op basis van een programma automatische computergegevens verwerken'.

³ *Kamerstukken II, 2023-2024, 34 372, nr. 31, p.6; Kamerstukken I, 2023-2024, 34 372, O, p.7-18; Kamerstukken II, 2017-2018, 34 372, nr. 29, p. 2, 10;*

⁴ Zie ook L.Ablon, A. Bogart, 'Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits', Rand Corporation (2017), p. ix en p. 107. Binnen de cybersecurity sector wordt de term zero days gebruikt in relatie tot kwetsbaarheden waarvoor (nog) geen patch of oplossing is vrijgegeven. Een leverancier of producent kan ervan afweten maar zonder patch blijft het een zero-day heten. Zero day komt van '0-dagen om te pachten voor release'.

Het debat leidde tot een beleidslijn van de (toenmalige) regering om tijdens het opsporingsonderzoek onderkende onbekende kwetsbaarheden aan de producent te melden, tenzij het zwaarwegend opsporingsbelang daarmee in het gedrang zou komen.⁵ Om dit uitgangspunt sterker in de wet te verankeren, hebben de Kamerleden Recourt en Tellegen een amendement voorgesteld dat het uitstellen van de melding van een onbekende kwetsbaarheid bij het binnendringen ex art. 126bnba Sv reguleert; art. 126ffa Sv.⁶ Dit amendement is aangenomen en met de Wet Computercriminaliteit III (CCIII) ingevoerd. De wetgever heeft zodoende met de bepaling van art. 126ffa Sv uitstel van de melding geregeld, maar een expliciete en formele *meldplicht* is wettelijk nergens vastgelegd. De procedure van 126ffa Sv is daarmee een uitzondering op een beleidslijn die niet is geformaliseerd.

Het team van de politie dat uitvoering geeft aan de hackbevoegdheid (hierna: DIGIT) en de landelijk officier van justitie voor Digital Intrusion (hierna: DIGIT officier van justitie)⁷ handelen conform de beleidslijn 'melden, tenzij'.

Hoewel tijdens de parlementaire behandeling enkele richtlijnen zijn geboden over hoe het OM en de politie dienen om te gaan met onbekende kwetsbaarheden die tijdens de uitvoering van de hackbevoegdheid worden onderkend, is voor de uitvoeringspraktijk weinig houvast te vinden in de toelichtingen en definities. Bij afwezigheid daarvan is dit handelingskader opgesteld. Het biedt overwegingen en relevante aanknopingspunten die van belang zijn bij de vraag welke kwetsbaarheden vallen onder het bereik van art. 126ffa Sv, wanneer kwetsbaarheden gemeld moeten worden, de wijze waarop het melden dient te gebeuren en in welke gevallen aanleiding kan bestaan het melden uit te stellen.

Daarbij wordt in eerste instantie uitgewerkt welke kwetsbaarheden vallen onder het bereik van art. 126ffa Sv. Voor die categorie kwetsbaarheden geldt namelijk een kader met beperkte beleidsvrijheid voor de politie en het Openbaar Ministerie. Voor kwetsbaarheden die niet vallen onder het bereik van art. 126ffa Sv, is in de (ethische) beoordeling om al dan niet te melden, het moment van melden en de wijze waarop wordt gemeld meer beleidsvrijheid voor de politie en het Openbaar Ministerie.

Dit handelingskader bevat een afwegingskader voor de DIGIT officier van justitie om de kwetsbaarheid bij de producent of leverancier te melden of uitstel van

⁵ Deze beleidslijn werd uiteengezet in de brief van de staatssecretaris van Veiligheid en Justitie en de ministers van Binnenlandse Zaken en Koninkrijksrelaties en Defensie d.d. 8 november 2016 (kamerstukken II, 2016/17, 26 643, nr. 428). In de later behandeling van de wet CCIII is dit standpunt steeds herhaald.

⁶ *Kamerstukken II*, 2016-2017, 34 372, nr. 14.

⁷ De DIGIT officier van justitie maakt onderdeel uit van een team bij het Landelijk Parket van het Openbaar Ministerie dat het gezag voert over de uitvoering van de hackbevoegdheid. Dit team wordt hierna aangeduid als LP DIGIT.

melding bij de rechter-commissaris te vorderen. Het doel van dit afwegingskader is om een transparante afweging te kunnen maken tussen enerzijds het operationele belang van aanwending van onbekende kwetsbaarheden door de politie bij het toepassen van de hackbevoegdheid in opsporingsonderzoeken, en anderzijds het maatschappelijk belang om gebruikers van producten (hardware/software) te beschermen tegen onbekende kwetsbaarheden waarmee hen schade kan worden berokkend. Met dit afwegingskader wordt de DIGIT officier van justitie in staat gesteld een onderbouwd besluit te nemen aan de hand van vaste stappen.

Bij het maken van dit handelingskader zijn de ervaringen van DIGIT en LP DIGIT met betrekking tot het gebruik van (on)kwetsbaarheden betrokken. Daarbij zijn ook de ervaringen van partners betrokken en is gekeken naar standaarden in de wereld van cybersecurity en informatiebeveiliging. Dit handelingskader is niet absoluut en kan op grond van voortschrijdend inzicht met enige regelmaat worden aangescherpt.

De volgende hoofdstukken gaan dieper in op de achtergrond, de totstandkoming en de kaders van de beleidslijn 'melden, tenzij' en art.126ffa Sv (hoofdstuk 2). De definitie van onbekende kwetsbaarheid en nadere invulling daarvan komt daarna aan de orde (hoofdstuk 3). Vervolgens wordt een afwegingskader voor de DIGIT officier van justitie uitgewerkt (hoofdstuk 4) en wordt beschreven op welk moment en welke wijze kwetsbaarheden moeten worden gemeld (hoofdstuk 5). Tot slot worden enkele bijzondere situaties besproken (hoofdstuk 6).

In bijlage A bij dit handelingskader is het stappenplan beschreven, dat begint vanaf het onderkennen van een onbekende kwetsbaarheid in het kader van een opsporingsonderzoek, tot het melden ervan aan de producent dan wel tot de beslissing van de rechter-commissaris om de melding tijdelijk uit te stellen. Tevens is een beknopte versie van het afwegingskader voor de DIGIT officier van justitie als bijlage B opgenomen.⁸

2 Parlementaire behandeling rondom onbekende kwetsbaarheden in het kader van de opsporing

Tijdens de parlementaire behandeling van de wet CCIII is uitgebreid gedebatteerd over het binnendringen door het technisch team van de politie met gebruikmaking van onbekende kwetsbaarheden en daarbij het risico van het in stand houden dan

⁸ Dit handelingskader vervangt de notitie 'Melden onbekende kwetsbaarheden ex art. 126ffa Sv' van 1 maart 2021.

wel onbekend laten van onbekende kwetsbaarheden. Leden van verschillende fracties toonden zich kritisch over het gebruik van onbekende kwetsbaarheden bij de voorgestelde bevoegdheid tot het op afstand binnendringen in een geautomatiseerde werk. Zij uitten hun zorgen over de noodzaak van het gebruik van onbekende kwetsbaarheden en de mogelijke inbreuk op persoonlijke levenssfeer en de internetveiligheid. Bij het ontbreken van een voorgestelde regeling over het gebruik van onbekende kwetsbaarheden bij toepassing van de hackbevoegdheid werd de minister bij de behandeling van de wet CCIII herhaaldelijk gevraagd daarover een standpunt in te nemen.

Separaat aan dit debat werd in het domein van de inlichtingen- en veiligheidsdiensten een soortgelijke discussie gevoerd.⁹ Daarbij rapporteerde de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) in 2017 in haar rapport over de hackbevoegdheid van de diensten ook over dit punt.¹⁰

Een en ander leidde ertoe dat de toenmalige staatssecretaris van Veiligheid en Justitie en de ministers van Binnenlandse Zaken en Koninkrijksrelaties en de Defensie op 8 november 2016 een gezamenlijke brief aan de Tweede Kamer stuurden over de omgang met onbekende kwetsbaarheden door de inlichtingen- en veiligheidsdiensten en door de politie en het Openbaar Ministerie.¹¹ In die brief verwoordde de regering een beleidslijn die er op neer komt dat de regering is gericht op een open, vrij en veilig internet en daarmee op vermindering van het aantal onbekende kwetsbaarheden. Ten behoeve van de veiligheid in de digitale samenleving staat voorop dat kwetsbaarheden die gebruikt kunnen worden voor het binnendringen in principe zo snel mogelijk aan de producent gemeld worden, opdat de noodzakelijke veiligheidsmaatregelen kunnen worden getroffen ter voorkoming van misbruik door derden van deze kwetsbaarheid.

Dat geldt ook voor onbekende kwetsbaarheden die in het kader van een opsporingsonderzoek ter kennis komen van de politie of het Openbaar Ministerie. De beleidslijn ten aanzien daarvan is als volgt.

“In het wetsvoorstel Computercriminaliteit III is de inzet in het kader van de opsporing alleen mogelijk voor een beperkt aantal ernstige strafbare

⁹ Deze discussie leidde tot een motie waarin werd beoogd de regering ertoe aan te zetten een regeling te creëren gericht op het afwegen van kwetsbaarheden die door de diensten werden signaleerd én die niet bekend werden gemaakt, omdat de diensten daarvan zelf gebruik willen maken (*Kamerstukken I 2014/15*, CVIII, nr. G.). Zie voor de reactie van de minister *Kamerstukken I 2014-2015*, CVIII, nr. N.

¹⁰ Toezichtsrapport nr. 53 over de inzet van de hackbevoegdheid door de AIVD en MIVD, d.d. 25 april 2017.

¹¹ *Kamerstukken II*, 2016-2017, 26 643, nr. 428.

feiten en is vooraf toestemming van een rechter-commissaris vereist. De proportionaliteit en subsidiariteit worden zo voorafgaand aan de inzet onafhankelijk getoetst. Politie en justitie hebben, net als in de fysieke wereld, een groot belang bij het voorkómen en beperken van criminaliteit. Het laten voortbestaan van een onbekende kwetsbaarheid kan een risico inhouden op (meer) slachtoffers van criminaliteit. 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.

Ook voor kwetsbaarheden die in een opsporingsonderzoek worden aangetroffen (*red.* 'ook' slaat hier terug op de alinea waarin geschetst is hoe de inlichtingendiensten hier mee omgaan) geldt echter dat er in uitzonderlijke gevallen redenen kunnen zijn die het melden (tijdelijk) in de weg staan. In dergelijke gevallen kan het Openbaar Ministerie, na een zorgvuldige afweging, besluiten de melding van een kwetsbaarheid uit te stellen. Dat kan zich bijvoorbeeld voordoen als de melding zou resulteren in onderkenning van het opsporingsonderzoek door de verdachte of als het een systeem betreft dat door criminelen is vervaardigd en/of vrijwel alleen voor criminele doeleinden wordt gebruikt. Deze afweging overstijgt het individuele opsporingsonderzoek en wordt daarom binnen het Openbaar Ministerie centraal genomen. Daarbij wordt onder meer gelet op de kans dat de kwetsbaarheid door kwaadwillenden wordt uitgebuit en het aantal onschuldige personen en organisaties dat hierdoor kwetsbaar is. Het uitstellen van het delen van informatie over aangetroffen onbekende kwetsbaarheden in wijdverbreide en regulier gebruikte hardware of software ligt niet in de rede."¹²

De brief en de daarin verwoordde beleidslijn leidde tot meerdere moties en amendementen, waaronder het in de inleiding genoemde amendement van leden Recourt en Tellegen.¹³ Met dat amendement werd de huidige tekst van art. 126ffa Sv geïntroduceerd.

art. 126ffa Sv

1. De officier van justitie kan op grond van een zwaarwegend opsporingsbelang bevelen dat het bekend maken aan de producent van een onbekende kwetsbaarheid voor het binnendringen in een geautomatiseerd werk, bedoeld in de artikelen 126nba, 126uba en 126zpa, wordt uitgesteld.
2. Een bevel als bedoeld in het eerste lid is schriftelijk en vermeldt . de kwetsbaarheid en het zwaarwegend opsporingsbelang.

¹² *Kamerstukken II*, 2016-2017, 26 643, nr. 428, p. 4/5.

¹³ *Kamerstukken II*, 2016-2017, 34 372, nr. 14.

3. Het bevel, bedoeld in het eerste lid, kan slechts worden gegeven na voorafgaande schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris.
4. Onder onbekende kwetsbaarheid als bedoeld in het eerste lid wordt verstaan een kwetsbaarheid in een geautomatiseerd werk waarvan aannemelijk is dat die niet bekend is of kan worden verondersteld niet bekend te zijn bij de producent van het apparaat of van het programma op basis waarvan automatisch computergegevens worden verwerkt, en die kan worden gebruikt om dat geautomatiseerde werk binnen te dringen.

Het amendement (en daarmee het artikel) werd als volgt toegelicht:

“Dit amendement beoogt om de regel dat kwetsbaarheden in geautomatiseerde werken door de officier van justitie moeten worden gemeld sterker in de wet te verankeren. Het uitgangspunt zijn integere en veilige geautomatiseerde werken. De overheid dient dit te bevorderen. Vanwege de risico’s die kwetsbaarheden in een geautomatiseerd werk met zich mee brengen, is de regel dat bekende kwetsbaarheden worden gemeld om de eigenaar van dat werk in staat te stellen die kwetsbaarheid te verhelpen. Het voorliggend wetsvoorstel biedt echter de mogelijkheid om op grond van een zwaarwegend opsporingsbelang een kwetsbaarheid niet te melden. Dit amendement regelt dat de officier van justitie het bevel om een kwetsbaarheid niet te melden pas kan geven na een machtiging hiertoe door de rechter-commissaris. Hiermee wordt een onafhankelijke rechterlijke toets in de wet gebracht waarmee voorkomen kan worden dat de officier van justitie mogelijk te gemakkelijk het opsporingsbelang boven de veiligheid van een geautomatiseerd werk laat prevaleren.”¹⁴

De beleidslijn ‘melden, tenzij’ lijkt daarbij door de opstellers als regel te zijn opgevat, terwijl – zoals in de inleiding al werd opgemerkt – die niet is geformaliseerd in een wettelijke of ministeriele regeling. Het gevolg daarvan is dat de toelichting en duiding van gehanteerde termen en praktische handvatten voor in te richten procedures beperkt bleven tot hetgeen in de brief en de toelichting op het amendement (summier) is verwoord.

De vraag van een aantal leden van de Tweede Kamer om heldere regels op te stellen over het soort onbekende kwetsbaarheden dat de overheid mag gebruiken en (tijdelijk) open mag houden, beantwoordde de minister met vergelijkbare bewoording als in de brief van 8 november 2016:

“Het beleid van de regering is gericht op een open, vrij en veilig internet en daarmee op vermindering van het aantal onbekende kwetsbaarheden. Het uitgangspunt van de regering is dat onbekende kwetsbaarheden in hard-of software zo snel mogelijk aan de betreffende fabrikant worden gemeld. Dat

¹⁴ *Kamerstukken II*, 2016-2017, 34 372, nr. 14, p. 2.

geldt ook voor onbekende kwetsbaarheden die in het kader van een opsporingsonderzoek ter kennis komen van de politie of het openbaar ministerie. (....)

Gezien de diverse vormen waarin onbekende kwetsbaarheden kunnen voorkomen is een afweging per individueel geval aangewezen. Met de hiervoor besproken procedurele waarborgen en kaders is naar mijn mening sprake van zorgvuldig en terughoudend beleid voor het in uitzonderlijke gevallen tijdelijk niet melden van onbekende kwetsbaarheden dat voldoende ruimte biedt voor de afweging in een individueel geval. Verdere formalisering acht ik onwenselijk.”¹⁵

Zodoende zijn ook hier een nadere toelichting en duiding van gehanteerde termen en praktische handvatten voor in te richten procedures beperkt gebleven.

Het debat over onbekende kwetsbaarheden in de Eerste Kamer richtte zich eveneens op de vraag wat het beleid was ten aanzien van onbekende kwetsbaarheden in het kader van het wetsvoorstel.¹⁶ Ook hier herhaalde de minister het beleid van de regering zoals op 8 november 2016 verwoord,¹⁷ aangevuld met hetgeen in het amendement van de leden Recourt en Tellegen was toegevoegd.¹⁸ De minister onderstreepte daarbij dat hij het afwegen van belangen bij uitstek zag als één van de kerntaken van zowel de zittende als staande magistratuur.¹⁹

De belangenafweging is zodoende de norm bij het gebruik van onbekende kwetsbaarheden in het kader van de hackbevoegdheid. Daarbij heeft de minister in grote lijnen enkele de uitgangspunten geschetst:

- 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.²⁰
- Voor kwetsbaarheden die in een opsporingsonderzoek worden aangetroffen geldt dat er in uitzonderlijke gevallen redenen kunnen zijn die het melden (tijdelijk) in de weg staan.²¹ Er moet dan wel sprake zijn van een zwaarwegend opsporingsbelang. Dit is het geval wanneer het

¹⁵ *Kamerstukken II*, 2017-2018, 34 372, nr. 27.

¹⁶ *Kamerstukken I*, 2017-2018, 34 372, G, p. 3-4.

¹⁷ *Kamerstukken I*, 2017-2018, 34 372, G, p. 4; *Kamerstukken II*, 2017-2018, 34 372, nr. 27.

¹⁸ *Kamerstukken I*, 2017-2018, 34 372, G, p. 4. Zie ook *Kamerstukken II*, 2016-2017, 34 372, nr. 14.

¹⁹ *Kamerstukken I*, 2017-2018, 34 372, G, p. 6.

²⁰ *Kamerstukken II*, 2016-2017, 26 643, nr. 428, p. 4-5.

²¹ *Kamerstukken II*, 2016-2017, 26 643, nr. 428, p. 4-5.

opsporingsbelang zwaarder weegt dan het maatschappelijk belang om de producent de mogelijkheid te bieden de kwetsbaarheid te verhelpen.²²

- Het uitstellen van het delen van informatie over aangetroffen onbekende kwetsbaarheden in wijdverbreide en regulier gebruikte hardware of software ligt niet in de rede.²³
- De afweging of er een zwaarwegend opsporingsbelang is, overstijgt het individuele opsporingsonderzoek. Daarom wordt deze beslissing binnen het Openbaar Ministerie centraal genomen door de DIGIT officier van justitie.²⁴
- De opdracht om een kwetsbaarheid te melden wordt gegeven aan DIGIT. Het technisch team van politie dat is belast met de uitvoering van de bevoegdheid (en dat onderdeel is van DIGIT) heeft namelijk het overzicht over het gebruik en melden van onbekende kwetsbaarheden.²⁵

In de praktijk blijkt echter dat deze algemene uitgangspunten ten aanzien van verschillende aspecten vragen oproepen en nadere invulling behoeven. Zo laat de wetsgeschiedenis onduidelijkheid bestaan over het moment en wijze van melden van een onbekende kwetsbaarheid die gebruikt kan worden voor het binnendringen en wordt niet duidelijk hoe moet worden omgegaan met onbekende kwetsbaarheden die buiten een concreet opsporingsonderzoek om of in het kader van een samenwerkingsverband worden ontdekt. Evenmin is geregeld welke rechter-commissaris bevoegd is om kennis te nemen van een vordering tot machtiging als bedoeld in art. 126ffa Sv geregeld.²⁶

De definitie van een onbekende kwetsbaarheid is daarbij zodanig ruim geformuleerd en summier toegelicht dat vragen ontstaan over de reikwijdte van het begrip. De huidige wet- en regelgeving geeft geen duidelijk antwoord op de vraag of een kwetsbaarheid per definitie elk gebrek of lek in een hard-of software omvat en aan welke criteria een onbekende kwetsbaarheid moet voldoen om een geautomatiseerd werk binnen te kunnen dringen. Bovendien is de wetgever beperkt ten aanzien van de vraag wanneer een kwetsbaarheid als bekend of onbekend moet worden beschouwd.

