gevangenisstraf van acht jaren of meer is gesteld. Bij algemene maatregel van bestuur kunnen echter andere misdrijven met een lagere wettelijke strafbedreiging worden aangewezen (artikelen 126nba/126uba/126zpa,eerste lid, onder c, Sv). In hoofdstuk 2 van dit besluit worden deze misdrijven aangewezen. Het betreft misdrijven die worden gepleegd met een geautomatiseerd werk en die een geautomatiseerd werk als doelwit hebben (computercriminaliteit in enge zin) en ernstige commune misdrijven die in toenemende mate met behulp van een geautomatiseerd werk worden gepleegd (gedigitaliseerde criminaliteit) waarbij vaak geen ander aanknopingspunt is voor de opsporing dan via het geautomatiseerde werk waarmee het misdrijf wordt gepleegd. Voor alle aangewezen misdrijven geldt dat er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders.
De toenemende digitalisering van de maatschappij leidt tot nieuwe veiligheidsrisico's en nieuwe mogelijkheden voor criminelen. Het aantal gevallen van computercriminaliteit waarbij computers niet alleen als middel worden ingezet, maar ook doelwit zijn, neemt toe. Van computercriminaliteit gaan grote dreigingen uit, zoals gevaar voor maatschappelijke ontwrichting en voor het vertrouwen in het financieel-economische systeem. Dat risico is onder meer aan de orde bij aanvallen via zogenoemde botnets, waarbij controle op afstand over een aanzienlijk aantal computers tot stand wordt gebracht door deze door middel van gerichte cyberaanvallen te besmetten met kwaadaardige software. Het netwerk van computers dat de botnet vormt kan worden ingezet om een grootschalige cyberaanvallen uit te voeren. Deze aanvallen kunnen vleiden tot ernstige economische schade en tot ontwrichting en vernietiging van vitale infrastructuren, zoals energiecentrales, vervoersnetwerken en overheidsnetwerken.
Ook op andere criminaliteitsterreinen maken criminelen steeds vaker gebruik van digitale technieken. Beroepscriminelen schermen hun activiteiten af door geavanceerde technische middelen in te zetten, wat het opsporingsonderzoek en de bewijsvergaring complex maakt. Ondermijnende criminaliteit, zoals witwassen, fraude en corruptie waarbij criminelen voor hun activiteiten gebruik maken van legale structuren en goederen, verplaatst zich naar het virtuele domein en ontwricht het maatschappelijk vertrouwen. Grootschalige financiële fraude wordt steeds vaker door technisch zeer capabele criminelen gepleegd. Zedenmisdrijven, zoals het verleiden of aanzetten van een minderjarige tot webcamseks, worden steeds vaker online gepleegd. De gevolgen hiervan kunnen indringend, ingrijpend en langdurig zijn en hebben niet alleen impact op het slachtoffer, maar ook op de omgeving en de samenleving als geheel.
Inzet van de binnendring- en onderzoeksbevoegdheid met het oog op het veiligstellen van digitaal bewijs voor voornoemde strafbare feiten en het stopzetten van criminele activiteiten draagt bij aan een effectieve aanpak van cybercrime en aan een veilig digitaal domein. Door de aanwijzing van misdrijven bij algemene maatregel van bestuur kan flexibel worden ingespeeld op de snelle ontwikkelingen in de cybercriminaliteit.

3. De uitvoering van een bevel van de officier van justitie

3.1. Het onderzoek in een geautomatiseerd werk
In dit besluit worden nadere regels gesteld over het onderzoek in een geautomatiseerd werk ter uitvoering van een bevel van de officier van justitie als bedoeld in de artikelen 126nba/uba/zpa Sv. Onder onderzoek in een geautomatiseerd werk wordt in deze toelichting verstaan: het op afstand en heimelijk binnendringen in een geautomatiseerd werk en het verrichten van bepaalde onderzoekshandelingen. Het binnendringen in een geautomatiseerd werk is het voorbereidende deel van het onderzoek. In de daarop volgende onderzoeksfase worden al dan niet met een technisch hulpmiddel onderzoekshandelingen verricht met het oog op bepaalde onderzoekdoelen en gegevens vastgelegd.
Bij het binnendringen in een geautomatiseerd werk kan gebruik worden gemaakt van verschillende technieken. In beginsel wordt gebruik gemaakt van zwakheden bij de gebruiker of kwetsbaarheden die bekend zijn bij de producent van het geautomatiseerde werk of de software. In het uitzonderlijke geval dat gebruik wordt gemaakt van een kwetsbaarheid waarvan aannemelijk is dat die niet bekend is of kan worden verondersteld bekend te zijn, kan de officier van justitie op grond van het wetsvoorstel computercriminaliteit III bevelen, na machtiging van de rechter-commissaris, dat de melding hiervan aan de producent wordt uitgesteld (artikel 126ffa

Sv).
De onderzoeksdoelen met het oog waarop onderzoek kan worden gedaan betreffen:
a. de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;
b. de uitvoering van een bevel tot stelselmatige observatie;
c. de uitvoering van een bevel tot het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie;
d. de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen;
e. de ontoegankelijkmaking van gegevens.
Het bevel van de officier bevat de onderzoeksdoelen met het oog waarop het bevel wordt afgegeven (artikelen 126nba/126uba, tweede lid, onder e, Sv en 126zpa, tweede lid, onder c, Sv). Als het gaat om de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, de vastlegging van gegevens of de ontoegankelijkmaking van gegevens dient het bevel een duidelijke omschrijving van de te verrichten handelingen te bevatten. Ook wordt in het bevel tot uitdrukking gebracht ten aanzien van welk deel van het geautomatiseerde werk en welke categorie van gegevens aan het bevel uitvoering wordt gegeven (artikelen 126nba/126uba/126zpa, tweede lid, onder f, Sv). Verder dient in het bevel een aanduiding van de aard en functionaliteit van het technische hulpmiddel te worden opgenomen (artikelen 126nba/126uba, tweede lid, onder d, en 126zpa, tweede lid, onder b, Sv).
Het wetsvoorstel computercriminaliteit III bevat grondslagen om bij of krachtens algemene maatregel van bestuur regels te stellen over het onderzoek in een geautomatiseerd werk. Het betreft ten eerste de deskundigheid en autorisatie van de bij het binnendringen in een geautomatiseerd werk en het verrichten van onderzoekshandelingen betrokken opsporingsambtenaren en de samenwerking met andere opsporingsambtenaren (artikel 126nba, achtste lid, onder a, Sv, dat van overeenkomstige toepassing wordt verklaard in de artikelen 126uba/126zpa, derde lid, Sv). Het betreft ten tweede verschillende organisatorische, procedurele en technische eisen met betrekking tot de onderzoeksfase waarin gegevens worden vastgelegd. Hierbij gaat het om de geautomatiseerde vastlegging van gegevens ter uitvoering van een bevel van de officier van justitie (artikel 126nba, achtste lid, onder b, Sv, dat van overeenkomstige toepassing wordt verklaard in de artikelen 126uba/126zpa, derde lid, Sv) en diverse aspecten met betrekking tot het doen van onderzoek met behulp van een technisch hulpmiddel (artikel 126ee Sv). De gegevens die tijdens de onderzoeksfase worden vastgelegd kunnen worden gebruikt als bewijs in een strafzaak. Gelet hierop dienen de betrouwbaarheid en integriteit van de gegevens onomstotelijk vast te staan, zowel in het belang van de betrokkene als in het belang van de opsporing. Door eisen te stellen aan onderzoeksproces en de verantwoording hiervan ontstaat een gegevensspoor dat herleidbaar is.
Bij het stellen van regels over het onderzoek in een geautomatiseerd werk is een zekere mate van techniekonafhankelijkheid in acht genomen. Techniek verandert snel en cybercriminaliteit ook. De bestrijding van cybercriminaliteit vraagt om enige flexibiliteit en abstractie van technische details. Het besluit heeft gelet hierop een kaderstellend karakter. Er worden eisen gesteld aan de organisatie, inrichting en controleerbaarheid van het onderzoeksproces. De uitwerking hiervan vindt plaats in de opsporingspraktijk, aan de hand van onder meer OM-aanwijzingen, (keurings)protocollen, handreikingen en mandaatbesluiten. De Inspectie Veiligheid en Justitie (hierna: Inspectie VenJ) houdt toezicht op de naleving van de regels die zijn neergelegd in het Wetboek van Strafvordering en in het onderhavige besluit bij de uitvoering van het onderzoek in een geautomatiseerd werk door opsporingsambtenaren.

3.2 Deskundigheid van opsporingsambtenaren
In hoofdstuk 3 van dit besluit worden regels gesteld over de opsporingsambtenaren die kunnen worden aangewezen voor het onderzoek in een geautomatiseerd werk, hun deskundigheid en de samenwerking tussen opsporingsambtenaren. Door het onderzoek in een geautomatiseerd werk voor te behouden aan opsporingsambtenaren die beschikken over specialistische kennis en vaardigheden op het terrein van ICT kan de kwaliteit en professionaliteit van het onderzoek worden geborgd. Op grond van het besluit kunnen opsporingsambtenaren van de politie, de Koninklijke marechaussee (Kmar) en de bijzondere opsporingsdiensten, en buitengewone

opsporingsambtenaren, bedoeld in artikel 141 Sv onder b, c en d, en 142 Sv door de korpschef worden aangewezen voor het binnendringen in een geautomatiseerd werk en al dan niet met behulp van een technisch hulpmiddel onderzoek doen, indien zij lid zijn van een technisch team. De politie heeft behoefte aan de bevoegdheid met het oog op de uitvoering van de politietaak, bedoeld in artikel 3 van de Politiewet 2012, namelijk de opsporing van computercriminaliteit en vormen van commune criminaliteit, waarbij geen andere aanknopingspunten zijn voor de opsporing van het misdrijf dan het gebruikte geautomatiseerde werk. Bij de Kmar bestaat de behoefte aan deze bevoegdheid met het oog op de uitvoering van de in artikel 4 van de Politiewet 2012 genoemde politietaken. Bij de FIOD/ECD bestaat behoefte aan deze bevoegdheid met het oog op de strafrechtelijke handhaving van de rechtsorde op bepaalde beleidsterreinen, bedoeld in artikel 3 van de Wet op de bijzondere opsporingsdiensten, te weten de opsporing van fraude en witwassen.
In verband met de behoefte aan specifieke expertise op het gebied van ICT kunnen naast de in artikel 141 Sv bedoelde opsporingsambtenaren ook buitengewone opsporingsambtenaren, bedoeld in artikel 142 Sv, die categoraal zijn aangewezen door de Minister van Veiligheid en Justitie, worden belast met het binnendringen in een geautomatiseerd werk en het doen van onderzoek. Hun opsporingsbevoegdheid strekt zich uit tot de in de categorale aanwijzing aangeduide feiten. De kwaliteit van een technisch team wordt geborgd door middel van opleidingseisen. Een opsporingsambtenaar kan lid worden van een technisch team, indien hij heeft voldaan aan door de Minister van Veiligheid en Justitie aangewezen kwalificaties, onder meer ten aanzien van kennis op het gebied van ICT. De opleidingseisen worden nader worden uitgewerkt in een ministeriële regeling, die tegelijk met dit besluit in werking treedt.
Gelet op de bijzondere expertise en de technische voorzieningen die nodig zijn voor het onderzoek in een geautomatiseerd werk wordt, in ieder geval gedurende de beginfase, de organisatie van de technische teams centraal belegd binnen de politieorganisatie. Binnen de Landelijke eenheid van de Nationale Politie worden één of meer technische teams ingericht die worden belast met het onderzoek in een geautomatiseerd werk. Deze teams voeren dit onderzoek uit ten behoeve van de politie, de Kmar en de bijzondere opsporingsdiensten.
Incidentele samenwerking tussen leden van een technisch team en andere opsporingsambtenaren is mogelijk, het besluit bevat hiervoor een voorziening. Een opsporingsambtenaar die geen lid is van een technisch team kan worden aangewezen voor het binnendringen in een geautomatiseerd werk en doen van onderzoek, indien hij beschikt over specifieke kennis en vaardigheden die nodig zijn voor de uitvoering van het onderzoek in een geautomatiseerd werk in het kader van een individueel opsporingsonderzoek. Dit staat ter beoordeling van de korpschef. Bij een positieve beoordeling wordt de opsporingsambtenaar op incidentele basis als deelnemer toegevoegd aan een technisch team en wordt hij gedurende het de uitvoering van het bevel begeleid door een lid van een technisch team.

3.3 Taakverdeling en functiescheiding gedurende het opsporingsonderzoek
Gedurende het opsporingsonderzoek, dat plaatsvindt onder het gezag van de officier van justitie, is er sprake van een strikte taakverdeling en functiescheiding. De opsporingsambtenaren die verantwoordelijk zijn voor de voorbereiding en de uitvoering van het onderzoek in een geautomatiseerd werk maken deel uit van een technisch team en behoren niet tot het tactische team. Het tactische team is belast met het uitvoeren van het operationele onderzoek.
De voorbereiding van het onderzoek in een geautomatiseerd werk start met een projectvoorstel van een tactisch team aan de officier van justitie, waarin het onderzoek in een concrete zaak wordt voorgesteld. Een projectplan kan afkomstig zijn van tactische rechercheteams van de politie, van de Kmar of van een bijzondere opsporingsdienst. Het projectplan bevat onder meer een beschrijving van de verdachte, de verdenking, de noodzaak om de onderzoeksbevoegdheid toe te passen en de gewenste resultaten van de toepassing van de bevoegdheid.
Vervolgens vraagt de officier van justitie een technisch team om advies over de haalbaarheid van het onderzoek. Voor de inschatting, beheersing en beperking van de risico's voor het geautomatiseerde werk is de deskundigheid van de opsporingsambtenaren van het technische team van essentieel belang. Omdat het technische team niet betrokken is bij het operationele onderzoek van het tactische team kan het niet worden beïnvloed bij het maken van afwegingen

met betrekking tot de haalbaarheid en de wijze van uitvoering van het binnendringen in en het verrichten van onderzoekshandelingen in een geautomatiseerd werk.
Het technische team stelt op basis van de intakegegevens en overige relevante gegevens een rapport haalbaarheidsonderzoek op voor de officier van justitie. Hierin wordt het plan van aanpak voor de uitvoering van een onderzoek in het geautomatiseerde werk uitgewerkt. In het rapport wordt onder meer opgenomen welke bevelen nodig zijn en welk technisch hulpmiddel moet worden gebruikt. De officier van justitie gebruikt het rapport haalbaarheidsonderzoek voor het verkrijgen van toestemming voor de inzet van de opsporingsbevoegdheid van het College van procureurs-generaal en de voorafgaande machtiging van de rechter-commissaris.
Het onderzoek in een geautomatiseerd werk kan worden uitgevoerd, zodra daartoe een bevel is afgegeven door de officier van justitie. Het onderzoek is voorbehouden aan de opsporingsambtenaren van een technisch team. In de hoofdstukken 3, 7, 8 en 9 van dit besluit wordt de taakverdeling uitgewerkt.
Na afgifte van een bevel zal een technisch team eerst voorverkenningen uitvoeren. Na analyse daarvan wordt een plan van aanpak voor het binnendringen in het geautomatiseerd werk opgesteld. Het plan van aanpak wordt getest in een proefopstelling.
Het daadwerkelijke onderzoek in het geautomatiseerde werk bestaat uit een voorbereidende fase en een onderzoekfase. De voorbereidende fase omvat het binnendringen in het geautomatiseerde werk volgens het vooraf geschreven plan van aanpak. Hierbij kunnen, zoals hiervoor is aangegeven, verschillende technieken worden gebruikt. De onderzoeksfase bestaat uit het uitvoeren van onderzoekshandelingen in een geautomatiseerd werk. De onderzoekshandelingen kunnen worden verricht met behulp van een technisch hulpmiddel, een softwareapplicatie die gegevens detecteert, registreert en transporteert. Het gebruik van een technisch hulpmiddel is echter niet strikt noodzakelijk: onderzoekshandelingen kunnen ook ad hoc en handmatig plaatsvinden.
De tijdens een onderzoek in een geautomatiseerd werk met een technisch hulpmiddel geregistreerde gegevens worden automatisch vastgelegd op een technische infrastructuur van een technisch team. De vastgelegde gegevens zijn uitsluitend toegankelijk voor de door de korpschef aangewezen ambtenaren. Tactische opsporingsambtenaren hebben geen toegang tot de gegevens. De technische infrastructuur is beveiligd tegen wijziging van de vastgelegde gegevens en kennisneming hiervan door onbevoegden.
De resultaten van het onderzoek worden door het technische team ter beschikking gesteld aan het tactische team. Zo nodig kan het technische team, op basis van technische criteria, zorgdragen voor voorafgaande filtering van de onderzoeksgegevens, zodat binnen de categorieën van gegevens die in het bevel van de officier zijn opgenomen uitsluitend die gegevens die van belang zijn voor het opsporingsonderzoek ter beschikking komen van het tactische team. Bij het opnemen van vertrouwelijke communicatie of het opnemen van telecommunicatie of de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen, zoals email-verkeer, kan niet worden uitgesloten dat gegevens worden verkregen over andere personen die bij de communicatie zijn betrokken. Deze gegevens zijn niet van belang voor het opsporingsonderzoek. In dat geval wordt uitsluitend het email-verkeer waarvan de email-adressen zijn opgenomen op een vooraf opgestelde lijst ter beschikking gesteld van het tactische onderzoeksteam. In het bevel dient melding te worden gemaakt van het feit dat binnen de categorie van gegevens waarvoor het bevel wordt afgegeven uitsluitend die onderzoeksgegevens die van belang zijn voor het opsporingsonderzoek ter beschikking worden gesteld van het tactische team.
De organisatorische scheiding tussen het technische team en het tactische team behoeft de samenwerking tussen de teams gedurende het opsporingsonderzoek niet te belemmeren. De officier van justitie onder wiens leiding het opsporingsonderzoek plaatsvindt vervult hierbij een schakelfunctie. Afhankelijk van het verloop van het onderzoek kan de grens tussen het technisch optreden en het tactisch optreden verschillen, maar de samenwerking zal dusdanig plaatsvinden dat het tactisch team geen enkele invloed kan uitoefenen op het binnendringen in het geautomatiseerde werk en de plaatsing, inzet en verwijdering van een technisch hulpmiddel.

3.4. Vastlegging van gegevens over de uitvoering van een bevel (logging)
De digitale omgeving waarin het onderzoek in een geautomatiseerd werk plaatsvindt maakt het

mogelijk om gedurende de onderzoeksfase doorlopend en automatisch gegevens vast te leggen over de uitvoering van het bevel van de officier van justitie. Hierdoor kan zowel tijdens de uitvoering van bevel van de officier als na afloop hiervan worden vastgesteld of een handeling of bewerking heeft plaatsgevonden die van invloed is op de betrouwbaarheid en integriteit van de vastgelegde gegevens. Deze vorm van elektronische verslaglegging over de uitvoering van een bevel wordt ook wel aangeduid als "logging".
In hoofdstuk 4 van dit besluit worden regels gesteld over de logging. Gedurende de uitvoering van een bevel worden gegevens over onderzoekshandelingen die worden verricht doorlopend en automatisch worden vastgelegd. Onder de logging van de onderzoekshandelingen valt ook de vastlegging van de gegevens die door een technisch hulpmiddel worden geregistreerd, de zogenaamde bewijslogging. De bewijslogging dient plaats te vinden op een technische infrastructuur van een technisch team. Het functioneren van de technische infrastructuur wordt eveneens doorlopend en automatisch gelogd.
De logging dient zodanig te zijn ingericht dat op basis hiervan kan worden vastgesteld of en zo ja wanneer een onregelmatigheid heeft plaatsgevonden, die van invloed is op de betrouwbaarheid en integriteit van de tijdens de onderzoeksfase vergaarde gegevens. Indien dat het geval is, maakt de opsporingsambtenaar van een technisch team hiervan proces-verbaal op, dat aan de officier van justitie wordt gezonden, zodat de officier van justitie en de rechter kunnen bepalen in hoeverre de geconstateerde onregelmatigheid afbreuk doet aan de bewijskracht van de tijdens het onderzoek vastgelegde gegevens.
Het voorbereidende deel van het onderzoek, het binnendringen in een geautomatiseerd werk, behoeft niet te worden gelogd, omdat de handelingen die in dit deel van het onderzoek plaatsvinden niet van invloed zijn op de betrouwbaarheid en de integriteit van het bewijs. Als in een strafzaak vragen zouden rijzen over de wijze van binnendringen, is het aan de rechter om hierover te oordelen. Zo nodig kan een rechter overgaan tot het horen van de betrokken opsporingsambtenaar of kan hij een deskundige raadplegen.
De logging is ten eerste en vooral bedoeld voor de interne controle van de tijdens de onderzoeksfase verrichte handelingen. Daarnaast maakt de bewijslogging het mogelijk om de met een technisch hulpmiddel geregistreerde gegevens achteraf te verantwoorden in een strafzaak. Die verantwoording vindt plaats aan de hand van de processen-verbaal en andere voorwerpen waaraan gegevens kunnen worden ontleend die voor het onderzoek in de zaak van betekenis zijn (artikel 126aa Sv). De officier van justitie houdt bij het samenstellen van het strafdossier rekening met bijzondere belangen zoals de afscherming van methodieken en middelen. Deze belangen kunnen een minder gedetailleerde verantwoording rechtvaardigen. Als bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk gebruik gemaakt wordt van een gekeurd technisch hulpmiddel zal in het proces-verbaal van de inzet worden verwezen naar het keuringsnummer, waardoor de samenstelling van het hulpmiddel ter bescherming van de opsporingsbelangen, kan worden afgeschermd.
Indien tijdens de behandeling van een strafzaak twijfels zouden rijzen over de betrouwbaarheid en de integriteit van het tijdens het onderzoek vergaarde bewijs, kan de rechter de volledige informatie opvragen of een deskundige raadplegen. Hierbij staat de rechter de procedure zoals omschreven in artikel 187d Sv ter beschikking, waarin de rechter-commissaris kan beletten dat antwoorden op vragen ter kennis komen van de verdachte en diens raadsman, indien er een gegrond vermoeden bestaat dat door de openbaarmaking een zwaarwegend opsporingsbelang wordt geschaad.

3.5. Het doen van onderzoek met een gekeurd technisch hulpmiddel

3.5.1. Algemeen

Het doen van onderzoek in een geautomatiseerd werk met het oog op in het bevel van de officier van justitie opgenomen onderzoeksdoelen kan plaatsvinden met een technisch hulpmiddel. Een technisch hulpmiddel is een sofwareapplicatie die functionaliteiten bevat waarmee gegevens kunnen worden gedetecteerd, geregistreerd en getransporteerd. Het transport van de geregistreerde gegevens vindt plaats naar een technische infrastructuur, een opslaglocatie in beheer van de politie, waarop de gegevens worden vastgelegd. De vastgelegde gegevens kunnen als bewijs dienen in een strafzaak. Gelet hierop is het essentieel dat de gegevens betrouwbaar,

integer en herleidbaar zijn.
In de hoofdstukken 5 tot en met 9 van dit besluit worden regels gesteld over technische hulpmiddelen waarmee onderzoek wordt gedaan in een geautomatiseerd werk. Deze regels hebben ten eerste betrekking op de technische eisen waaraan technische hulpmiddelen moeten voldoen en de voorafgaande goedkeuring hiervan. Ten tweede worden regels gesteld over de toegang tot, plaatsing, inzet en verwijdering van technische hulpmiddelen en de vastlegging van met een technisch hulpmiddel geregistreerde gegevens op een technische infrastructuur binnen de politieorganisatie.
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 en een richtmicrofoon.
Op grond van het wetsvoorstel computercriminaliteit III wordt het mogelijk om deze bevoegdheden uit te oefenen nadat heimelijk en op afstand is binnengedrongen in een geautomatiseerd werk. In het onderhavige besluit worden eisen gesteld aan technische hulpmiddelen die worden gebruikt bij de inzet van de bestaande bijzondere opsporingsbevoegdheden in het kader van een onderzoek in een geautomatiseerd werk. Alsdan en 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.