Voor deze verdere invulling lijkt de minister ruimte te hebben gelaten aan het Openbaar Ministerie en de politie.

²² *Kamerstukken I*, 2017-2018, 34 372, G, p. 6 (NMvA I).

²³ *Kamerstukken II*, 2016-2017, 26 643, nr. 428, p. 4-5.

²⁴ *Kamerstukken II*, 2016-2017, 26 643, nr. 428, p. 4-5. Zie ook *Kamerstukken I*, 2017/18, 34 372, G, p. 6 (NMvA I).

²⁵ *Kamerstukken I*, 201-2017, 34 372, D, p. 23 (MvA I).

²⁶ De bepalingen in Sv die de relatieve competentie regelen, sluiten niet aan op art. 126ffa Sv.

3 Definitie van onbekende kwetsbaarheid

Het volgende hoofdstuk richt zich op de definitie van kwetsbaarheid in de context van cybersecurity en strafvordering. Het behandelt de vraag wanneer een kwetsbaarheid als bekend of onbekend kan worden beschouwd bij de producent en of de bekendheid van een kwetsbaarheid bij de gebruiker relevant is. Het bespreekt de reikwijdte van art. 126ffa Sv en de zwakheden in systemen die buiten de kaders van art. 126ffa Sv vallen.

3.1 Definitie 'kwetsbaarheid in het kader van cybersecurity

Bestaande internationale bronnen en technische specificaties die van toepassing zijn in cybersecurity – zoals standaarden voor informatiebeveiliging en vulnerability disclosure (ISO 27001 en ISO 29147) de Internet Security Glossy (RFC4949) en Common Weakness Enumeration (CWE) van de MITRE Corporation – geven een gedetailleerder beeld van de betekenis van een kwetsbaarheid of *vulnerability* dan tijdens de behandeling van de wetsvoorstel CCIII naar voren is gekomen. Hoewel een eenduidige definitie van een kwetsbaarheid ook uit die bronnen niet volgt, zijn er zeker drie belangrijke componenten aan te wijzen als het gaat om een kwetsbaarheid in een geautomatiseerd systeem.

- 1) 'weakness': er moet sprake zijn van een fout of zwakheid in een systeem;
- 2) 'exploitable': die zwakheid moet voor de aanvaller te benutten of te 'misbruiken' zijn;
- 3) 'violation of security policy': het gebruik van die zwakheid door een aanvaller leidt tot het doorbreken van een (relevant) veiligheidseigenschap, zoals vertrouwelijkheid, integriteit en beschikbaarheid.

Veel voorkomende zwakheden ontstaan door programmeerfouten, waarbij de code van de programmeur een fout bevat die het systeem verzwakt. Daarnaast kunnen zwakheden ook ontstaan door verkeerde configuratie van software of tijdens de ontwerpfase voordat de code zelfs is geschreven. Zwakheden kunnen in categorieën onderverdeeld worden met behulp van de publieke standaard CWE.²⁷

Wanneer een zwakheid eenmaal is gevonden, volgt de vraag of deze toegankelijk is voor een aanvaller. Met deze toegankelijkheid wordt bedoeld dat een potentiële aanvaller de zwakheid zou kunnen 'triggeren' met een hulpmiddel, een stuk code of een actie. De zwakheid wordt dan op een dusdanige manier aangesproken dat

²⁷ De CWE is een internationaal gemeenschapsproject dat erop gericht is gebreken in software en hardware beter te begrijpen en geautomatiseerde tools te creëren die bugs of gebreken kan identificeren, verhelpen en voorkomen. Zie <https://cwe.mitre.org/>

het systeem iets anders doet dan wat het behoort te doen. In principe gaat het om een theoretische toegankelijkheid, de mogelijkheid om de zwakheid te benutten als de gelegenheid zich zou voordoen. Daadwerkelijke toegang tot het systeem is daarbij niet vereist. In het verlengde van deze 'toegankelijkheid' ligt de exploiteerbaarheid van een zwakheid. Dat wil zeggen dat de zwakheid kan worden uitgebuit of misbruikt. Een zwakheid die misbruikt kan worden is in beginsel ook een zwakheid die voor de aanvaller toegankelijk is. Andersom hoeft dat niet het geval te zijn; niet elke voor de aanvaller toegankelijke zwakheid is per definitie ook te misbruiken.

Dit misbruik maken of uitbuiten van een zwakheid moet tot het doorbreken van een bepaalde veiligheidseigenschap leiden. In beginsel staat het effect op de vertrouwelijkheid, integriteit en beschikbaar van de hard- of software centraal bij de vraag of sprake is van een inbreuk op de beveiligingseigenschappen. Als de (theoretische) mogelijkheid om misbruik te maken van een zwakheid in hard- of software leidt tot een aantasting van de vertrouwelijkheid, integriteit en beschikbaar van de hard-of software kunnen we spreken van een kwetsbaarheid of *vulnerability*. Uit het voorgaande volgt ook dat als een zwakheid niet toegankelijk is voor een aanvaller, niet uitgebuit of misbruikt kan worden, of niet leidt tot een aantasting van de vertrouwelijkheid, integriteit en beschikbaar van de hard-of software er geen sprake is van een kwetsbaarheid.²⁸

3.2 Onbekende kwetsbaarheid ex art. 126ffa Sv

De hiervoor beschreven nuancering van het begrip kwetsbaarheid kan worden benut bij de beoordeling van de vraag of sprake is van een kwetsbaarheid zoals bedoeld in de beleidsbrief van 8 november 2016 of is vastgelegd in art. 126ffa Sv.

In die brief wordt een eerste invulling gegeven van de term 'kwetsbaarheden'.

'Om een geautomatiseerd werk binnen te dringen is het gebruik van kwetsbaarheden in hard- en software één van de methoden. Indien een kwetsbaarheid bij de desbetreffende fabrikant bekend is, dan kan deze de kwetsbaarheid verhelpen door een update, patch of nieuwe versie van het product uit te brengen. Veel kwetsbaarheden zijn echter niet bekend bij de fabrikant. In dat geval is het voor de fabrikant niet mogelijk de kwetsbaarheid te verhelpen. Onbekende kwetsbaarheden blijven soms jarenlang onopgemerkt. Indien een ander dan de fabrikant een dergelijke kwetsbaarheid vindt, dan wordt dit ook wel een «zero-day vulnerability»

²⁸ Een vergelijkbare definitie vindt men terug in het beleid van de Amerikaanse overheid rondom het gebruik van onbekende kwetsbaarheden. Volgens het Amerikaanse *Vulnerabilities Equities Process* is een exploit 'a tool, code or action designed to take advantage of a vulnerability and execute unexpected or unintended behavior, or impact confidentiality, integrity, or vulnerability of availability of information.'

genoemd. Een dergelijke kwetsbaarheid kan worden gebruikt om binnen te dringen door software te schrijven die van de kwetsbaarheid gebruik maakt. In dat geval is er sprake van een «zero day exploit».²⁹

In deze brief wordt een koppeling gemaakt tussen het binnendringen van een geautomatiseerd werk en de toepassing daarbij van (on)bekende kwetsbaarheden. Die koppeling komt ook terug in art. 126ffa Sv en de definitie van onbekende kwetsbaarheid die daarin wordt gegeven. Art. 126ffa lid 4 Sv luidt als volgt:

‘Onder onbekende kwetsbaarheden als bedoeld in het eerste lid wordt verstaan een kwetsbaarheid in een geautomatiseerd werk waarvan aannemelijk is dat die niet bekend is of kan worden verondersteld niet bekend te zijn bij de producent van het apparaat of van het programma op basis waarvan automatisch computergegevens worden verwerkt, en die kan worden gebruikt om dat geautomatiseerde werk binnen te dringen.’

Op basis van deze definitie en in navolging van de beleidslijn ‘melden, tenzij’ is zodoende sprake van een onbekende kwetsbaarheid indien:

- aannemelijk is dat die niet bekend is of kan worden verondersteld niet bekend te zijn bij de producent van het apparaat of van het programma op basis waarvan automatisch computergegevens worden verwerkt, en;
- die kan worden gebruikt om dat geautomatiseerde werk binnen te dringen.

Kwetsbaarheden die niet gebruikt kunnen worden om binnen te dringen, maar gebruikt kunnen worden voor andere handelingen vallen op basis van deze definitie dus niet onder de verplichting tot melden.³⁰ Dit kunnen kwetsbaarheden zijn die enkel gebruikt kunnen worden voor het verrichten van onderzoekshandelingen, zoals bijvoorbeeld een kwetsbaarheid die benut kan worden om gegevens ontoegankelijk te maken (ex art. 126nba lid 1 sub e Sv). Het kan ook gelden voor kwetsbaarheden die worden gebruikt bij de aanwending van andere opsporingsbevoegdheden dan art. 126nba Sv. Zoals bijvoorbeeld een kwetsbaarheid die gebruikt kan worden om – na inbeslagname – met fysieke toegang tot een device toegang te krijgen tot opgeslagen versleutelde gegevens.

Kwetsbaarheden die bekend zijn, vallen op basis van deze definitie evenmin onder de verplichting tot melden.

²⁹ *Kamerstukken II*, 2016-2017, 26 643, nr. 428, p.2.

³⁰ Dit neem niet weg dat – gelet op de algemene uitgangspunten die door de minister zijn geschetst en tijdens de parlementaire behandeling zijn onderschreven – met het oog op de veiligheid in de digitale wereld altijd gekeken moet worden naar de noodzaak en mogelijkheden om dergelijke kwetsbaarheden toch publiekelijk kenbaar te (laten) maken.

3.3 Wanneer is een kwetsbaarheid (on)bekend?

De vraag die vervolgens rijst, is wanneer een kwetsbaarheid bekend of onbekend is. Uit art. 126ffa Sv volgt dat een kwetsbaarheid onbekend is wanneer aannemelijk is dat die niet bekend is of niet kan worden verondersteld bekend te zijn bij de producent. Een nadere duiding aan de term 'bekendheid' ontbreekt. Art. 126ffa Sv noch de wetsgeschiedenis geven handvatten aan de hand van welke factoren beoordeeld kan worden of een producent deze wetenschap heeft of aannemelijk is dat die wetenschap er is.

Op basis van de ervaringen van DIGIT en LP DIGIT, uitgangspunten bij cybersecurity en ervaringen van partners zijn een aantal factoren te benoemen die helpen bij het bepalen of een kwetsbaarheid bekend of onbekend is.

- 1) Er is een *Common Vulnerabilities and Exposures* - nummer (hierna: CVE-nummer) voor die specifieke kwetsbaarheid beschikbaar/toegekend;³¹
- 2) Er is informatie over de kwetsbaarheid gepubliceerd op openbare en beschikbare bronnen, zoals relevante internetfora en blogs. De mate van bekendheid en toegankelijkheid van het platform of het bericht zal daarbij van belang zijn om te beoordelen of aannemelijk is dat de producent daar bekend mee is;
- 3) Er is een algemeen beschikbare en gepubliceerde patch en/of update voor de kwetsbaarheid uitgebracht;
- 4) Er zijn mitigerende maatregelen beschikbaar voor de betreffende kwetsbaarheid en deze zijn gepubliceerd bij de producent / een nationaal Computer Emergency Response Team (CERT) / een lid van Forum of Incident Response and Security Teams (FIRST) of een andere gezaghebbende bron;³²
- 5) De kwetsbaarheid betreft een gedocumenteerde functionaliteit (bijvoorbeeld een handleiding van een product of een

³¹ Het Common Vulnerabilities and Exposures (CVE) systeem is een referentie methode voor publiekelijk bekende kwetsbaarheden in computersystemen. Iemand die een dergelijke kwetsbaarheid ontdekt kan deze aanmelden. Indien de melding aan een aantal voorwaarden voldoet, wordt deze door een CVE Numbering Authority (CNA) online gepubliceerd in een CVE list. Het doel van deze lijst is om informatie over bekende kwetsbaarheden te delen, zodat bedrijven die de software gebruiken zich tegen aanvallen kunnen beschermen. Meer informatie over CVE is te vinden op www.cve.org.

Een punt van aandacht is dat CVE en CWE twee verschillende dingen zijn.

³² In veel gevallen zal tussen het bekend worden van de kwetsbaarheid en (installatie van) de patch enige tijd zitten, waarbij mitigerende maatregelen worden genomen en gepubliceerd om de impact van de schade te beperken. Men kan denken aan het informeren van het grotere publiek door een nieuwsbericht de wereld in te brengen waarin wordt afgeraden bepaalde producten te gebruiken.

- voorgeprogrammeerd standaard wachtwoord) die een nadelige impact heeft op beschikbaarheid, integriteit en/of vertrouwelijkheid;
- 6) De politie beschikt over informatie waarin afdoende onderbouwd staat dat de kwetsbaarheid bij de producent bekend is.

3.3.1 Bekendheid bij de producent v. bekendheid bij de gebruiker

Opmerkelijk is dat de vraag of gebruikers van hard- of software bekend hadden kunnen zijn met de kwetsbaarheid door de wetgever niet als relevant lijkt te worden beschouwd, terwijl uit de praktijk volgt dat bekendheid bij de (eind)gebruiker vanuit het oogpunt van cybersecurity en het maatschappelijk belang evengoed van betekenis is. Zoals in de voorgaande paragraaf is opgemerkt, gaat het bij bekendheid van een kwetsbaarheid om de bekendheid ervan bij de producent. In de brief van 8 november 2016 wordt geformuleerd dat het melden van onbekende kwetsbaarheden is gericht op de fabrikant of producent van hard- en software. Er zijn in die brief geen overwegingen gewijd aan de situatie dat op het niveau van een gebruiker implementatie of configuratie fouten worden gemaakt of de gebruiker hard- en software anders gebruikt dan door de producent beoogt. Evenmin is een voorziening getroffen voor de situatie waarin de politie kennis over een kwetsbaarheid deelt met een producent, maar deze er voor kiest die kwetsbaarheid niet te verhelpen en niet aan de gebruikers kenbaar te maken. Ook in de tekst van art. 126ffa Sv staat de producent centraal.

De wijze van implementatie, configuratie en gebruik door de gebruiker van een geautomatiseerd werk zal doorgaans invloed hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van dat geautomatiseerd werk en de zich daarop bevindende gegevens. Dit kunnen keuzes zijn waarbij de beveiliging wordt opgeofferd aan beschikbaarheids-of gebruiksgemak of de operationele betrouwbaarheid. Maar er kan ook sprake zijn onvoldoende kundigheid bij een gebruiker. Daarnaast kan het voorkomen dat een gebruiker een geautomatiseerd werk anders dan op de door de fabrikant beoogde wijze gebruikt of kiest voor een wijze van gebruik van de beschikbare apparaat eigenschappen die een niet-standaard werking mogelijk maken of de functionaliteit van het apparaat vergroten of verkleinen.

Voor geen van deze situaties is in de brief van 8 november 2016 of art. 126ffa Sv een voorziening getroffen. De consequentie daarvan is dat kwetsbaarheden die zich voordoen op het niveau van gebruikers van hard- en software buiten het bestek vallen van de geformuleerde beleidslijn 'melden, tenzij' en het bepaalde in artikel 126ffa Sv. Ze vallen daarmee ook buiten het hierna weergegeven afwegingskader.

3.4 Kwetsbaarheden die in het kader van een opsporingsonderzoek aan het licht komen

Bij de parlementaire behandeling van de wet CCIII benadrukt de minister bij herhaling dat het melden van onbekende kwetsbaarheden door de politie ziet op

kwetsbaarheden die in het kader van een opsporingsonderzoek aan het licht komen c.q. bekend worden, worden gebruikt of kwetsbaarheden die in een opsporingsonderzoek worden aangetroffen. Daarmee lijkt de minister beoogd te hebben het uitgangspunt om de kwetsbaarheid te melden te verbinden aan het opsporingsonderzoek en de feitelijke uitvoering van de bevoegdheid ex art. 126nba Sv. Deze koppeling met het opsporingsonderzoek blijkt zowel uit de formulering bij de behandeling in de Tweede Kamer³³ als bij de behandeling in de Eerste Kamer.³⁴

In deze koppeling aan een opsporingsonderzoek zit een zekere dualiteit met het herhaaldelijk benoemen dat de politie of het Openbaar Ministerie zo spoedig mogelijk melding maken van onbekende kwetsbaarheden als ze daar kennis over verwerven. Door deze formulering ontstaat onduidelijkheid over de vraag of dit direct melden ook betrekking heeft op onbekende kwetsbaarheden waar de politie bekend mee raakt buiten het bestek van een opsporingsonderzoek. Bij de behandeling in de Eerste Kamer lijkt D66 te proberen om dit concreter te krijgen. Ze stellen de minister de volgende vragen:

“De leden van de fractie van D66 meenden dat een onbekende kwetsbaarheid direct zou moeten worden gemeld na ontdekking daarvan door de politie of het openbaar ministerie, en hebben gevraagd wat het beleid is ten aanzien van onbekende kwetsbaarheden in het kader van het voorliggende wetsvoorstel. Deze leden hebben tevens gevraagd of de regering van mening is dat onbekende kwetsbaarheden zo snel mogelijk moeten worden gemeld.”³⁵

Bij de beantwoording op die vraag herhaalt de minister dat het gaat om onbekende kwetsbaarheden die in het kader van een opsporingsonderzoek bekend worden.³⁶

Het een en ander leidt tot de conclusie dat onbekende kwetsbaarheden die buiten een concreet opsporingsonderzoek om bij DIGIT bekend worden, buiten het afwegingskader van art. 126ffa Sv vallen.

Zodra dergelijke kwetsbaarheden op een later moment ex art. 126nba Sv worden ingezet in het kader van een opsporingsonderzoek, dan vallen ze vanaf dat moment onder het bereik van art. 126ffa Sv en zal vanaf dat moment een afweging gemaakt moeten worden of er aanleiding is om het melden uit te stellen.

³³ *Kamerstukken II*, 2016–2017, 26 643, nr. 428, p. 4; *Kamerstukken II*, 2017–2018, 34 372, nr. 27, p. 13/14.

Kamerstukken II, 2018–2019, 34 372, nr. 29, p. 8.

³⁴ *Kamerstukken I*, 2016–2017, 34 372, D, p. 20 en 23; *Kamerstukken I*, 2017–2018, 34 372, G, p. 4 en 8.

3.5 Specifieke situaties in het kader van definitie 'kwetsbaarheid'

Naast de hiervoor benoemde algemene detaillering van het begrip kwetsbaarheid en de specificering daarvan in art. 126ffa Sv zijn er enkele specifieke situaties te benoemen die niet betrokken zullen worden in het afwegingskader voor het melden van een onbekende kwetsbaarheid.³⁷

3.5.1 Designkeuzes

Sommige zwakheden in hard- en software zijn het gevolg van implementatie/programmeer keuzes van een producent. Het kan bijvoorbeeld zo zijn dat een zwakheid alleen in zeer moeilijke omstandigheden is te misbruiken, het voordeel van een aanvaller dusdanig beperkt is dat de zwakheid wordt getolereerd, de producent een kosten-baten afweging heeft gemaakt of waarbij de veiligheidsmaatregelen door de producent moedwillig zijn opgeofferd ten bate van beschikbaarheids-of gebruiksgemak of de operationele betrouwbaarheid. Hoewel sommige van dit soort designkeuzes een nadelige impact kunnen hebben op de beschikbaarheid, integriteit en/of vertrouwelijkheid en daar misbruik van gemaakt kan worden, merken wij ze niet aan als kwetsbaarheid. In een dergelijk geval heeft de producent de keuze gemaakt dat misbruik van die zwakheid geen '*violation of security policy*' oplevert. De eigenschappen die dan doorbroken worden zijn door de producent niet geduid als (voldoende relevante) veiligheidseigenschap.

3.5.2 Systeem ontbeert beveiligingseigenschappen

In het verlengde van gemaakte designkeuzes is er hard- en software zonder inherente beveiligingseigenschappen. Dat kan bijvoorbeeld het geval zijn als een producent het product niet heeft ontworpen met de intentie om online beschikbaar te zijn. Voor dergelijke hard- en software geldt eveneens dat het verkrijgen van toegang tot een dergelijk product geen '*violation of security policy*' oplevert.

3.5.3 End-of-life

Hard- en software hebben naast hun feitelijke levensduur een economische levensduur. Tijdens deze economische levensduur zal een producent hardware doorgaans ondersteunen met nieuwe versies van software en de bij software doorgaans updates uitbrengen waarin verbeteringen worden doorgevoerd of veiligheidsproblemen worden verholpen. Zodra een product niet meer wordt ondersteund of niet meer wordt voorzien van updates is dat product end-of-life.

³⁷ Eenzelfde benadering vindt men terug in het Amerikaanse Patch Act 2017 waarin een concreet aantal gevallen van kwetsbaarheden is benoemd dat buiten het afwegingskader valt. De Amerikaanse visie op dit punt lijkt te zijn dat sommige kwetsbaarheden door hun ernstig gebrekkige ontwerp en vormgeving geen onbekende kwetsbaarheden kunnen zijn en dus niet gewogen dan wel gemeld moeten worden.

In dergelijke gevallen valt van een melding van een onbekende kwetsbaarheid veelal niet te verwachten dat dit tot een patch zal leiden.

De in deze paragraaf beschreven specifieke zwakheden of kwetsbaarheden kunnen niet gerekend worden tot onbekende kwetsbaarheden in de zin van art. 126ffa Sv. Om die reden worden deze niet betrokken in het afwegingskader voor het melden van onbekende kwetsbaarheden ex art.126ffa Sv.³⁸

3.6 Samenvatting

Dit hoofdstuk behandelde de definitie van een kwetsbaarheid in de context van cybersecurity en strafvordering. Hieruit blijkt dat de bestaande internationale bronnen en technische specificaties die van toepassing zijn in cybersecurity een gedetailleerder beeld geven van de betekenis van een kwetsbaarheid of *vulnerability* dan tijdens de behandeling van de wetsvoorstel CCIII naar voren is gekomen.

Uit die bronnen en specificaties volgt dat kwetsbaarheden fouten of zwakheden in een geautomatiseerd werk zijn, die toegankelijk en exploiteerbaar zijn en die leiden tot het doorbreken van een (relevant) veiligheidseigenschap. In de context van strafvordering komt daarbij dat het doorbreken van een (relevant) veiligheidseigenschap bestaat uit het heimelijk en op afstand, in een concreet onderzoek binnendringen van een specifieke geautomatiseerde werk. Daarnaast dient het aannemelijk te zijn dat de onbekende kwetsbaarheid niet bekend is of kan worden verondersteld niet bekend te zijn bij de producent van het apparaat of van het programma op basis waarvan automatisch computergegevens worden verwerkt.

Kwetsbaarheden die bekend zijn of niet gebruikt kunnen worden om binnen te dringen, maar gebruikt kunnen worden voor andere handelingen vallen op basis van deze definitie niet onder de verplichting tot melden.

De vraag of een kwetsbaarheid bekend of onbekend is hangt van een aantal factoren af, zoals bijvoorbeeld of de producent een beschikbare en gepubliceerde patch voor die kwetsbaarheid heeft uitgebracht, of een CVE-nummer voor die specifieke kwetsbaarheid beschikbaar is, of bijvoorbeeld informatie over de kwetsbaarheid gepubliceerd is op openbare en beschikbare bronnen.

Hoewel de bekendheid bij de gebruikers in de context van cybersecurity en het maatschappelijk belang relevant is, staat in art. 126ffa Sv de producent centraal. Kwetsbaarheden die zich voordoen op het niveau van gebruikers van hard- en software vallen buiten het bestek van de geformuleerde beleidslijn 'melden, tenzij'

³⁸ Dat neemt niet weg dat rekening zal worden gehouden met eventuele maatschappelijke risicofactoren en indien nodig zullen mitigerende maatregelen worden getroffen of zal worden gekeken of melden toch gepast is.

en het bepaalde in artikel 126ffa Sv daarmee ook buiten het hierna weergegeven afwegingskader.

Onbekende kwetsbaarheden die buiten het kader van een opsporingsonderzoek om bij de politie/het Openbaar Ministerie bekend worden, vallen in principe ook buiten het afwegingskader van art. 126ffa Sv. Zodra deze kwetsbaarheden op een later moment in een concreet onderzoek ex art. 126nba Sv worden ingezet zal vanaf dat moment een afweging moeten worden gemaakt of er aanleiding is om het melden uit te stellen.

Tot slot zijn op basis van cybersecurity principes en *best practices* van binnenlandse-en buitenlandse partners enkele specifieke situaties onderkend waarbij de zwakheid niet onder de definitie van kwetsbaarheid valt en daarmee niet betrokken zal worden bij het afwegingskader. Te denken valt aan zwakheden die het gevolg zijn van gebrekkige implementatie of programmeerkeuzes van een producent. Andere voorbeelden zijn zwakheden in hardware/software die essentiële beveiligingseigenschappen missen en hardware of software die end-of-life is.

4 Afwegingskader melden onbekende kwetsbaarheden

Wanneer eenmaal is vastgesteld dat sprake is van een onbekende kwetsbaarheid in de zin van art. 126ffa Sv volgt de vraag of redenen bestaan om de melding van die onbekende kwetsbaarheid uit te stellen. Voor onbekende kwetsbaarheden die vallen onder het bereik van art. 126ffa Sv heeft de wetgever tijdens de parlementaire behandeling een aantal uitgangspunten benoemd voor het maken van die afweging.³⁹

Door de minister werd benoemd dat in uitzonderlijke gevallen redenen kunnen bestaan die het melden van onbekende kwetsbaarheden door politie en Openbaar Ministerie tijdelijk in de weg staan.⁴⁰ In zulke gevallen kan het Openbaar Ministerie, na een zorgvuldige afweging, besluiten de melding van een kwetsbaarheid uit te stellen.⁴¹ Deze afweging overstijgt het individuele opsporingsonderzoek en wordt daarom centraal binnen het Openbaar Ministerie

³⁹ Die uitgangspunten zijn hieronder beschreven, nader uitgewerkt en geconcretiseerd. Deze uitgangspunten kunnen ook dienen voor de weging of kwetsbaarheden die niet vallen onder het bereik van art. 126ffa Sv, maar waar wel aanleiding voor bestaat om deze te melden bij de producent of anderszins kunnen worden gemitigeerd.

⁴⁰ *Kamerstukken I*, 2017/2018, 34 372, G, p. 3-4.

⁴¹ *Kamerstukken II*, 2016/2017, 26 643, nr. 428, p. 4 -5.

genomen.⁴² Op grond van art. 126ffa Sv heeft de officier van justitie een machtiging van de rechter-commissaris nodig als zij/hij uitstel van de melding wil bevelen.

Het melden van onbekende kwetsbaarheden houdt een afweging in tussen enerzijds het maatschappelijk belang en anderzijds het opsporingsbelang. Van zwaarwegend opsporingsbelang is sprake wanneer het opsporingsbelang zwaarder weegt dan het maatschappelijk belang om de producent de mogelijkheid te bieden de kwetsbaarheid te verhelpen.⁴³ Het gaat daarbij niet zozeer om een afweging tussen cyberveiligheid en «offline»-veiligheid, maar om een afweging tussen het belang van de opsporing en het belang van het bevorderen van de mogelijkheid voor de producent om de onbekende kwetsbaarheid te verhelpen en daarmee de veiligheid van gebruikers van de desbetreffende producten te bevorderen.⁴⁴

4.1 Zwaarwegend opsporingsbelang

Uit de parlementaire geschiedenis bij art. 126nba Sv en art. 126ffa Sv volgen twee voorbeelden van zwaarwegende opsporingsbelangen.

Er is sprake van zwaarwegend opsporingsbelang indien de melding zou resulteren in het tenietdoen van het heimelijke karakter van het opsporingsonderzoek.⁴⁵ In de praktijk betekent dit doorgaans dat het melden van een onbekende kwetsbaarheid zicht kan geven op de concrete en afgeschermdde modus operandi van DIGIT of eventuele opsporingsbelangen- en kansen in het onderzoek kan frustreren. Bovendien kan de melding het individueel belang van een concrete zaak schaden, bijvoorbeeld wanneer de verdachte vroegtijdig op de hoogte zou raken van het onderzoek tegen hem.

Een andere belangrijke reden om uitstel van de melding te bevelen is wanneer de onbekende kwetsbaarheid een systeem of computerprogramma betreft dat door criminelen is vervaardigd en/of vrijwel alleen voor criminele doeleinden wordt gebruikt.⁴⁶ De aard en gebruikers van bepaalde software kunnen zodanig malafide zijn dat een melding van de kwetsbaarheid aan de producent in het maatschappelijk verkeer als onredelijk en onacceptabel zou worden geacht. Daarbij bestaat het reële risico dat de makers dankzij de melding wijzer worden, de software aanscherpen of door ontwikkelen en voor crimineel gebruik

⁴² *Kamerstukken II*, 2016/2017, 26 643, nr. 428, p. 4 5.

⁴³ *Kamerstukken I*, 2018/2019, 34 372, nr. 29, p. 8 / 9.

⁴⁴ *Kamerstukken I*, 2017–2018, 34 372, G, p. 7.

⁴⁵ *Kamerstukken II*, 2016/17, 26 643, nr. 428, p. 4-5 en *Kamerstukken I*, 2016/2017, 34 372, D, p. 18-19.

⁴⁶ *Kamerstukken II*, 2018/19, 34 372, nr. 27, p. 13-14 (Verslag II); *Kamerstukken II*, 2018/19, 34 372, nr. 29 p. 8/9 (Verslag II); *Kamerstukken II*, 2016/17, 26 643, nr. 428, p. 4-5; *Kamerstukken I*, 2016-2017, 34 372, D, p. 18-19 (MvA I)

toegankelijk laten, terwijl de methodieken van DIGIT in zo'n geval zijn prijsgegeven en de opsporingskansen teniet gedaan.

Een nadere toelichting wanneer het opsporingsbelang zou worden geschaad, volgt niet uit de wetsgeschiedenis.

Als het gaat om opsporingskansen zijn ook toekomstige opsporingskansen van belang. Zo overwoog de rechter-commissaris - in een onderzoek waarin het OM een machtiging vorderde op grond van art. 126ffa Sv - dat met het uitstel van de bekendmaking van de onbekende kwetsbaarheid de mogelijkheden worden vergroot dat ook in de toekomst de kwetsbaarheid in een opsporingsonderzoek kan worden gebruikt.⁴⁷ Het opsporingsbelang werd hiermee als zeer zwaarwegend beschouwd. Eenzelfde benadering vindt men terug in de parlementaire geschiedenis rondom art. 187d Sv, waarbij onder het algemeen opsporingsbelang werd begrepen ook het belang om in de toekomst nogmaals van een bepaalde informant gebruik te maken.⁴⁸

De term 'zwaarwegend opsporingsbelang' komt in het Wetboek van Strafvordering op enkele plekken terug. In art. 187d Sv is een regeling getroffen waarbij een rechter-commissaris kan beletten dat antwoorden op vragen betreffende een bepaald gegeven ter kennis komen van de officier van justitie, de verdachte en diens raadsman, indien er geground vermoeden bestaat dat door de openbaarmaking van dit gegeven bepaalde belangen worden geschaad.⁴⁹ Een van die belangen is een zwaarwegend opsporingsbelang.⁵⁰ De Memorie van Toelichting bij die bepaling spreekt van reële en zwaarwegende opsporingsbelangen, waarmee vermoedelijk bedoeld wordt dat er een voldoende ernstige gevaar voor schending moet bestaan. Als voorbeeld noemt de wetgever de gegevens over de concrete uitvoering van specifieke opsporingsmethoden en technieken.⁵¹ Daaronder zouden gegevens kunnen vallen die de gebruikte strategieën en technieken prijsgeven. Een concreet voorbeeld wordt niet genoemd, maar ter

⁴⁷ Rb Den Haag 1 januari 2013, ECLI:NL:RBDHA:2013:19764.

NB De uitspraakdatum is geanonimiseerd, maar om systeemtechnische redenen is in de metadata een fictieve uitspraakdatum opgenomen.

⁴⁸ *Kamerstukken II*, 1996-1997, 25 403, nr. 3, p. 19 en p. 115.

⁴⁹ Art. 187d Sv. De memorie van toelichting bij art. 187d Sv noemt in dit verband gegevens betreffende de identiteit van de getuige en bijvoorbeeld de identiteit van de informant, indien die niet de getuige is, of informatie over opsporingstechnieken. Vgl. *Kamerstukken II* 1996-1997, 25 403, 3, p. 20.

⁵⁰ Een zwaarwegend opsporingsbelang kan grond zijn voor het handhaven van de anonimiteit en het horen bij de rechter-commissaris buiten aanwezigheid van de verdediging ex art. 187a lid 2 Sv. Het Europees Hof voor de rechten van de mens heeft in het arrest Lüdi van 15 juni 1992 overwogen dat een opsporingsbelang grond kan zijn voor het handhaven van de anonimiteit van een getuige. Vgl. EHRM 15 juni 1992, nr. 12433/86 (Lüdi tegen Zwitserland)

⁵¹ *Kamerstukken II* 1996-1997, 25 403, nr. 3, p. 19.

illustratie kan men denken aan handelingen bij het plaatsen van technische hulpmiddelen ten behoeve van het toepassen van OVC. De plaatsing daarvan wordt in principe niet geverbaliseerd, omdat deze van de buitenwereld afgeschermd moet blijven om het (toekomstig) opsporingsbelang te waarborgen.

Ook bij het in art. 126ff Sv geformuleerde doorlaatverbod komt de term zwaarwegend opsporingsbelang terug, maar is dat niet nader omschreven.

Beide bepalingen zijn ingevoerd met de Wet Bijzondere opsporingsbevoegdheden. In de Memorie van Toelichting bij die wet staat de wetgever wat uitgebreider stil bij de noodzaak om bepaalde informatie af te kunnen schermen in een opsporingsonderzoek, maar ook hier geeft de wetgever beperkt invulling aan de term zwaarwegend.⁵² De invulling lijkt vooral aan de uitvoeringspraktijk te worden gelaten:

"Bij de beoordeling of van een zwaarwegend opsporingsbelang sprake is, zullen altijd de concrete omstandigheden van het geval bepalend zijn. Of vervolgens een goed oordeel in de zaak toestaat dat informatie verborgen blijft, zal steeds alleen moeten worden beoordeeld door de zittingsrechter."⁵³

Andere bronnen die behulpzaam kunnen zijn bij de nadere invulling van dit criterium, lijken er niet te zijn. De rechtspraak over zwaarwegend opsporingsbelang heeft met name betrekking op de inzet van informaten en anonieme getuigen en het belang van afscherming van hun (persoons)gegevens. Die rechtspraak centreert zich daarmee rond de criteria die hiervoor zijn besproken. In OM beleidsregels komt de term beperkt voor en wordt niet verder uitgewerkt. Tot slot komt in het initiatief wetsvoorstel 'Wet Zeroday's Afwegingsproces'⁵⁴ het criterium "zwaarwegend opsporingsbelang" eveneens terug. De toelichting en behandeling van dit voorstel bevatten echter evenmin nieuwe of andere uitleg dan hiervoor al is beschreven.

Resumerend volgt uit het voorgaande dat door de wetgever geformuleerd uitgangspunten voor het beoordelen van de vraag of sprake is van een zwaarwegend opsporingsbelang zijn:

- 1) als de melding zou resulteren in het tenietdoen van het heimelijke karakter van het opsporingsonderzoek;
- 2) als het een systeem of computerprogramma betreft dat door criminelen is vervaardigd en/of vrijwel alleen voor criminele doeleinden wordt gebruikt;

⁵² *Kamerstukken II* 1996-1997, 25403, nr. 3, p. 19.

⁵³ *Kamerstukken II* 1996-1997, 25 403, 3, p. 19.

⁵⁴ *Kamerstukken II*, 2018-2019, 35 257. Dit wetsvoorstel is op 19 juli 2019 ingediend, maar tot op heden niet aangenomen door de Tweede Kamer. Er is op dit moment geen zicht op een nadere behandeling van het voorstel in de Tweede Kamer.

3) als door het melden informatie wordt prijsgegeven over de concrete uitvoering van specifieke opsporingsmethoden- en technieken;

Het is daarbij aan de uitvoeringspraktijk om de mate van 'zwaarwegendheid' van het opsporingsbelang nader in te vullen.

Naast (nationale) opsporingsbelangen kunnen ook andere belangen bestaan, terwijl die niet terug komen in de beleidslijn 'melden, tenzij' en het bepaalde in artikel 126ffa Sv. Opmerkelijk is dat een van de andere belangen van art. 187d Sv niet is overgenomen; het belang van de staatsveiligheid. Het is zeer wel denkbaar dat een door de politie onderkende onbekende kwetsbaarheid ook relevant is voor de taakstellingen van de inlichtingen- en veiligheidsdiensten en melden van die kwetsbaarheid belangen van nationale veiligheid schaadt. Daarnaast kan het voorkomen dat een onbekende kwetsbaarheid onder voorwaarde van geheimhouding is gedeeld.

4.2 Maatschappelijk belang

In de beleidsbrief van 8 november 2016 verwoordt het kabinet dat het een vrij, open en veilig internet wil bevorderen en zodoende (onbekende) kwetsbaarheden in hard- en software wil beperken. Het maatschappelijk belang beoogt kort gezegd de internetveiligheid en persoonlijke levenssfeer van internetgebruikers te waarborgen. In het kader van art. 126ffa Sv gaat het daarnaast om het belang van integere en veilige geautomatiseerde werken.⁵⁵ De mate van kans dat de kwetsbaarheid door kwaadwillenden zou worden uitgebuit en het aantal onschuldige personen en organisaties dat hierdoor kwetsbaar wordt, zijn twee door de wetgever genoemde factoren die van belang zijn bij de afweging van het maatschappelijk belang om de kwetsbaarheid bij de producent te melden of uitstel van melding te bevelen.