3.5.2. Technische eisen

Om de betrouwbaarheid en integriteit van technische hulpmiddelen, de betrouwbaarheid en integriteit van de hiermee geregistreerde gegevens en de herleidbaarheid van de gegevens te borgen stelt het besluit diverse technische eisen aan een technisch hulpmiddel. Een technisch hulpmiddel moet in staat zijn om gegevens op zodanige wijze te registreren dat de inhoud identiek is aan de in een geautomatiseerd werk gedetecteerde gegevens. Ook moet een technisch hulpmiddel geregistreerde gegevens kunnen voorzien van de datum en tijd van de registratie. Verder moet een technisch hulpmiddel de geregistreerde gegevens kunnen voorzien van een uniek kenmerk, dat bij vastlegging van de gegevens op de opslaglocatie wordt herkend, zodat de herkomst van de gegevens te allen tijde kan worden vastgesteld.
De integriteit van de met een technisch hulpmiddel vergaarde gegevens, waarmee gedoeld wordt op de zekerheid dat een gegeven niet is gewijzigd of hiervan onbevoegd kennis is genomen, wordt geborgd door eisen te stellen aan de beveiliging van een technisch hulpmiddel en de door een technisch hulpmiddel geregistreerde en getransporteerde gegevens. Naast technische eisen aan het technische hulpmiddel stelt het besluit ook eisen met betrekking tot de kwaliteit van de technische infrastructuur waarop de met een technisch hulpmiddel geregistreerde gegevens worden vastgelegd.
Om de rechtmatigheid van de inzet van een hulpmiddel te kunnen garanderen vereist het besluit dat een technisch hulpmiddel zodanig is ingericht dat het mogelijk is om uitsluitend de in het bevel van de officier van justitie aangegeven functionaliteit(en) van een technisch hulpmiddel in te schakelen en uitsluitend gegevens te detecteren en registeren ten behoeve van deze functionaliteit.

3.5.3. Keuring

Voordat een technisch hulpmiddel wordt ingezet, dient het goedgekeurd te worden door een keuringsdienst. Als bij het verrichten van onderzoekshandelingen gebruik wordt gemaakt van een goedgekeurd hulpmiddel mag er vanuit worden gegaan dat aan de wettelijke eisen is voldaan.
Een onderdeel van de Landelijke eenheid van de Nationale Politie, de keuringsdienst van de Dienst landelijke operationele samenwerking, is momenteel belast met de keuring van de traditionele technische hulpmiddelen die worden ingezet bij stelselmatige observatie, het opnemen van vertrouwelijke communicatie en het opnemen van telecommunicatie. Deze keuringsdienst wordt

eveneens aangewezen voor de keuring van technische hulpmiddelen die gebruikt worden voor het verrichten van onderzoekshandelingen in een geautomatiseerd werk. Het besluit bevat de mogelijkheid om andere organisaties als keuringsdienst aan te wijzen. Om de kwaliteit en consistentie van de keuring te waarborgen stelt een keuringsdienst een keuringsprotocol op. Een keuringsprotocol behoeft de voorafgaande goedkeuring van de Minister van Veiligheid en Justitie. Van de keuring wordt een rapport opgemaakt, waarin bij goedkeuring wordt vermeld dat het technische hulpmiddel voldoet aan de technische eisen die het besluit stelt. Bij de goedkeuring wordt aan het technische hulpmiddel een referentienummer toegekend. Dit referentienummer kan gedurende het opsporingsonderzoek worden gebruikt om het hulpmiddel aan te duiden zodat de samenstelling van het hulpmiddel, ter bescherming opsporingsbelangen, kan worden afgeschermd. De mogelijkheid bestaat om sofwareapplicaties van verschillende producenten te betrekken of deze zelf binnen de politieorganisatie te (laten) ontwerpen, mits aan de wettelijke vereisten voor keuring wordt voldaan. De ervaring leert dat producenten van software veelvuldig gebruik maken van softwareupdates ter verbetering van het product. Indien de werking van een technisch hulpmiddel of een onderdeel hiervan door een softwareupdate zodanig wijzigt dat niet meer wordt voldaan aan de technische eisen vindt herkeuring plaats van het technische hulpmiddel of van het gewijzigde onderdeel hiervan.

3.6. Het doen van onderzoek zonder goedgekeurd technisch hulpmiddel
Het is denkbaar dat bij het verrichten van onderzoekshandelingen technische hulpmiddelen, worden gebruikt die zich naar hun aard niet lenen 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. Indien het onderzoeksbelang dit dringend vordert kan de officier van justitie bepalen dat een niet gekeurd technisch hulpmiddel wordt ingezet. Na afloop van het onderzoek kan alsnog goedkeuring plaatsvinden, tenzij de aard van het hulpmiddel zich naar het oordeel van de officier hiertegen verzet. De betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens zullen dan op andere wijze moeten worden geborgd. Ook als onderzoekshandelingen zonder goedgekeurd hulpmiddel plaatsvinden worden de verrichte onderzoekshandelingen en het functioneren van de technische infrastructuur gelogd.
In bepaalde gevallen kunnen onderzoekshandelingen beter handmatig worden verricht, zodat het gebruik van een technisch hulpmiddel achterwege kan blijven. Hierbij kan worden gedacht aan de situatie dat gegevens direct na het binnendringen kunnen worden ingezien of worden overgenomen ten behoeve van het vaststellen van de identiteit van het geautomatiseerde werk. De vraag of de inzet van een technisch hulpmiddel noodzakelijk is, is onder meer afhankelijk van de aard van de inzet, de aard van het geautomatiseerde werk en de vraag of de gegevens zonder inzet van een technisch hulpmiddel als rechtmatig bewijs kunnen worden aangemerkt. De advisering van de officier van justitie hieromtrent vindt plaats door het technische team.

4. Bewaartermijnen
De gegevens die al dan niet met een technisch hulpmiddel ter uitvoering van een bevel van de officier worden vastgelegd vallen onder een gedifferentieerd regime wat betreft de bewaartermijnen. De processen-verbaal en andere voorwerpen waaraan gegevens kunnen worden ontleend die zijn verkregen door observatie, het opnemen van vertrouwelijke communicatie en het opnemen van telecommunicatie met behulp van een technisch hulpmiddel worden door de officier van justitie, voor zover die niet bij de processtukken zijn gevoegd, ter beschikking gehouden van het onderzoek (artikel 126cc, eerste lid, Sv). Zodra twee maanden zijn verstreken nadat de zaak is geëindigd en de notificatie, bedoeld in artikel 126bb Sv is verricht, doet de officier van justitie de processen-verbaal en andere voorwerpen vernietigen. De procedure is uitgewerkt in het Besluit bewaren en vernietigen niet-gevoegde stukken.
De gegevens die zijn verkregen door de toepassing van de bevoegdheid met het oog op andere onderzoekshandelingen en al dan niet met een technisch hulpmiddel zijn gegenereerd vallen onder het regime van de Wet politiegegevens (Wpg). Afhankelijk van het specifieke doel van de verwerking kan de bewaartermijn verschillen. Doorgaans zullen de gegevens worden verwerkt met het oog op de ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval (artikel 9, eerste lid, Wpg). Zodra de gegevens niet langer noodzakelijk zijn

voor het doel van het onderzoek, worden deze verwijderd of gedurende een periode van maximaal een half jaar bewaard teneinde te bezien of zij aanleiding geven tot een nieuw onderzoek als bedoeld in het eerste lid of een nieuwe verwerking als bedoeld in artikel 10 Wpg. Na afloop van deze termijn worden de gegevens verwijderd (artikel 9, derde lid, Wpg). De situatie dat de gegevens niet langer noodzakelijk zijn voor het doel van het onderzoek zal – in geval van een opsporingsonderzoek dat heeft geleid tot een vervolging – pas optreden op het moment dat de rechter ten aanzien van de zaak onherroepelijk heeft beslist. Als de zaak niet is opgelost en niet is ingezonden aan het openbaar ministerie, wordt het onderzoek meestal wel voortgezet maar op een minder intensief niveau. De gegevens kunnen in dat geval nodig blijven voor het vervolg van het onderzoek en voor het geval dat het team opnieuw bijeen wordt geroepen vanwege nieuwe aanknopingspunten. De gegevens blijven dan doorgaans nodig voor het doel van het onderzoek tot uiterlijk het moment waarop de feiten, waar het onderzoek zich op richt zijn verjaard. Daarna kunnen de gegevens niet meer nodig zijn voor het doel van het onderzoek en moeten zij worden verwijderd (Kamerstukken II 2005/06, 30 327, nr. 3, blz. 45/46). De verwijderde politiegegevens worden gedurende een termijn van vijf jaren bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen en vervolgens gearchiveerd of vernietigd.
De logging wordt bewaard met het oog op de verantwoording van de verrichte onderzoekshandelingen en het functioneren van de technische infrastructuur waarop de met een technisch hulpmiddel geregistreerde gegevens worden vastgelegd. Deze gegevens worden verwerkt met het oog op de opsporing van strafbare feiten en vallen eveneens onder de reikwijdte van de Wpg. Dit betekent dat de gegevens doorgaans moeten worden verwijderd zodra deze niet langer noodzakelijk zijn voor het doel van het onderzoek. Dit geldt in zijn algemeenheid voor de logging van gegevens, dus ook voor de logging met betrekking tot het verrichten van onderzoekshandelingen met het oog op observatie, het opnemen van vertrouwelijke communicatie of het opnemen van telecommunicatie met behulp van een technisch hulpmiddel.

5. Systeemtoezicht

De Inspectie VenJ houdt toezicht op het functioneren van het wettelijke systeem rond de uitvoering van een bevel tot onderzoek in een geautomatiseerd werk. De Inspectie VenJ is belast met het toezicht op de taakuitvoering door de politie op grond van artikel 57, eerste lid, onderdeel d, van de Wet veiligheidsregio's. Artikel 126nba, zevende lid, Sv, (dat van overeenkomstige toepassing is verklaard in de artikelen 126uba/126zpa, derde lid, Sv) bepaalt dat het door de Inspectie uitgeoefende toezicht zich mede uitstrekt over de uitvoering van een bevel tot het binnendringen in een geautomatiseerd werk en onderzoek doen door de opsporingsambtenaren van de bijzondere opsporingsdiensten, bedoeld in artikel 141, onderdeel d, Sv en de buitengewone opsporingsambtenaren, bedoeld in artikel 142, eerste lid, onderdeel b, Sv.
Het toezicht van de Inspectie VenJ heeft betrekking op de naleving van de wettelijke regels die zijn neergelegd in het Wetboek van Strafvordering en het onderhavige besluit en omvat zowel de gevallen die in het kader van de door de officier van justitie ingestelde strafvervolging van een verdachte aan het oordeel van de rechter worden voorgelegd als gevallen die niet tot strafvervolging leiden. Concreet zal het systeemtoezicht van de Inspectie VenJ betrekking hebben op aspecten als de autorisatie van de opsporingsambtenaren voor handelingen ter uitvoering van een bevel van de officier van justitie, de expertise en kennis van de betrokken opsporingsambtenaren, de logging van gegevens over de uitvoering van een bevel, de inzet van een technisch hulpmiddel, de vastlegging van de met een technisch hulpmiddel geregistreerde gegevens op een technische infrastructuur, de beveiliging van gegevens en het gebruik van de gegevens, inclusief de bewaring en vernietiging daarvan. De inspecteurs beschikken over de bevoegdheden voor het toezicht op de naleving op grond van de Algemene wet bestuursrecht (Awb) (artikel 57, derde lid, Wet veiligheidsregio's, artikelen 5:12 tot en met 5:20 Awb).
De Inspectie VenJ werkt op basis van een werkprogramma dat jaarlijks wordt vastgesteld. Voor de invulling van het toezicht zullen naar verwachting de volgende vormen worden gebruikt: doorlichting, thematisch onderzoek en incidentonderzoek. Na afloop van een onderzoek wordt een rapport opgesteld. Het vastgestelde inspectierapport wordt aan de Minister van Veiligheid en Justitie aangeboden en door de Minister openbaar gemaakt.

Om de verhouding tussen taakuitoefening door de Inspectie VenJ en het verstrekkingenregime van de Wpg te verhelderen past dit besluit het Besluit politiegegevens aan. Daarmee wordt de verplichting tot verstrekking van politiegegevens in het kader van de toezichthoudende taak van de Inspectie VenJ expliciet wettelijk vastgelegd.

6. Europeesrechtelijke aspecten

Het vrij verkeer van goederen en diensten binnen de Europese Unie brengt met zich dat lidstaten in de nationale wetgeving geen eisen aan goederen en keuringen mogen stellen die leiden tot beperking van het vrije verkeer tussen de lidstaten. De technische eisen die in het besluit worden gesteld aan de technische hulpmiddelen waarmee onderzoekshandelingen in een geautomatiseerd werk worden verricht en de voorgeschreven keuring kunnen worden aangemerkt als een inbreuk op het vrije verkeer. Daarom is een wederzijdse erkenningsclausule opgenomen voor hulpmiddelen en keuringen.

Dit besluit biedt de mogelijkheid om naast de keuringsdienst van de Landelijke eenheid van de Nationale Politie andere keuringsdiensten aan te wijzen voor de keuring van technische hulpmiddelen. Als van deze mogelijkheid gebruik wordt gemaakt, dan worden hierover bij ministeriële regeling regels gesteld. Afhankelijk van de gekozen systematiek kan sprake zijn van een dienst van algemeen economisch belang of een niet-economische dienst van algemeen belang. Bij het opstellen van de ministeriële regeling zal dan toetsing plaatsvinden aan de daarvoor geldende EU-kaders, zoals de richtlijn 2006/123/EG van het Europees Parlement en de Raad van de Europese Unie van 12 december 2006 betreffende diensten op de interne markt (PbEU L 376) (Dienstenrichtlijn).

Het ontwerpbesluit is op **PM** gemeld aan de Europese Commissie onder richtlijn 2015/1535/EU (richtlijn van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende diensten van de informatiemaatschappij (codificatie van richtlijn 98/34/EG en 98/48/EG, 'de notificatierichtlijn')).

7. Financiële gevolgen

Het is de verwachting dat de nieuwe opsporingsbevoegdheid niet leidt tot structurele toename van de totale opsporingsinspanning. De uitvoering van het onderzoek in een geautomatiseerd werk vindt plaats bij een onderdeel van de Landelijke eenheid van de Nationale Politie. De Nationale Politie ontvangt jaarlijks een bijzondere bijdrage van €13,8 miljoen voor de digitale professionalisering en vernieuwing van de organisatie, onder meer ter bestrijding van cybercrime. De aanschaf en implementatie van ICT-hulpmiddelen ter voorbereiding op de invoering van het onderzoek in een geautomatiseerd werk geschiedt uit dit budget. De personeels- en IV-capaciteit en de structurele kosten voor beheer en onderhoud komen ten laste van de algemene begroting van de politie. Aan de begroting van de politie is bij najaarsnota structureel een bedrag toegevoegd voor de aanpak van cybercrime. Voor 2017 bedraagt de bijdrage € 1,4 miljoen, voor 2018 en verdere jaren € 1,5 miljoen. Deze bijdragen zijn bedoeld voor de versterking van personele en materiële capaciteit door opleiding en ICT-middelen en – tools. Voor zover het besluit leidt tot werklastgevolgen bij het openbaar ministerie en de rechtspraak worden de kosten gedekt binnen het reguliere budget.

8. Adviezen

PM.

II. Artikelsgewijze toelichting

Hoofdstuk 1 Algemene bepalingen

Artikel 1 Definities
Artikel 1 bevat een definitiebepaling van een aantal relevante begrippen in het besluit. Het meest gebruikte begrip is het begrip "technisch hulpmiddel" (onderdeel g). Hieronder wordt verstaan: softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel. Onder bevel (onderdeel a) wordt verstaan: een bevel van de officier van justitie als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid, Sv. Op grond van het wetsvoorstel computercriminaliteit III kan het doen van onderzoek al dan niet met een technisch hulpmiddel plaatsvinden. Van doen van onderzoek zonder technisch hulpmiddel is sprake als bij het onderzoek geen gebruik wordt gemaakt van software die gegevens detecteert, registreert en transporteert.
Een "onderzoekshandeling" is een handeling van een opsporingsambtenaar van een technisch team die met het oog op een onderzoeksdoel als bedoeld in de artikelen 126nba, eerste lid, a tot en met e, 126uba, eerste lid, onder a tot en met e, en 126zpa, eerste lid, Sv wordt verricht ter uitvoering van een bevel. Gedurende de uitvoering van een bevel vindt doorlopende en automatische vastlegging van gegevens plaats over de verrichte onderzoekshandelingen.
Met de definitie van "technische infrastructuur" (onderdeel h) wordt gedoeld op de opslaglocatie voor de met een technisch hulpmiddel geregistreerde gegevens. Uit deze definitie, in combinatie met de definitie van "technisch team" (onderdeel i), vloeit voort dat de vastlegging van geregistreerde gegevens dient plaats te vinden op een technische voorziening binnen de politieorganisatie. Deze eis wordt gesteld om de betrouwbaarheid en integriteit van de door een technisch hulpmiddel geregistreerde gegevens te borgen en onbevoegde wijziging of kennisneming hiervan te voorkomen. In de definitie van "technisch team" is de centrale plaatsing van dit team als herkenbaar onderdeel binnen de Landelijke eenheid tot uitdrukking gebracht.

Hoofdstuk 2 Toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijkmaken van gegevens

Artikel 2 Aanwijzing misdrijven
In dit artikel wordt een aantal ernstige misdrijven aangewezen waarvoor de binnendring- en onderzoeksbevoegdheid met het oog op de vastlegging van gegevens en ontoegankelijkmaking van gegevens kan worden toegepast. Het betreft misdrijven die met of met behulp van een geautomatiseerd werk worden gepleegd waarop een wettelijke strafbedreiging van minder dan acht jaren gevangenisstraf staat, maar die niettemin dermate ernstig zijn dat er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders.
De eerste categorie van misdrijven die worden aangewezen zijn computermisdrijven in enge zin, waarbij het misdrijf met een geautomatiseerd werk wordt gepleegd of betrekking heeft op een geautomatiseerd werk. Deze misdrijven zijn verspreid opgenomen in het Wetboek van Strafrecht. Het betreft in de eerste plaats de strafbaarstellingen van computervredebreuk, waaronder het gebruik van een botnet (artikelen 138ab Sr) en van ernstige "spam" of "bombing" (artikel 138b Sr), die zijn opgenomen in de Titel over de misdrijven tegen de openbare orde (Boek II, Titel V). Het wetsvoorstel computercriminaliteit III voegt hieraan strafbaarstellingen inzake het overnemen en helen van gegevens (artikelen 138c en 139g) toe, deze misdrijven worden eveneens aangewezen. Ook de bepalingen uit deze Titel over het aftappen of opnemen van gegevens (artikel 139d) zijn relevant, voor zover het gaat om het aftappen en opnemen van computergegevens. Daarnaast gaat het om de artikelen 161, eerste lid, 161bis en 161sexies, waarin de vernieling van geautomatiseerde werken en werken voor de vitale infrastructuur strafbaar is gesteld. Deze strafbepalingen maken onderdeel uit van Boek II, Titel VII, misdrijven waardoor de algemene veiligheid van personen of goederen in gevaar wordt gebracht. Ook Boek II, Titel XXVII (vernieling) bevat enkele computermisdrijven. Het betreft de artikelen 350a, 350c en 350d (beschadiging van computergegevens), deze misdrijven worden eveneens aangewezen voor de toepassing van de bevoegdheid.

De tweede categorie van misdrijven betreft ernstige commune misdrijven met een grote maatschappelijke impact die in toenemende mate worden gepleegd met behulp van een geautomatiseerd werk. Bij deze vormen van gedigitaliseerde criminaliteit is het geautomatiseerde werk waarvan gebruik wordt gemaakt bij het plegen van het misdrijf vaak het enige aanknopingspunt voor de opsporing. Aangewezen worden diverse ernstige ondermijnende misdrijven die strafbaar zijn gesteld in verschillende titels van het Wetboek van Strafrecht (Boek II, Titel V, misdrijven tegen de openbare orde, Titel VIII, misdrijven tegen het openbaar gezag Titel XII, valsheid in geschrifte, Titel XXXA Witwassen), te weten de rekrutering voor terrorisme (artikelen 131 en 205 Sr), het deelnemen aan een criminele organisatie (artikel 140 Sr), mensensmokkel (artikel 197a Sr) corruptie (artikelen 177, 179, 182, 200 Sr), fraude (artikelen 225, 226, 227, 231, 231a, 232 Sr) en witwassen (artikel 420bis Sr).
Ook spionagemisdrijven (artikelen 98, 98c Sr), waarmee een inbreuk wordt gemaakt op de veiligheid van de staat (Boek II, Titel I), worden in toenemende mate langs digitale weg gepleegd. Hetzelfde geldt voor het plaatsen van een valse bom of het doen van een valse bommelding (artikel 142 Sr, Boek II, Titel V), waarmee een ernstige inbreuk wordt gemaakt op de openbare orde en waardoor overheidsdiensten in hun functioneren worden belemmerd. Ook zedenmisdrijven met minderjarigen (artikelen 240b, 247, 248a en 248e Sr, Boek II, Titel XIV,) en het misdrijf stalking (artikel 285b Sr, Titel XVIII), waarmee een inbreuk wordt gemaakt op de seksuele dan wel persoonlijke levenssfeer van een ander, vinden steeds vaker online plaats.
Voor een effectieve bestrijding van voornoemde ernstige strafbare feiten zijn digitale opsporingsmogelijkheden onontbeerlijk. Door toepassing van de bevoegdheid met het oog het vastleggen dan wel ontoegankelijkmaken van gegevens kan digitaal bewijs worden vergaard voor het gepleegde strafbare feit en kunnen criminele activiteiten worden beëindigd.

Hoofdstuk 3 Deskundigheid van opsporingsambtenaren

Artikel 3 Lidmaatschap van een technisch team
Artikel 3 regelt dat het binnendringen in een geautomatiseerd werk en het al dan niet met een technisch hulpmiddel onderzoek doen is voorbehouden aan de door de korpschef aangewezen opsporingsambtenaren van de politie, de Kmar, de bijzondere opsporingsdiensten en buitengewoon opsporingsambtenaren, bedoeld in artikel 141 Sv onder b, c en d, en 142 Sv, die lid zijn van een technisch team. Door het onderzoek in een geautomatiseerd werk voor te behouden aan deskundigen van een technisch team wordt de kwaliteit en de professionaliteit van dit onderzoek geborgd.
Binnen de Landelijke eenheid worden één of meer technische teams ingericht die kunnen worden belast met het binnendringen in een geautomatiseerd werk en het verrichten van onderzoekshandelingen. Deze teams voeren het onderzoek in een geautomatiseerd werk uit ten behoeve van de politie, de Kmar en de bijzondere opsporingsdiensten. Opsporingsambtenaren kunnen lid worden van een technisch team, indien zij voldoen aan door de Minister van Veiligheid en Justitie bepaalde kwalificaties. De kwalificaties waaraan een lid van een technisch team moet voldoen worden uitgewerkt in een ministeriële regeling. Een lid van een technisch team zal onder meer moeten beschikken over voldoende kennis en vaardigheden met betrekking tot ICT en kennis over het juridisch kader waarbinnen het onderzoek in een geautomatiseerd werk plaatsvindt. Ook vaardigheden met betrekking het opmaken van processen-verbaal zullen deel uitmaken van de opleidingseisen. Het lidmaatschap van een technisch team is een specialistische functie, het doorlopen van de volledige politieopleiding is gelet hierop niet nodig. De leden van het technische team zullen naar verwachting vooral zogenaamde zij-instromers zijn.
De opsporingsambtenaren van een technisch team behoren niet tot het tactische team dat is belast met het tactische onderzoek. Deze functiescheiding vermindert het risico op tunnelvisie.
Het toezicht op de naleving van de deskundigheidseisen maakt onderdeel uit van het systeemtoezicht van de Inspectie VenJ.