Een andere belangrijke afwegingsomstandigheid is de mate waarin de desbetreffende hard-of software wordt gebruikt bij de vitale infrastructuur of regulier en wijdverbreid is in de maatschappij.⁵⁶ Een uitgebreide toelichting volgt niet uit de parlementaire geschiedenis, maar de wetgever doelde hiermee mogelijk op kwetsbaarheden in een van de besturingssystemen van Microsoft, of (andere) systemen die veelvuldig gebruikt worden door bijvoorbeeld ziekenhuizen, de financiële sector en energiesector. Het niet op tijd verhelpen van die kwetsbaarheid kan grote maatschappelijke impact tot gevolg hebben. De wetgever overweegt daarover dat het uitstellen van het melden van informatie

⁵⁵ Beslissing op een vordering tot machtiging uitstel melding onbekende kwetsbaarheid, Rb Den Haag, 1 januari 2013, ECLI:NL:RBDHA:2013:19764.

NB De uitspraakdatum is geanonimiseerd, maar om systeemtechnische redenen is in de metadata een fictieve uitspraakdatum opgenomen.

⁵⁶ *Kamerstukken II*, 2018-2019, 34 372, nr. 29, p. 8 / 9.

over aangetroffen onbekende kwetsbaarheden in wijdverbreide en regulier gebruikte hardware of software niet in de rede ligt.⁵⁷

4.2.1 Inschatting maatschappelijk risico

Om tot een gedegen afweging te kunnen komen zullen de maatschappelijke risico's moeten worden ingeschat. In de wetsgeschiedenis zijn geen verwijzingen te vinden naar hulpmiddelen en instrumenten die kunnen helpen bij het in kaart brengen van de maatschappelijke risico's. De wetgever lijkt daar bij de behandeling van artikel 126ffa Sv weinig aandacht aan te hebben besteed.

In de cybersecurity sector zijn dergelijke hulpmiddelen/instrumenten wel aanwezig. Daarbij ligt de focus met name bij de evaluatie van de ernst van de kwetsbaarheid en de impact voor het systeem of de slachtoffers. In de praktijk wordt veelvuldig gebruik gemaakt van CVSS-scores. CVSS wordt gebruikt om prioriteit te geven aan het verhelpen van kwetsbaarheden en zo de kritieke en algemene risico's voor de organisatie in kwestie te verminderen.⁵⁸ CVSS staat voor *Common Vulnerability Scoring System* en is bedoeld om kwetsbaarheden op een gestandaardiseerde manier te evalueren en te rangschikken. Dit systeem is inmiddels uitgegroeid tot een industriestandaard en is zodoende een waardevol instrument om te gebruiken voor de beoordeling van de vraag wat de impact van de kwetsbaarheid is op potentiële slachtoffers. Hieronder zal nader uitgewerkt worden hoe de CVSS-score gebruikt kan worden voor de inschatting van maatschappelijke risico's bij onbekende kwetsbaarheden als bedoeld in art. 126ffa Sv.

De CVSS score geeft echter geen inzicht in de omvang van een bepaalde kwetsbaarheid of de impact op de Nederlandse maatschappij, terwijl dat door de wetgever ook relevant gevonden wordt. Voor een vollediger beeld zal daarom tevens een inschatting moeten worden gemaakt van de omvang van de kwetsbaarheid en de gevolgen van het niet (op tijd) verhelpen van die kwetsbaarheid in bredere maatschappelijke zin. Hoe vaak en door wie de kwetsbare software/hardware allemaal wordt gebruikt, zijn belangrijke vragen om (zo goed als mogelijk) te achterhalen of de kwetsbaarheid een significant risico inhoudt voor de maatschappij in de algemene zin. We spreken in dat kader over 'de voetafdruk' van de kwetsbaarheid. Ook ten aanzien van die 'voetafdruk' zal hieronder toegelicht worden hoe die gebruikt kan worden bij de inschatting van maatschappelijke risico's.

4.2.2 De CVSS-score: de ernst van de kwetsbaarheid en potentiële impact van de onbekende kwetsbaarheid voor het systeem of het slachtoffer

⁵⁷ Kamerstukken I, 2017-2018, 34 372, G, p. 9.

⁵⁸ Zie websites van SANS (www.sans.org) en FIRST (www.first.org).

Ten behoeve van de beoordeling van de ernst en de potentiële impact van de onbekende kwetsbaarheid kan met het CVSS model een score worden berekend. Hiervoor kan bijvoorbeeld gebruik worden gemaakt van tools van FIRST. Hoe hoger de uitkomst van de berekende CVSS-score, hoe impactvoller de kwetsbaarheid voor het geautomatiseerd werk en de gebruiker ervan.

Het CVSS genereert een score van 0 tot 10 op basis van de ernst van de kwetsbaarheid. Een score van 0 betekent dat een kwetsbaarheid minder significant is dan de hoogste kwetsbaarheid met een score van 10. De CVSS-waarden zijn gegroepeerd en kunnen variëren van Hoog, Medium en Laag.⁵⁹ Het CVSS combineert vele factoren om een score te kunnen genereren. Omdat dit systeem steeds aangepast wordt aan de geldende uitgangspunten, volstaan we hier met het noemen van enkele belangrijke uit versie 4.0.

- Hoe kan de aanvaller toegang krijgen tot het systeem ('attack vector')
- Hoe complex is het om de kwetsbaarheid te exploiten ('attack complexity');
- Welke privileges heeft de aanvaller nodig voor hij de kwetsbaarheid kan exploiten ('privileges required');
- Of interactie van de gebruiker nodig is om de kwetsbaarheid succesvol te kunnen exploiten ('user interaction');
- Ongeautoriseerde toegang tot gevoelige informatie ('confidentiality');
- Mogelijkheid voor ongeautoriseerde aanpassingen ('integrity') en; Mogelijkheid voor weigering van toegang tot geautomatiseerde gebruiker ('availability').

4.2.3 De voetafdruk: de omvang van de kwetsbaarheid

Zoals gezegd is de voetafdruk een indicator van de omvang van de kwetsbaarheid en de potentiële gevolgen als de kwetsbaarheid niet, of niet op tijd wordt verholpen. De voetafdruk is lastig meetbaar en een concreet, nauwkeurig instrument of specifieke elementen die kunnen helpen bij de beoordeling ervan ontbreken in de wetsgeschiedenis en de industriestandaarden. Uit de praktijk en ervaringen van partners volgen enkele vragen die relevant kunnen zijn bij het onderzoek naar de voetafdruk van de kwetsbaarheid. Daarbij is aansluiting gezocht bij de voorbeelden die de wetgever heeft aangedragen. Zoals de vraag of de kwetsbare hardware/software gebruikt wordt bij de vitale infrastructuur of regulier en wijdverbreid is in de maatschappij. In de onderstaande tabel zijn de relevante vragen weergegeven.

⁵⁹ Tijdens het schrijven van dit handelingskader maakt DIGIT gebruik van de 4^e en laatste versie van CVSS, de CVSS-v4. Bij elke nieuwe versie zal DIGIT beoordelen in hoeverre de wijzigingen ten opzichte van de laatste versie relevant zijn voor de berekening van de potentiële maatschappelijke impact.

Soms kunnen deze vragen op een doelgerichte manier worden beantwoord. Als dat niet mogelijk is, kan gebruik worden gemaakt van de kwalificatie Hoog, Gemiddeld en Laag. Hoe hoger de kwalificatie, hoe groter de voetafdruk en hoe risicovoller de kwetsbaarheid is voor de maatschappij.

	Voetafdruk van de onbekende kwetsbaarheid	
1.	Wat is het geschatte marktaandeel van het kwetsbare product in Nederland?	Zover bekend: aantal organisaties of percentage marktaandeel
2.	Hoe frequent wordt het kwetsbare product naar schatting in Nederland gebruikt?	Zover bekend: aantal organisaties of particulieren in Nederland
3.	Binnen welke sectoren en bedrijven wordt het kwetsbare product zover bekend gebruikt? Score per sector.	• Rijksoverheid • Lokale overheden • Vitale-en topsectoren • Groot zakelijk • MKB • Particulieren

DIGIT kan bij beantwoording van die vragen verschillende bronnen bevragen, waaronder politiesystemen en bronnen van andere opsporingsdiensten, (semi-)publieke bronnen en commerciële bronnen.

Bij de beantwoording van deze vragen gaat het om het geven van een redelijke inschatting. Bij voorkeur is die inschatting onderbouwd en zo specifiek mogelijk. Als dat niet mogelijk is, kan de inschatting worden gegeven met de kwalificatie Hoog, Gemiddeld en Laag. Hoe hoger de kwalificatie, hoe groter de voetafdruk en hoe risicovoller de kwetsbaarheid is voor de maatschappij.

4.2.4 Aanvullende informatie

Onder bepaalde omstandigheden kan aanvullende informatie over de kwetsbaarheid nodig zijn om de maatschappelijke risico's beter te begrijpen. DIGIT zal - eventueel op verzoek van DIGIT officier van justitie- onderzoeken of nadere informatie beschikbaar is. De volgende vragen kunnen daarbij houvast bieden.

- Is de onbekende kwetsbaarheid te verhelpen met een patch?
- Zit de onbekende kwetsbaarheid in andere versies van hetzelfde product?
- Zit de onbekende kwetsbaarheid in andere producten van dezelfde producent?

- Zit de onbekende kwetsbaarheid in soortgelijke producten van andere producenten?

Aanvullend onderzoek is optioneel en zal niet voor alle onbekende kwetsbaarheden plaatsvinden; er is geen verplichting om verdiepend technisch onderzoek uit te voeren naar elke kwetsbaarheid.

Kort resumerend, DIGIT zal in samenwerking met DIGIT officier van justitie middels een CVSS-score en een evaluatie van de omvang van een onbekende kwetsbaarheid (de voetafdruk) inzichtelijk proberen te maken wat de potentiële gevolgen voor de Nederlandse maatschappij zouden zijn wanneer de kwetsbaarheid door een kwaadwillende actor zou worden gebruikt.

4.3 Samenvatting toepassing afwegingskader

Op grond van hetgeen onder 4.1 en 4.2 is beschreven kunnen via een gestructureerde denkwijze de relevante elementen worden verzameld om een beslissing te nemen op de vraag of een onbekende kwetsbaarheid moet worden gemeld of dat aanleiding bestaat om – na een daartoe verkregen machtiging van de rechtercommissaris – uitstel te bevelen.

Uit het voorgaande blijkt dat het melden van een onbekende kwetsbaarheid een afweging inhoudt tussen enerzijds het maatschappelijk belang en anderzijds opsporingsbelang; van zwaarwegend opsporingsbelang is sprake wanneer het opsporingsbelang zwaarder weegt dan het maatschappelijk belang om de producent de mogelijkheid te bieden de kwetsbaarheid te verhelpen.

Door de wetgever geformuleerde uitgangspunten voor het beoordelen van de vraag of sprake is van een zwaarwegend opsporingsbelang zijn:

- als de melding zou resulteren in het tenietdoen van het heimelijke karakter van het opsporingsonderzoek;
- als het een systeem of computerprogramma betreft dat door criminelen is vervaardigd en/of vrijwel alleen voor criminele doeleinden wordt gebruikt;
- als door het melden informatie wordt prijs gegeven over de concrete uitvoering van specifieke opsporingsmethoden- en technieken;

Als het gaat om opsporingskansen zijn ook toekomstige opsporingskansen van belang.

De term 'zwaarwegend opsporingsbelang' komt in het Wetboek van Strafvordering op enkele plekken terug, maar is meestal beperkt beschreven. Het is daarbij aan de uitvoeringspraktijk om de mate van 'zwaarwegendheid' van het opsporingsbelang nader in te vullen.

Het maatschappelijk belang beoogt de internetveiligheid en persoonlijke levenssfeer van internetgebruikers te waarborgen. In het kader van art. 126ffa Sv gaat het daarnaast om het belang van integere en veilige geautomatiseerde werken.⁶⁰

De mate van kans dat de kwetsbaarheid door kwaadwillenden zou worden uitgebuit en het aantal onschuldige personen en organisaties dat hierdoor kwetsbaar wordt, zijn twee door de wetgever genoemde factoren die van belang zijn bij de afweging van het maatschappelijk belang om de kwetsbaarheid bij de producent te melden of uitstel van melding te bevelen.

Een andere belangrijke afwegingsomstandigheid is de mate waarin de desbetreffende hard-of software wordt gebruikt bij de vitale infrastructuur of regulier en wijdverbreid is in de maatschappij.⁶¹ De wetgever overweegt daarover dat het uitstellen van het melden van informatie over aangetroffen onbekende kwetsbaarheden in wijdverbreide en regulier gebruikte hardware of software niet in de rede ligt.⁶²

Om tot een gedegen afweging te kunnen komen, zullen de maatschappelijke risico's moeten worden ingeschat. Daarbij ligt de focus met name bij de evaluatie van de ernst van de kwetsbaarheid en de impact voor het systeem of de slachtoffers. CVSS wordt gebruikt om prioriteit te geven aan het verhelpen van kwetsbaarheden en zo de kritieke en algemene risico's voor de organisatie in kwestie te verminderen.⁶³ Voor een vollediger beeld zal daarnaast een inschatting moeten worden gemaakt van de omvang van de kwetsbaarheid en de gevolgen van het niet (op tijd) verhelpen van die kwetsbaarheid in bredere maatschappelijke zin. Hoe vaak en door wie de kwetsbare software/hardware allemaal wordt gebruikt, zijn belangrijke vragen om (zo goed als mogelijk) te achterhalen of de kwetsbaarheid een significant risico inhoudt voor de maatschappij in de algemene zin.

4.4 Ethische beoordeling

Vanuit ethisch oogpunt kan het in bepaalde gevallen wenselijk zijn om ook kwetsbaarheden in overweging te nemen die niet onder het bovengenoemde wegingskader vallen. Zo kan vroegtijdig een inschatting worden gemaakt van de mogelijke maatschappelijk risico's en kan potentiële schade worden

⁶⁰ Beslissing op een vordering tot machtiging uitstel melding onbekende kwetsbaarheid, Rb Den Haag, 1 januari 2013, ECLI:NL:RBDHA:2013:19764.

NB De uitspraakdatum is geanonimiseerd, maar om systeemtechnische redenen is in de metadata een fictieve uitspraakdatum opgenomen.

⁶¹ *Kamerstukken II*, 2018-2019, 34 372, nr. 29, p. 8 / 9.

⁶² *Kamerstukken I*, 2017-2018, 34 372, G, p. 9.

⁶³ Zie websites van SANS (www.sans.org) en FIRST (www.first.org).

geminimaliseerd. Risicobeoordeling en preventie zijn hierbij de belangrijkste uitgangspunten. Door dit soort kwetsbaarheden in bepaalde mate te beoordelen op hun ernst en omvang wordt bijgedragen aan het maatschappelijk belang van veilig internet en een zorgvuldige en verantwoorde omgang met geautomatiseerde werken.

De afwegingen en oriëntatiepunten die in het hierboven geschetste handelingskader zijn besproken, kunnen ook relevant zijn voor een ethische beoordeling van kwetsbaarheden die buiten de reikwijdte van artikel 126ffa Sv vallen. Zo kan het zwaarwegend opsporingsbelang tegen het licht van maatschappelijk belang worden gelegd en kan een inschatting van maatschappelijke risico's worden gemaakt. Indien die beoordeling daar aanleiding voor geeft, kan DIGIT in overeenstemming met DIGIT officier van justitie toch de beslissing nemen om de kwetsbaarheid bij de makers te melden of kunnen andere mitigerende maatregelen worden getroffen

Welke maatregelen het meest geschikt zijn en op welk moment moet worden gehandeld, zal per geval worden bekeken. Het een en ander ligt ter professionele beoordeling en discretie van DIGIT, in zorgvuldig overleg met DIGIT officier van justitie.

5 Moment en wijze van melden

De opdracht om de kwetsbaarheid te melden, komt terecht bij het team dat belast is met de uitvoering van de 126nba Sv: DIGIT. Bij dat team is het overzicht over het gebruik en melden van onbekende kwetsbaarheden.⁶⁴ Het uitgangspunt is dat onbekende kwetsbaarheden in beginsel direct of zo snel mogelijk aan de leverancier of fabrikant worden gemeld,⁶⁵ maar op welke wijze en onder welke voorwaarden dat zou moeten gebeuren heeft de wetgever niet bepaald noch zijn deze aspecten tijdens de parlementaire behandeling voldoende aan bod gekomen.

⁶⁴ *Kamerstukken I*, 2016/2017, 34 372, D, p. 23.

⁶⁵ *Kamerstukken I*, 2017-2018, 34 372, G, p. 3-4; *Kamerstukken I*, 2016-2017, 34 372 D, p. 25. Over de betekenis van de term 'direct' is eerder verwarring ontstaan. In de optiek van DIGIT en landelijk officier van justitie DIGIT wordt met 'direct' bedoeld 'terstond', en niet 'rechtstreeks' (zonder tussenkomst van derden). Dat met 'direct' terstond of zo snel mogelijk door de wetgever werd bedoeld, volgt ook uit hiervoor aangehaalde kamerstukken.

5.1 Moment van melding

Hiervoor is stilgestaan bij de keuze die wetgever lijkt te hebben gemaakt om het melden van onbekende kwetsbaarheden te verbinden aan het ontdekken daarvan in het kader van een opsporingsonderzoek. Uit de wetsgeschiedenis volgt geen dwingende verplichting om een onbekende kwetsbaarheid die gebruikt kan worden voor het binnendringen *onmiddellijk* na ontdekking daarvan te melden bij de fabrikant of leverancier. Wat de wetgever met het onderscheid tussen 'direct' en 'zo spoedig mogelijk' precies heeft bedoeld, is niet nader beschreven of toegelicht. Het impliceert in elk geval dat moment waarop het melden gebeurt, zal wisselen en per geval moet worden beoordeeld. Uiteraard zal conform het uitgangspunt sneller worden gemeld naarmate de onbekende kwetsbaarheid significanter is (dus hoe groter het maatschappelijk risico is).

Het is daarom van belang dat DIGIT met DIGIT officier van justitie periodiek bespreekt welke (onbekende) kwetsbaarheid zij heeft onderkend, hoe die kwetsbaarheid eruit ziet en wat de impact is. Daarna zal worden beoordeeld of de onbekende kwetsbaarheid moet worden gemeld of dat uitstel van melding via de rechterlijke toets aan de orde is.

5.2 De relatieve competentie van de rechter-commissaris

Zoals in hoofdstukken 2 en 4 kort is benoemd vereist het bevel tot uitstel van melding van een onbekende kwetsbaarheid een machtiging van de rechter-commissaris. Ten aanzien van artikel 126ffa Sv zijn in het Wetboek van Strafvordering geen specifieke regels opgenomen over welke rechter-commissaris bevoegd is om te oordelen over de vordering tot het verkrijgen van die machtiging. De regels rond de relatieve competentie van een rechter zijn vooral gekoppeld aan pleegplaats van een strafbaar feit of de locatie van een verdachte.

Zoals in paragraaf 3.4 uiteen is gezet gaat het om onbekende kwetsbaarheden die in het kader van een opsporingsonderzoek bekend worden. Op grond van een in dat kader gegeven machtiging ex art. 126nba Sv zal er daarom een rechter-commissaris betrokken zijn bij dat lopende onderzoek. De vordering tot machtiging om de melding uit te stellen, staat echter vaak los van het opsporingsonderzoek en overstijgt het belang van die individuele zaak. Om die reden is het niet direct logisch dat een vordering tot machtiging wordt gericht aan het kabinet van de rechter-commissaris van de rechtbank waar ook het opsporingsonderzoek gaande is. Daarbij kan het ook voorkomen dat een onderzoek niet een enkele pleegplaats heeft of dat er al zicht is op een concrete verdachte.⁶⁶

⁶⁶ Dit is bijvoorbeeld aan de orde bij onderzoeken naar grootschalige computercriminaliteit.

Verder is het belangrijk om te erkennen dat de benodigde kennis en expertise voor de beoordeling van een onbekende kwetsbaarheid niet noodzakelijkerwijs bij elke rechter-commissaris aanwezig is. Het indienen van vorderingen bij telkens verschillende rechter-commissarissen kan dan tot uiteenlopende beoordelingen leiden, wat de uniformiteit van de rechtspraak niet ten goede komt en het risico op versnippering kan vergroten.

Met het oog op het belang van uniformiteit en de waarborging van kwaliteit en deskundigheid wordt in de praktijk ervoor gekozen de vordering tot het uitstel van de melding aan rechters-commissarissen van de rechtbank Den Haag en rechtbank Amsterdam te richten. Deze rechtbanken hebben inmiddels (ruime) ervaring met de hackbevoegdheid en artikel 126ffa Sv.

In een gepubliceerde beschikking van de rechter-commissaris van 12 augustus 2021 acht de rechter-commissaris van de rechtbank Den Haag zich bevoegd tot kennisneming van de vordering op grond dat de afweging van de officier van justitie om de vordering tot hem te richten niet onredelijk of onbegrijpelijk is.⁶⁷ De DIGIT officier van justitie had gemotiveerd dat hij de vordering bij de rechter-commissaris in Den Haag had ingediend, omdat de vordering specifieke kennis en expertise bij de rechter-commissaris vereist en dit bij het kabinet van de rechter-commissaris van de rechtbank Den Haag aanwezig was.

5.3 Wijze van melding

Zoals in de inleiding al is benoemd heeft de wetgever als uitgangspunt gesteld dat de onbekende kwetsbaarheid aan de producent moet worden gemeld om de eigenaar van het geautomatiseerde werk in staat te stellen die kwetsbaarheid te verhelpen.⁶⁸ De wijze waarop dat zou moeten gebeuren, heeft de wetgever niet nader uitgewerkt of toegelicht. Uit de wettekst noch uit de wetsgeschiedenis volgt expliciet de verplichting voor DIGIT om rechtstreeks, zonder tussenkomst van een derde partij, aan de producent te melden.

5.1.2c



⁶⁷ Rb Den Haag 1 januari 2013, ECLI:NL:RBDHA:2013:19764.

NB De uitspraakdatum is geanonimiseerd, maar om systeemtechnische redenen is in de metadata een fictieve uitspraakdatum opgenomen.

⁶⁸ Zie o.a. Kamerstukken II, 2016–2017, 34 372, nr. 14.

5.1.2c



5.4 Samenvatting

Een belangrijk punt van overweging voor DIGIT en DIGIT officier van justitie is het moment en wijze van melden van onbekende kwetsbaarheden wanneer er geen gegronde redenen bestaan om uitstel van die melding te bevelen. Uit de wetsgeschiedenis volgt geen dwingende verplichting om een onbekende kwetsbaarheid die gebruikt kan worden voor het binnendringen *terstond* na ontdekking te melden bij de fabrikant of leverancier. Tijdens de parlementaire behandeling zijn termen 'direct' en 'zo spoedig mogelijk' gebruikt, en lijkt hiermee vooral het belang van tijdig optreden te worden benadrukt. Het exacte moment

⁶⁹ Leidraad Coordinated Vulnerability Disclosure, 2018, voorwoord.

⁷⁰ Besluit onderzoek in een geautomatiseerd werk (Stb. 2018, 340), p. 31 (NvT); *Kamerstukken II*, 2018-2019, 34 372, nr. 27. Zie ook Leidraad Coordinated Vulnerability Disclosure, 2018, p. 14.

waarop het melden gebeurt, zal echter per geval wisselen en dient per geval te worden beoordeeld.

Indien de afweging tot de conclusie zou leiden dat er gegronde redenen bestaan om melding (tijdelijk) uit te stellen, zal DIGIT officier van justitie een vordering tot uitstel van die melding aan de rechter-commissarissen van de rechtbanken Den Haag of Amsterdam richten.

5.1.2c

6 Bijzondere situaties

In de wetsgeschiedenis zijn enkele bijzondere situaties besproken die aanleiding geven tot nadere toelichting als het gaat om de werkwijze die DIGIT hanteert. Specifiek gaat het hierbij om commerciële binnendringsoftware en producten van criminelen. Uit de praktijk rijzen daarnaast vragen over de mogelijke werkwijze ten aanzien van onbekende kwetsbaarheden die DIGIT in het kader van een samenwerkingsverband verkrijgt en onbekende kwetsbaarheden in producten van antidemocratische landen die in het kader van een opsporingsonderzoek aan het licht komen. Dit laatste onderdeel richt zich op bespreking van deze vier specifieke vraagstukken.

6.1 Commerciële binnendringsoftware

Een bijzondere categorie vormen onbekende kwetsbaarheden in commerciële binnendringsoftware. Daarover zijn tijdens de parlementaire behandeling diverse vragen gesteld en is uitvoerig debat gevoerd. Uit de wetsgeschiedenis volgt dat het gebruik van commerciële binnendringsoftware van derden waarvan niet duidelijk is of deze van bekende of onbekende kwetsbaarheden gebruikmaakt, tot het uiterste geval is beperkt.⁷¹ Bij brief van 7 december 2023 heeft de minister van Justitie en Veiligheid dit nader genuanceerd door te benoemen dat het goed mogelijk is dat software van een externe leverancier relatief vaak wordt ingezet ten opzichte van het aantal inzetten, omdat minder ingrijpende methoden veelal niet volstaan.⁷²

⁷¹ Besluit onderzoek in een geautomatiseerd werk (Stb. 2018, 340), p. 15 (NvT); *Kamerstukken II* 2018-2019, 34 372, nr. 29, p. 10; *Kamerstukken II* 2015-2016, 34 372, nr. 3, p. 34-35; *Kamerstukken I*, 2016-2017, 34 372, D, p. 18-25; *Kamerstukken I* 2017-2018, 34 372, G, p. 9-12; *Kamerstukken II* 2016/17, 26 643, nr. 428.

⁷² *Kamerstukken II* 2023-2024, 34 372, nr. 31, p. 16-17.

De wetgever heeft zodoende goed bevonden dat in bepaalde situaties gebruik wordt gemaakt van extern binnendringsoftware waarin bekende en onbekende kwetsbaarheden zitten. Daarbij is geen verplichting voor de politie of het Openbaar Ministerie opgenomen om kennis te nemen van die kwetsbaarheden voordat dergelijke producten aangeschaft worden of onderzoek te doen naar de vraag of er onbekende kwetsbaarheden in een product zitten. Indien de politie of het openbaar ministerie echter kennis verwerft over onbekende kwetsbaarheden in extern binnendringsoftware, dan moeten ook deze in beginsel gemeld worden aan de fabrikant van de desbetreffende hard- of software.⁷³

In bepaalde situaties schaft DIGIT producten aan die gebruikt kunnen worden voor het binnendringen en die vermoedelijk *exploits* bevatten die gebruik maken van een of meerdere onbekende kwetsbaarheden in producten. DIGIT weet niet of en zo ja, welke onbekende kwetsbaarheden in een bepaald binnendringsoftware zitten. DIGIT is daarnaast contractueel verplicht om af te zien van 'reverse engineeren'. Zodoende is het DIGIT niet toegestaan te onderzoeken of en welke kwetsbaarheden in een eventuele *exploit* worden uitgebuit. Daarbij zullen eventuele onbekende en bekende kwetsbaarheden veelal onderdeel zijn van het intellectueel eigendomsrecht van een fabrikant van een dergelijk product. Dit intellectueel eigendomsrecht wordt door leveranciers van binnendringsoftware goed beschermd. De aanschaf van dergelijke producten vindt daarom pas plaats na ondertekening van een Non-Disclosure Agreement ('NDA'). Als DIGIT eventuele onbekende kwetsbaarheden onverhoopt zou ontdekken kan ze deze niet bekend maken zonder contractbreuk te plegen.

6.2 Onbekende kwetsbaarheden van (samenwerkings-)partners

Het is denkbaar dat in het kader van de opsporing een nationale of internationale partner haar kennis over onbekende kwetsbaarheden deelt met DIGIT, dan wel dat DIGIT bekend raakt met onbekende kwetsbaarheden in het kader van een (research) samenwerkingsverband.⁷⁴

In het eerste geval is de kennis over de kwetsbaarheid vergaard door een andere partij en is deze partij dus ook eigenaar van de kennis over de kwetsbaarheid. Kennis over kwetsbaarheden zal in de praktijk alleen gedeeld worden in vertrouwen en onder strikte voorwaarde van geheimhouding, om zo de

⁷³ Kamerstukken I, 2016-2017, 34 372, D, p. 22.

⁷⁴ Deze paragraaf heeft geen betrekking op de situatie waarin een partner een onbekende kwetsbaarheid met DIGIT deelt in het kader van een concreet opsporingsonderzoek, met het uitdrukkelijke doel om die kwetsbaarheid in dat specifieke opsporingsonderzoek bij het binnendringen van een geautomatiseerde werk te gebruiken. Zodra DIGIT een onbekende kwetsbaarheid in het kader van de uitvoering van een bevel ex art. 126nba Sv gebruikt, geldt het in hoofdstuk 4 beschreven afwegingskader.

afscherming van middelen en methodes te kunnen garanderen. Het doorbreken van deze geheimhouding zou toekomstige (nationale en internationale) samenwerking grote schade kunnen toebrengen en eventueel het opsporings- of veiligheidsbelang (ook van de partner) in gevaar kunnen brengen. In de eerder genoemde beleidsbrief en de parlementaire behandeling van de wet CCIII zijn aan deze situatie geen overwegingen gewijd.

Dit afwegingskader kan behulpzaam zijn bij de beoordeling van de vraag of DIGIT gebruik kan en wil maken van een onbekende kwetsbaarheid die in het kader van de opsporing door een (inter)nationale partner met haar is gedeeld.

De bovengenoemde beoordeling richt zich op twee belangrijke pijlers:

- 1) de vraag of de (buitenlandse) partner een eigen afwegingsproces heeft;
- 2) de vraag of het maatschappelijk risico voor de Nederlandse samenleving significant is.

Indien de partner een eigen afwegingsproces heeft en geen significant risico voor de Nederlandse samenleving aan de orde is, zal de betreffende kwetsbaarheid niet worden betrokken in dit afwegingskader. DIGIT en LP DIGIT nemen tot uitgangspunt dat de primaire verantwoordelijkheid voor het melden van onbekende kwetsbaarheden bij de partij ligt die eigenaar van die kennis is.

De situatie is anders wanneer wordt ingeschat dat de onbekende kwetsbaarheid wel een significant maatschappelijk risico zou vormen voor de Nederlandse maatschappij, dan wel wanneer de risico inschatting van de Nederlandse maatschappij niet in de beoordeling van de (internationale) partner meeweegt. In dat geval kan de onbekende kwetsbaarheid volgens het beleidskader worden gewogen en zo nodig zal DIGIT de betreffende partner aanmoedigen de kwetsbaarheid te melden aan de producent. DIGIT en LP DIGIT zullen zonder voorafgaande toestemming van de partner zelf geen melding maken of uitstel bij de rechter-commissaris vorderen, maar kunnen in een dergelijk geval wel afzien van het gebruik van de kwetsbaarheid. In uitzonderlijke gevallen is het treffen van mitigerende maatregelen niet uitgesloten.

Relevant voor gebruik van een dergelijke kwetsbaarheid door DIGIT is dus dat de (inter)nationale partner een eigen afwegingsproces heeft, of wanneer de impact van de inzet van een onbekende kwetsbaarheid in de Nederlandse maatschappij naar schatting verwaarloosbaar is. Is dat niet het geval, is terughoudendheid in de samenwerking geboden.⁷⁵

In het belang van innovatieve en technische doorontwikkeling is het voor DIGIT cruciaal om samenwerkingsverbanden aan te gaan met (inter)nationale partners.

⁷⁵ In de praktijk zal DIGIT niet snel een samenwerkingsverband aangaan met instanties die niet in dezelfde mate oog hebben voor een zorgvuldige afwegingskader en respect voor grondrechten en internetveiligheid.

In dergelijke (research) samenwerkingsverbanden zal DIGIT voor zover mogelijk streven om recht te doen aan zowel het maatschappelijk belang van veilig internet als het belang van geheimhouding van informatie over de te ontwikkelen middelen en methodes. Bij dergelijke samenwerkingsverbanden kan de vraag wie de eigenaar is van informatie over exploiteerbare kwetsbaarheden minder duidelijk zijn. Het is daarom wenselijk om bij het aangaan van dergelijke samenwerkingen duidelijkheid te verschaffen over de kaders die gelden voor DIGIT bij de omgang met onbekende kwetsbaarheden.

Daarbij zal lang niet in alle (research) samenwerkingsverbanden de rol en betrokkenheid van DIGIT dusdanig groot zijn dat van (mede-)eigenaarschap mag worden gesproken dat de verantwoordelijkheid voor het melden ervan bij DIGIT ligt. Wanneer onbekende kwetsbaarheden in het kader van een research samenwerkingsverband worden onderkend, zal de vraag welke betrokkenheid en mate van eigenaarschap DIGIT heeft bij de kennis over een exploiteerbare onbekende kwetsbaarheid daarom voorafgaand aan de twee hiervoor beschreven pijlers moten worden beantwoord.

6.3 Producten van antidemocratische landen

Tijdens de uitvoering van haar taken kan DIGIT stuiten op onbekende kwetsbaarheden in producten (hardware/software) die vrijwel uitsluitend worden gebruikt in landen waar sprake is van doelbewuste en structurele schending of niet-naleving van democratische rechtstatelijke principes, zoals Rusland, China, Iran en Noord-Korea. Het doorlopen van het afwegingskader kan in die situatie wel nuttig zijn en langdurig uitstel ligt daarbij in de rede. Het eventueel melden van de kwetsbaarheid aan de producent zal in een dergelijke situatie echter niet het door de regering beoogde effect hebben. Het doel van het melden is om bij te dragen aan een verbetering van staatsrechtelijke principes, de bescherming van gebruikers te versterken en de algehele internetveiligheid te verbeteren. In antidemocratische landen zoals die hiervoor zijn opgesomd zal het melden zelden dit effect hebben.

Het is goed voorstelbaar dat deze regimes structureel en weloverwogen gebruik van onbekende kwetsbaarheden om hun eigen samenleving en eigen bevolking digitaal onder controle te houden. Een melding van een onbekende kwetsbaarheid aan producenten van hard- en software in landen zoals Rusland, China, Iran of Noord-Korea brengt een bovengemiddeld risico met zich dat onderzoeken en modus operandi van DIGIT worden onderkend. Het valt bovendien te verwachten dat een dergelijke melding van een onbekende kwetsbaarheid juist leidt tot een verslechtering van de lokale mensenrechtensituatie en de algehele veiligheid van de samenleving. Het is redelijk voorspelbaar dat door DIGIT gemelde onbekende kwetsbaarheden elders binnen die staat (zullen) worden aangewend om de eigen samenleving en bevolking afgeschermd te kunnen controleren, of nadat een door

DIGIT gemelde onbekende kwetsbaarheid is verholpen, met hetzelfde doel naar andere onbekende kwetsbaarheden wordt gezocht.

Tot slot is het voor DIGIT niet mogelijk om op betrouwbare wijze te achterhalen wat het effect is geweest van melding van een onbekende kwetsbaarheid aan producenten van hard- en software in landen zoals Rusland, China, Iran en Noord-Korea.

Het is denkbaar dat in verschillende antidemocratische landen aldaar verblijvende Nederlandse en Westerse personen en organisaties soms gedwongen of genoodzaakt worden om bepaalde hardware/software te gebruiken. Als DIGIT die onbekende kwetsbaarheden in die hardware/software niet afwegen en niet melden, dan zijn en blijven de Nederlandse en andere Westerse gebruikers kwetsbaar voor misbruik, waaronder spionage. Tegelijkertijd bestaat er geen garantie dat die onbekende kwetsbaarheden wel worden verholpen, en als ze worden verholpen is er geen enkele garantie dat het regime geen andere middelen toepast om alsnog controle op die gebruikers van de hardware/software uit te oefenen. Het melden zal het risico op controle van die regimes geenszins verminderen.

Een uitzondering vormen onbekende kwetsbaarheden in producten afkomstig van Rusland, China, Iran en Noord-Korea maar waarvan de gebruikers (niet zijnde overwegend criminele gebruikers) zich bevinden in Nederland (of samenwerkingspartners van Nederland). In dat geval is het denkbaar dat DIGIT tot maatregelen besluit die het maatschappelijk (digitaal) veiligheidsrisico doen verminderen, bijvoorbeeld door gebruikers in Nederlands of gebruikers in overheidsdienst in het buitenland te informeren of andere mitigerende maatregelen te nemen.

6.4 Producten van criminelen

Extra aandacht verdienen ook onbekende kwetsbaarheden in producten of systemen die door criminelen zijn vervaardigd en/of hoofdzakelijk voor criminele doeleinden worden gebruikt. In hoofdstuk 4.1 is benoemd dat de wetgever hierin een bijzondere omstandigheid zag om uitstel van de melding bij de rechter-commissaris te vorderen en vervolgens te bevelen.

Uit onderzoek naar crypto communicatiediensten, maar ook uit ransomware-, phishing-, en CSAM-zaken van afgelopen jaren en de actie tegen de criminele darkwebmarkets Hansa en Genesis, is gebleken dat de georganiseerde criminaliteit gebruik maakt specifiek van, voor en door hen ontwikkelde software. Het is denkbaar dat onbekende kwetsbaarheden in dergelijke software onder het bereik van artikel 126ffa Sv kunnen vallen.

De huidige regeling van 126ffa Sv voorziet niet in afstel van een melding en de rechter-commissaris dient dan ook over het uitstel van die melding te beslissen.⁷⁶ Melden van deze kwetsbaarheden aan de makers van de software zou de criminaliteit faciliteren doordat hun software daardoor veiliger wordt. Het is aannemelijk dat de kennis over de kwetsbaarheid zal worden misbruikt bij de inrichting van nieuwe malafide systemen voor criminele doeleinden en zodoende de opsporing naar (de producenten van) dergelijke systemen ernstig wordt bemoeilijkt.⁷⁷

Op dit moment is de praktijk zo dat langdurig uitstel mogelijk is in deze gevallen, maar dat de uitstelverzoeken wel periodiek moeten worden herhaald. Dat brengt – gelet op de noodzaak deze gevoelige informatie goed te beschermen – een aanzienlijk werklast met zich mee voor de betrokken instanties. Conform de beleidsreactie van de minister op de wetsevaluatie van WODC zal de komende periode worden bezien of het melden van onbekende kwetsbaarheden in software gemaakt voor en door criminelen uitgesloten kan worden van het bereik van artikel 126ffa Sv na een machtiging daartoe van de rechter-commissaris.⁷⁸ Tot die tijd zal DIGIT officier van justitie uitstel van het melden aan de rechter-commissaris vorderen, waarbij langdurig uitstel in de rede ligt.