Artikel 4 Incidentele samenwerking
Artikel 4 biedt een voorziening voor de incidentele samenwerking tussen opsporingsambtenaren. Een opsporingsambtenaar van de politie, de Kmar, de bijzondere opsporingsdiensten of een buitengewoon opsporingsambtenaar die geen lid is van een technisch team kan door de korpschef

worden aangewezen voor het binnendringen in een geautomatiseerd werk en doen van onderzoek als hij beschikt over specifieke kennis en vaardigheden die nodig zijn voor de uitvoering van een bevel in een individueel opsporingsonderzoek. Hierbij kan worden gedacht aan de situatie dat een opsporingsambtenaar van een bijzondere opsporingsdienst met specifieke kennis op het gebied van digitale fraude wordt toegevoegd aan een technisch team in verband met gewenste technische expertise op dit gebied in een bepaald onderzoek. De korpschef beoordeelt of een opsporingsambtenaar beschikt over voldoende specifieke kennis en vaardigheden voor het onderzoek. De korpschef kan deze bevoegdheid desgewenst mandateren aan het hoofd van het onderdeel van de Landelijke eenheid waar de technische teams worden ondergebracht. Om de kwaliteit en professionaliteit van het onderzoek te borgen bepaalt artikel 4 dat een opsporingsambtenaar die op ad hoc basis deelneemt aan een technisch team gedurende de uitvoering van het onderzoek wordt begeleid door een lid van een technisch team.

Hoofdstuk 4 Geautomatiseerde vastlegging van gegevens over de uitvoering van een bevel (logging)

Artikelen 5 tot en met 7 Vastlegging van gegevens, vaststelling onregelmatigheden en betrouwbaarheid en integriteit gegevens

Artikel 5 bepaalt dat alle onderzoekshandelingen die gedurende de uitvoering van een bevel van de officier van justitie worden verricht en het functioneren van de technische infrastructuur van een technisch team doorlopend en geautomatiseerd worden vastgelegd. Dit wordt ook wel logging genoemd. Er wordt gelogd op het niveau van de autorisatie, op het niveau van de verrichte onderzoekshandelingen en op het niveau van de werking van het systeem. Ter aanvulling op de automatische logging kan ook handmatige verslagging plaatsvinden over de uitvoering van een bevel, bijvoorbeeld in de vorm van een journaal. Zowel onderzoekshandelingen die met een technisch hulpmiddel plaatsvinden als onderzoekshandelingen waarbij de inzet van een technisch hulpmiddel achterwege blijft worden gelogd. Hierdoor zal steeds inzichtelijk zijn welke handelingen gedurende de onderzoeksfase door het technische team zijn verricht en is controle op de uitvoering van het bevel van de officier van justitie mogelijk.

Onder de logging van de onderzoekshandelingen valt ook de vastlegging van gegevens van door een technisch hulpmiddel geregistreerde gegevens, de zogenaamde bewijslogging. De vastlegging van de geregistreerde gegevens dient ingevolge artikel 24 van dit besluit plaats te vinden op een technische infrastructuur van een technisch team. Op grond van artikel 6 moet zowel tijdens de onderzoeksfase als achteraf vastgesteld kunnen worden of zich gedurende de uitvoering van het bevel een onregelmatigheid heeft voorgedaan, die van invloed is op de betrouwbaarheid van de op de technische infrastructuur vastgelegde gegevens. Indien dat het geval is, wordt hiervan proces-verbaal opgemaakt, dat aan de officier van justitie wordt gezonden.

In artikel 7 worden eisen gesteld ter borging van de kwaliteit van de logging. De gelogde gegevens mogen niet mogen worden bewerkt, zijn uitsluitend toegankelijk voor daartoe door de korpschef geautoriseerde ambtenaren en moeten beveiligd zijn tegen wijziging of onbevoegde kennisneming. Het voorbereidende deel van het onderzoek, het binnendringen in een geautomatiseerd werk, behoeft niet te worden gelogd, omdat de handelingen die in dit deel van het onderzoek plaatsvinden niet van invloed zijn op de betrouwbaarheid en de integriteit van het bewijs.

De gelogde gegevens moeten worden verwijderd zodra deze niet langer noodzakelijk zijn voor het doel van het onderzoek. Toezicht op de naleving van de regels over de logging vindt plaats door de Inspectie VenJ.

De logging dient ten eerste en vooral ter interne controle van de uitvoering van het bevel van de officier van justitie. Daarnaast kunnen door middel van de logging de verrichte onderzoekshandelingen worden verantwoord. De gedurende een opsporingsonderzoek verrichte opsporingshandelingen en de hiermee vergaarde gegevens worden neergelegd in een proces-verbaal (artikel 152 Sv). De officier van justitie voegt de processen-verbaal en andere voorwerpen die gegevens bevatten die voor het onderzoek in de zaak van betekenis zijn bij de processtukken (artikel 126aa Sv). In het geval in een strafzaak twijfel ontstaat over de wijze waarop de gegevens zijn verkregen of over de betrouwbaarheid van de verkregen gegevens, bijvoorbeeld op grond van een verweer van de verdachte of diens raadsman, kan aan de hand van de logging hierover verantwoording worden afgelegd.

Hoofdstuk 5 Technische eisen met betrekking tot een technisch hulpmiddel

Hoofdstuk 5 bevat de technische eisen waaraan een technisch hulpmiddel moet voldoen. Als bij de uitvoering van een bevel van de officier van justitie gebruik wordt gemaakt van een goedgekeurd technisch hulpmiddel mag er vanuit worden gegaan dat aan de wettelijke eisen is voldaan. In hoofdstuk 6 van dit besluit worden regels gesteld over de keuringsprocedure.

Artikelen 8 en 9 Gerichte werking, gerichte detectie en registratie
De artikelen 8 en 9 stellen eisen aan de inrichting en werking van een technisch hulpmiddel. De eerste eis betreft de gerichte werking van een technisch hulpmiddel (artikel 8). Het verrichten van onderzoekshandelingen met behulp van een technisch hulpmiddel in een geautomatiseerd werk vindt plaats binnen de grenzen van het bevel van de officier van justitie. Het bevel bevat (onder meer) een aanduiding van de aard en functionaliteit(en) van het technische hulpmiddel. Softwareapplicaties met behulp waarvan onderzoekshandelingen in een geautomatiseerd werk worden verricht beschikken naar hun aard vaak over verschillende functionaliteiten. Om te waarborgen dat de onderzoekshandelingen binnen de grenzen van het bevel van de officier van justitie worden verricht, bepaalt artikel 8 van het besluit dat een technisch hulpmiddel zodanig is ingericht dat de werking ervan kan worden beperkt tot de in het bevel vermelde functionaliteit of functionaliteiten. Hierbij kan worden gedacht aan functionaliteiten als het opnemen van geluid, het maken van screenshots, het vastleggen van toetsaanslagen of het doorzoeken van bepaalde bestandsmappen en het vastleggen van gegevens hieruit.
Bij de keuring wordt getoetst of een technisch hulpmiddel instellingen bevat waarmee de werking van een technisch hulpmiddel kan worden beperkt tot een bepaalde functionaliteit of tot bepaalde functionaliteiten. De keuringsdienst stelt bij de keuring een handleiding op voor het gebruik van een hulpmiddel, waarin wordt aangegeven welke instellingen bij gebruik van een technisch hulpmiddel voor een bepaalde functionaliteit moeten worden aangevinkt. Bij de plaatsing van een technisch hulpmiddel wordt hierover verantwoording afgelegd in een proces-verbaal (artikel 22 van het besluit).
De in artikel 9 gestelde eis ligt in het verlengde van artikel 8. Een technisch hulpmiddel moet in staat zijn uitsluitend gegevens te detecteren en te registreren ten behoeve van de in het bevel vermelde functionaliteit of functionaliteiten. De eis in artikel 8, tweede lid, is overgenomen uit artikel 11 van het Besluit technische hulpmiddelen strafvordering en heeft betrekking op technische hulpmiddelen die worden ingezet ten behoeve van het opnemen van telecommunicatie. Het technische hulpmiddel dient in staat te zijn om uitsluitend van een vooraf opgegeven nummer de telecommunicatie op te nemen.

Artikelen 10, 11 en 12 Betrouwbaarheid en integriteit, herleidbaarheid, datum tijd
De in de artikelen 10 tot en met 12 gestelde technische eisen strekken ertoe de betrouwbaarheid, integriteit en herleidbaarheid van de met een technisch hulpmiddel geregistreerde gegevens te garanderen. Een technisch hulpmiddel detecteert gegevens in het geautomatiseerde werk, registreert de gedetecteerde gegevens en transporteert de gegevens naar de technische infrastructuur van het technisch team. Omdat de met een technisch hulpmiddel vastgelegde gegevens kunnen dienen als bewijs in een strafzaak, is het van essentieel belang dat de betrouwbaarheid en integriteit van de gegevens vaststaan en dat de gegevens herleidbaar zijn. Dit kan allereerst worden bereikt door te eisen dat de inhoud van de gegevens die door een technisch hulpmiddel worden geregistreerd identiek is aan de inhoud van de gegevens die worden gedetecteerd in het geautomatiseerde werk. Dit wordt geregeld in artikel 10, eerste lid. Met gedetecteerde gegevens wordt gedoeld op de gegevens die een technisch hulpmiddel waarneemt in een te onderzoeken geautomatiseerd werk. Een voorbeeld is het lezen van een bestand op een computer van een verdachte. Van geregistreerde gegevens is sprake als het technische hulpmiddel de gedetecteerde gegevens overneemt uit het geautomatiseerde werk. De eis heeft betrekking op de inhoud van de gegevens. Niet is van belang op welke wijze de metadata worden geregistreerd. Als de in het geautomatiseerde werk gedetecteerde gegevens door het technische hulpmiddel in een ander format worden geregistreerd (een voorbeeld is een SMS die op een mobiel apparatuur

als PDU is opgeslagen en die door een technisch hulpmiddel in ASCII coding wordt geregistreerd) zal na de vastlegging van de gegevens op de technische infrastructuur de omzetting van het format met een applicatie moeten worden uitgelokt. Bij de keuring zal worden gekeurd of het technische hulpmiddel een voorziening bevat om de inhoud van de geregistreerde gegevens zichtbaar te maken.
Artikel 10, tweede lid, vereist dat een technisch hulpmiddel beveiligd is tegen wijziging van de werking ervan en tegen de wijziging en kennisneming van geregistreerde gegevens door onbevoegden. Hierbij dient te worden opgemerkt dat in de ICT nooit volledige garanties tegen beïnvloeding van buitenaf kunnen worden gegeven. Wel kan die beïnvloeding zo moeilijk mogelijk worden gemaakt. Bij de keuring wordt getoetst of er beveiligingsmaatregelen aanwezig zijn die beïnvloeding van een technisch hulpmiddel van buitenaf naar de stand van de techniek zo goed mogelijk tegengaan. Hierbij kan worden gedacht aan het aanwezig zijn van authenticatiemaatregelen voor de communicatie met het technische hulpmiddel.
Als een technisch hulpmiddel niet constant met de technische infrastructuur communiceert – het zal in de praktijk regelmatig voorkomen dat een verdachte offline is - dan kan een vorm van tussenopslag nodig zijn. Gelet hierop dient een technisch hulpmiddel beveiligd te zijn tegen wijziging van geregistreerde gegevens en kennisneming hiervan door onbevoegden. Hierbij kan naar de huidige stand van de techniek worden gedacht aan maatregelen als versleuteling van de gegevens met een digitale handtekening. Hierdoor wordt bereikt dat de door een technisch hulpmiddel geregistreerde gegevens na de registratie niet meer leesbaar en toegankelijk zijn.
Om te waarborgen dat de gegevens afkomstig zijn van het ter uitvoering van een bevel van de officier geplaatste technische hulpmiddel wordt in artikel 11 de eis gesteld dat een technisch hulpmiddel een uniek gegeven toevoegt aan de geregistreerde gegevens. Uit dit gegeven moet de relatie met het geplaatste technische hulpmiddel blijken. Hierbij kan worden gedacht aan een code die bij de plaatsing aan het technisch hulpmiddel is toegevoegd. De technische infrastructuur moet in staat zijn om bij de vastlegging van de geregistreerde gegevens het unieke gegeven te herkennen. Op deze wijze kan een herleidbaar gegevensspoor worden gecreëerd.
Artikel 12 vereist dat een technisch hulpmiddel de geregistreerde gegevens voorziet van de datum en tijd van de registratie. Hierdoor wordt inzichtelijk op welk moment een onderzoekshandeling heeft plaatsgevonden. De eis van datum- en tijdregistratie betekent niet dat er doorlopend datum- en tijdregistratie moet plaatsvinden gedurende de inzet van een technisch hulpmiddel. Artikel 12 staat er niet aan de in de weg dat een technisch hulpmiddel uitsluitend gegevens registreert als er gegevens van het te onderzoeken geautomatiseerde werk worden ontvangen. De strekking van de eis is dat zodra er gegevens worden geregistreerd door een technisch hulpmiddel er zekerheid bestaat over de datum en het tijdstip van de gegevensregistratie door het technische hulpmiddel. Door middel van de logging van de onderzoekshandelingen en het functioneren van de technische infrastructuur kan controle plaatsvinden op het functioneren van een technisch hulpmiddel. Indien zich gedurende de inzet van een technisch hulpmiddel onregelmatigheden voordoen die van invloed zijn op de kwaliteit van de vastgelegde gegevens kan hierover verantwoording worden afgelegd aan de hand van de logging.

Artikel 13 Transport geregistreerde gegevens
Op grond van artikel 13, eerste lid, van het besluit dient een technisch hulpmiddel zodanig te zijn ingericht dat geregistreerde gegevens automatisch worden getransporteerd naar een technische infrastructuur, die in beheer is bij een technisch team. Deze eis wordt gesteld om onbevoegde toegang van derden tot de met een technisch hulpmiddel geregistreerde gegevens te voorkomen. De keuring van een technisch hulpmiddel strekt zich uit tot het transport naar de opslaglocatie. De technische infrastructuur waarop de vastlegging van met een technisch hulpmiddel geregistreerde gegevens plaatsvindt wordt niet gekeurd. Om de integriteit van de op de technische infrastructuur vastgelegde gegevens te borgen dienen de geregistreerde gegevens tijdens het transport beveiligd te zijn tegen wijziging en kennisneming door onbevoegden (tweede lid). Bij de beoordeling van deze eis kunnen de wijze van beveiliging van de werking van een technisch hulpmiddel en de wijze van beveiliging van de geregistreerde gegevens worden betrokken.

Hoofdstuk 6 Keuring van een technisch hulpmiddel

Artikelen 14 en 15 Voorafgaande goedkeuring, herkeuring en keuring achteraf
Uitgangspunt is bij de inzet gebruik wordt gemaakt van een vooraf goedgekeurd technisch hulpmiddel. Dit wordt geregeld in artikel 14, eerste lid, van het besluit. Een technisch hulpmiddel kan uitsluitend worden goedgekeurd als het voldoet aan de artikelen 8 tot en met 13 gestelde eisen (tweede lid). Dit wordt beoordeeld tijdens de keuring. Artikel 14, derde lid, bevat regels over de herkeuring van technische hulpmiddelen. Herkeuring is aan de orde als de werking van een gekeurd technisch hulpmiddel of een onderdeel hiervan zodanig wijzigt dat redelijkerwijs kan worden aangenomen dat het hulpmiddel niet langer voldoet aan de in de artikelen 8 tot en 13 gestelde eisen. De herkeuring zal naar zijn aard vooral gericht zijn op de gewijzigde onderdelen van de software, die door de producent meestal in een zogenaamd "change log" worden omschreven. In het geval dat een software update zodanig kort voor de inzet van een technisch hulpmiddel plaatsvindt dat geen herkeuring heeft kunnen plaatsvinden, biedt het besluit de mogelijkheid van herkeuring achteraf (vierde lid).
Van het uitgangspunt van een voorafgaande keuring kan worden afgeweken indien een dringend onderzoeksbelang daartoe noodzaakt. Deze uitzondering is geregeld in artikel 15. Hierbij kan worden gedacht aan de situatie dat 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 nagaan of het beoogde technische hulpmiddel naar verwachting zal voldoen aan de in de artikel 8 tot en met 13 gestelde technische eisen. In het bevel van de officier van justitie wordt expliciet vermeld dat een niet gekeurd technisch hulpmiddel wordt ingezet (tweede lid).
Als hoofdregel geldt dat een technisch hulpmiddel dat niet vooraf is goedgekeurd, na afloop van de inzet alsnog ter keuring aan de keuringsdienst wordt aangeboden (derde lid). Indien naar het oordeel van de officier van justitie de aard van een technisch hulpmiddel zich tegen keuring achteraf verzet, kan hij bepalen dat een technisch hulpmiddel niet ter keuring wordt aangeboden. 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. Indien de officier van justitie besluit om, gelet op de aard van het technische hulpmiddel, keuring achteraf achterwege te laten, dient hij de noodzakelijke procedurele maatregelen te treffen om rechterlijke controle op de inzet mogelijk te maken. Hierbij kan worden gedacht aan een uitgebreide omschrijving van de functionele specificaties van het op maat gemaakte technische hulpmiddel in het proces-verbaal, het vooraf en achteraf maken van een forensische kopie of het audiovisueel vastleggen van het onderzoeksproces. Daarnaast kunnen een digitale kopie van de software en de broncode bij het proces-verbaal worden gevoegd. 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 gegenereerde gegevens. Ook onderzoekshandelingen die zonder gekeurd technisch hulpmiddel worden verricht worden gelogd, evenals het functioneren van de technische infrastructuur. In geval van twijfel kan zo nodig via de logging verantwoording worden afgelegd over de verrichte handelingen en het vergaarde bewijsmateriaal.

Artikelen 16 tot en met 19 Keuringsdienst, keuringsprotocol, keuringsrapport
In de artikelen 16 tot en met 19 van dit besluit wordt de keuringsprocedure omschreven. Artikel 16 stelt regels over de aanwijzing van keuringsdiensten. De keuring van technische hulpmiddelen zal primair worden opgedragen aan een onderdeel van de Landelijke eenheid, thans de keuringsdienst van de Dienst Landelijke Operationele Samenwerking (eerste lid). De keuringsdienst dient een onafhankelijk en objectief oordeel te geven over de ter keuring aangeboden technische hulpmiddelen. Dit dient ook tot uitdrukking te komen in de plaatsing van de keuringsdienst binnen de politieorganisatie. Bij ministeriële regeling kunnen regels worden

gesteld over de aanwijzing van de keuringdienst van de Landelijke eenheid (derde lid).
De mogelijkheid bestaat om een andere organisatie aan te wijzen als keuringsdienst (tweede lid). Als van deze mogelijkheid gebruik wordt gemaakt worden hierover bij ministeriële regeling regels gesteld (vierde lid). Afhankelijk van de gekozen systematiek kan sprake zijn van een dienst van algemeen economisch belang of een niet-economische dienst van algemeen belang. Bij het opstellen van de ministeriële regeling zal toetsing aan de geldende EU-kaders plaatsvinden.
De keuring van technische hulpmiddelen wordt uitgevoerd op basis van een keuringsprotocol waarin de wijze waarop de keuring plaatsvindt wordt vastgelegd (artikel 17). Daarnaast kunnen in het keuringsprotocol de criteria worden opgenomen die bij de keuring worden gehanteerd. Het keuringsprotocol wordt in samenspraak tussen de keuringsdienst en het openbaar ministerie opgesteld. Een keuringsprotocol behoeft voorafgaande goedkeuring van de Minister van Veiligheid en Justitie. Het is niet wenselijk dat de keuringsdiensten bij keuring van soortgelijke technische hulpmiddelen verschillende keuringsprotocollen hanteren. Indien andere keuringsdiensten worden aangewezen, zal de keuringsdienst van de Landelijke eenheid een coördinerende rol worden toebedeeld bij het opstellen en het gebruik van keuringsprotocollen. De keuring is gericht op die onderdelen van het technische hulpmiddel die van belang zijn voor de detectie, registratie en het transport van gegevens naar een technische infrastructuur. Om de consistentie en de kwaliteit van de keuring te waarborgen wordt de keuring uitgevoerd op basis van voornoemd keuringsprotocol.
Artikel 18, eerste lid, bepaalt dat de korpschef een technisch hulpmiddel ter keuring kan aanbieden bij een keuringsdienst. Van de keuring wordt een rapport opgemaakt, waarin de bevindingen van de keuringsdienst worden vastgelegd (tweede lid). De keuring vindt proefondervindelijk plaats. Bij goedkeuring van een technisch hulpmiddel wordt vermeld dat het hulpmiddel voldoet aan de in de artikelen 8 tot en met 13 vermelde eisen (derde lid, onderdeel a). In het keuringsrapport wordt aan een technisch hulpmiddel een uniek keuringsnummer toegekend (derde lid, onderdeel b). In de processen-verbaal die gedurende het opsporingsonderzoek worden opgesteld kan naar dit keuringsnummer worden verwezen. Op deze wijze kan het gebruik van het middel afgeschermd worden ter bescherming van opsporingsbelangen, terwijl de rechter en de verdediging de zekerheid hebben dat het ingezette technische hulpmiddel voldoet aan de wettelijke eisen. Het keuringsrapport bevat verder een omschrijving van de werking van een technisch hulpmiddel en een aanduiding van de functionaliteit of functionaliteiten van het hulpmiddel (derde lid, onderdelen c en d). Bij het opstellen van het rapport haalbaarheidsonderzoek ter advisering van de officier van justitie kan het technische team zich hierop baseren.
In het derde lid, onderdeel e, wordt de mogelijkheid gecreëerd om te voldoen aan een of meer in het besluit gestelde technische eisen via het stellen van procedurele waarborgen bij de keuring. De huidige keuringspraktijk heeft uitgewezen dat hieraan behoefte bestaat. Een voorbeeld betreft het ontbreken van een technisch geborgde datum/tijd functie. Dat kan worden opgelost door in een keuringsrapport verplichte procedurele waarborgen te stellen, waardoor materieel aan de technische eisen kan worden voldaan. In de processen-verbaal over de opsporingshandelingen kan hierover verantwoording worden afgelegd. In het keuringsrapport wordt ook melding gemaakt van relevante informatie met betrekking tot de werking van een functionaliteit of functionaliteiten van een technisch hulpmiddel, zoals relevante informatie ten behoeve van de plaatsing, inzet of verwijdering van het technische hulpmiddel (derde lid, onderdeel f).
Het rapport van een keuringsdienst bevat de periode waarvoor de keuring geldt zolang de werking hiervan ongewijzigd is (derde lid, onderdeel g). Indien de werking van een technisch hulpmiddel of een onderdeel hiervan zodanig wijzigt dat niet meer voldaan wordt aan de in dit besluit gestelde technische eisen, dient herkeuring plaats te vinden (artikel 14, tweede lid). Na afloop van de in het keuringsrapport genoemde periode kan de keuringsdienst besluiten het technische hulpmiddel opnieuw te keuren of de periode waarvoor de keuring geldt te verlengen.
In artikel 19 wordt geregeld dat de keuringsdienst van de Landelijke eenheid een centrale registratie bijhoudt van de eigen keuringsrapporten en, indien aanwezig, van de keuringsrapporten van andere keuringsdiensten.

Artikel 20 Wederzijdse erkenning
Het beginsel van vrij verkeer van goederen en diensten binnen de Europese Unie brengt met zich

dat lidstaten in de nationale wetgeving geen eisen aan goederen en keuringen mogen stellen die leiden tot beperking van het vrije verkeer tussen de lidstaten. De technische eisen die het besluit stelt aan technische hulpmiddelen en de door het besluit voorgeschreven keuring van technische hulpmiddelen kunnen worden opgevat als een inbreuk op het vrije verkeer. Daarom is in dit artikel een wederzijdse erkenningsclausule opgenomen voor goederen en keuringen.

Hoofdstuk 7 Toegang tot en plaatsing van een technisch hulpmiddel

Artikelen 21 en 22 Toegang en plaatsing van een technisch hulpmiddel
Artikel 21 bepaalt dat de toegang tot technische hulpmiddelen centraal wordt geregistreerd. De korpschef wijst één of meer ambtenaren aan die met de registratie zijn belast. Na vertoon van het bevel van de officier van justitie met daarin een aanduiding van de aard en functionaliteit van het technische hulpmiddel verschaft een met registratie belaste ambtenaar toegang tot een technisch hulpmiddel ten behoeve van de plaatsing ervan. De toegang tot een technisch hulpmiddel wordt verleend voor de periode die nodig is voor de uitvoering van het bevel.
De plaatsing van een technisch hulpmiddel vindt plaats door een opsporingsambtenaar van een technisch team (artikel 22). Dit kan een op grond van de artikelen 3 of 4 van dit besluit aangewezen lid van of deelnemer aan een technisch team zijn.
Het technisch team zal in de praktijk eerst een voorverkenning opstellen. Na analyse daarvan wordt een plan van aanpak voor het binnendringen opgesteld dat wordt getest in een proefopstelling. Nadat is binnengedrongen in het geautomatiseerde werk wordt het technische hulpmiddel geplaatst. Het tweede lid vereist dat bij de plaatsing van een technisch hulpmiddel uitsluitend de in het bevel van de officier van justitie aangeduide functionaliteiten worden ingeschakeld. Hierover dient verantwoording te worden afgelegd in een proces-verbaal. Bij de plaatsing kan het technische hulpmiddel van een uniek gegeven worden voorzien, waarmee de relatie tussen het geplaatste technische hulpmiddel en de met het hulpmiddel vastgelegde gegevens op een technische infrastructuur kan worden aangetoond. De Inspectie VenJ en houdt toezicht op de naleving van de toegang- en plaatsingprocedures en de vereiste autorisaties.

Hoofdstuk 8 Inzet van een technisch hulpmiddel

Artikelen 23 tot en met 27 Inzet van een technisch hulpmiddel en vastlegging van gegevens op een technische infrastructuur
In artikel 23 wordt geregeld dat de inzet van een technisch hulpmiddel plaatsvindt door een opsporingsambtenaar van een technisch team. Van de inzet wordt proces-verbaal opgemaakt. Tijdens de inzet kunnen afhankelijk van de ingeschakelde functionaliteit(en) verschillende soorten gegevens worden geregistreerd. De vastlegging van de geregistreerde gegevens vindt plaats op een technische infrastructuur. Dit betreft een technische voorziening van een technisch team, die is bedoeld voor de vastlegging van de met een technisch hulpmiddel geregistreerde gegevens (artikel 24). Om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te borgen stelt het besluit eisen aan de inrichting van de technische infrastructuur waarop de gegevens worden vastgelegd (artikelen 25 tot en met 27 van het besluit). De gegevens mogen niet inhoudelijk worden bewerkt en dienen te worden beveiligd tegen wijziging en kennisneming hiervan door onbevoegden (artikel 25). De vastgelegde gegevens zijn uitsluitend toegankelijk voor de door de korpschef aangewezen ambtenaren. Tactische opsporingsambtenaren hebben geen toegang. De technische infrastructuur moet in staat zijn om het unieke gegeven dat door het technische hulpmiddel aan de geregistreerde gegevens is toegevoegd te herkennen (artikel 26). Zo kan de herkomst van de vastgelegde gegevens worden vastgesteld.
Bij de vastlegging van gegevens op de technische infrastructuur worden de datum en tijd geregistreerd (artikel 27). Hierdoor bestaat zekerheid over de datum en het tijdstip van de vastlegging. Het kan voorkomen dat de datum en tijd in de technische infrastructuur van de politie afwijken van de ingestelde datum en tijd van het te onderzoeken geautomatiseerd werk. Een technisch team heeft geen invloed op de datum en tijd die een verdachte heeft ingesteld in zijn computer of smartphone. Na overlegging van de onderzoeksresultaten door het technische team aan het tactische team kan het tactische team het tijdsverloop reconstrueren.
Via de logging kan controle worden uitgeoefend op de verrichte onderzoekshandelingen en het

functioneren van de technische infrastructuur. Zowel tijdens de uitvoering van een bevel als achteraf moet kunnen worden vastgesteld of wijziging dan wel onbevoegde kennisneming van de ter uitvoering van een bevel vastgelegde gegevens heeft plaatsgevonden. Indien een onregelmatigheid wordt vastgesteld die van invloed is op de kwaliteit van de met een technisch hulpmiddel geregistreerde gegevens dient hiervan proces-verbaal te worden opgemaakt door een opsporingsambtenaar van een technisch team. Dit proces-verbaal wordt aan de officier van justitie gezonden (artikel 6). De Inspectie VenJ houdt toezicht op de naleving van de regels en procedures omtrent de inzet van een technisch hulpmiddel en de vastlegging van gegevens op een beveiligde technische infrastructuur.

Hoofdstuk 9 Verwijdering van een technisch hulpmiddel

Artikelen 28 en 29 Verwijdering van een technisch hulpmiddel, beëindiging transport gegevens
Hoofdregel is dat een technisch hulpmiddel wordt verwijderd uit het te onderzoeken geautomatiseerde werk, nadat het onderzoeksdoel is bereikt of de periode waarvoor het bevel is afgegeven is verstreken (artikel 28). De verwijdering geschiedt door een opsporingsambtenaar van een technisch team. Sommige softwareapplicaties bieden de functionaliteit van een zelfstandige vernietiging van de software na verloop van een bepaalde, vooraf ingestelde, periode.
Vanuit de opsporing bestaat belang bij de verwijdering: bij voorkeur dient te worden voorkomen te dat het gebruik van het technische hulpmiddel bekend wordt. Niettemin kan het voorkomen dat een technisch hulpmiddel niet verwijderd kan worden, bijvoorbeeld omdat voor verwijdering soms meer beheerrechten nodig zijn dan voor de plaatsing. Als het hulpmiddel niet verwijderd kan worden, dan dient het transport van de gegevens te worden beëindigd. Dit wordt geregeld in artikel 29. Van de verwijdering van het technisch hulpmiddel dan wel het stopzetten van het transport van de gegevens wordt proces-verbaal opgemaakt, dat aan de officier van justitie wordt gezonden. Op basis van de logging kan worden gecontroleerd of de ontvangst van gegevens op de technische infrastructuur daadwerkelijk is beëindigd.
Indien de niet of niet volledige verwijdering van een technisch hulpmiddel risico's oplevert voor het onderzochte geautomatiseerde werk stelt het technisch team de officier van justitie hiervan in kennis en stelt het informatie beschikbaar ten behoeve van de volledige verwijdering. De officier van justitie stelt de beheerder van het geautomatiseerde werk daarvan in kennis.
De Inspectie VenJ houdt toezicht op de naleving op de juiste uitvoering van de verwijderingsprocedure.

Hoofdstuk 10 Wijziging overige wet- en regelgeving

Artikel 30 Wijziging Besluit politiegegevens
Artikel 30 strekt tot wijziging van artikel 4:3, eerste lid, van het Besluit politiegegevens. In de Wpg is geregeld dat de politie persoonsgegevens aan derden kan verstrekken met het oog op een zwaarwegend algemeen belang (artikel 18, eerste lid, Wpg). De personen en instanties aan wie, evenals de taak ten behoeve waarvan de politiegegevens worden verstrekt, worden aangewezen bij of krachtens algemene maatregel van bestuur. Dit is uitgewerkt in het Besluit politiegegevens. Om de verhouding tussen de taakuitoefening door de Inspectie VenJ en het verstrekkingenregime van de Wpg te verhelderen wordt artikel 4:3 van het Besluit politiegegevens aangepast en wordt de verplichting tot verstrekking van politiegegevens die worden verwerkt op grond van de artikelen 8, 9, 10 en 13 van de Wpg, ten behoeve van de toezichthoudende taak van de Inspectie VenJ expliciet vastgelegd.
De toezichthoudende taak van de Inspectie VenJ betreft het toezicht op de taakuitvoering door de politie (artikel 57, eerste lid, onderdeel d, Wet veiligheidsregio's) alsmede het onderzoek in een geautomatiseerd werk dat wordt gedaan door de opsporingsambtenaren van de bijzondere opsporingsdiensten en de buitengewone opsporingsambtenaren (artikel 126nba, zevende lid, Sv). De verplichting om gegevens te verstrekken met het oog op de uitvoering van de taken van de Inspectie VenJ omvat de politiegegevens die worden verwerkt ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval en de gegevens die worden verwerkt met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (artikelen 9, eerste lid, en 10, eerste lid, onderdelen a en

c, Wpg). Het gaat hier om zachte gegevens, die binnen de politie worden verwerkt door onder meer de criminele inlichtingeneenheden en de regionale inlichtingendiensten.

Hoofdstuk 11 Inwerkingtreding

Artikelen 31 en 32 Citeertitel en inwerkingtreding
Dit besluit heeft als citeertitel "Besluit onderzoek in een geautomatiseerd werk" en treedt tegelijk in werking met het wetsvoorstel computercriminaliteit III. De datum van inwerkingtreding wordt bepaald op **PM.**

De Staatssecretaris van Veiligheid en Justitie,

Van: Plas, Theo van der (T.G.)
Verzonden: woensdag 10 mei 2017 00:27
Aan: 10.2.e politie.nl>;10.2.e @klpd.politie.nl>;10.2.e @politie.nl>;10.2.e @politie.nl>
Onderwerp: onderzoek politieacaedmie CC 3

Hallo 10.2.e

Via10.2.e die je daarover de documentatie hebt toegestuurd, begreep ik dat CC 3 in een onderzoeksvoorstel van de politieacademie staat opgenomen. Met als opdrachtgever10.2.e .
Ik kan me niet herinneren dat we hierover eerder hebben gesproken en even snel de stukken scannend vind ik het 12-14
Ik weet ook niet of dit in de stuurgroep aan de orde is geweest? Wat zijn de overwegingen geweest om hier in te stappen ?
Wil je dit – gelet op de rollen –bespreken met Marjolein, voorzover dat al niet gedaan is, zodat we kunnen afwegen welke reactie hierbij passend is ?

Alvast bedankt,

drs. T.G. (Theo) van der Plas EMPM
Programmadirecteur Digitalisering en Cybercrime
Nieuwe Uitleg 1, 2514 BP Den Haag
Postbus 17107, 2502 CC Den Haag
M (06)10.2.e
E-mail:10.2.e @politie.nl

Van: Plas, Theo van der (T.G.)
Verzonden: woensdag 10 mei 2017 00:41
Aan: 10.2.e @politie.nl>
CC: 10.2.e @politie.nl>;10.2.e @klpd.politie.nl>; 10.2.e @politie.nl>
Onderwerp: RE: Hoofdlijnennotitie CCIII BOO 12 mei 2017.pptx

Ha 10.2.e veel te veel tekst op de dia's; moet terug worden gebracht naar de essentie met paar kernwoorden. De rest konden of kunnen ze teruglezen in het document.
En nog even goed kijken naar de besluiten. 12-14

drs. T.G. (Theo) van der Plas EMPM
Programmadirecteur Digitalisering en Cybercrime
Nieuwe Uitleg 1, 2514 BP Den Haag
Postbus 17107, 2502 CC Den Haag

Van: Smit-Arnold Bik, Marjolein (C.P.M.)
Verzonden: woensdag 10 mei 2017 08:09
Aan: Plas, Theo van der (T.G.); 10.2.e 10.2.e 10.2.e
Onderwerp: RE: onderzoek politieacaedmie CC 3

Beste allemaal,

Het zegt mij ook niks, ik heb ik dit kader nog nooit met 10.2.e gesproken en ik stel ook voor dat als hij betrokken moet zijn dat via de begeleidingscommissie en de portefeuillehouder gaat. Theo, pak jij dit verder op of moet ik iets doen?

Groeten,

Marjolein

Van: 10.2.e @politie.nl>
Datum: 10 mei 2017 13:33:14 CEST
Aan: Plas, Theo van der (T.G.) 10.2.e @politie.nl>
CC: 10.2.e @politie.nl>, 10.2.e @klpd.politie.nl>10.2.e @politie.nl>
Onderwerp: RE: Hoofdlijnennotitie CCIII BOO 12 mei 2017.pptx

Hoi Theo,

Nieuwe versie.

Groet,

10.2.e

Van: DIVKNP
Verzonden op: donderdag 11 mei 2017 13:35
Aan: Post TJZ
CC: 10.2.e [KNP] (K)"
Onderwerp: Ontwerp besluit 2017-0021103

Beste collega,

Bijgevoegd poststuk is gedigitaliseerd en geregistreerd onder kenmerk 2017-0021103
Met jullie medewerking vormen wij goed geordende en toegankelijke dossiers. Het is daarom van groot belang dat vervolgcorrespondentie wordt voorzien van bovengenoemd kenmerk.
Deze vervolgcorrespondentie bij digitale verzending versturen met 10.2.e @knp.politie.nl in CC en bij fysieke verzending de poststukken getekend en voorzien van kenmerk aanleveren bij team DIV.

Vragen? Neem contact met ons op.
06-10.2.e

10.2.e @knp.politie.nl
Met vriendelijke groet,
Team DIV/Staf KL

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Van: 10.2.e [KNP] (K)
Verzonden: donderdag 11 mei 2017 14:59
Aan: 10.2.e
Onderwerp: Fwd: Ontwerp besluit 2017-0021103
Bijlagen: Scan_11-05-2017_13-24-22.pdf

Ter behandeling

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Bijlage is gelijk aan doc. 650 (pag 391)

Van: Plas, Theo van der (T.G.)
Verzonden: donderdag 11 mei 2017 19:48
Aan: 10.2.e @politie.nl>
CC: 10.2.e @klpd.politie.nl>;10.2.e @politie.nl>; 10.2.e @politie.nl>
Onderwerp: RE: Hoofdlijnennotitie CCIII BOO 12 mei 2017.pptx

Ok, thanks, denk dat we het zo wel gaan redden; gaat om de discussie beetje te geleiden. Vanavond nog even de notitie lezen. En dan gaan we er voor.

Groeten, Theo

Met vriendelijke groet,

Drs. Theo G. van der Plas EMPM
Programmadirecteur Digitalisering & Cybercrime
Nieuwe Uitleg 1, 2514 BP Den Haag
Postbus 17107, 2502 CC Den Haag

Van: 10.2.e
Verzonden: donderdag 11 mei 2017 20:30
Aan: Plas, Theo van der (T.G.)
CC: 10.2.e 10.2.e 10.2.e
Onderwerp: RE: Hoofdlijnennotitie CCIII BOO 12 mei 2017.pptx
Bijlagen: Hoofdlijnennotitie CCIII BOO 12 mei 2017.pptx

Hoi Theo,

Kleine aanpassing gedaan ivm verschijnen besluit gisteren. Zo is alles weer actueel. Ik ben er morgen rond 9.45 uur.
Ik zal zorgen dat ik de presentatie ook op stick bij mij heb. Ik stuur hem in ieder geval even naar de secretaris van het BOO.

Ik zie je in Utrecht.

Groet,

10.2.e
PS 1 Klinkt goed!
PS 2 Klinkt ook goed!

Hoofdlijnennotitie CCIII

BOO 12 mei 2017

«waakzaam en dienstbaar»

Update politiek/wetgeving

- Voorlopig verslag EK - 3 april
- Antwoord MVenJ – uiterlijk 15 mei
- Deskundigenbijeenkomst EK - 20 juni
- Besluit formele consultatie – 10 mei (7 juli reactie)

Update notitie

- Besproken 10.2.e , 10.2.e en Theo
- Met name HRM-component
- 2 scenario’s
- BOO → BBVO → KMTO
- KMTO in juni?

Uitgangspunten notitie

- Focus op “binnendringen”
- Twee fases, experimenteren en implementeren
- Centraal (gezamenlijk) inrichten

Scenario's

1. LE wer[7-12] fte. Afroming eenheden formatieruimte v[7-12] fte.
2. LE wer[7-12] fte. Eenheden lever[7-12] fte op basis van TTW voor 2 jaar.

Besluiten

1. Sectorhoofd DLOS krijgt opdracht implementatie.
2. Starten met centrale werving
3. Opstarten wervingscampagne.

Vragen

Ruimte voor discussie

Van: 10.2.e **Namens** 10.2.e
Verzonden: woensdag 17 mei 2017 15:16
Aan: Plas, Theo van der (T.G.)10.2.e @politie.nl>
CC: 10.2.e @politie.nl>; 10.2.e @politie.nl>
Onderwerp: Verslag BOO 12/5: Hoofdlijnennotitie CCIII
Urgentie: Hoog

Hoi Theo,

Zoals afgelopen vrijdag afgesproken, stuur ik je hierbij de concepttekst uit het verslag van het BOO van afgelopen vrijdag.
Graag jouw reactie en eventuele aanvullingen hierop.

De heren Van der Plas en10.2.e sluiten aan om dit agendapunt toe te lichten. De achtergrond en komende tijdlijn
wordt benoemd. Het HRM-component ligt vandaag voor. Gevraagd wordt een keuze te maken tussen 2 scenario's:
1. de Landelijke Eenheid wer7-12 fte voor de centrale voorziening. Vanuit de eenheden wordt daarnaast formatieruimte ter grootte v7-12 fte afgeroomd ten behoeve van de Landelijke Eenheid;
2. de Landelijke Eenheid wer7-12 fte voor de centrale voorziening. Vanuit de eenheden wordt daarnaast in tota7-12 fte door een gekwalificeerde medewerker tewerkgesteld bij de voorziening.
Er wordt kort gediscussieerd over de keuze voor de7-12 fte, de vraag of er formatieruimte is geclaimd per wet en de scenario's.
Het BOO is het eens met hetgeen voorligt, maar heeft er geen vertrouwen in dat deze mensen daadwerkelijk terug keren naar de eenheden. Daarvoor moet een goede visie worden ontwikkeld. We willen met elkaar naar een duurzame kennis ontwikkeling binnen de eenheden.
Na de zomer ziet het BOO deze koers graag terug op de agenda.
Actie: dhr. v.d. Plas

Daarnaast wordt aandacht gevraagd voor de werving van het personeel. Een helder profiel voor de medewerker is belangrijk. Geadviseerd wordt 7-12 hierin mee te nemen.

Afgesproken wordt het onderwerp Cyber ieder kwartaal te agenderen voor het BOO. Op deze manier kan het BOO aangehaakt blijven bij de ontwikkelingen op dit gebied, zoals de ervaringen van de cyberteams welke al in werking zijn.
Actie: dhr. v.d. Plas / secretaris BOO

Met vriendelijke groet,

10.2.e
Adviseur 9
Politie I Korpsstaf I Afdeling Bestuursondersteuning I Team Bestuurszaken
Nieuwe Uitleg 1, 2514 BP Den Haag
Postbus 17107 I 2502 CC Den Haag

Van: 10.2.e
Verzonden: woensdag 17 mei 2017 15:29
Aan: Plas, Theo van der (T.G.); 10.2.e
CC: 10.2.e
Onderwerp: Tweede Kamer vragenuur

Ter info uit het vragenuur van gisteren.
Gr
10.2.e

Verzonden van mijn Samsung

Vragen Van Toorenburg
Vragen van het lid Van Toorenburg aan de staatssecretaris van Veiligheid en Justitie over **het bericht "Massale wereldwijde cyberaanval"**.

Mevrouw **Van Toorenburg** (CDA):
Voorzitter. Vanmorgen reed ik de parkeerplaats van Q-Park op. Zonder dat ik mijn abonnement hoefde te laten zien, ging de slagboom open. Dat is winst, dacht ik. Het was er wel voller dan normaal. Meerdere mensen zullen vanmorgen hebben ervaren dat Q-Park openstond.

Ik dacht: laat ik een keertje luchtig beginnen, want zo kent u mij niet. Maar die luchtigheid kan ik wel meteen achter me laten, want we hebben hier een serieus probleem bij de kop. Afgelopen vrijdag werden we opgeschrikt door een weergaloze aanval van gijzelingssoftware, die talloze computers en organisaties infecteerde in ruim 150 landen. En het was ontwrichtend, zeker in Groot-Brittannië, waar de ziekenhuizen het slachtoffer werden. Maar ook andere landen en bedrijven zijn getroffen.

Nou lijkt de schade in Nederland mee te vallen. Dat is goed nieuws, maar het neemt de zorgen niet weg. Het zou namelijk heel goed kunnen dat men ons simpelweg niet op de korrel nam. De vraag is dus allereerst: is Nederland voldoende beveiligd? En zijn we voldoende scherp of lopen we nog steeds serieuze risico's? Als we mevrouw Zorko, een soort directeur veiligheid in Nederland, kunnen geloven, dan is het allemaal goed op orde. Ze doet zelfs een beetje luchtig. Want als een bedrijf zijn software niet al op orde had, dan heeft het daar nou wel voor gezorgd, zegt ze. Maar volgens het rapport dat we vandaag hebben ontvangen, moeten we serieus aan de bak. Er zijn plannen genoeg, maar de middelen ontbreken. Zo vat ik het rapport maar even samen. Ik krijg daarop graag een reactie van de staatssecretaris.

Er is ook een gebrek aan sturing, aldus het rapport. Zorko zegt: dat is juist goed; we polderen ons de goede kant op. Ik ben benieuwd naar de reactie van de staatssecretaris hierop. Ook de informatie-uitwisseling tussen publiek en privaat schiet tekort, en er is te weinig deskundigheid. Kortom, er is sprake van grote dreigingen en grote zorgen. Wat heeft de staatssecretaris daarop te zeggen?

Staatssecretaris **Dijkhoff**:
Voorzitter. Mevrouw Van Toorenburg wijst er terecht op dat de schade in andere landen groter is. Zij stelt ook terecht de vraag: is dat omdat wij geluk hadden of omdat we zo veel beter zijn? Als de schade zich had voorgedaan in landen waar de cybersecurity op een laag niveau lag, dan zou je nog kunnen zeggen dat wij onze beveiliging beter op orde hebben. Maar bij de landen die zwaar geraakt zijn, zitten ook medekoplopers van Nederland op het gebied van cybersecurity. Ik denk dus inderdaad dat het ook met toeval te maken heeft. Het hangt af van wie er als eersten worden getarget en welke systemen zo in elkaar

zitten dat het als een worm van het ene naar het andere door kan kruipen. In deze situatie is gebruik of misbruik gemaakt van een kwetsbaarheid in systemen die al langer bekend was, waarvoor ons NCSC in maart en april al gewaarschuwd was en waar ook al een patch voor was. Als mevrouw Van Toorenburg vraagt of Nederland voldoende beveiligd is, zou ik dus bijna willen zeggen: kennelijk niet. Er was immers sprake van een kwetsbaarheid die we kenden en die we ook konden repareren, maar niet iedereen die verantwoordelijk is voor cybersecurity in zijn of haar organisatie heeft die update gedraaid. Als die update is gedraaid of dat SMB-protocol is uitgezet, dan kom je niet binnen. Die bewustwording is nog niet ver genoeg gevorderd. We lopen daarin nog risico's. Het gaat om netwerken, dus de zwakste schakel kan een ingang zijn tot cruciale systemen. Dit bewijst maar weer dat de scherpte nog beter moet worden. Het is nooit af. Je kunt niet zeggen: ik heb nu updates gedraaid en ik kan nu weer een jaar vooruit. Je moet blijven opletten.