6.5 Samenvatting

In bepaalde situaties schaft DIGIT producten aan die gebruikt kunnen worden voor het binnendringen en die vermoedelijk *exploits* bevatten die gebruik maken van een of meerdere onbekende kwetsbaarheden in producten. DIGIT weet vaak niet of en zo ja, welke onbekende kwetsbaarheden in een bepaald binnendringingssoftware zitten. De wetgever heeft daarbij goed bevonden dat in bepaalde situaties gebruik wordt gemaakt van extern binnendringingssoftware waarin bekende en onbekende kwetsbaarheden zitten. Daarbij is geen verplichting voor de politie of het Openbaar Ministerie opgenomen om kennis te nemen van die kwetsbaarheden voordat dergelijke producten aangeschaft worden of onderzoek te doen naar de vraag of er onbekende kwetsbaarheden in een product zitten.

⁷⁶ In de eindrapportage van de PG Hoge Raad (PGHR) van september 2022 stelt de procureur-generaal dat artikel 126ffa Sv daarmee zijn doel voorbijschiet. Ook de onderzoekers van het Wetenschappelijk Onderzoek- en Datacentrum (WODC) constateerden in het kader van de wetsevaluatie CCIII dat het informeren van personen met criminele intenties dat hun systeem een kwetsbaarheid bevat, een knelpunt is voor de opsporingspraktijk. De onderzoekers stelden bovendien dat de meldplicht een risico vormt voor en de samenwerking bemoeilijkt met nationale, maar ook internationale partijen.

⁷⁷ Rb Den Haag, 1 januari 2013, ECLI:NL:RBDHA:2013:19764.

⁷⁸ *Kamerstukken II*, 2023-2024, 34 372, nr. 31, p. 20.

Als het gaat om onbekende kwetsbaarheden van samenwerkingspartners, wordt het voornoemde afwegingskader niet toegepast indien die (inter)nationale partner kennis over onbekende kwetsbaarheden deelt onder vermelding dat zij eigenaar is en blijft van de verstrekte informatie en DIGIT met die derde partij overeenkomt dat het die informatie zonder voorafgaande toestemming niet met derden zal delen.

Onbekende kwetsbaarheden in producten van criminelen en in producten van antidemocratische landen vormen een bijzondere categorie. Op dit moment is de praktijk zo dat langdurig uitstel mogelijk is in het geval dat DIGIT stuit op een onbekende kwetsbaarheid in producten die door criminelen of voor criminele doeleinden is gebouwd, maar dat uitstelverzoek zal wel periodiek moeten worden herhaald.

Ten aanzien van onbekende kwetsbaarheden in producten van antidemocratische landen worden deze niet gemeld. Een uitzondering vormen producten van deze landen waarvan de gebruikers zich in Nederland bevinden (en deze niet overwegend crimineel zijn) of Nederlandse gebruikers in overheidsdienst in het buitenland. Onder deze omstandigheden kan DIGIT tot maatregelen besluiten die het maatschappelijk (digitaal) veiligheidsrisico doen verminderen.

BIJLAGE A

Stappenplan handelingskader onbekende kwetsbaarheid

Stappen	TAAK	WIE
1	DIGIT meldt bij LP DIGIT wanneer zij bekend raken met een mogelijk onbekende kwetsbaarheid.	DIGIT
2	DIGIT beoordeelt het opsporingsbelang, of nader verdiepend onderzoek naar de onbekende kwetsbaarheid wenselijk is, welke mitigerende maatregelen mogelijk zijn en wat het advies aan LP DIGIT zou zijn.	DIGIT
3	DIGIT levert informatie aan LP DIGIT over de onbekende kwetsbaarheid en de informatie die nodig is om tot een afweging te komen.	DIGIT
4	LP DIGIT beoordeelt of sprake is van een onbekende kwetsbaarheid als bedoeld in art. 126ffa Sv en of sprake is van een zwaarwegend opsporingsbelang om melding van de kwetsbaarheid uit te stellen.	LP DIGIT

OPTIE A - Er is geen sprake van een onbekende kwetsbaarheid als bedoeld in art. 126ffa Sv

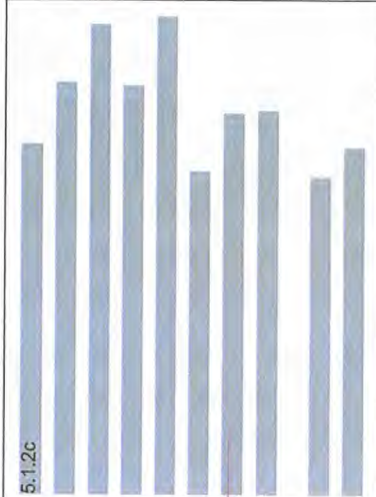
A 5	Ingeval het gaat om een onbekende kwetsbaarheid die niet valt onder het regime van art. 126ffa, beoordelen DIGIT en LP DIGIT de noodzaak en het maatschappelijk belang om de onbekende kwetsbaarheid alsnog te melden of anderszins te mitigeren (ethische beoordeling).	DIGIT en LP DIGIT
-----	---	-------------------

OPTIE B en C - Er is wel sprake van een onbekende kwetsbaarheid als bedoeld in art. 126ffa Sv

OPTIE B - melden uitstellen

B 5	Wanneer het om een onbekende kwetsbaarheid gaat als bedoeld in art. 126ffa Sv en het voornemen bestaat om de melding van de kwetsbaarheid uit te stellen , maakt DIGIT een proces-verbaal ten behoeve van de vordering tot machtiging aan de rechter-commissaris.	DIGIT
B 6	DIGIT levert een aanvraagproces-verbaal aan LP DIGIT	DIGIT
B 7	LP DIGIT zorgt voor het parketnummer van de aanvraag.	LP DIGIT

OPTIE C - melden

C 5		DIGIT
C 6		DIGIT en LP DIGIT
C 7		DIGIT

B 8	LP DIGIT zorgt voor vordering tot machtiging voor het uitstel van het melden van een onbekende kwetsbaarheid aan de rechter-commissaris. Als de machtiging wordt verleend, maakt LP DIGIT een bevel op dat naar DIGIT wordt gestuurd. Als er geen machtiging wordt verleend, wordt er verder gehandeld conform stap 5 C.	LP DIGIT
B 9	LP DIGIT en DIGIT houden de termijnen voor verleend uitstel bij. Indien aan het einde van de bevolen termijn tot uitstel nog steeds sprake is van een zwaarwegend opsporingsbelang, wordt door LP DIGIT een nieuw verzoek tot uitstel gedaan bij de rechter-commissaris. Stappen 6, 7 en 8 worden herhaald. Als er geen reden is voor verlenging van het bevel wordt er verder gehandeld conform stap 5 C.	DIGIT en LP DIGIT
B 10	LP DIGIT houdt een apart dossier bij voor uitstel melden onbekende kwetsbaarheden.	LP DIGIT
B 11	LP DIGIT archiveert het dossier uitstel melden onbekende kwetsbaarheden.	LP DIGIT

C 8	DIGIT houdt een dossier van het melden van de onbekende kwetsbaarheid.	DIGIT
C 9	DIGIT archiveert het dossier van het melden onbekende kwetsbaarheid.	DIGIT

BIJLAGE B

Hoofdvragen onbekende kwetsbaarheid

Vraag 1) Is de zwakheid een kwetsbaarheid in de zin van art. 126ffa Sv?

- a) Is de kwetsbaarheid een zwakheid in hardware/software die toegankelijk en exploiteerbaar is, en die leidt tot doorbreking van betrouwbaarheid, vertrouwelijkheid en integriteit van die hardware/software?
 - b) Kan de kwetsbaarheid gebruikt worden om binnen te dringen in het geautomatiseerde werk?
 - c) Is de kwetsbaarheid in het kader van een opsporingsonderzoek aan het licht gekomen, aangetroffen of gebruikt?
- Indien alle vragen bevestigend zijn beantwoord:
→ ga door naar vraag 2
 - Indien een of meerdere vragen ontkennend is/zijn beantwoord:
→ is er aanleiding om op ethische gronden de kwetsbaarheid te melden of anderszins te mitigeren? Zo ja, melden bij de producent of mitigerende maatregelen treffen.

Vraag 2) Is de kwetsbaarheid een onbekende kwetsbaarheid in de zin van art. 126ffa Sv?

Of de kwetsbaarheid onbekend is of kan worden verondersteld niet bekend te zijn bij de producent, kan worden beoordeeld aan de hand van de volgende factoren:

- a) Er is een CVE-nummer voor de specifieke kwetsbaarheid beschikbaar/toegekend;
 - b) Er is informatie over de kwetsbaarheid gepubliceerd op openbare en beschikbare bronnen relevante internetfora en blogs;
 - c) Er is een algemeen beschikbare en gepubliceerde patch voor de kwetsbaarheid uitgebracht;
 - d) Er zijn mitigerende maatregelen beschikbaar voor de betreffende kwetsbaarheid en deze zijn gepubliceerd bij de producent / een nationaal CERT / een lid van FIRST of een andere gezaghebbende bron;
 - e) De kwetsbaarheid betreft een gedocumenteerde functionaliteit die een nadelige impact heeft op de beschikbaarheid, integriteit en/of vertrouwelijkheid;
 - f) De politie beschikt over informatie waarin afdoende onderbouwd staat dat de kwetsbaarheid bij de producent bekend is.
- Is de kwetsbaarheid onbekend:
→ ga door naar vraag 3
 - Is de kwetsbaarheid bekend:

→ is er aanleiding om op ethische gronden de kwetsbaarheid onder de aandacht te brengen? 5.1.2c

Vraag 3) Is een (zwaarwegend) opsporingsbelang aanwezig?

- a) Is bescherming van de heimelijkheid van het onderzoek noodzakelijk / zou de melding resulteren in het tenietdoen van het heimelijke karakter van het onderzoek?
 - b) Betreft het een kwetsbaarheid in een systeem of computerprogramma dat door criminelen is vervaardigd en/of vrijwel alleen voor criminele doeleinden wordt gebruikt?
 - c) Wordt door het melden informatie prijsgegeven over de concrete uitvoering van specifieke opsporingsmethoden- en technieken?
 - d) Heeft de kwetsbaarheid in de toekomst hoge operationele waarde?
 - e) Is er een ander belang voor de opsporing dat zwaarwegend is?
- Indien een of meerdere vragen bevestigend is/zijn beantwoord:
 - ga door naar vraag 4
 - Indien geen enkele vraag bevestigend is beantwoord
 - melden bij de producent

Vraag 4: Is een maatschappelijk belang aanwezig?

- a) Wat is de CVSS-score van de onbekende kwetsbaarheid?
- b) Wat is de voetafdruk van de onbekende kwetsbaarheid?
 - Wat is het geschatte marktaandeel van het kwetsbare product in Nederland?
 - Is het een kwetsbaarheid in producten die in wijdverbreid en regulier gebruik zijn?
 - Hoe frequent wordt het kwetsbare product naar schatting in Nederland gebruikt?
 - Wat is het aantal onschuldige personen en organisaties dat hierdoor kwetsbaar wordt?
 - Binnen welke sectoren en bedrijven wordt het kwetsbare product zover bekend gebruikt?
 - Is het een kwetsbaarheid in hardware/software in gebruik bij de vitale infrastructuur?

AFWEGINGSKADER

- ❖ Maatschappelijke belang < zwaarwegend opsporingsbelang
 - uitstel van melden bevelen (na machtiging rechter-commissaris)
- ❖ Maatschappelijke belang > zwaarwegend opsporingsbelang
 - melden bij de producent

Melden onbekende kwetsbaarheden ex art. 126ffa Sv

Landelijk Parket - DIGIT

Aanleiding

Tijdens de parlementaire behandeling van artikel 126nba Wetboek van Strafvordering (Sv) is uitgebreid debat gevoerd over binnendringen door het technisch team van de politie met gebruikmaking van onbekende kwetsbaarheden en daarbij het risico van het in stand/onbekend laten van onbekende kwetsbaarheden.

Door de minister van Justitie en Veiligheid is daarbij herhaaldelijk benadrukt dat zijn beleid is gericht op een open, vrij en veilig internet en daarmee op vermindering van het aantal onbekende kwetsbaarheden. Ten behoeve van de veiligheid in de digitale samenleving staat voorop dat kwetsbaarheden in principe zo snel mogelijk aan de producent gemeld worden, opdat de noodzakelijke veiligheidsmaatregelen kunnen worden getroffen ter voorkoming van misbruik door derden van deze kwetsbaarheid. Dat geldt ook voor onbekende kwetsbaarheden die in het kader van een opsporingsonderzoek ter kennis komen van de politie of het openbaar ministerie.¹

Om dit uitgangspunt sterker in de wet te verankeren, hebben de Kamerleden Recourt en Tellegen een amendement voorgesteld dat het gebruik van onbekende kwetsbaarheden bij het binnendringen ex art. 126bnba Sv reguleert; art. 126ffa Sv. Daarmee is een wettelijke regeling getroffen voor een specifieke categorie van onbekende kwetsbaarheden. Dit amendement is aangenomen en met de Wet Computercriminaliteit III ingevoerd.

Artikel 126ffa Sv luid als volgt:

1. *De officier van justitie kan op grond van een zwaarwegend opsporingsbelang bevelen dat het bekend maken aan de producent van een onbekende kwetsbaarheid voor het binnendringen in een geautomatiseerd werk, bedoeld in de artikelen 126nba, 126uba en 126zpa, wordt uitgesteld.*
2. *Een bevel als bedoeld in het eerste lid is schriftelijk en vermeldt:*
 - a. *de kwetsbaarheid en*
 - b. *het zwaarwegend opsporingsbelang.*

¹ Dit standpunt werd uiteengezet in de brief van de staatssecretaris van Veiligheid en Justitie en de ministers van Binnenlandse Zaken en Koninkrijksrelaties en Defensie d.d. 8 november 2016 (kamerstukken II, 2016/17, 26 643, nr. 428). In de later behandeling van de wet CCIII is dit standpunt steeds herhaald.

3. Het bevel, bedoeld in het eerste lid, kan slechts worden gegeven na voorafgaande schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris.
4. Onder onbekende kwetsbaarheid als bedoeld in het eerste lid wordt verstaan een kwetsbaarheid in een geautomatiseerd werk waarvan aannemelijk is dat die niet bekend is of kan worden verondersteld niet bekend te zijn bij de producent van het apparaat of van het programma op basis waarvan automatisch computergegevens worden verwerkt, en die kan worden gebruikt om dat geautomatiseerde werk binnen te dringen.

Vooraf bij de behandeling in de Eerste Kamer zijn voor de praktijk bruikbare handvatten gegeven. In deze notitie zijn de belangrijkste elementen met betrekking tot het melden van onbekende kwetsbaarheden beschreven. Dat is vervolgens uitgewerkt in een werkproces voor het melden (en het eventueel uitstellen van melding) van onbekende kwetsbaarheden.

Algemene uitgangspunten

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.² Ook voor kwetsbaarheden die in een opsporingsonderzoek worden aangetroffen geldt echter dat er in uitzonderlijke gevallen redenen kunnen zijn die het melden (tijdelijk) in de weg staan.³ Er moet dan wel sprake zijn van een zwaarwegend opsporingsbelang. Dit is het geval wanneer het opsporingsbelang zwaarder weegt dan het maatschappelijk belang om de producent de mogelijkheid te bieden de kwetsbaarheid te verhelpen.⁴

Het uitstellen van het delen van informatie over aangetroffen onbekende kwetsbaarheden in wijdverbreide en regulier gebruikte hardware of software ligt niet in de rede.⁵

De afweging of er een zwaarwegend opsporingsbelang is, overstijgt het individuele opsporingsonderzoek. Daarom wordt deze beslissing binnen het Openbaar Ministerie centraal genomen door de Landelijk DIGIT officier van justitie.⁶

² Kamerstukken II, 2016/17, 26 643, nr. 428, p. 4-5

³ Kamerstukken II, 2016/17, 26 643, nr. 428, p. 4-5

⁴ Kamerstukken I, 2017/18, 34 372, G, p. 6 (NVMA I)

⁵ Kamerstukken II, 2016/17, 26 643, nr. 428, p. 4-5

⁶ Kamerstukken II, 2016/17, 26 643, nr. 428, p. 4-5. Zie ook Kamerstukken I, 2017/18, 34 372, G, p. 6 (NVMA I)

De opdracht om een kwetsbaarheid te melden wordt gegeven aan DIGIT LE. Het technisch team van politie dat is belast met de uitvoering van de bevoegdheid (en dat onderdeel is van DIGIT LE) heeft namelijk het overzicht over het gebruik en melden van onbekende kwetsbaarheden.⁷

Categorieën kwetsbaarheden

Bij toepassing van art. 126nba Sv kan onderscheid worden gemaakt tussen verschillende categorieën van kwetsbaarheden.⁸

1. Bekende kwetsbaarheid die niet gebruikt kan worden om binnen te dringen
2. Bekende kwetsbaarheid die gebruikt kan worden om binnen te dringen
3. Onbekende kwetsbaarheid die niet gebruikt kan worden om binnen te dringen
4. **Onbekende kwetsbaarheid die gebruikt kan worden om binnen te dringen**

Ad 1. en 2. Bekende kwetsbaarheden

Van een bekende kwetsbaarheid kan worden gesproken als in redelijkheid verondersteld kan worden dat een producent op de hoogte is / kan zijn van de betreffende kwetsbaarheid. Het is niet noodzakelijk dat daarop veiligheidsmaatregelen zijn gevolgd of dat een gebruiker eveneens op de hoogte is van een kwetsbaarheid.

Uit navolgende kan bijvoorbeeld blijken dat een producent op de hoogte is van een kwetsbaarheid:

- a. Als de producent de kwetsbaarheden gepatcht heeft.
- b. Als kennis over kwetsbaarheden door derden in het openbaar gedeeld wordt (bijvoorbeeld op internetfora of in nieuwsberichten).

5.1.2c

Ten aanzien categorie 1 en 2, is geen sprake van een onbekende kwetsbaarheid als bedoeld in artikel 126ffa lid 1 Sv. Er hoeft zodoende geen melding aan de producent gedaan te worden.