Ik denk dat de doorlichting die we hebben laten doen, accuraat is. Je kunt het op allerlei manieren bekijken, maar de doorlichting laat zien dat er nog heel veel te doen is, ook voor Nederland. Ten opzichte van andere landen kunnen we ook trots zijn, maar het probleem groeit sneller dan wij kunnen bijbenen. Het rapport geeft ook aan dat we het in Nederland heel knap doen met de middelen die we wel hebben. Ik zou bijna zeggen: als je erin investeert, zoals we bij de vorige begroting ook een stap hebben gezet, weet je in elk geval dat het geld goed besteed zal worden en dat ze er goed mee overweg kunnen. Ik denk dat ik door de spreektijd voor de eerste reactie heen ben.

Mevrouw **Van Toorenburg** (CDA):
We geven de staatssecretaris ruim de tijd voor zijn tweede reactie. Ik wil wel een aantal punten uitlichten. Kijk bijvoorbeeld naar de ziekenhuizen. Daar blijken we nog een heel serieuze slag te moeten maken. In Engeland zijn juist de ziekenhuizen heftig getroffen. We hebben daar begin dit jaar al een alarmerend bericht over gekregen. De minister van VWS heeft gezegd: inderdaad moeten we hier de komende vier jaar nog van alles doen. Serieus, voorzitter, de minister zei "de komende vier jaar". Ik denk dat we ons dat niet kunnen permitteren. Ik krijg daarop graag een reactie van de staatssecretaris.

Ik wil ook graag weten wat de stand van zaken is ten aanzien van het computer emergency response team voor de zorg, dat hiermee bezig zou zijn.

We weten dat 75% van de gemeenten te maken heeft gehad met datalekken. Ze zouden een aantal zaken op orde hebben gebracht. Ons is geworden dat dit nog niet is gebeurd. Sterker nog, ik kreeg vanmorgen nog het bericht dat er ambtenaren zijn die op verre afstand sluizen en bruggen bedienen met een digitale infrastructuur die niet meer is dan houtje-touwtje. Ik denk dat dit nu de belangrijkste punten zijn om aan te kaarten: gemeenten, ambtenaren en ziekenhuizen.

Ik wil er nog één ding bij halen. De staatssecretaris zegt terecht dat er wel wordt gekeken naar de mogelijkheden om het te verbeteren. Maar ik begrijp dat we nog niet eens scherp hebben wat daadwerkelijk onze vitale infrastructuur is. Ik begrijp dat ziekenhuizen er soms wel en soms niet toe behoren: academische ziekenhuizen wel en andere ziekenhuizen niet. Ook daarvan zouden we met elkaar moeten weten waar onze zwakke plekken zitten en wat we eraan doen als er een grote crisis is die Nederland raakt.

Staatssecretaris **Dijkhoff**:
Het liefste zou je zeggen: we wijzen één iemand aan in Nederland die ervoor zorgt dat alles veilig is. Maar zo werkt het dus niet. In die zin snap ik de opmerking van mevrouw Zorko over het polderen wel. Iedereen moet uiteindelijk zelf zijn zaken op orde hebben. Als een organisatie cruciaal is voor onze samenleving, moeten wij als overheid hogere eisen stellen aan die organisatie, zodat zij dat zelf doet.

Als het gaat om ziekenhuizen en vitale infrastructuur, is het juist nu cruciaal dat we die duidelijkheid bieden in de implementatie van de Netwerk- en informatiebeveiligingsrichtlijn. Daar zijn wij ook flink mee bezig. Binnenkort gaat de implementatie van de richtlijn in consultatie. Ook op andere terreinen, zoals de gegevensverwerking en de meldplicht cybersecurity zijn wij, vooruitlopend op Europese regelgeving, aan de slag gegaan. Deze Kamer heeft dat al behandeld; het ligt nu in de senaat. Wij zouden er graag verder mee gaan.

Wij sturen op de verantwoordelijkheden die iedereen heeft, maar uiteindelijk moet iedereen zijn eigen zaak op orde hebben. Er is echt nog veel te doen. Laat afgelopen weekend een wake-upcall zijn voor iedereen om de eigen verantwoordelijkheid hierin te nemen. Als je dat niet doet, kan ook een ander daar flink last van hebben.

Mevrouw **Van Toorenburg** (CDA):
Dan toch nog even over die ziekenhuizen. Voorlopig hebben ze nog steeds vier jaar om het op orde te krijgen. Ik denk dat dat onbestaanbaar is. Daar wil ik graag een concrete reactie op, is het niet hier, dan via de minister. Die datalekken bij de gemeenten zijn er nog steeds. Er is vier jaar geleden gesproken over mogelijke wetgeving om hier dwingender in te zijn. Wanneer is het moment om dat te doen? Kortom, ik begrijp dat er van alles gebeurt, maar ik heb nog niet helemaal helder wat wij daadwerkelijk gaan doen als er een grote crisis is.

Staatssecretaris **Dijkhoff**:
Al die maatregelen waar mevrouw Van Toorenburg terecht naar vraagt, zijn vooral bedoeld om zo'n crisis te voorkomen, om die kwetsbaarheden te verminderen. Als er zo'n crisis is, zie ik dat in Nederland alle schotten verdwijnen en dat iedereen heel hard op zoek gaat naar een oplossing, publiek en privaat bij elkaar. Ik zal mijn collega van VWS vragen of zij u kan informeren over de stand van zaken. Ik heb begrepen dat zij ook hierin aanleiding ziet om het belang van informatiebeveiliging in haar sector nogmaals onder de aandacht te brengen en daarbij tot spoed te manen.

Het is goed dat wij met die meldplicht die datalekken bij gemeenten naar boven krijgen. Zo zien wij hoe groot het probleem is en kunnen wij er gericht aan werken. Ze zijn niet allemaal hoogtechnologisch, het zijn ook weleens verkeerd meegestuurde bestanden. Als je merkt dat je een lek hebt gehad, moet je het repareren en daarna in overtreffende trap dwingen tot dichten van de gaten.

De heer **Verhoeven** (D66):
Het is natuurlijk wel saillant dat een partij als het CDA, die warm voorstander was van het openlaten van kwetsbaarheden in het internet voor het gebruik door inlichtingendiensten, nu vragen stelt over deze wereldwijde cyberaanval, zonder daar ook maar met één woord over te spreken. Daar wil ik graag nog een vraag over stellen.

We kunnen het hebben over veiligheid en investeren — dat is allemaal hartstikke goed — maar het gaat hier natuurlijk over de fundamentele keuze of wij kwetsbaarheden in het internet openlaten om ze te laten gebruiken door inlichtingendiensten, zodat die daarmee verdachten kunnen hacken. De NSA is hackingtools kwijtgeraakt aan criminelen. Deze aanval heeft laten zien dat dat heel gevaarlijk is. D66 heeft hier in de afgelopen maanden bij wetgeving die hierover ging herhaaldelijk op gewezen. Ik ben heel benieuwd of het kabinet tot inkeer komt en ziet dat dit serieuze risico's met zich meebrengt. De CTIVD heeft geadviseerd om duidelijk beleid te voeren voor het gebruik van kwetsbaarheden en er niet elke keer aan voorbij te gaan dat dat een reëel risico is. Zal het kabinet dat advies opvolgen?

De **voorzitter**:
Voordat ik de staatssecretaris het woord geef, zie ik dat mevrouw Van Toorenburg kort wil reageren op de

opmerking van de heer Verhoeven over het CDA. Het telt dus niet als een vraag en mevrouw Van Toorenburg mag dus ook geen vraag stellen.

Mevrouw **Van Toorenburg** (CDA):
Ik zou eigenlijk alleen maar willen zeggen dat het een beetje sneu is dat de heer Verhoeven dit doet. Ik denk dat hij zich vreselijk gepasseerd voelt dat hij de vraag niet eerder heeft kunnen stellen. Ik denk dat hij daarom zo uithaalt. Laat het een compliment zijn dat wij die wetten hebben behandeld en dat ze in de Eerste Kamer liggen. Laat de Eerste Kamer ze gauw behandelen!

Staatssecretaris **Dijkhoff**:
De heer Verhoeven snijdt wat bochten af in zijn vraagstelling. Het kabinet heeft hier geen wet neergelegd zonder oog voor dit risico. De wet gaat uit van het melden van kwetsbaarheden en ze zo snel mogelijk verhelpen. Er zitten processen en procedures in om in uitzonderlijke gevallen melding van een kwetsbaarheid uit te stellen in verband met een opsporingsonderzoek. Deze casus toont aan waarom die balans in het wetsvoorstel zo goed is. Je wilt ten eerste voorkomen dat het nog een keer gebeurt. Ten tweede wil je het gat zo snel mogelijk dichten. Ten derde wil je degene die erachter zit oppakken. Om dat laatste te kunnen doen, heb je bepaalde bevoegdheden nodig.

Wat ook duidelijk is, is dat een kwetsbaarheid als deze, die al bekend en gemeld was en waarvoor al een reparatie bestond — het gaat niet om iets wat recentelijk nog is stilgehouden — nooit de toets van niet-melding van het wetsvoorstel had doorstaan. Deze kwetsbaarheid zit namelijk zo diep en wijdverbreid in belangrijke systemen dat het OM in dit geval niet eens zou hebben aangevraagd om haar in het opsporingsbelang open te mogen houden; dat hebben we nagevraagd. Deze zou sowieso gemeld zijn.

De heer **Hijink** (SP):
De staatssecretaris lijkt te vergeten dat deze aanval niet had kunnen plaatsvinden als de overheid, in dit geval de Amerikaanse overheid, de NSA, gewoon haar werk had gedaan, namelijk burgers, bedrijven en overheden beschermen. Dat heeft zij niet gedaan. Zij heeft doelbewust een bestaand lek in software opengehouden om daar dankbaar misbruik en gebruik van te kunnen maken. De staatssecretaris zegt dan dat mensen maar netjes hun updates moeten doen, en daar heeft hij ook wel gelijk in, maar dat helpt natuurlijk niet als de overheid tegelijkertijd zelf doelbewust misbruik en gebruik maakt van achterdeurtjes die in software bestaan. Mijn vraag is dan ook of de staatssecretaris bereid is om de hackwet die nu in de Eerste Kamer voorligt, nog te gaan aanpassen, zodat de overheid niet zelf medeverantwoordelijk wordt voor dit soort aanvallen, sterker nog, het internet uiteindelijk een stuk onveiliger maakt.

Staatssecretaris **Dijkhoff**:
Nee, die wet ga ik niet aanpassen, want daarin zitten nu net regelingen om per keer af te wegen welk belang prevaleert. In dit geval zou de kwetsbaarheid onder die wet zeker niet stiekem gebruikt en niet opengehouden zijn. De NSA heeft de kwetsbaarheid in dit geval inderdaad ooit niet gemeld. Daarna is ze wel aan het licht gekomen en daarom waren er al reparaties voor. Zelfs als een kwetsbaarheid algemeen bekend is en er ook een reparatie voor is, zie je dus dat je die kwetsbaarheid nog steeds kunt misbruiken. Het is dus niet zo dat alle systemen geüpdatet zijn zodra een kwetsbaarheid gemeld is. Ik denk dat ons wetsvoorstel een goede balans heeft. De hoofdregel daarbij is: een kwetsbaarheid die je ontdekt moet worden gemeld, onder strikte voorwaarden en met de uitzonderingen die we destijds bij de wetsbehandeling hebben besproken.

De **voorzitter**:
Dank u wel.

Verstuurd vanaf mijn iPhone

CCIII factsheet
18-05-2017

De wetgeving

- Ligt bij EK, Schriftelijke vragen zijn beantwoord
- AMVB is formeel aangeboden ter consultatie- deadline 7 juli
  (Na escalatie door Theo richting Arie IJzerman heeft alsnog afstemming plaatsgevonden)
- Deskundigenbijeenkomst EK (NB: in combinatie met het wetsvoorstel ANPR 28 dagen opslag, wat ongunstig is, er zullen verbanden worden gelegd tussen de wetsvoorstellen, verhouding vrijheid/privacy-veiligheid) - 20 juni
- Gewenste en afgesproken datum inwerkingtreding

Stand van zaken:

- Vooral nadruk op de bevoegdheid tot "binnendringen in een geautomatiseerd werk"(ook wel hacken genoemd)
- Er wordt door het project gewerkt aan de voorbereiding van de implementatie van het binnendringen (technische proefomgeving, werkprocessen etc.)
- Er is een aantal technisch experts beschikbaar, maar dit blijkt te beperkt voor de verdere voorbereiding en uitvoering van de wet.
- omgeving wordt op landelijke niveaus ingericht binnen LE DLOS (vanwege kosten, complexiteit, beperkt beschikbaar gekwalificeerd personeel.)
-Er is een projectplan in voorbereiding dat 1 juli wordt opgeleverd ter besluitvorming.

Hoofdlijnennotitie

- 12 mei is een hoofdlijnennotitie besproken in BOO; BBVO en KMT volgen.
- Focus op "binnendringen" en belang van extra capaciteit voor de voorbereiding en na implementatie.
- Twee fases, experimenteren en implementeren
- Centraal (gezamenlijk) inrichten (vanwege kosten, complexiteit en politiek bestuurlijke gevoeligheid. Is ook toezegging aan TK.
- Capaciteit binnen het voorbereidingsteam is een probleem, twee scenario's besproken met BOO:
  - LE wer7-12 fte. Afroming eenheden formatieruimte v7-12 fte.
  - LE wer7-12 fte. Eenheden lever7-12 fte op basis van TTW voor 2 jaar

  Besluit BOO: is akkoord met laatste scenario, mits er een visie komt met de nadere duiding en koers hoe we dit duurzaam tot stand kunnen brengen. Dit zal dan na de zomer op de agenda komen. Daarnaast wordt aandacht gevraagd voor de werving van het personeel. Een helder profiel voor de medewerker is belangrijk. Geadviseerd wordt 7-12 hierin mee te nemen.
  Afgesproken wordt het onderwerp Cyber ieder kwartaal te agenderen voor het BOO. Op deze manier kan het BOO aangehaakt blijven bij de ontwikkelingen op dit gebied, zoals de ervaringen van de cyberteams welke al in werking zijn.

Aandachtspunten:

- **Onvoldoende capaciteit**

Vandaar in BOO besproken capaciteit vanuit eenheden beschikbaar te stellen voor 2 jaar. Dit voorstel moet nog naar BBVO en KMT.

- **Structurele financiering**

Het is op hooflijnen duidelijk wat de structurele kosten zijn na implementatie. Dit deelt Theo nog met jou. In de projectfase kan financiering vanuit de tijdelijk gelden voor Digitalisering en Cybercrime komen. Structureel moet het uit bestaande middelen komen.

- **Aanschaf software**

Ligt politiek/bestuurlijk gevoelig en is duur (maar structurele kosten zijn nog moeilijk in te schatten).

- **Draagvlak voor centrale oplossing**

Recente signalen dat eenheden en officieren mogelijk buiten de centrale voorziening in de eenheden deze bevoegdheid zelf willen uitvoeren. Wordt meegenomen in besprekingen BOO en KMT.

-**Relatie met Wannecry ransomware aanval van afgelopen weekend**

Kwam doordat NSA gebruik maakte van dit lek van Microsoft. Maar het middel dat ze gebruikten is op straat komen te liggen en nu gebruikt door criminelen (of statelijke actoren, is nog onduidelijk). Tegenstanders van de wet zullen dit aangrijpen als voorbeeld dat de politie deze bevoegdheid niet moet krijgen. Ons weerwoord is

- dat de wet met veel waarborgen is omgeven en dat er een meldplicht is als de politie onbekende kwetsbaarheden vindt.
- dat het OM heeft aangegeven dat deze kwetsbaarheid zou zijn gemeld.
- dat deze kwetsbaarheid al geruime tijd bekend was en gepatched door Microsoft. Toch hebben veel mensen/bedrijven de update niet geïnstalleerd.

Van: 10.2.e
Verzonden: donderdag 18 mei 2017 10:44
Aan: 10.2.e @politie.nl>; Plas, Theo van der (T.G.)
10.2.e @politie.nl>
Onderwerp: RE: Verslag BOO 12/5: Hoofdlijnennotitie CCIII

Beste 10.2.e

Wat ik hier nog in mis is het besluit van het BOO om akkoord te gaan met scenario 2 mits er uiteindelijk ook een visie komt met de nadere duiding en koers hoe we dit duurzaam tot stand kunnen brengen. Dit zal dan na de zomer op de agenda komen.

Zo heb ik de conclusie van het BOO opgeschreven.

@Theo, klopt dit zo?

Gr.

10.2.e

Van: 10.2.e @politie.nl>
Datum: 18 mei 2017 11:02:31 CEST
Aan: 10.2.e politie.nl>, Plas, Theo van der (T.G.)
10.2.e @politie.nl>, 10.2.e @politie.nl>
CC: 10.2.e @politie.nl>
Onderwerp: RE: Verslag BOO 12/5: Hoofdlijnennotitie CCIII

Hoi 10.2.e

Dank voor je reactie.
Het verslag bestaat uit meerdere kolommen, o.a. het 'besluit' en de 'toelichting'. Onderstaande tekst was enkel hetgeen er tijdens het BOO is besproken, dus de toelichting.
In de kolom 'besluit' staat geen er aan het BOO wordt gevraagd, zoals in de oplegnota beschreven. Dat was in jullie geval zoveel, dat ik dat voor de leesbaarheid niet in de mail heb geplakt ;-)
Daarin heb ik genoteerd dat het BOO akkoord gaat met scenario 2, incl. de mits.

Met vriendelijke groet,

10.2.e
Adviseur /9
Politie I Korpsstaf I Afdeling Bestuursondersteuning I Team Bestuurszaken
Nieuwe Uitleg 1, 2514 BP Den Haag
Postbus 17107 I 2502 CC Den Haag

Van: Plas, Theo van der (T.G.)
Verzonden: donderdag 18 mei 2017 23:19
Aan: 10.2.e Secretaris.BOO
CC: 10.2.e
Onderwerp: RE: Verslag BOO 12/5: Hoofdlijnennotitie CCIII

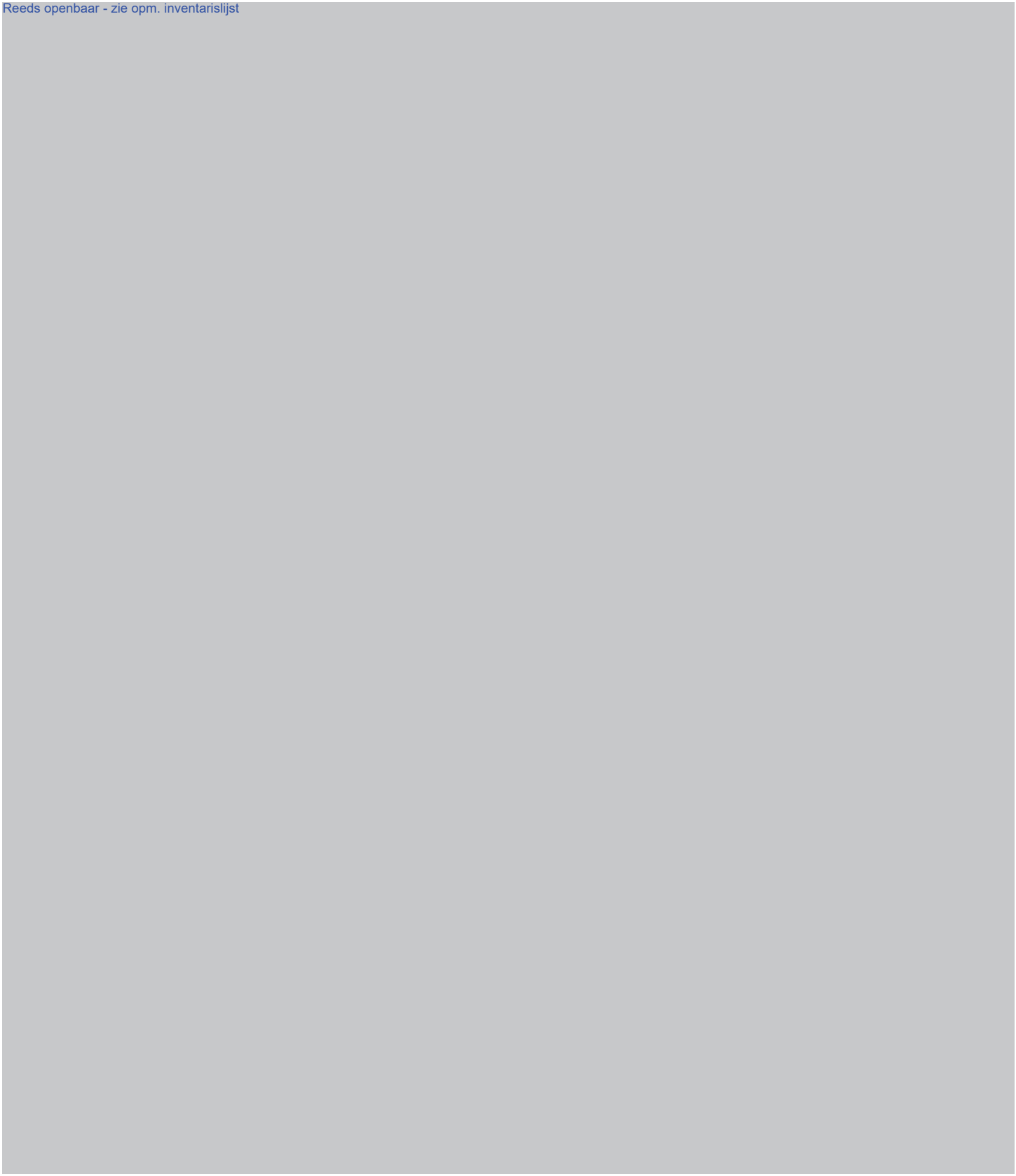
Hallo.
Ik kan me niet herinneren dat dit zo sterk is neergezet, dat 12-14

Dat zou inderdaad terug moeten komen in een bredere visie, op de hele ontwikkeling van CC3, zoals dit na de zomer graag terug wordt gezien.
Zoiets ? Kijk even mee 10.2.e aub

Met vriendelijke groet,

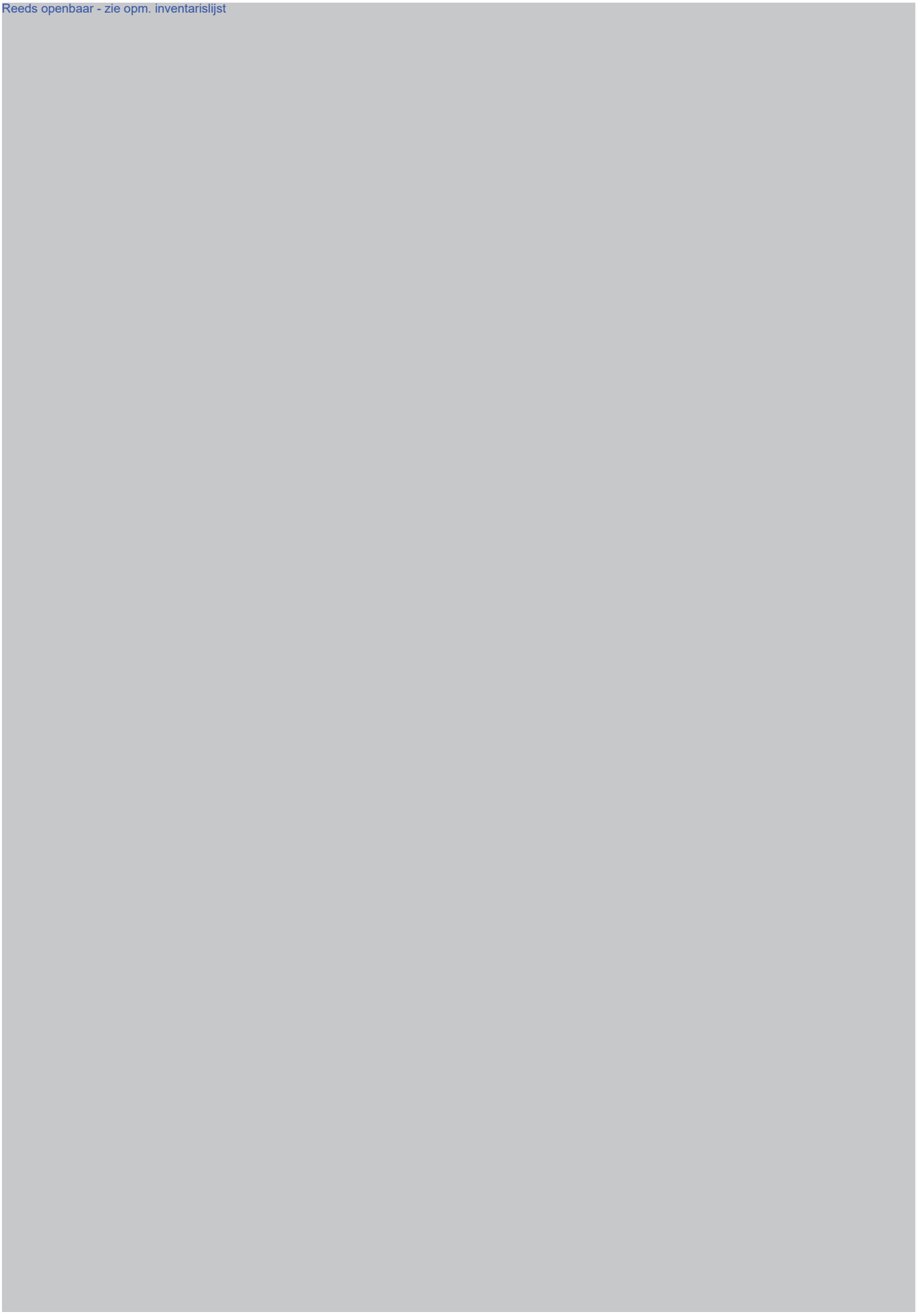
Drs. Theo G. van der Plas EMPM

Programmadirecteur Digitalisering & Cybercrime
Nieuwe Uitleg 1, 2514 BP Den Haag
Postbus 17107, 2502 CC Den Haag


Reeds openbaar - zie opm. inventarislijst

Reeds openbaar - zie opm. inventarislijst

Reeds openbaar - zie opm. inventarislijst




Reeds openbaar - zie opm. inventarislijst

Verslag

Overleg
Begeleidingscommissie CCIII

Datum
01-06-2017
Tijdstip
15.00 – 17.00 uur
Locatie
Driebergen, LE, F2

Organisatieonderdeel
LE / DLOS

Behandeld door
10.2.e

E-mail
10.2.e politie.nl

Aanwezig
Marjolein Smit, 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e j, 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e (verslag)
Gasten: Theo van der Plas, 10.2.e & 9

Afwezig
10.2.e (vervangen door 10.2.e), 10.2.e

1. **Opening, voorstellen en vaststelling agenda**
   10.2.e heet iedereen welkom. In het bijzonder de programmadirecteur Theo van der Plas. Een korte voorstelronde volgt.
   Agenda wordt zonder aanvullingen vastgesteld.