Ad 3. Onbekende kwetsbaarheden die niet gebruikt kan worden om binnen te dringen

Gelet op de definitie van art. 126ffa lid 4 Sv ziet die bepaling op een kwetsbaarheid:

- waarvan aannemelijk is dat die niet bekend is of kan worden verondersteld niet bekend te zijn bij de producent van het apparaat of van het programma op basis waarvan automatisch computergegevens worden verwerkt en

⁷ Kamerstukken I, 2011/17, 34 372, D, p. 23 (MvA I)

⁸ Zie ook Kamerstukken I, 2017/18, 34 372, G, p. 4 (NMVA I)

- die kan worden gebruikt om dat geautomatiseerde werk binnen te dringen (als bedoeld in art. 126nba Sv)

Er dient dus een onderscheid gemaakt te worden tussen de kwetsbaarheden die geëxploiteerd kunnen worden bij het binnendringen in een geautomatiseerd werk ex art. 126nba Sv en kwetsbaarheden die daar niet voor gebruikt worden.⁹ De laatste groep kwetsbaarheden valt dus niet onder art. 126ffa Sv. Dit kunnen kwetsbaarheden zijn die enkel gebruikt kunnen worden voor het verrichten van onderzoekshandelingen, maar ook kwetsbaarheden die worden gebruikt bij de aanwending van andere opsporingsbevoegdheden dan art. 126nba Sv.

Artikel 126ffa Sv brengt ook geen impliciete verplichting met zich mee om onbekende kwetsbaarheden die niet voor het binnendringen ex art. 126nba Sv kunnen worden gebruikt, te melden bij de producent. Uiteraard zal – gelet op de algemene uitgangspunten die door de minister zijn geschetst en tijdens de parlementaire behandeling zijn onderschreven – met het oog op de veiligheid in de digitale wereld altijd gekeken worden naar de noodzaak en mogelijkheden om dergelijke onbekende kwetsbaarheden toch te melden aan de producenten.^{5.1.2c}

Ad 4. Onbekende kwetsbaarheid die gebruikt kan worden om binnen te dringen Melden

Zoals al werd opgemerkt moeten onbekende kwetsbaarheden die

- kunnen worden gebruikt bij het binnendringen ex art. 126nba Sv en
- waarvan aannemelijk is dat ze nog onbekend zijn

in beginsel direct of zo spoedig mogelijk worden gemeld aan de fabrikant van de desbetreffende hardware of software.¹⁰

Voor het melden van een onbekende kwetsbaarheid wordt verwezen naar onderstaand werkproces.

Uitstel

Indien er zwaarwegende opsporingsbelangen zijn die zich tegen direct melden verzetten, kan er in uitzonderlijke gevallen uitstel van de melding worden bevolen.¹¹ Er is

⁹ De wetgever heeft het tijdens de parlementaire behandeling – naast deze definitie – ook steeds over onbekende kwetsbaarheden die “in het kader van een opsporingsonderzoek aan het licht komen”. Dat zou betekenen dat een onbekende kwetsbaarheid die los van een concreet opsporingsonderzoek wordt ontdekt, buiten de verplichting om te melden zou vallen. Dit kan bijvoorbeeld aan de orde zijn als binnendringing mogelijkheden worden gezocht die algemeen inzetbaar zijn.

¹⁰ Kamerstukken II, 2016/17, 26 643, nr. 428, p. 4-5

¹¹ Kamerstukken II, 2016/17, 26 643, nr. 428, p. 4-5

sprake van een zwaarwegend opsporingsbelang wanneer het opsporingsbelang zwaarder weegt dan het maatschappelijk belang om de producent de mogelijkheid te bieden de kwetsbaarheid te verhelpen.¹²

In de parlementaire geschiedenis worden twee voorbeelden gegeven van situaties waarin sprake is van een zwaarwegend opsporingsbelang.

1. Als de melding zou resulteren in het tenietdoen van het heimelijke karakter van het opsporingsonderzoek.¹³
2. Als het een systeem of computerprogramma betreft dat door criminelen is vervaardigd en/of vrijwel alleen voor criminele doeleinden wordt gebruikt. Het melden van een onbekende kwetsbaarheid in dergelijke gevallen zou het effect hebben criminaliteit te faciliteren.¹⁴

Ten aanzien van voorbeeld 2 geeft de wetgever aan dat langduriger uitstel van de melding aan de fabrikant dan aan de orde kan zijn.¹⁵

Met betrekking tot de afweging of sprake is van een zwaarwegend opsporingsbelang benoemt de wetgever een aantal factoren die een rol kunnen spelen.¹⁶

- Hoe groot de kans is dat de kwetsbaarheid door kwaadwillenden wordt uitgebuit.
- Het aantal onschuldige personen en organisaties dat hierdoor kwetsbaar is.
- Hoe groot het aantal onschuldige personen en organisaties is dat kwetsbaar wordt door het achterwege blijven van de melding.
- In hoeverre de desbetreffende hardware of software wordt gebruikt bij de vitale infrastructuur of regulier en wijdverbreid in de maatschappij.
- Of het een systeem betreft dat door criminelen is vervaardigd en/of vrijwel alleen voor criminele doeleinden wordt gebruikt.

Te allen tijde dient dus ten eerste acht te worden geslagen op het risico dat het niet melden van een onbekende kwetsbaarheid (mogelijk) gevolgen heeft voor de (schade aan de) digitale wereld en (onschuldige) gebruikers.^{5.1.2c}

5.1.2c

¹² Kamerstukken I, 2017/18, 34 372, G, p. 6 (NVMA I)

¹³ Kamerstukken II, 2016/17, 26 643, nr. 428, p. 4-5 en Kamerstukken I, 2016/17, 34 372, D, p. 18-19 (MvA I)

¹⁴ . Kamerstukken II, 2018/19, 34 372, nr. 27, p. 13-14 (Verslag II) en Kamerstukken II, 2018/19, 34 372, nr. 29 p. 8/9 (Verslag II), Kamerstukken II, 2016/17, 26 643, nr. 428, p. 4-5, Kamerstukken I, 2016/17, 34 372, D, p. 18-19 (MvA I)

¹⁵ Kamerstukken I, 2016/17, 34 372, D, p. 18-19 (MvA I)

¹⁶ Kamerstukken II, 2016/17, 26 643, nr. 428, p. 4-5 en Kamerstukken I, 2017/18, 34 372, G, p. 6 (NMVA I)

Naarmate het risico bij niet melden aanzienlijker is, dient het zwaarwegend opsporingsbelang groter te zijn om tot een verzoek tot uitstel van het melden van deze onbekende kwetsbaarheid te komen.

Omstandigheden die onder andere een rol kunnen spelen bij de beoordeling of sprake is van een zwaarwegend opsporingsbelang zijn:

1. Individuele zaak: het melden van een onbekende kwetsbaarheid kan zicht geven op de concrete (afgeschermd) modus operandi van DIGIT en/of kan concrete opsporingsbelangen en –kansen in het onderzoek frustreren.
2. Noodzaak: indien geen lichter middel beschikbaar is om een gelijkelijk doel te bereiken, kan het belang van de opsporing in gedrang komen bij het melden van een onbekende kwetsbaarheid.
3. Geheimhouding: indien een onbekende kwetsbaarheid onder voorwaarden van geheimhouding is gedeeld, kan melding van een dergelijke onbekende kwetsbaarheid lopende (buitenlandse) onderzoeken in gevaar brengen.

Voor het afzien van het direct melden van een onbekende kwetsbaarheid is machtiging van de rechter-commissaris vereist. Deze machtiging is tijdelijk. De periode van geldigheid van de machtiging is wettelijk niet nader ingekaderd. Het wordt door de wetgever aan de interactie tussen de officier van justitie en rechter-commissaris gelaten om te komen tot nadere inkadering van de periode van geldigheid van het uitstel. In de parlementaire geschiedenis komt daarbij naar voren dat het in de rede ligt om voor de periode van uitstel van de melding aan te sluiten bij de periode van geldigheid van de machtiging voor het onderzoek in het geautomatiseerde werk waarbij het voornemen bestaat gebruik te maken van de betreffende kwetsbaarheid. Deze periode is maximaal 4 weken en kan worden verlengd. Daarbij vind de wetgever het ook in de rede liggen dat de rechter-commissaris bij de beoordeling van een eventueel verzoek tot verlenging van het bevel tot het onderzoek in een geautomatiseerd werk tevens het bevel tot uitstel van de melding van de kwetsbaarheid toetst.¹⁷ Het staat de rechter-commissaris daarbij vrij hierbij te consulteren wie hij of zij nodig acht.¹⁸

Bij de weging of er zwaarwegende belangen zijn die nopen tot het vorderen van uitstel van het melden van een onbekende kwetsbaarheid is geen betrokkenheid van de Inlichtingen- en Veiligheidsdiensten voorzien.¹⁹ Een dergelijke beslissing kan echter wel invloed hebben op hun werkzaamheden. Over de voorgenomen beslissing of er zwaarwegende belangen zijn die nopen tot het vorderen van uitstel van het melden van een onbekende kwetsbaarheid worden de Inlichtingen- en Veiligheidsdiensten

¹⁷ Kamerstukken I, 2016/17, 34 372, D, p. 18-19 (MvA I)

¹⁸ Kamerstukken I, 2017/18, 34 372, G, p. 6 (NVMA I)

¹⁹ Kamerstukken I, 2017/18, 34 372, G, p.6 (NMVA I)

geïnformeerd. Op die manier kunnen de gevolgen van het voorgenomen besluit daar tijdig worden ingeschat.

Voor het vragen van uitstel van het melden van onbekende kwetsbaarheden, die gebruikt kunnen worden voor het binnendringen van een geautomatiseerd werk, wordt verwezen naar onderstaand werkproces.

Onbekende kwetsbaarheden in criminele software (malware)

Een bijzondere categorie vormen onbekende kwetsbaarheden in door criminelen vervaardigde / hoofdzakelijk gebruikte software. Art. 126ffa Sv maakt geen onderscheid tussen dergelijke criminele software en software voor regulier gebruik. De regeling van art.126ffa Sv voorziet niet in afstel van een melding aan de producent. Dat betekent dat een onbekende kwetsbaarheid in malware, door criminelen vervaardigde of hoofdzakelijk gebruikte software uiteindelijk gemeld moet worden aan de crimineel die het heeft geproduceerd.

Door de wetgever is wel op diverse plekken aangegeven dat in dergelijke gevallen reden kan bestaan om (tijdelijk) te bevelen dat van melding wordt afgezien.²⁰

Kwetsbaarheden in commerciële binnendringing software

Een bijzondere categorie vormen onbekende kwetsbaarheden in commerciële binnendringingssoftware. Indien de politie of het openbaar ministerie bekend raakt met onbekende kwetsbaarheden in dergelijke binnendringingssoftware valt dat ook onder het regime van artikel 126ffa Sv.²¹

1 maart 2021

LP DIGIT - 5.1.2e en 5.1.2e

	Toegezonden	Afgerond
LP DIGIT	20-08-2020	16-02-2021
Afgestemd LE DIGIT	20-08-2020	16-02-2021
RechercheOvJ LP	01-03-2021	01-03-2021

²⁰ Kamerstukken II, 2018/19, 34 372, nr. 27, p. 14 (Verslag II), Kamerstukken II, 2018/19, 34 372, nr. 29 p. 8/9 (Verslag II), Kamerstukken I, 2016/17, 34 372, B, p. 17-19 (Verslag I), Kamerstukken I, 2016/17, 34 372, D, p. 19 (MvA I) en Kamerstukken I, 2017/18, 34 372, G, p. 4 (NMVA I).

²¹ Kamerstukken I, 2017/18, 34 372, D, p. 22 (MvA I) Zie ook

Werkproces uitstel melden onbekende kwetsbaarheid

	TAAK	Wie?
1.	LE Digit overlegt direct met LP Digit wanneer zij bekend raken met een mogelijke onbekende kwetsbaarheid.	LE Digit
2.	LP Digit beoordeelt of sprake is van een onbekende kwetsbaarheid als bedoeld in art. 126ffa Sv en of sprake is van een zwaarwegend opsporingsbelang om melding van de kwetsbaarheid uit stellen.	LP Digit
3.	Wanneer het voornemen bestaat om de melding van de kwetsbaarheid uit te stellen, maakt LE Digit een proces-verbaal op ten behoeve van de vordering tot machtiging aan de rechter-commissaris.	LE Digit
4.	5.1.2c 	LP/LE Digit
5.	Dit aanvraagproces-verbaal wordt aangeleverd aan LP Digit.	LE Digit
6.	LP/LE Digit zorgt voor registratienummer van de aanvraag.	LP/LE Digit
7.	LP Digit zorgt voor vordering tot machtiging voor het uitstel van het melden van een onbekende kwetsbaarheid aan de rechter-commissaris. Als de machtiging wordt verleend, maakt LP Digit een bevel. Dit bevel wordt aan LE Digit gestuurd. Deze stukken worden niet op parketnummer, maar op registratienummer opgemaakt. Als er geen machtiging wordt verleend, wordt er verder gehandeld conform het 'Werkproces melden onbekende kwetsbaarheid'.	LP Digit LP Digit
8.	LP Digit en LE Digit houden de termijnen voor verleend uitstel bij. Indien aan het einde van de bevolen termijn tot uitstel nog steeds sprake is van een zwaarwegend opsporingsbelang, wordt door LP Digit een nieuw verzoek tot uitstel gedaan bij de rechter-commissaris. Zie vanaf 3. Als er geen reden is voor verlening van het bevel (of er geen machtiging wordt verleend), wordt er verder gehandeld conform het 'Werkproces melden onbekende kwetsbaarheid'.	LP Digit LE Digit LP Digit
9.	LP Digit houdt apart dossier bij voor uitstel melden onbekende kwetsbaarheden.	LP Digit
10.	LP Digit archiveert het uitstel melden onbekende kwetsbaarheden.	LP Digit

Werkproces melden onbekende kwetsbaarheid

	TAAK	Wie?
1.	LE Digit overlegt direct met LP Digit wanneer zij bekend raken met een mogelijk onbekende kwetsbaarheid.	LE Digit
2.	LP Digit beoordeelt of sprake is van een onbekende kwetsbaarheid als bedoeld in art. 126ffa Sv en of sprake is van een zwaarwegend opsporingsbelang om melding van de kwetsbaarheid uit stellen.	LP Digit
3.	5.1.2c [Redacted]	LP/LE Digit
4.	Wanneer er geen zwaarwegend opsporingsbelang is dat zich tegen melden verzet, wordt de kwetsbaarheid door LE Digit onderzoek gedaan naar de contactgegevens van de producent van de software of hardware met de aangetroffen kwetsbaarheid.	LE Digit
	3a. Indien geen contactgegevens van de producent te achterhalen zijn, registreert LE Digit dit. LE Digit informeert LP Digit hierover. 5.1.2c [Redacted]	LE Digit
	3b. Indien contactgegevens van de producent te achterhalen zijn, draagt LE Digit er zorg voor dat de mededeling en benodigde informatie over de aangetroffen kwetsbaarheid bij de producent bekend worden.	LE Digit LE Digit
4.	LE Digit archiveert de mededelingen.	LE Digit

Handreiking omgaan met verzoeken t.a.v. artikel 126ffa Sv in een individuele strafzaak

Landelijk Parket - DIGIT

Aanleiding

Op 12 augustus 2021 is op rechtspraak.nl een beslissing gepubliceerd met betrekking tot het melden van onbekende kwetsbaarheden ex artikel 126ffa Sv. Deze beslissing zou aanleiding kunnen zijn voor vragen / onderzoekswensen in individuele strafzaken waarin sprake is van een bevel ex art. 126nba/uba/zpa Sv (de hackbevoegdheid). Deze handreiking bevat informatie hoe met verzoeken daaromtrent om gegaan kan worden.

Algemeen

Op grond van artikel 126ffa Sv kan – na machtiging van de rechter-commissaris – uitstel worden bevolen voor het melden van onbekende kwetsbaarheden, indien sprake is van een zwaarwegend opsporingsbelang.

Artikel 126ffa Sv

1. De officier van justitie kan op grond van een zwaarwegend opsporingsbelang bevelen dat het bekend maken aan de producent van een onbekende kwetsbaarheid voor het binnendringen in een geautomatiseerd werk, bedoeld in de artikelen 126nba, 126uba en 126zpa, wordt uitgesteld.
2. Een bevel als bedoeld in het eerste lid is schriftelijk en vermeldt:
 - a. de kwetsbaarheid en
 - b. het zwaarwegend opsporingsbelang.
3. Het bevel, bedoeld in het eerste lid, kan slechts worden gegeven na voorafgaande schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris.
4. Onder onbekende kwetsbaarheid als bedoeld in het eerste lid wordt verstaan een kwetsbaarheid in een geautomatiseerd werk waarvan aannemelijk is dat die niet bekend is of kan worden verondersteld niet bekend te zijn bij de producent van het apparaat of van het programma op basis waarvan automatisch computergegevens worden verwerkt, en die kan worden gebruikt om dat geautomatiseerde werk binnen te dringen.

Een vordering/bevel op grond van artikel 126ffa Sv is onlosmakelijk verbonden met de inzet van de hackbevoegdheid (artikel 126nba/uba/zpa Sv).

Bij de beoordeling of sprake is van een zwaarwegend opsporingsbelang dient te worden afgewogen hoe dit belang zich verhoudt tot het maatschappelijk belang van het melden van kwetsbaarheden. Factoren die hierbij een rol kunnen spelen zijn of het een systeem betreft dat door criminelen is vervaardigd en/of vrijwel alleen voor criminele doeleinden wordt gebruikt, hoe groot de kans is dat de kwetsbaarheid door kwaadwillenden wordt uitgebuit, hoe groot het aantal onschuldige personen en organisaties is dat kwetsbaar wordt door het

achterwege blijven van de melding en in hoeverre de desbetreffende hardware of software wordt gebruikt bij de vitale infrastructuur of regulier en wijdverbreid in de maatschappij.¹

De afweging of er een zwaarwegend opsporingsbelang is, overstijgt het individuele opsporingsonderzoek. Daarom wordt deze beslissing binnen het Openbaar Ministerie centraal genomen.² Dit doet de landelijk officier van justitie voor Digital Intrusion (DIGIT)³, die werkzaam is bij het landelijk parket. Deze DIGIT officier van justitie beveelt – na machtiging van de rechter-commissaris – desgewenst het uitstellen van melding

Beslissing rechter-commissaris

Op 12 augustus 2021 is op rechtspraak.nl een beslissing van de rechter-commissaris op een vordering tot uitstel van het melden van onbekende kwetsbaarheden ex artikel 126ffa Sv gepubliceerd.

<https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2013:19764>

Deze vordering is gedaan door de DIGIT officier van justitie. De rechter-commissaris heeft de vordering toegewezen.

In zijn algemeenheid overweegt de RC ten aanzien van een vordering ex artikel 126ffa Sv 'Uit de wetsgeschiedenis volgt dat een vordering als de onderhavige het individuele opsporingsonderzoek overstijgt. Deze vordering is niet gedaan in het kader van opsporing van strafbare feiten.'

De publicatie is (gedeeltelijk) geanonimiseerd, zodat onbekend blijft welke onbekende kwetsbaarheden het betreft en onder welke omstandigheden deze bij DIGIT bekend zijn geworden.

Gevolgen voor strafzaken

Nu publicatie heeft plaatsgevonden, kan het voorkomen dat in individuele strafzaken vragen over de genoemde beslissing worden gesteld of getracht wordt nadere informatie te verkrijgen over de betreffende onbekende kwetsbaarheden en/of omstandigheden waaronder deze onderkend zijn.

Dergelijke vragen zullen om de volgende redenen onbeantwoord kunnen blijven.