2. **Besluitenlijst vorige vergadering**
   Verslag wordt zonder wijzigingen vastgesteld.

3. **Governance CCIII**
   Het is belangrijk om de governance van het programma CCIII op heldere en eenduidige manier te regelen, gezien het grote strategische belang voor de Nationale Politie; de tijdsdruk; de complexiteit van het onderwerp en de gesignaleerde risico's die uit de onlangs uitgevoerde risicoanalyse CCIII naar voren zijn gekomen. Het programma CCIII heeft sinds de start te maken gehad met extreem veel wisselingen in bemensing en rollen van zowel leiding als projectadvisering. Ook de introductie van de nieuwe rol van programmadirecteur Digitalisering en Cybercrime is nieuw. De programmamanager en zijn plv. zijn feitelijk de enige continue factor. Een duidelijke governance en continuïteit in besturing zijn ook vanuit dat perspectief van essentieel belang. Onder governance in CCIII wordt begrepen de samenhangende rolverdeling en sturingsverantwoordelijkheden en –bevoegdheden tussen programmadirecteur digitalisering & cybercrime; sectorhoofd DLOS; de stuurgroep CCIII en programmamanager CCIII. Dit voorstel is tot stand gekomen na oriënterende gesprekken met de programmadirecteur, sectorhoofd DLOS en de programmamanager CCIII. Daarnaast is gekeken naar de praktijk van effectieve rolverdelingen in lijn- en programmamanagement.
   Op basis van gezamenlijke bespreking kan het governancemodel CCIII definitief worden vastgesteld en opgenomen in het realisatieplan.

   CCIII is geen project maar een programma
   Een project is gericht op een concreet resultaat binnen tijd en budget. Waar bij een project de te bewandelen weg vooraf kan worden bedacht (inclusief noodzakelijke middelen als tijd en geld), wordt in een programma de weg gaandeweg vormgegeven.
   Een programma is gericht op toegevoegde waarde en dus op baten (financieel en niet financieel) voor de sponsors en stakeholders. Een programma omvat een unieke, tijdelijke opgave, uit te voeren in een tijdelijk samenwerkingsverband. Complexe veranderopgaven als CCIII kunnen het beste via programmasturing worden vormgegeven omdat het gaat om strategische veranderopgaven met een groot aantal belanghebbenden en de druk om binnen beperkte tijd in een zorgvuldig proces resultaten te bereiken. Zowel de bestaande organisatie als de programmaorganisatie geven uitvoering aan het programma. Concrete onderdelen

Overleg
Klik hier als u tekst wilt invoeren

Datum
Klik hier als u een datum wilt invoeren.

Pagina
2 van 6

van het programma worden projectmatig gerealiseerd of via agile/scrum werkvormen. Dit wordt in de mijlpalenplanning en realisatieplan verder uitgewerkt. Het programma transformeert het huidige laboratorium naar een werkende proefopstelling op 1 januari 2018 en levert CCIII als nieuwe werkende voorziening op 1 januari 2019 op en draagt het dan over aan de staande organisatie.

Succesfactoren
Je kunt afspreken wat je wilt, zo lang je maar samen optrekt, ieder in zijn eigen rol respecteert daarop aanspreekbaar is en je voldoende besliskracht verwerft.

Opdrachtgever en opdrachtnemer
De **opdrachtgever** (Theo van der Plas) is eigenaar van het programma CCIII en daarmee eindverantwoordelijk. Hij moet het mandaat hebben gekregen van de korpsleiding om het programma te besturen en beslissingen te nemen. De programmadirecteur ziet CCIII als een hefboom voor vernieuwing van de politieorganisatie en een mogelijkheid om de politie in het speelveld meer zichtbaar en actief te positioneren als samenwerkingspartner.
De **opdrachtnemer** (Marjolein Smit) stelt zich verantwoordelijk voor het behalen van de programmaresultaten. De opdrachtnemer vraagt en krijgt daartoe de middelen en de bevoegdheden die zij daarvoor nodig heeft.
Het sectorhoofd DLOS heeft als ambitie om het programmaresultaat van CCIII neer te zetten en het een voorbeeldfunctie te late vervullen voor effectieve samenwerking tussen opsporingsdiensten.
De **programmamanager** 10.2.e is verantwoordelijk voor het opzetten van het programma, de inrichting van de programmaorganisatie, de dagelijkse leiding van het programma en de rapportage en communicatie vanuit het programma. De programmamanager is de ‘smeerolie’ in het verbinden, inspireren en motiveren van alle bij het programma betrokken disciplines. De programmamanager levert het programma op 1 januari 2019 op aan de staande organisatie.

Rolverdeling opdrachtgever, opdrachtnemer en programmamanager
Aanwezigen zijn akkoord met de voorgestelde rolverdeling.

Begeleidingscommissie
Uit de risicoanalyse CCIII is naar voren gekomen dat de stuurgroep niet bevoegd is om beslissingen te nemen.
Betrokkenheid van belangrijke stakeholders is van groot belang voor een goed en gedragen programmaresultaat. Daarom dient de stuurgroep omgevormd te worden naar een begeleidingscommissie.
De verantwoordelijkheid van leden van de begeleidingscie reikt verder dan aanwezigheid op de vergaderingen. De leden treden, ieder voor hun eigen domein, op als ambassadeur en kennispartner van het programma. Feitelijk fungeert de begeleidingscie als sponsorgroep. Lidmaatschap van de begeleidingscie houdt in het binnen de deelnemende organisaties promoten van de verandering, het mogelijk maken dat het beoogde resultaat bereikt kan worden en dat de verwachte baten gerealiseerd kunnen worden. De begeleidingscie vormt de link tussen de programmaorganisatie en de bestaande organisatie(s).
Geadviseerd wordt om de stuurgroep om te vormen tot begeleidingscommissie, de samenstelling van de begeleidingscommissie te ijken en een vergaderschema op te stellen met een zes- tot acht wekelijkse cyclus met aansprekende topics, afgestemd op het concept programmaplanning.

Hoewel de begeleidingscommissie formeel niet beslissingsbevoegd is, zal ze adviezen formuleren die als feitelijk als besluit gezien kunnen worden. Het belangrijkste is dat we met zijn allen de schouders er onder zetten om stappen voorwaarts te maken. In gezamenlijkheid afspraken nakomen. Het moet voelen dat het van ons allen is en dat CCIII ons gaat helpen.
DLOS maa7-12 fte vrij voor het lab, de partners participeren m7-12 f.t.e. en

Overleg
Klik hier als u tekst wilt invoeren

Datum
Klik hier als u een datum wilt invoeren.

Pagina
3 van 6

daarnaast wordt er per Eenhe7-12 fte gevraagd. Opdrachtgever en opdrachtnemer moeten mandaat en beslissingsbevoegdheid organiseren.
Opdrachtnemer is verbindende schakel naar 7-12 en de programmadirecteur naar andere doelgroepen.
10.2.e en 10.2.e geven aan eerst behoefte te hebben aan een duidelijk PID of Realisatieplan, gericht op het bereiken van resultaten, capaciteit, benodigde hard-/software, financiering, governance en huisvesting. Daarnaast aan een stuurgroep die kan beslissen. De begeleidingscie is adviserend; besluiten worden genomen in het driehoeksoverleg tussen programmadirecteur, opdrachtnemer en programmamanager CIII. Omissie is de afwezigheid van IV in deze notitie. Afspraak is dat 10.2. en 10.2.e daartoe een aanvullend voorstel doen. 10.2.e
Samenstelling en rol begeleidingscommissie is akkoord.

Vergaderschema
* Voortgangsoverleg opdrachtnemer/programmamanager: eens per twee weken
* Driehoeksoverleg opdrachtgever/opdrachtnemer/programmamanager: eens per 4 weken
* Begeleidingscommissie: eens per zes tot acht weken

4. **Concept mijlpalenplanning en succesfactoren in realisatie CCIII**
10.2.e licht de mijlpalenplanning CCIII en de succesfactoren in realisatie CCIII beknopt toe. De sheets zijn als bijlage bijgevoegd.

Veranderaanpak
- Geen blauwdruk, maar een ontwikkelaanpak
- Informatie delen waar het kan, tenzij
- Realistische ambities:
* Aanpak is maatwerk;
* Ontwikkelen kost tijd;
* Inwerktijd van minimaal 1 jaar.
- Geen schotten na (A) screening
- Prioritering door OM/LP
- Inzichtelijk maken capaciteit en doorlooptijd naar OM
- Kennis en ervaring uitleren ‘aan het land’
- Lef/durf om te beginnen met steun/vertrouwen leiding & politiek
- Prioriteren/toewijzen middelen
- Doorbreken cultuur ‘dat alles speciaal is’
- Leren van andere landen/Europol/ENLETS: Duitsland, Noorwegen, Verenigd Koninkrijk, België, Finland, Zweden, Zwitserland, Oostenrijk, Canada en Israël

Verbinden met buiten
- Ketenaanpak met het OM (en ZM)
- Samenwerking met AIVD, MIVD en DCC
- Samenwerking met de wetenschap

Verbinden met binnen
-Verbinden met klanten/eenheden
- Uitleren kennis aan eenheden van begin af aan
- Boven- en onderwereld top (leiding) en uitvoering (specialisten)
- Specialisten van TDO’s, tactische recherche en LE betrekken in realisatie (denkkracht en kennis)
- Versterken keten (samenwerking met AO en kennis AO)
- Ondersteunen van operaties met huidige BOB bevoegdheden

Communicatie (kernbegrip)
- Belang en kansen
- Vanuit programma met 1 stem naar buiten (en naar binnen)

Overleg
Klik hier als u tekst wilt invoeren

Datum
Klik hier als u een datum wilt invoeren.

Pagina
4 van 6

- Meer zichtbaar worden als programma
- Goede mediastrategie
- CCIII beeldend maken d.m.v. 5 operationele scenario's
- Open communicatie, delen waar het kan, tenzij
- Zeggen wat je doet (hacken)
- Vaste gezichten
- Presentatie in overlegvormen als 7-12 dagen

etc.

Juridisch
- Praktische werkbare wetgeving
- Juridische eisen vertaald naar organisatie opgaven

4. Versterking programma – organisatie CCIII

a) Presentatie programma organisatie door 10.2.e. Er is nog ontzettend veel te doen en de tijd is beperkt. Dat vraagt om versterking van de programmaorganisatie door een aanpak met een zestal taakgroepen:

Taakgroep mens - denkkracht en participatie in de werkgroep.
* Werving & selectie
* Opleiding en certificering medewerkers
* Screening
* Aanwijzing
* Opleidingen OM

Taakgroep Techniek
7-12

Taakgroep juridisch
* Advisering Besluit Onderzoek Geautomatiseerd Werk
* Beantwoording vragen
* Vertaling juridische eisen naar organisatieopgaven

Taakgroep organisatie
* Werkprocessen in concept geformuleerd
* Organisatie ontwerp
* Keuring

Taakgroep huisvesting
* Realisatie huisvesting KT
* Verhuizing
* Realisatie huisvesting LT

Taakgroep communicatie
* Communicatieplan
*Voorlichting TDO
* Voorlichting tactische recherche
* Verwachtingenmanagement

Er is een dringende behoefte aan een goede teamleider; suggesties zijn welkom. In de aanpak is balans tussen denken en doen. We gaan plannen en organiseren. We vertalen de ambitie naar opgaven voor de taakgroepen die voorstellen ontwikkelen om deze opgaven te realiseren. Onze uitdaging is om de rest van Nederland er bij te betrekken. 'Sense of Urgency' is nu wel aanwezig. **b)** Participatie vanuit de organisaties en organisatieonderdelen van leden

Overleg
Klik hier als u tekst wilt invoeren

Datum
Klik hier als u een datum wilt invoeren.

Pagina
5 van 6

begeleidingscommissie
Leden van de begeleidingscommissie worden gevraagd om actieve deelname in de taakgroepen vanuit hun eigen discipline te organiseren. De persoonlijke benadering vanuit de rol van ambassadeur moet leidend zijn. De KMar wil commitment tonen. Verzoek om dit onderwerp in bila's aan te snijden. Defensie heeft als prio meer samenwerking met de Politie.

Elke taakgroep heeft een aannemer. Vanuit Communicatie en HRM missen we nog een goede professional als aannemer Advies is om voor CCIII een PDC-team te formeren.
@ 10.2.e : verzoek aan hoofd PDC tot instellen van een PDC team en participatie in de begeleidingscommissie.
@ Leden begeleidingscommissie: Leden van de begeleidingscommissie gaan op zoek naar geschikte deelnemers in de taakgroepen en geven namen door aan Peter.
@10.2.e r: 10.2.e werkt de opzet voor 1 juli a.s. verder uit en Inventariseert waar de gaten zitten.

5. Presentatie ENLETS - **Gast:** 10.2.e

Wat is ENLETS? European Network of Law Enforcement Technology Services

Niet onder reikwijdte

ENLETS en CCIII
- Internationale wereld: human factor
- Makelaarsfunctie; ENLETS en CCIII in verbinding
- EU platform; maar ook daarbuiten
- Veel activiteiten en relaties af te stemmen.

6. Mededelingen

a) Stand van zaken wetgeving
Hoorzitting Eerste Kamer op 20 juni a.s. Iedereen kan/mag vanuit zijn eigen standpunten reageren. 3 thema's: uitvoerbaar, privacy en noodzaak.

b) Hoofdlijnennotitie (mondeling)
Notitie is (nog) niet breed verspreid. Is 12 mei jl. behandeld in het BOO. Daar is ingezien dat er niet ontkomen kan worden om capaciteit te leveren. 10.2.e

Overleg
Klik hier als u tekst wilt invoeren

Datum
Klik hier als u een datum wilt invoeren.

Pagina
6 van 6

uit zijn zorgen over het gebrek aan urgentiebesef/ committement van sommige regionale eenheden. Er is echter geen weg terug. HET BOO heeft groen licht gegeven voor de hoofdlijnennotitie.

c) 10.2.e wijst op het belang dat de tactiek aansluit bij de (CCIII) techniek. Dit vraagstuk hangt samen met de eis van functiescheiding en wordt in de taakgroep organisatie verder uitgewerkt.
KMar: leg de lijn voor de tactiek naar de contactpartners**.**

7. Rondvraag

8. **Sluiting**
Marjolein sluit de vergadering en dankt iedereen voor zijn/haar inbreng.

Van: 10.2.e
Verzonden: dinsdag 6 juni 2017 11:56
Aan: Plas, Theo van der (T.G.) 10.2.e @politie.nl>
CC: 10.2.e @politie.nl>; 10.2.e @klpd.politie.nl>
Onderwerp: Acties/Afspraken BOO 12 mei, inzake 'Hoofdlijnennotitie Computercriminaliteit III'

Ola Theo,

Vanuit het concept verslag BOO 12 mei jl. haal ik de onderstaande acties, afspraken en tijdpad voor jouw onderwerp 'Hoofdlijnennotitie Computercriminaliteit III'.
Wellicht heb je deze al via de mail binnen… anders hierbij in ieder geval onderstaand uit het verslag geknipt…

Verzoek (*uiterlijk donderdag 8 juni)*
Mocht je nog op/aanmerkingen hebben op onderstaand: vrijdag 9 juni is het volgende BOO en zal dit verslag worden vastgesteld.
Graag vóór die tijd dus reactie via mij aan 10.2.e aub…

Alvast dank!
Cu greetz 10.

Dhr. Van der Plas	Hoofdlijnennotitie Computercriminaliteit III	Het BOO neemt kennis van: - de notitie over het programma CCIII en specifiek de implementatie van de bevoegdheid tot 'heimelijk op afstand binnendringen in een geautomatiseerd werk'; - de fasering die in het programma is aangebracht in een fase 1 van experimenteren (tot 1 juli) die leidt tot een nader onderbouwd realisatieplan voor fase 2 (vanaf 1 juli), waarin de PIOFACH aspecten concreet zijn uitgewerkt. Dit definitieve realisatieplan wordt voor 1 juli aan het KMT ter besluitvorming voorgelegd; - de keuze om de voorziening in ieder geval voorlopig centraal in te richten, vanwege de politiek-bestuurlijke gevoeligheden rond deze bevoegdheid en vanwege de complexiteit en potentieel hoge kosten van de implementatie; - het feit dat er op dit moment in fase 1en 2 onvoldoende capaciteit beschikbaar is in de voorziening om de benodigde experimenten uit te voeren die noodzakelijk	De heren Van der Plas en 9 te lichten. De achtergrond en ko component ligt vandaag voor. G tussen 2 scenario's: 1. de Landelijke Eenheid wer Vanuit de eenheden wordt va 7-12 te afgeroomd ten b 2. de Landelijke Eenheid wer Vanuit de eenheden wordt gekwalificeerde medewerk Er wordt kort gediscussieerd ov of er formatieruimte is geclaimd Het BOO is akkoord met scenar dat deze mensen daadwerkelijk Daarvoor moet een goede visie duiding en koers hoe we dit duu Na de zomer ziet het BOO deze **dhr. v.d. Plas** Daarnaast wordt aandacht gevr Een helder profiel voor de mede 7-12 hierin mee te nemen.

		zijn om tijdig een voldoende onderbouwd plan van aanpak voor de implementatie op te kunnen stellen; - het feit dat het lab CCIII in eerste instantie als een Eigen Beheerde Organisatie (EBO) is ingericht en dat de definitieve voorziening CCIII in de toekomst zal worden ingepast in de infrastructuur van de Nationale Politie. Het BOO maakt de keuze voor scenario 2: *"De Landelijke Eenheid wer[7-12] te voor de centrale voorziening. Vanuit de Eenheden wordt daarnaast in tota[7-12] e door een gekwalificeerde medewerker tewerkgesteld bij de voorziening. Hiermee wordt, gezamenlijk met de partners, een voorziening van[7-12] e gecreëerd. Na 2 jaar keren de medewerkers terug naar hun eenheid, waardoor de kennisontwikkeling van de eenheden een impuls krijgt. Het is dus lonend om te investeren voor de eenheden. Terugkeer zal gefaseerd plaatsvinden om een braindrain van de nieuwe eenheid te voorkomen".* Het BOO heeft er geen vertrouwen in dat deze mensen daadwerkelijk terugkeren naar de eenheden. Daarvoor moet een goede visie worden ontwikkeld met een nadere duiding en koers hoe we dit duurzaam tot stand kunnen brengen. Na de zomer komt deze koers op de agenda van het BOO. Het BOO besluit op basis van bovenstaande keuze dat: - het sectorhoofd van de DLOS van de Landelijke Eenheid de opdracht krijgt om de voorziening op basis van deze notitie en het realisatieplan in te richten en tot werking te brengen; - er gestart wordt met de centrale werving. Eenheden (incl. DLOS) te vragen vacatureruimte ter beschikking te stellen; - daartoe een landelijke wervingscampagne wordt gestart, waarbij medewerkers van de eenheden mee kunnen solliciteren.	Afgesproken wordt het onderwe voor het BOO. Op deze manier ontwikkelingen op dit gebied, zo welke al in werking zijn. **Actie: dhr. v.d. Plas / secretar**

Met vriendelijke groet,

10.2.e
Adviseur

Politie | Landelijke Eenheid |

Van: 10.2.e @gmail.com>
Verzonden: zondag 11 juni 2017 11:28
Aan: 10.2.e
Onderwerp: lastige vragen
Bijlagen: Lastige vragen voor de ronde tafel 1e kamer.docx

Bijgaand een paar vragen.

Met vriendelijke groeten, with regards
9
+316 10.2.e


Niet onder reikwijdte

Van: 10.2.e @eerstekamer.nl]
Verzonden: dinsdag 13 juni 2017 15:36
Aan: Plas, Theo van der (T.G.) 10.2.e @politie.nl>; 10.2.e @politie.nl>
Onderwerp: Deskundigenbijeenkomst privacy Eerste Kamer

Geachte heer Van der Plas, geachte 10.2.e ,

Allereerst wil ik u hartelijk danken voor uw deelname namens de Nationale Politie aan de deskundigenbijeenkomst op **dinsdag 20 juni 2017** over de wetsvoorstellen Vastleggen en bewaren kentekengegevens door politie (33542) en Computercriminaliteit III (34372). Hierbij stuur ik u nog enige praktische informatie over deze bijeenkomst. Ten eerste vindt u in de bijlage de informatie zoals deze in eerste instantie naar alle inleiders van thema I is gestuurd. Als het goed is, heeft u deze informatie reeds van het ministerie van Veiligheid en Justitie ontvangen, maar voor de zekerheid heb ik deze nog bijgevoegd.