Afscherming binnendringen

Het gaat om onbekende kwetsbaarheden die gebruikt kunnen worden voor het binnendringen van een geautomatiseerd werk. In de wetsgeschiedenis van artikel 126nba Sv

¹ Kamerstukken I 2017/18, 34 372, G, p.6.

² Kamerstukken II 2017/18, 34 372, nr. 27, p. 14.

³ Verder 'de DIGIT officier van justitie'

komt expliciet naar voren dat de methoden voor het binnendringen in een geautomatiseerd werk niet aan de openbaarheid prijsgegeven kunnen worden, omdat deze dan niet meer kunnen worden gebruikt.⁴ Afscherming van de methoden (en eventueel daarbij gebruikte (on)bekende kwetsbaarheden) is essentieel voor toekomstige effectieve uitvoering van de hackbevoegdheid. Om deze reden zal in een strafzaak dan ook geen informatie over de wijze van binnendringen worden verstrekt aan rechtbank, de zaaksofficier en de verdediging. Dat betekent dat ook geen informatie zal worden verstrekt over het eventuele gebruik van onbekende kwetsbaarheden bij dat binnendringen.

Beschermde belang van art. 126ffa Sv (Veilig internet)

Uit de wetsgeschiedenis van art. 126ffa Sv volgt dat het beleid van de regering gericht is op een open, vrij en veilig internet en daarmee op vermindering van het aantal onbekende kwetsbaarheden.⁵ In dat kader bestaat het maatschappelijk belang dat onbekende kwetsbaarheden in hard- of software zo snel mogelijk aan de desbetreffende fabrikant worden gemeld. Op deze wijze kan de fabrikant maatregelen treffen tegen misbruik van deze kwetsbaarheden door onbevoegden. Tegen deze achtergrond is artikel 126ffa Sv in de wet opgenomen: ook politie en Openbaar Ministerie dienen te streven naar een zo veilig mogelijke digitale samenleving.

Het belang dat met die bepaling wordt gediend, is dus uitdrukkelijk niet het belangen van een individu en staat niet in relatie tot de opsporing van strafbare feiten van dat individu, maar om het belang van de maatschappij op een open, vrij en veilig internet. Het beschermde belang is niet het belang van een verdachte op een eerlijk proces.

De vraag of in een individuele strafzaak bij het binnendringen in een geautomatiseerd werk op grond van art. 126nba/uba/zpa Sv gebruik is gemaakt van een onbekende kwetsbaarheid is daarmee niet relevant voor enige in de strafzaak te nemen beslissing. Dat geldt ook voor vragen over de wijze van kennisname van/over onbekende kwetsbaarheden of de omstandigheden waaronder deze bekend zijn geworden. Deze vragen zijn niet relevant zijn voor de beslisvragen van artikel 348 en 350 Sv in een individuele strafzaak.

Geen bewijs ten aanzien van het onderzochte strafbare feit

Een vordering tot het uitstel van het melden van onbekende kwetsbaarheden heeft geen enkele relatie tot het vergaren en van relevante informatie ten behoeve van de opsporing van strafbare feiten. Een vordering tot uitstel van het melden van onbekende kwetsbaarheden wordt om die redenen ook buiten een strafrechtelijk onderzoek gedaan.

⁴ Kamerstukken II 2015/16, 34 372, nr. 3, p. 103.

⁵ Kamerstukken II 2017/18, 34 372, nr. 27, p. 13.

Conclusie

De conclusie van het voorgaande is dat er geen rechtens te respecteren belang in een individuele strafzaak bestaat om nader informatie te verstrekken over het eventuele gebruik van een onbekende kwetsbaarheid, de wijze van kennisname van/over onbekende kwetsbaarheden of de omstandigheden waaronder deze bekend zijn geworden.

Gelet op het zwaarwegende belang van afscherming van methodieken van binnendringen, zal in individuele strafzaken noch bevestigend, noch ontkennend gereageerd worden op een vraag of kwetsbaarheden onderkend / gebruikt zijn in dat onderzoek.

Concept tekstblok voor reactie

De verdediging wenst inzake te krijgen of in onderhavig onderzoek gebruik is gemaakt van onbekende kwetsbaarheden.

Het Openbaar Ministerie kan in onderhavige zaak bevestigen, noch ontkennen dat bij het binnendringen ex artikel 126nba/uba/zpa Sv onbekende kwetsbaarheden zijn gebruikt en/of informatie verkregen is over onbekende kwetsbaarheden.

De door de verdediging opgeworpen vragen zijn niet relevant voor enige in deze strafzaak te nemen beslissing.

Onder onbekende kwetsbaarheden in de zin van artikel 126ffa Sv worden kwetsbaarheden verstaan die kunnen worden gebruikt voor het binnendringen in een geautomatiseerd werk zoals bedoeld in artikel 126nba/uba/zpa Sv. In de wetsgeschiedenis is benadrukt dat methoden voor het binnendringen in een geautomatiseerd werk niet aan de openbaarheid prijsgegeven kunnen worden, omdat deze dan niet meer kunnen worden gebruikt.⁶

Uit de wetsgeschiedenis komt daarnaast naar voren dat een beslissing tot uitstel van het melden van onbekende kwetsbaarheden het individuele opsporingsonderzoek overstijgt.⁷ Een beslissing tot uitstel van het melden van onbekende kwetsbaarheden betreft een afweging tussen het belang van de maatschappij op een open, vrij en veilig internet en het algemene opsporingsbelang. Het betreft geen beslissing die een rechtens te respecteren belang van een individuele verdachte raakt. Het beschermd belang van artikel 126ffa Sv is niet het belang van een verdachte op een eerlijk proces.

Slechts indien sprake is van een zwaarwegend opsporingsbelang zal de RC machtiging verlenen tot het uitstel. Hiervan is bijvoorbeeld sprake als een melding het heimelijke karakter van een opsporingsonderzoek teniet kan doen of het effect heeft criminaliteit te faciliteren. Het gaat dan ook niet om het vergaren van informatie in het kader van de opsporing van concrete strafbare feiten. Een eventuele vordering tot uitstel van het melden van onbekende kwetsbaarheden wordt om die reden dan ook buiten een strafrechtelijk onderzoek gedaan.

De slotsom van het voorgaande is dat de door de verdediging opgeworpen vragen over de kennis van/over onbekende kwetsbaarheden of de omstandigheden waaronder deze bekend zijn geworden, niet relevant zijn voor enige in onderhavige strafzaak te nemen beslissing.

⁶ Kamerstukken II 2015/16, 34 372, nr. 3, p. 103.

⁷ Dit is ook zo overwogen in de beslissing van de RC.

12 augustus 2021

LP Digit - 

	Toegezonden	Afgerond
LP DIGIT	19-07-2021	12-08-2021
Afgestemd LE DIGIT	19-07-2021	12-08-2021
Afgestemd rechercheOvJ LP	12-08-2021	

BR

Van: 5.1.2e (Landelijk Parket)
Verzonden: woensdag 5 januari 2022 17:27
Aan: 5.1.2e (LP Rotterdam); 5.1.2e; 5.1.2e
CC: 5.1.2e (Landelijk Parket)
Onderwerp: moment van melden van onbekende kwetsbaarheden
Bijlagen: kst-26643-428 (brief onbekende kwetsbaarheden).pdf

Categorieën: DIGIT

Ha,

Ik ben de parlementaire geschiedenis in gedoken om helderheid te krijgen over de vraag op welk moment een onbekende kwetsbaarheid moet worden gemeld; bij ontdekking of bij gebruik in een concreet opsporingsonderzoek.

Het antwoord op dit vraag blijkt niet eenduidig. Dat komt doordat de wetgever nergens in een wet of AMvB heeft geregeld dat er een verplichting tot melden van een onbekende kwetsbaarheid is; anders gezegd, art. 126ffa Sv biedt een uitzondering op een hoofdregel die nooit is geformuleerd. Die hoofdregel ligt nu opgeslagen in bijgevoegde brief.

De discussie over onbekende kwetsbaarheden is op bij de behandeling van het wetsvoorstel in de vaste commissie voor Justitie en Veiligheid uitgebreid gevoerd. D66 en SP waren daar blijkens het op 8 maart 2016 vast gestelde verslag (Tweede Kamer, vergaderjaar 2016–2017, 34 372, nr. 5) kritisch en stelde veel vragen. De minister heeft die beantwoord in de nota n.a.v. het verslag van 8 november 2016 (Tweede Kamer, vergaderjaar 2016–2017, 34 372, nr. 6). Gelijk met die nota is een brief aan de kamer gestuurd vanuit Veiligheid en Justitie, binnenlands zaken en defensie over de omgang met onbekende kwetsbaarheden (Tweede Kamer, vergaderjaar 2016–2017, 26 643, nr. 428). Bij de beantwoording van alle vragen, verwijst de minister consequent naar deze brief. In die brief schrijft de minister:

"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. Ook voor kwetsbaarheden die in een opsporingsonderzoek worden aangetroffen geldt echter dat er in uitzonderlijke gevallen redenen kunnen zijn die het melden (tijdelijk) in de weg staan." (NB 'ook' slaat hier terug op de alinea waarin geschetst is hoe de diensten hier mee omgaan).

Tweede Kamer, vergaderjaar 2016–2017, 26 643, nr. 428, p. 4

Dit leidt tot diverse amendementen. Waaronder het aangenomen amendement van Recourt en Tellegen (Tweede Kamer, vergaderjaar 2016–2017, 34 372, nr. 14). In de toelichting op dat amendement staat:

"Dit amendement beoogt om de regel dat kwetsbaarheden in geautomatiseerde werken door de officier van justitie moeten worden gemeld sterker in de wet te verankeren. Het uitgangspunt zijn integere en veilige geautomatiseerde werken. De overheid dient dit te bevorderen. Vanwege de risico's die kwetsbaarheden in een geautomatiseerd werk met zich mee brengen, is de regel dat bekende kwetsbaarheden worden gemeld om de eigenaar van dat werk in staat te stellen die kwetsbaarheid te verhelpen."

Vervolgens wordt er in 2 nadere vergaderingen in 2018 van de vaste commissie over gesproken. Dat leidt tot de volgende antwoorden van de minister.

"Het beleid van de regering is gericht op een open, vrij en veilig internet en daarmee op vermindering van het aantal onbekende kwetsbaarheden. Het uitgangspunt van de regering is dat onbekende kwetsbaarheden in hard- of software zo snel mogelijk aan de desbetreffende fabrikant worden gemeld. Dat geldt ook voor onbekende kwetsbaarheden die in het kader van een opsporingsonderzoek ter kennis komen van de politie of het openbaar ministerie. In uitzonderlijke gevallen kunnen er echter redenen zijn die het melden tijdelijk in de weg staan."

Tweede Kamer, vergaderjaar 2017–2018, 34 372, nr. 27, p 13/14

en

"Het op afstand heimelijk binnendringen in een geautomatiseerd werk is een specialistische techniek, waarvoor grote deskundigheid op het gebied van informatie- en communicatietechnologie is vereist. Toepassing is voorbehouden aan de daartoe speciaal aangewezen opsporingsambtenaren die over deze expertise beschikken en die deel uitmaken van een speciaal team, een technisch team bij de Landelijke eenheid van de Nationale politie. In een ministeriële regeling worden de eisen die worden gesteld aan de kennis en vaardigheden verder uitgewerkt. Centraal in deze ministeriële regeling staat de opleiding, training en certificering van de opsporingsambtenaren die onderdeel zijn van technisch team. Van leden van het technisch team wordt verwacht dat zij hun kennis en vaardigheden actueel houden. De dynamische ontwikkelingen in het vakgebied van digitalisering en cybercrime vereisen dat.

Naast technische vaardigheden hebben de opsporingsambtenaren van een technisch team ook kennis van het juridisch kader, mede in verband met (de advisering over) het gebruik van onbekende kwetsbaarheden. Na de inwerkingtreding van de Wet computercriminaliteit III bevat artikel 126ffa Sv de verplichting om onbekende kwetsbaarheden die bekend zijn geworden bij het toepassen van de bevoegdheid te melden bij de producent."

Tweede Kamer, vergaderjaar 2018–2019, 34 372, nr. 29, p.8

Dit geeft m.i. een diffuus beeld. Enerzijds wil de wetgever dat er z.s.m. gemeld wordt. Anderzijds wordt dat steeds gekoppeld aan een lopende zaak en een kwetsbaarheid die bij een concrete inzet wordt gevonden/toegepast. Met de optie dat zonder concrete zaak en in het algemeen kwetsbaarheden zouden worden gezocht, lijkt geen rekening te zijn gehouden. Dat wordt in de Eerste Kamer niet beter.

De discussie over onbekende kwetsbaarheden begint daar in de Memorie van antwoord:

"Als de politie of het openbaar ministerie kennis verwerft van onbekende kwetsbaarheden in hard- of software waarmee heimelijk en op afstand een geautomatiseerd werk kan worden binnengedrongen, dan worden deze in beginsel gemeld aan de fabrikant van de desbetreffende hard- of software. In uitzonderlijke gevallen kunnen er redenen zijn die het melden tijdelijk in de weg staan."

Eerste Kamer, vergaderjaar 2016–2017, 34 372, D, p. 18

"Hierboven, bij de eerdere beantwoording van soortgelijke vragen van de leden van de fracties van D66 en de SP, is reeds ingegaan op het gebruik van onbekende kwetsbaarheden, door sommigen zero day kwetsbaarheden genoemd. In aanvulling hierop wijs ik er op dat het wetsvoorstel naar aanleiding van het amendement Recourt/Tellegen (Kamerstukken II 2016/17, 30 372, nr. 14) een verplichting

introduceert om onbekende kwetsbaarheden die de politie bekend zijn geworden bij het toepassen van de bevoegdheid van 126nba Sv te melden."

Eerste Kamer, vergaderjaar 2016–2017, 34 372, D, p. 20

"Indien de politie of het openbaar ministerie kennis verwerft over onbekende kwetsbaarheden in hard- of software waarmee op afstand heimelijk een geautomatiseerd werk kan worden binnengedrongen, dan worden deze in beginsel gemeld aan de fabrikant van de desbetreffende hard- of software. Dat is ook het geval indien door de politie aangekochte software hiervan gebruik maakt."

Eerste Kamer, vergaderjaar 2016–2017, 34 372, D, p. 22

"Voor kwetsbaarheden die in een opsporingsonderzoek worden aange- troffen geldt dat er in uitzonderlijke gevallen redenen kunnen zijn die het melden (tijdelijk) in de weg staan."

Eerste Kamer, vergaderjaar 2016–2017, 34 372, D, p. 23

In het nadere verslag na een expert sessie (Eerste Kamer, vergaderjaar 2017–2018, 34 372, G) wordt dat nog meer geconcretiseerd. Met name D66 dringt dan aan om concreet te maken wanneer gemeld moet worden.

"De leden van de fractie van D66 meenden dat een onbekende kwetsbaarheid direct zou moeten worden gemeld na ontdekking daarvan door de politie of het openbaar ministerie, en hebben gevraagd wat het beleid is ten aanzien van onbekende kwetsbaarheden in het kader van het voorliggende wetsvoorstel. Deze leden hebben tevens gevraagd of de regering van mening is dat onbekende kwetsbaarheden zo snel mogelijk moeten worden gemeld."

Eerste Kamer, vergaderjaar 2017–2018, 34 372, G, p. 3/4

De regering antwoordt op die specifieke vraag in de zelfde tweeledige wijze als eerder:

"Uitgangspunt is dat onbekende kwetsbaarheden aan de leverancier of fabrikant worden gemeld. Dit geldt ook voor de politie en het openbaar ministerie als zij in het kader van een opsporingsonderzoek bekend worden met onbekende kwetsbaarheden in hard- of software; deze zullen zo snel mogelijk aan de desbetreffende producent worden gemeld."

Eerste Kamer, vergaderjaar 2017–2018, 34 372, G, p. 4

"Het uitgangspunt van de regering is dat onbekende kwetsbaarheden in hard- of software zo snel mogelijk aan de desbetreffende producent worden gemeld. Dat geldt ook voor onbekende kwetsbaarheden die in het kader van een opsporingsonderzoek ter kennis komen van de politie of het openbaar ministerie."

Eerste Kamer, vergaderjaar 2017–2018, 34 372, G, p. 8

Ik krijg niet helder of de antwoorden van de minister bewust ontwijkend zijn of dat hiermee gedacht werd en concreet antwoord te geven. Ik neig naar de gedachte dat het laatste het geval is en men het idee had dat dit altijd in het kader van een concreet onderzoek zou gebeuren.

Laten we dit komende week met elkaar bespreken.

Gr. 5.1.2e

BR

Van: 5.1.2e (Landelijk Parket)
Verzonden: donderdag 3 februari 2022 14:34
Aan: 5.1.2e, 5.1.2e
CC: 5.1.2e (Landelijk Parket); 5.1.2e (LP Rotterdam); 5.1.2e (Landelijk Parket Rotterdam))
Onderwerp: Tijdelijk kader voor moment van melden van onbekende kwetsbaarheden
Opvolgingsvlag: Opvolgen
Vlagstatus: Met vlag

Ha,

In navolging van onze bespreken dinsdag. De wetsgeschiedenis laat helaas teveel onduidelijkheid bestaan (en ontstaan) over het moment van melden van een onbekende kwetsbaarheid die gebruikt kan worden voor het binnendringen. Dat maakt dat we daarin zelf ruimte hebben om de richting te bepalen. Dat moeten we vooral niet alleen willen doen, maar – op termijn en als we het verder hebben uitgewerkt – voorleggen aan wijze mensen in ons beider organisaties. 5.1.2c

Ik vind namelijk dat we moeten voorkomen dat diverse diensten binnen de rijksoverheid hier anders mee om gaan.

Tot die tijd hanteren we het volgende kader.

- Er is geen dwingende verplichting om een onbekende kwetsbaarheid die gebruikt kan worden voor het binnendringen direct na ontdekking te melden bij de fabrikant of leverancier. Het uitgangspunt blijft dat de kwetsbaarheid wordt gemeld, maar het moment waarop dat gebeurt, zal wisselen. Hoe meer schade een kwetsbaarheid aanricht, hoe sneller gemeld moet worden.
- We bespreken daarom gevonden kwetsbaarheden zodra voldoende duidelijk is hoe die kwetsbaarheid er uit ziet en wat de impact is. We beoordelen dan of er direct gemeld moet worden of dat we (kunnen) wachten tot we definitievere kaders hebben vastgesteld.
- Zodra een gevonden kwetsbaarheid voor het binnendringen in het kader van een opsporingsonderzoek bekend wordt (of wordt ingezet), moeten we of melden of ex 126ffa Sv uitstel van de meldverplichting vragen.

@ 5.1.2e Kan je dit kader in het journaal vastleggen zodat voor de inspectie duidelijk is welk kader voor jullie is geschetst?

Gr. 5.1.2e

Van: 5.1.2e (Landelijk Parket) <5.1.2e@om.nl>
Verzonden: woensdag 5 januari 2022 17:27
Aan: 5.1.2e (LP Rotterdam) <5.1.2e@om.nl>; 5.1.2e <5.1.2e@politie.nl>; 5.1.2e <5.1.2e@politie.nl>
CC: 5.1.2e (Landelijk Parket) <5.1.2e@om.nl>
Onderwerp: moment van melden van onbekende kwetsbaarheden

Reeds beoordeeld





Reeds beoordeeld