Het definitieve tijdstip van de bijeenkomst is inmiddels vastgesteld: de bijeenkomst zal plaatsvinden van **09.00 uur tot 12.15 uur**. Verder verwijs ik graag naar het definitieve programma in de bijlage. De bijeenkomst vindt plaats in de plenaire zaal van de Eerste Kamer, en staat onder leiding van de voorzitter van de vaste commissie voor Veiligheid en Justitie (V&J), 10.2.e . Per thema krijgen de inleiders ieder 5 minuten om hun visie ten aanzien van het desbetreffende thema te geven. Aangezien u samen de Nationale Politie vertegenwoordigd op de bijeenkomst, krijgt u beiden elk 5 minuten om een visie te geven. Na het geven van de visies volgt een discussie met de aanwezige senatoren. De Dienst Verslag en Redactie (DVR) van de Kamer zal een woordelijk verslag van de bijeenkomst maken dat na afloop wordt gepubliceerd, en publiek kan zowel in de zaal als via de livestream de bijeenkomst volgen**.**

Tevens vindt u in de bijlage bij deze e-mail de consultatieversie van het ontwerpbesluit Onderzoek in een geautomatiseerd werk (EK 34372, C) en de brief inzake rectificatie cijfers gestolen blanco kentekenplaten (EK 33542, D). Ten aanzien van deze documenten heeft de commissie V&J eerder besloten deze graag bij de deskundigenbijeenkomst te willen betrekken, uiteraard voor zover dat op uw inbreng van toepassing is. Daarnaast vindt u in de bijlage ter informatie de memorie van antwoord ten aanzien van het wetsvoorstel Computercriminaliteit III (EK 34372, D), die de Eerste Kamer gisteren ontvangen heeft.

U kunt zich dinsdag melden bij de receptie op het adres **Binnenhof 22**. Graag wil ik er nog op wijzen dat bij binnenkomst van het Eerste Kamergebouw gevraagd kan worden een geldig legitimatiebewijs te tonen.

Ik hoop u hiermee voldoende geïnformeerd te hebben. Als u nog vragen heeft, hoor ik het graag.

Met vriendelijke groet,

10.2.e
Stafmedewerker

Eerste Kamer *der Staten-Generaal*
Binnenhof 22
Postbus 20017
2500 EA Den Haag

Van: 10.2.e
Verzonden: dinsdag 13 juni 2017 15:39
Aan: 10.2.e 10.2.e 10.2.e ; 10.2.e
Onderwerp: FW: Deskundigenbijeenkomst privacy Eerste Kamer
Bijlagen: Informatie Nationale Politie.pdf; Programma deskundigenbijeenkomst privacy.pdf; EK 34372, C.pdf; EK 33542, D.pdf; EK 34372, D.pdf

Ter info.

Gr.

10.2.e

De vaste Kamercommissie voor Veiligheid en Justitie (V&J) organiseert op dinsdag 20 juni 2017 een deskundigenbijeenkomst over de momenteel bij de Eerste Kamer aanhangige wetsvoorstellen Vastleggen en bewaren kentekengegevens door politie[1] en Computercriminaliteit III[2]. De deskundigenbijeenkomst strekt ertoe meer inzicht te krijgen ten aanzien van bepaalde overkoepelende aspecten van deze wetsvoorstellen. De drie thema's zijn: 1. Noodzaak en belang van de voorgestelde wetgeving, 2. Te respecteren privacywetgeving, databescherming en Europees kader, 3. Uitvoerbaarheid en handhaafbaarheid. Voor deze bijeenkomst wordt slechts een beperkt aantal deskundigen en organisaties uitgenodigd.

De bijeenkomst vindt plaats op **dinsdag 20 juni 2017 in de ochtend** in het gebouw van de Eerste Kamer. Een definitief aanvangstijdstip moet nog vastgesteld worden. De bijeenkomst zal drie uur duren.
Per thema krijgen de inleiders ieder 5 minuten om hun visie ten aanzien van het desbetreffende thema te geven. Hierna volgt een discussie met de aanwezige senatoren. Graag nodigt de commissie voor V&J u uit om uw visie te geven ten aanzien van het thema 'Uitvoerbaarheid en handhaafbaarheid'. Bij dit thema moet u denken aan vragen als:

- Wat is de impact van de onderwerpen van thema 1 en thema 2 op de uitvoerbaarheid en handhaafbaarheid van de wetsvoorstellen?
- Is de deskundigheid en accountability bij de actoren die de wetsvoorstellen moeten uitvoeren en handhaven up-to-date?
- Welke overige problemen voorziet u in de uitvoerbaarheid en handhaafbaarheid van de wetsvoorstellen?

De leden van de commissie voor V&J hebben tevens te kennen gegeven om voorafgaand aan de bijeenkomst graag geïnformeerd te worden over de kernpunten van de bijdragen van de inleiders. Zij vragen u dan ook om als voorbereiding op de bijeenkomst uw beargumenteerde visie op het thema kort en bondig kenbaar te maken in de vorm van een notitie. Hierbij moet u denken aan ongeveer een à twee A4'tjes. Alle ontvangen notities zullen gebundeld beschikbaar worden gesteld aan de deelnemers en onder de aandacht van de leden van de commissie worden gebracht. Uw notitie kunt u sturen naar het e-mailadres: 10.2.e @eerstekamer.nl. De deadline hiervoor is **vrijdag 9 juni 2017**.

Overigens willen wij u er nog graag op wijzen dat de bijeenkomst openbaar is. Dit houdt in dat – bij beschikbaarheid van de plenaire zaal – belangstellenden aanwezig kunnen zijn op de publieke tribune en dat de bijeenkomst ook via de website van de Eerste Kamer te volgen is. Het woordelijk verslag van de bijeenkomst wordt na afloop gepubliceerd.

[1] *Kamerstukken* 33 542.

[2] *Kamerstukken* 34 372.

Deskundigenbijeenkomst privacy

- in het kader van de wetsvoorstellen Vastleggen en bewaren kentekengegevens door politie (33542) en Computercriminaliteit III (34372) -

Commissie voor Veiligheid en Justitie (V&J)

dinsdag 20 juni 2017, 9.00 - 12.15 uur
Eerste Kamer, Plenaire zaal, Binnenhof 22, Den Haag

Programma

Vanaf 08.45 uur	**Ontvangst** (Noenzaal)
09.00 uur	**Welkom** (Plenaire zaal) Voorzitter commissie V&J, [redacted] (tevens voorzitter van de bijeenkomst)
09.05 - 10.05 uur **<u>Thema I:</u> Noodzaak en belang van de voorgestelde wetgeving**	**Inleidingen** (max. 5 min.): 1. [redacted] - NVSA (Nederlandse Vereniging van Strafrechtadvocaten) 2. [redacted] - Openbaar Ministerie 3. [redacted] 4. [redacted] - Universiteit Leiden 5. [redacted] - NCSC (Nationaal Cyber Security Centrum) 6. [redacted] - Universiteit van Amsterdam en advocaat [redacted] **Discussie** (max. 25 min.)
10.05 - 11.00 uur **<u>Thema II:</u> Te respecteren privacywetgeving, databescherming en Europees kader**	**Inleidingen** (max. 5 min.): 1. A. (Aleid) Wolfsen - Autoriteit Persoonsgegevens 2. [redacted] - Amnesty International Nederland 3. [redacted] - NVJ (Nederlandse Vereniging van Journalisten) 4. [redacted] - Rathenau Instituut 5. [redacted] - Universiteit van Amsterdam 6. [redacted] - Tilburg University en NIAS (Netherlands Institute for Advanced Study in the Humanities and Social Sciences) **Discussie** (max. 25 min.)

11.00 - 11.15 uur	**Pauze**
11.15 - 12.15 uur **<u>Thema III:</u> Uitvoerbaarheid en handhaafbaarheid**	**Inleidingen** (max. 5 min.): 1. T.G. (Theo) van der Plas en 9 - Nationale Politie 2. 9 - Bits of Freedom 3. 9 - Microsoft Benelux 4. 9 - Google 5. 9 - Fox-IT 6. 9 - Radboud Universiteit Nijmegen **Discussie** (max. 25 min.)
12.15 uur	**Afsluiting bijeenkomst**

Besluit van * houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd en het al dan niet met een technisch hulpmiddel onderzoek doen als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering (Besluit onderzoek in een geautomatiseerd werk)

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Op de voordracht van de Staatssecretaris van Veiligheid en Justitie van (PM datum), nr. (PM);

Gelet op de artikelen 126nba, eerste en achtste lid, 126uba, eerste en derde lid, 126zpa, eerste en derde lid, en 126ee van het Wetboek van Strafvordering en artikel 18, eerste lid, van de Wet politiegegevens;

De Afdeling advisering van de Raad van State gehoord (advies PM datum, nr. PM);

Gezien het nader rapport van de Staatssecretaris van Veiligheid en Justitie van (PM datum), nr. (PM);

Hebben goedgevonden en verstaan:

Hoofdstuk 1 Algemene bepalingen

Artikel 1 Definities
In dit besluit wordt verstaan onder:
a. bevel: bevel van de officier van justitie als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, 126zpa, eerste lid, van het Wetboek van Strafvordering;
b. korpschef: korpschef als bedoeld in artikel 27 van de Politiewet 2012;
d. onderzoekshandeling: handeling van een opsporingsambtenaar van een technisch team met het oog op een doel als bedoeld in de artikelen 126nba, eerste lid, onder a tot en met e, 126uba, eerste lid, onder a tot en met e, en 126zpa, eerste lid, onder a tot en met e, van het Wetboek van Strafvordering ter uitvoering van een bevel;
e. Onze Minister: Minister van Veiligheid en Justitie;
f. Landelijke eenheid: Landelijke eenheid als bedoeld in artikel 3, eerste lid, van het Besluit beheer politie;
g. technisch hulpmiddel: softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel;
h. technische infrastructuur: technische voorziening van een technisch team bedoeld voor de vastlegging van de door een technisch hulpmiddel geregistreerde gegevens;
i. technisch team: onderdeel van de Landelijke eenheid dat kan worden belast met de uitvoering van een bevel.

Hoofdstuk 2 Toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijkmaken van gegevens

Artikel 2 Aanwijzing van misdrijven
Als misdrijven als bedoeld in de artikelen 126nba, eerste lid, onder c, 126uba, eerste lid, onder c, en 126zpa, eerste lid, onder c, van het Wetboek van Strafvordering worden aangewezen de misdrijven, bedoeld in de artikelen 98, eerste en tweede lid, 98c, eerste lid, 131, eerste en tweede lid, 138ab, eerste tot en met derde lid, 138b, eerste tot en met derde lid, 138c, 139c, eerste lid, 139d, eerste tot en met derde lid, 139g, eerste lid, 140, eerste lid, 142a, eerste en tweede lid, 160, 161, aanhef en onder 1°, 161bis, aanhef en onder 1° en 2°, 161sexies, aanhef en onder 1°, 177, eerste en tweede lid, 179, 182, eerste en tweede lid, onder 1°, 197a, eerste en tweede lid, 200, eerste lid, 205, eerste en derde lid, 225, eerste en tweede lid, 226, eerste lid, 227, eerste lid, 231, eerste en tweede lid, 231a, eerste en tweede lid, 232, eerste en tweede lid, 240b, eerste lid, 247, 248a, 248e, 285b, eerste lid, 350a, eerste tot en met derde lid, 350c, eerste lid, 350d, 363, eerste en tweede lid en 420bis, eerste lid, van het Wetboek van Strafrecht.

Hoofdstuk 3 Deskundigheid van opsporingsambtenaren

Artikel 3 Lidmaatschap van een technisch team
1. Een opsporingsambtenaar als bedoeld in de artikelen 141, onder b, c en d, en 142 van het Wetboek van Strafvordering kan door de korpschef worden aangewezen voor het binnendringen in een geautomatiseerd werk en het, al dan niet met een technisch hulpmiddel, onderzoek doen, bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid, van het Wetboek van Strafvordering, indien hij lid is van een technisch team.
2. Een opsporingsambtenaar als bedoeld in het eerste lid kan lid worden van een technisch team indien hij heeft voldaan aan door Onze Minister aangewezen kwalificaties.

Artikel 4 Incidentele samenwerking
1. In aanvulling op artikel 3 kan een opsporingsambtenaar als bedoeld in de artikelen 141, onder b, c en d, en 142 van het Wetboek van Strafvordering die geen lid is van een technisch team door de korpschef worden aangewezen voor het binnendringen in een geautomatiseerd werk en het, al dan niet met een technisch hulpmiddel, onderzoek doen, bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid, van het Wetboek van Strafvordering, indien hij naar het oordeel van de korpschef beschikt over specifieke kennis en vaardigheden, benodigd voor de uitvoering van een bevel.
2. Indien een opsporingsambtenaar als bedoeld in het eerste lid wordt aangewezen wordt hij als deelnemer toegevoegd aan een technisch team en wordt hij tijdens de uitvoering van het bevel begeleid door een lid van een technisch team.

Hoofdstuk 4 Geautomatiseerde vastlegging van gegevens over de uitvoering van een bevel

Artikel 5 Vastlegging van gegevens
Gedurende de uitvoering van een bevel worden doorlopend en automatisch gegevens vastgelegd over de verrichte onderzoekshandelingen en het functioneren van de technische infrastructuur.

Artikel 6 Vaststelling van onregelmatigheden
1. De vastlegging van gegevens, bedoeld in artikel 5, vindt op zodanige wijze plaats dat zowel tijdens de periode, vermeld in het bevel, waarbinnen aan het bevel uitvoering moet worden gegeven als na afloop daarvan kan worden vastgesteld of tijdens die periode een handeling of bewerking heeft plaatsgevonden die van invloed is op de betrouwbaarheid en integriteit van de ter uitvoering van het bevel vastgelegde gegevens.
2. Indien een handeling of bewerking als bedoeld in het eerste lid wordt geconstateerd maakt een opsporingsambtenaar van een technisch team daarvan proces-verbaal op, dat aan de officier van justitie wordt gezonden.

Artikel 7 Betrouwbaarheid en integriteit gegevens
1. De inhoud van de vastgelegde gegevens, bedoeld in artikel 5, wordt niet bewerkt.
2. De vastgelegde gegevens zijn uitsluitend toegankelijk voor door de korpschef aangewezen ambtenaren.
3. Bij de vastlegging van gegevens worden maatregelen getroffen om wijziging of kennisneming van de ter uitvoering van een bevel vastgelegde gegevens door onbevoegden te voorkomen en achteraf te kunnen vaststellen of wijziging of kennisneming hiervan heeft plaatsgevonden.

Hoofdstuk 5 Technische eisen met betrekking tot een technisch hulpmiddel

Artikel 8 Gerichte werking
Een technisch hulpmiddel is zodanig ingericht dat de werking ervan kan worden beperkt tot de in het bevel vermelde functionaliteit of functionaliteiten.

Artikel 9 Gerichte detectie en registratie
1. Een technisch hulpmiddel detecteert en registreert uitsluitend gegevens ten behoeve van de in het bevel vermelde functionaliteit of functionaliteiten.
2. Een technisch hulpmiddel dat een functionaliteit of functionaliteiten bevat ten behoeve van het opnemen van telecommunicatie detecteert en registreert uitsluitend de communicatie die

plaatsvindt met gebruikmaking van één of meer nummers van de individuele gebruiker of gebruikers op wie het bevel betrekking heeft.

Artikel 10 Betrouwbaarheid en integriteit
1. Een technisch hulpmiddel registreert gegevens op zodanige wijze dat de inhoud van de geregistreerde gegevens identiek is aan de inhoud van de gedetecteerde gegevens.
2. Een technisch hulpmiddel is beveiligd tegen wijziging van de werking hiervan en tegen wijziging en kennisneming van de geregistreerde gegevens door onbevoegden.

Artikel 11 Herleidbaarheid
Een technisch hulpmiddel voorziet de geregistreerde gegevens van een uniek gegeven.

Artikel 12 Datum en tijd
Een technisch hulpmiddel voorziet de geregistreerde gegevens van de datum en tijd waarop de registratie plaatsvindt.

Artikel 13 Transport
1. Een technisch hulpmiddel transporteert de geregistreerde gegevens automatisch naar een technische infrastructuur.
2. Een technisch hulpmiddel beveiligt de geregistreerde gegevens tijdens het transport naar een technische infrastructuur tegen wijziging of kennisneming hiervan door onbevoegden.

Hoofdstuk 6 Keuring van een technisch hulpmiddel

Artikel 14 Voorafgaande keuring en herkeuring
1. Voordat een technisch hulpmiddel wordt ingezet ter uitvoering van een bevel wordt het goedgekeurd door een keuringsdienst.
2. Een technisch hulpmiddel wordt uitsluitend goedgekeurd indien het voldoet aan de in de artikelen 8 tot en met 13 gestelde eisen.
3. Indien een technisch hulpmiddel of een onderdeel hiervan zodanig wijzigt dat redelijkerwijs kan worden aangenomen dat de werking niet langer voldoet aan de in de artikelen 8 tot en met 13 genoemde eisen, vindt voorafgaand aan de inzet van het technische hulpmiddel herkeuring plaats door een keuringsdienst van het gewijzigde technische hulpmiddel of van het gewijzigde onderdeel.
4. In afwijking van het derde lid kan de herkeuring na afloop van de inzet plaatsvinden indien de wijziging van de werking van een technisch hulpmiddel of een onderdeel hiervan zodanig kort voor de inzet van het technische hulpmiddel plaatsvindt dat voorafgaande herkeuring niet mogelijk is.

Artikel 15 Inzet zonder voorafgaande keuring
1. Indien het onderzoeksbelang dit dringend vordert, kan de officier van justitie bepalen dat een technisch hulpmiddel wordt ingezet ondanks het feit dat niet of niet geheel wordt voldaan aan artikel 14, eerste lid.
2. De officier van justitie vermeldt in het bevel dat toepassing is gegeven aan het eerste lid.
3. Na afloop van de inzet wordt het technische hulpmiddel of een niet gekeurd onderdeel hiervan alsnog gekeurd door een keuringsdienst, tenzij de aard van het technische hulpmiddel of het niet gekeurde onderdeel hiervan zich naar het oordeel van de officier van justitie daartegen verzet.

Artikel 16 Keuringsdienst
1. Onze Minister wijst een onderdeel van de Landelijke eenheid aan als keuringsdienst.
2. Onze Minister kan één of meer andere organisaties aanwijzen als keuringsdienst.
3. Bij ministeriële regeling kunnen regels worden gesteld over de aanwijzing van de keuringsdienst, bedoeld in het eerste lid.
4. Indien Onze Minister voornemens is één of meer andere organisaties aan te wijzen als keuringsdienst worden hierover bij ministeriële regeling regels gesteld.

Artikel 17 Keuringsprotocol
1. Een keuringsdienst legt de wijze van keuring vast in een keuringsprotocol.
2. Een keuringsprotocol behoeft voorafgaande goedkeuring door Onze Minister.

Artikel 18 Keuringsrapport
1. De korpschef biedt een technisch hulpmiddel ter keuring aan bij een keuringsdienst.
2. Een keuringsdienst legt de resultaten van de keuring vast in een keuringsrapport.
3. Het keuringsrapport van een goedgekeurd technisch hulpmiddel vermeldt ten minste:
a. dat het technische hulpmiddel voldoet aan de artikel 8 tot en met 13 gestelde eisen;
b. een referentienummer;
c. een omschrijving van de werking van het technische hulpmiddel;
d. een aanduiding van de functionaliteit of functionaliteiten van het technische hulpmiddel;
e. relevante verplichte vervangende procedurele waarborgen waarmee voldaan kan worden aan één of meer eisen, bedoeld in de artikelen 8 tot en met 13;
f. relevante informatie met betrekking tot de werking van een functionaliteit of functionaliteiten van het technische hulpmiddel;
g. de periode waarvoor de keuring geldt, zolang de werking van het technische hulpmiddel ongewijzigd is.

Artikel 19 Registratie van keuringsrapporten
De keuringsdienst van een onderdeel van de Landelijke eenheid houdt een centrale registratie bij van de keuringsrapporten.

Artikel 20 Wederzijdse erkenningsclausule
1. Met technische hulpmiddelen als bedoeld in dit besluit worden gelijkgesteld technische hulpmiddelen die rechtmatig zijn vervaardigd of in de handel zijn gebracht in een andere lidstaat van de Europese Unie of in een staat, niet zijnde een lidstaat van de Europese Unie, die partij is bij een tot een douane-unie strekkend Verdrag, dan wel rechtmatig zijn vervaardigd in een staat die partij is bij een tot een vrijhandelszone strekkend Verdrag dat Nederland bindt, en die voldoen aan eisen die een beschermingsniveau bieden dat ten minste gelijkwaardig is aan het niveau dat met de nationale eisen wordt nagestreefd.
2. Met een keuringsrapport als bedoeld in dit besluit wordt gelijkgesteld een verklaring van goedkeuring, afgegeven door een onafhankelijke keuringsinstelling in een andere lidstaat van de Europese Unie dan wel in een staat, niet zijnde een lidstaat van de Europese Unie, die partij is bij een daartoe strekkend of mede daartoe strekkend Verdrag dat Nederland bindt, welke verklaring is afgegeven op basis van onderzoekingen die een beschermingsniveau bieden dat ten minste gelijkwaardig is aan het niveau dat met de nationale onderzoekingen wordt nagestreefd.

Hoofdstuk 7 Toegang tot en plaatsing van een technisch hulpmiddel

Artikel 21 Toegang
1. De korpschef wijst één of meer ambtenaren aan die zijn belast met de centrale registratie van de toegang tot goedgekeurde technische hulpmiddelen.
2. Een met registratie belaste ambtenaar verschaft, na ontvangst van een kopie van het bevel, een met plaatsing belaste opsporingsambtenaar toegang tot een technisch hulpmiddel.
3. De toegang tot een technisch hulpmiddel wordt verleend voor de in het bevel vermelde periode waarbinnen aan het bevel uitvoering moet worden gegeven.
4. Een met registratie belaste ambtenaar registreert ten minste:
a. een aanduiding van het technische hulpmiddel waartoe toegang wordt verleend;
b. het tijdstip van toegangverlening;
c. de in het bevel vermelde aanduidingen van de aard en functionaliteit van een technisch hulpmiddel;
d. de in het bevel vermelde periode waarbinnen aan het bevel uitvoering moet worden gegeven.

Artikel 22 Plaatsing
1. De plaatsing van een technisch hulpmiddel in een geautomatiseerd werk vindt plaats door een opsporingsambtenaar van een technisch team.
2. De opsporingsambtenaar beperkt bij de plaatsing van een technisch hulpmiddel de werking ervan tot de in het bevel vermelde functionaliteit of functionaliteiten.
3. De opsporingsambtenaar maakt proces-verbaal op van de plaatsing, dat aan de officier van justitie wordt gezonden.

Hoofdstuk 8 Inzet van een technisch hulpmiddel

Artikel 23 Inzet
1. De inzet van een technisch hulpmiddel in een geautomatiseerd werk vindt plaats door een opsporingsambtenaar van een technisch team.
2. De opsporingsambtenaar maakt proces-verbaal op van de inzet, dat aan de officier van justitie wordt gezonden.

Artikel 24 Technische infrastructuur
De vastlegging van de door een technisch hulpmiddel geregistreerde gegevens vindt plaats op een technische infrastructuur.

Artikel 25 Betrouwbaarheid en integriteit
1. De inhoud van de op een technische infrastructuur vastgelegde gegevens wordt niet bewerkt.
2. De vastgelegde gegevens zijn uitsluitend toegankelijk voor door de korpschef aangewezen ambtenaren.
3. Bij de vastlegging van gegevens worden maatregelen getroffen om wijziging of kennisneming van de vastgelegde gegevens door onbevoegden te voorkomen en achteraf te kunnen vaststellen of wijziging of kennisneming hiervan heeft plaatsgevonden.

Artikel 26 Herleidbaarheid
Een technische infrastructuur is zodanig ingericht dat bij de vastlegging van gegevens het door een technisch hulpmiddel geregistreerde unieke gegeven wordt herkend.

Artikel 27 Datum en tijd
Een technische infrastructuur is zodanig ingericht dat bij de vastlegging van gegevens de datum en tijd van de vastlegging worden geregistreerd.

Hoofdstuk 9 Verwijdering van een technisch hulpmiddel

Artikel 28 Verwijdering
1. Een technisch hulpmiddel wordt verwijderd uit een geautomatiseerd werk zodra een bevel is uitgevoerd of uiterlijk zodra de periode, vermeld in het bevel, waarbinnen aan het bevel uitvoering moet worden gegeven is verlopen.
2 De verwijdering van een technisch hulpmiddel vindt plaats door een opsporingsambtenaar van een technisch team.
3. De opsporingsambtenaar maakt proces-verbaal op van de verwijdering, dat aan de officier van justitie wordt gezonden.

Artikel 29 Niet of niet volledige verwijdering
1. 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.
2. 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.
3. De opsporingsambtenaar maakt proces-verbaal op van de niet of niet volledige verwijdering, dat aan de officier van justitie wordt gezonden.

Hoofdstuk 10 Wijziging overige wet- en regelgeving

Artikel 30 Wijziging Besluit politiegegevens

Aan artikel 4:3, eerste lid, onderdeel a, van het Besluit politiegegevens wordt, onder vervanging van de punt aan het slot door een puntkomma, een onderdeel toegevoegd, luidende:

- De inspectie, bedoeld in artikel 57, eerste lid, van de Wet veiligheidsregio's, met het oog op de uitvoering van de taken, bedoeld in artikel 65, eerste lid, van de Politiewet 2012 en op de uitvoering van een bevel, als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid en 126zpa, eerste lid, van het Wetboek van Strafvordering, door de ambtenaren, bedoeld in artikel 141, onderdeel d, en de personen, bedoeld in artikel 142, eerste lid, onderdeel b, van het Wetboek van Strafvordering.

Hoofdstuk 11 Slotbepalingen

Artikel 31 Inwerkingtreding
Dit besluit treedt in werking op een bij koninklijk besluit te bepalen tijdstip.

Artikel 32 Citeertitel
Dit besluit wordt aangehaald als: Besluit onderzoek in een geautomatiseerd werk.

Lasten en bevelen dat dit besluit met de daarbij behorende nota van toelichting in het Staatsblad zal worden geplaatst.

De Staatssecretaris van Veiligheid en Justitie,

NOTA VAN TOELICHTING

I. Algemeen

1. Inleiding

Het wetsvoorstel computercriminaliteit III (Kamerstukken I 2016/17 34 372, A) versterkt het juridische instrumentarium voor de opsporing en vervolging van computercriminaliteit. Het wetsvoorstel sluit aan bij de snelle ontwikkelingen van de technologie, het internet en de computercriminaliteit en zet de lijn voort die is ingezet met de Wet computercriminaliteit I (1993) en de Wet computercriminaliteit II (2006).

Het wetsvoorstel verleent de officier van justitie de bevoegdheid om, onder strikte voorwaarden, te bevelen dat een opsporingsambtenaar heimelijk en op afstand een geautomatiseerd werk dat in gebruik is bij een verdachte binnendringt en hierin, al dan niet met een technisch hulpmiddel, onderzoek doet met oog op bepaalde onderzoeksdoelen (artikelen 126nba, 126uba en 126zpa van het Wetboek van Strafvordering (Sv)). Deze onderzoeksdoelen betreffen: de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, de uitvoering van een bevel tot stelselmatige observatie, de uitvoering van een bevel tot het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie, de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen en de ontoegankelijkmaking van gegevens. Het op afstand heimelijk binnendringen in een geautomatiseerd werk en het doen van onderzoek is noodzakelijk geworden door de voortschrijdende techniek en het wijdverbreide gebruik van geautomatiseerde werken voor communicatie en de verwerking en opslag van gegevens.

Het wetsvoorstel computercriminaliteit III bevat een aantal grondslagen om bij of krachtens algemene maatregel van bestuur regels te stellen over de uitoefening van deze bevoegdheid. Het betreft ten eerste de grondslag om de inzet van de bevoegdheid voor het doen van onderzoek waarbij het geautomatiseerde werk wordt binnengedrongen met het oog op twee specifieke onderzoeksdoelen, het vastleggen van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen en het ontoegankelijk maken van gegevens, mogelijk te maken bij verdenking van bij algemene maatregel van bestuur aangewezen misdrijven (artikelen 126nba/126uba/126zpa, eerste lid, Sv). Het betreft ten tweede de mogelijkheid om nadere regels te stellen over de deskundigheid en autorisatie van de bij het onderzoek in een geautomatiseerd werk betrokken opsporingsambtenaren, de samenwerking met andere opsporingsambtenaren en de geautomatiseerde vastlegging van gegevens ter uitvoering van een bevel van de officier van justitie (artikel 126nba, achtste lid, onder a en b, Sv, dat van overeenkomstige is verklaard in de artikelen 126uba/126zpa, derde lid, Sv). Ten derde kunnen nadere regels gesteld worden over verschillende aspecten met betrekking tot het doen van onderzoek met een technisch hulpmiddel (artikel 126ee Sv). Het onderhavige besluit geeft uitvoering aan deze bepalingen.

Naast voornoemde delegatiegrondslagen biedt het wetsvoorstel een facultatieve grondslag om bij algemene maatregel van bestuur nadere regels te stellen over de toepassing van de binnendring- en onderzoeksbevoegdheid in gevallen waarin niet bekend is waar de gegevens zijn opgeslagen (artikel 126nba, negende lid, Sv, dat van overeenkomstige toepassing is verklaard in de artikelen 126uba/126zpa, derde lid, Sv). Vooralsnog wordt van deze mogelijkheid geen gebruik gemaakt; de uitwerking hiervan vindt plaats in een Aanwijzing van het College van procureurs-generaal.

2. Toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijkmaken van gegevens

Op grond van het wetsvoorstel computercriminaliteit III mag de bevoegdheid tot het binnendringen in een geautomatiseerd werk en doen van onderzoek met het oog op het vastleggen van gegevens of het ontoegankelijkmaken van gegevens, gelet op de mate van inbreuk die hiermee wordt gemaakt op de persoonlijke levenssfeer, in beginsel uitsluitend worden toegepast bij een verdenking van een misdrijf waarop naar de wettelijke omschrijving een

gevangenisstraf van acht jaren of meer is gesteld. Bij algemene maatregel van bestuur kunnen echter andere misdrijven met een lagere wettelijke strafbedreiging worden aangewezen (artikelen 126nba/126uba/126zpa,eerste lid, onder c, Sv). In hoofdstuk 2 van dit besluit worden deze misdrijven aangewezen. Het betreft misdrijven die worden gepleegd met een geautomatiseerd werk en die een geautomatiseerd werk als doelwit hebben (computercriminaliteit in enge zin) en ernstige commune misdrijven die in toenemende mate met behulp van een geautomatiseerd werk worden gepleegd (gedigitaliseerde criminaliteit) waarbij vaak geen ander aanknopingspunt is voor de opsporing dan via het geautomatiseerde werk waarmee het misdrijf wordt gepleegd. Voor alle aangewezen misdrijven geldt dat er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders.
De toenemende digitalisering van de maatschappij leidt tot nieuwe veiligheidsrisico's en nieuwe mogelijkheden voor criminelen. Het aantal gevallen van computercriminaliteit waarbij computers niet alleen als middel worden ingezet, maar ook doelwit zijn, neemt toe. Van computercriminaliteit gaan grote dreigingen uit, zoals gevaar voor maatschappelijke ontwrichting en voor het vertrouwen in het financieel-economische systeem. Dat risico is onder meer aan de orde bij aanvallen via zogenoemde botnets, waarbij controle op afstand over een aanzienlijk aantal computers tot stand wordt gebracht door deze door middel van gerichte cyberaanvallen te besmetten met kwaadaardige software. Het netwerk van computers dat de botnet vormt kan worden ingezet om een grootschalige cyberaanvallen uit te voeren. Deze aanvallen kunnen vleiden tot ernstige economische schade en tot ontwrichting en vernietiging van vitale infrastructuren, zoals energiecentrales, vervoersnetwerken en overheidsnetwerken.
Ook op andere criminaliteitsterreinen maken criminelen steeds vaker gebruik van digitale technieken. Beroepscriminelen schermen hun activiteiten af door geavanceerde technische middelen in te zetten, wat het opsporingsonderzoek en de bewijsvergaring complex maakt. Ondermijnende criminaliteit, zoals witwassen, fraude en corruptie waarbij criminelen voor hun activiteiten gebruik maken van legale structuren en goederen, verplaatst zich naar het virtuele domein en ontwricht het maatschappelijk vertrouwen. Grootschalige financiële fraude wordt steeds vaker door technisch zeer capabele criminelen gepleegd. Zedenmisdrijven, zoals het verleiden of aanzetten van een minderjarige tot webcamseks, worden steeds vaker online gepleegd. De gevolgen hiervan kunnen indringend, ingrijpend en langdurig zijn en hebben niet alleen impact op het slachtoffer, maar ook op de omgeving en de samenleving als geheel.
Inzet van de binnendring- en onderzoeksbevoegdheid met het oog op het veiligstellen van digitaal bewijs voor voornoemde strafbare feiten en het stopzetten van criminele activiteiten draagt bij aan een effectieve aanpak van cybercrime en aan een veilig digitaal domein. Door de aanwijzing van misdrijven bij algemene maatregel van bestuur kan flexibel worden ingespeeld op de snelle ontwikkelingen in de cybercriminaliteit.

3. De uitvoering van een bevel van de officier van justitie

3.1. Het onderzoek in een geautomatiseerd werk

In dit besluit worden nadere regels gesteld over het onderzoek in een geautomatiseerd werk ter uitvoering van een bevel van de officier van justitie als bedoeld in de artikelen 126nba/uba/zpa Sv. Onder onderzoek in een geautomatiseerd werk wordt in deze toelichting verstaan: het op afstand en heimelijk binnendringen in een geautomatiseerd werk en het verrichten van bepaalde onderzoekshandelingen. Het binnendringen in een geautomatiseerd werk is het voorbereidende deel van het onderzoek. In de daarop volgende onderzoeksfase worden al dan niet met een technisch hulpmiddel onderzoekshandelingen verricht met het oog op bepaalde onderzoekdoelen en gegevens vastgelegd.
Bij het binnendringen in een geautomatiseerd werk kan gebruik worden gemaakt van verschillende technieken. In beginsel wordt gebruik gemaakt van zwakheden bij de gebruiker of kwetsbaarheden die bekend zijn bij de producent van het geautomatiseerde werk of de software. In het uitzonderlijke geval dat gebruik wordt gemaakt van een kwetsbaarheid waarvan aannemelijk is dat die niet bekend is of kan worden verondersteld bekend te zijn, kan de officier van justitie op grond van het wetsvoorstel computercriminaliteit III bevelen, na machtiging van de rechter-commissaris, dat de melding hiervan aan de producent wordt uitgesteld (artikel 126ffa

Sv).
De onderzoeksdoelen met het oog waarop onderzoek kan worden gedaan betreffen:
a. de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;
b. de uitvoering van een bevel tot stelselmatige observatie;
c. de uitvoering van een bevel tot het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie;
d. de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen;
e. de ontoegankelijkmaking van gegevens.
Het bevel van de officier bevat de onderzoeksdoelen met het oog waarop het bevel wordt afgegeven (artikelen 126nba/126uba, tweede lid, onder e, Sv en 126zpa, tweede lid, onder c, Sv). Als het gaat om de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, de vastlegging van gegevens of de ontoegankelijkmaking van gegevens dient het bevel een duidelijke omschrijving van de te verrichten handelingen te bevatten. Ook wordt in het bevel tot uitdrukking gebracht ten aanzien van welk deel van het geautomatiseerde werk en welke categorie van gegevens aan het bevel uitvoering wordt gegeven (artikelen 126nba/126uba/126zpa, tweede lid, onder f, Sv). Verder dient in het bevel een aanduiding van de aard en functionaliteit van het technische hulpmiddel te worden opgenomen (artikelen 126nba/126uba, tweede lid, onder d, en 126zpa, tweede lid, onder b, Sv).
Het wetsvoorstel computercriminaliteit III bevat grondslagen om bij of krachtens algemene maatregel van bestuur regels te stellen over het onderzoek in een geautomatiseerd werk. Het betreft ten eerste de deskundigheid en autorisatie van de bij het binnendringen in een geautomatiseerd werk en het verrichten van onderzoekshandelingen betrokken opsporingsambtenaren en de samenwerking met andere opsporingsambtenaren (artikel 126nba, achtste lid, onder a, Sv, dat van overeenkomstige toepassing wordt verklaard in de artikelen 126uba/126zpa, derde lid, Sv). Het betreft ten tweede verschillende organisatorische, procedurele en technische eisen met betrekking tot de onderzoeksfase waarin gegevens worden vastgelegd. Hierbij gaat het om de geautomatiseerde vastlegging van gegevens ter uitvoering van een bevel van de officier van justitie (artikel 126nba, achtste lid, onder b, Sv, dat van overeenkomstige toepassing wordt verklaard in de artikelen 126uba/126zpa, derde lid, Sv) en diverse aspecten met betrekking tot het doen van onderzoek met behulp van een technisch hulpmiddel (artikel 126ee Sv). De gegevens die tijdens de onderzoeksfase worden vastgelegd kunnen worden gebruikt als bewijs in een strafzaak. Gelet hierop dienen de betrouwbaarheid en integriteit van de gegevens onomstotelijk vast te staan, zowel in het belang van de betrokkene als in het belang van de opsporing. Door eisen te stellen aan onderzoeksproces en de verantwoording hiervan ontstaat een gegevensspoor dat herleidbaar is.
Bij het stellen van regels over het onderzoek in een geautomatiseerd werk is een zekere mate van techniekonafhankelijkheid in acht genomen. Techniek verandert snel en cybercriminaliteit ook. De bestrijding van cybercriminaliteit vraagt om enige flexibiliteit en abstractie van technische details. Het besluit heeft gelet hierop een kaderstellend karakter. Er worden eisen gesteld aan de organisatie, inrichting en controleerbaarheid van het onderzoeksproces. De uitwerking hiervan vindt plaats in de opsporingspraktijk, aan de hand van onder meer OM-aanwijzingen, (keurings)protocollen, handreikingen en mandaatbesluiten. De Inspectie Veiligheid en Justitie (hierna: Inspectie VenJ) houdt toezicht op de naleving van de regels die zijn neergelegd in het Wetboek van Strafvordering en in het onderhavige besluit bij de uitvoering van het onderzoek in een geautomatiseerd werk door opsporingsambtenaren.

3.2 Deskundigheid van opsporingsambtenaren
In hoofdstuk 3 van dit besluit worden regels gesteld over de opsporingsambtenaren die kunnen worden aangewezen voor het onderzoek in een geautomatiseerd werk, hun deskundigheid en de samenwerking tussen opsporingsambtenaren. Door het onderzoek in een geautomatiseerd werk voor te behouden aan opsporingsambtenaren die beschikken over specialistische kennis en vaardigheden op het terrein van ICT kan de kwaliteit en professionaliteit van het onderzoek worden geborgd. Op grond van het besluit kunnen opsporingsambtenaren van de politie, de Koninklijke marechaussee (Kmar) en de bijzondere opsporingsdiensten, en buitengewone

opsporingsambtenaren, bedoeld in artikel 141 Sv onder b, c en d, en 142 Sv door de korpschef worden aangewezen voor het binnendringen in een geautomatiseerd werk en al dan niet met behulp van een technisch hulpmiddel onderzoek doen, indien zij lid zijn van een technisch team.
De politie heeft behoefte aan de bevoegdheid met het oog op de uitvoering van de politietaak, bedoeld in artikel 3 van de Politiewet 2012, namelijk de opsporing van computercriminaliteit en vormen van commune criminaliteit, waarbij geen andere aanknopingspunten zijn voor de opsporing van het misdrijf dan het gebruikte geautomatiseerde werk. Bij de Kmar bestaat de behoefte aan deze bevoegdheid met het oog op de uitvoering van de in artikel 4 van de Politiewet 2012 genoemde politietaken. Bij de FIOD/ECD bestaat behoefte aan deze bevoegdheid met het oog op de strafrechtelijke handhaving van de rechtsorde op bepaalde beleidsterreinen, bedoeld in artikel 3 van de Wet op de bijzondere opsporingsdiensten, te weten de opsporing van fraude en witwassen.
In verband met de behoefte aan specifieke expertise op het gebied van ICT kunnen naast de in artikel 141 Sv bedoelde opsporingsambtenaren ook buitengewone opsporingsambtenaren, bedoeld in artikel 142 Sv, die categoraal zijn aangewezen door de Minister van Veiligheid en Justitie, worden belast met het binnendringen in een geautomatiseerd werk en het doen van onderzoek. Hun opsporingsbevoegdheid strekt zich uit tot de in de categorale aanwijzing aangeduide feiten.
De kwaliteit van een technisch team wordt geborgd door middel van opleidingseisen. Een opsporingsambtenaar kan lid worden van een technisch team, indien hij heeft voldaan aan door de Minister van Veiligheid en Justitie aangewezen kwalificaties, onder meer ten aanzien van kennis op het gebied van ICT. De opleidingseisen worden nader worden uitgewerkt in een ministeriële regeling, die tegelijk met dit besluit in werking treedt.
Gelet op de bijzondere expertise en de technische voorzieningen die nodig zijn voor het onderzoek in een geautomatiseerd werk wordt, in ieder geval gedurende de beginfase, de organisatie van de technische teams centraal belegd binnen de politieorganisatie. Binnen de Landelijke eenheid van de Nationale Politie worden één of meer technische teams ingericht die worden belast met het onderzoek in een geautomatiseerd werk. Deze teams voeren dit onderzoek uit ten behoeve van de politie, de Kmar en de bijzondere opsporingsdiensten.
Incidentele samenwerking tussen leden van een technisch team en andere opsporingsambtenaren is mogelijk, het besluit bevat hiervoor een voorziening. Een opsporingsambtenaar die geen lid is van een technisch team kan worden aangewezen voor het binnendringen in een geautomatiseerd werk en doen van onderzoek, indien hij beschikt over specifieke kennis en vaardigheden die nodig zijn voor de uitvoering van het onderzoek in een geautomatiseerd werk in het kader van een individueel opsporingsonderzoek. Dit staat ter beoordeling van de korpschef. Bij een positieve beoordeling wordt de opsporingsambtenaar op incidentele basis als deelnemer toegevoegd aan een technisch team en wordt hij gedurende het de uitvoering van het bevel begeleid door een lid van een technisch team.

3.3 Taakverdeling en functiescheiding gedurende het opsporingsonderzoek
Gedurende het opsporingsonderzoek, dat plaatsvindt onder het gezag van de officier van justitie, is er sprake van een strikte taakverdeling en functiescheiding. De opsporingsambtenaren die verantwoordelijk zijn voor de voorbereiding en de uitvoering van het onderzoek in een geautomatiseerd werk maken deel uit van een technisch team en behoren niet tot het tactische team. Het tactische team is belast met het uitvoeren van het operationele onderzoek.
De voorbereiding van het onderzoek in een geautomatiseerd werk start met een projectvoorstel van een tactisch team aan de officier van justitie, waarin het onderzoek in een concrete zaak wordt voorgesteld. Een projectplan kan afkomstig zijn van tactische rechercheteams van de politie, van de Kmar of van een bijzondere opsporingsdienst. Het projectplan bevat onder meer een beschrijving van de verdachte, de verdenking, de noodzaak om de onderzoeksbevoegdheid toe te passen en de gewenste resultaten van de toepassing van de bevoegdheid.
Vervolgens vraagt de officier van justitie een technisch team om advies over de haalbaarheid van het onderzoek. Voor de inschatting, beheersing en beperking van de risico’s voor het geautomatiseerde werk is de deskundigheid van de opsporingsambtenaren van het technische team van essentieel belang. Omdat het technische team niet betrokken is bij het operationele onderzoek van het tactische team kan het niet worden beïnvloed bij het maken van afwegingen

met betrekking tot de haalbaarheid en de wijze van uitvoering van het binnendringen in en het verrichten van onderzoekshandelingen in een geautomatiseerd werk.
Het technische team stelt op basis van de intakegegevens en overige relevante gegevens een rapport haalbaarheidsonderzoek op voor de officier van justitie. Hierin wordt het plan van aanpak voor de uitvoering van een onderzoek in het geautomatiseerde werk uitgewerkt. In het rapport wordt onder meer opgenomen welke bevelen nodig zijn en welk technisch hulpmiddel moet worden gebruikt. De officier van justitie gebruikt het rapport haalbaarheidsonderzoek voor het verkrijgen van toestemming voor de inzet van de opsporingsbevoegdheid van het College van procureurs-generaal en de voorafgaande machtiging van de rechter-commissaris.
Het onderzoek in een geautomatiseerd werk kan worden uitgevoerd, zodra daartoe een bevel is afgegeven door de officier van justitie. Het onderzoek is voorbehouden aan de opsporingsambtenaren van een technisch team. In de hoofdstukken 3, 7, 8 en 9 van dit besluit wordt de taakverdeling uitgewerkt.
Na afgifte van een bevel zal een technisch team eerst voorverkenningen uitvoeren. Na analyse daarvan wordt een plan van aanpak voor het binnendringen in het geautomatiseerd werk opgesteld. Het plan van aanpak wordt getest in een proefopstelling.
Het daadwerkelijke onderzoek in het geautomatiseerde werk bestaat uit een voorbereidende fase en een onderzoekfase. De voorbereidende fase omvat het binnendringen in het geautomatiseerde werk volgens het vooraf geschreven plan van aanpak. Hierbij kunnen, zoals hiervoor is aangegeven, verschillende technieken worden gebruikt. De onderzoeksfase bestaat uit het uitvoeren van onderzoekshandelingen in een geautomatiseerd werk. De onderzoekshandelingen kunnen worden verricht met behulp van een technisch hulpmiddel, een softwareapplicatie die gegevens detecteert, registreert en transporteert. Het gebruik van een technisch hulpmiddel is echter niet strikt noodzakelijk: onderzoekshandelingen kunnen ook ad hoc en handmatig plaatsvinden.
De tijdens een onderzoek in een geautomatiseerd werk met een technisch hulpmiddel geregistreerde gegevens worden automatisch vastgelegd op een technische infrastructuur van een technisch team. De vastgelegde gegevens zijn uitsluitend toegankelijk voor de door de korpschef aangewezen ambtenaren. Tactische opsporingsambtenaren hebben geen toegang tot de gegevens. De technische infrastructuur is beveiligd tegen wijziging van de vastgelegde gegevens en kennisneming hiervan door onbevoegden.
De resultaten van het onderzoek worden door het technische team ter beschikking gesteld aan het tactische team. Zo nodig kan het technische team, op basis van technische criteria, zorgdragen voor voorafgaande filtering van de onderzoeksgegevens, zodat binnen de categorieën van gegevens die in het bevel van de officier zijn opgenomen uitsluitend die gegevens die van belang zijn voor het opsporingsonderzoek ter beschikking komen van het tactische team. Bij het opnemen van vertrouwelijke communicatie of het opnemen van telecommunicatie of de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen, zoals email-verkeer, kan niet worden uitgesloten dat gegevens worden verkregen over andere personen die bij de communicatie zijn betrokken. Deze gegevens zijn niet van belang voor het opsporingsonderzoek. In dat geval wordt uitsluitend het email-verkeer waarvan de email-adressen zijn opgenomen op een vooraf opgestelde lijst ter beschikking gesteld van het tactische onderzoeksteam. In het bevel dient melding te worden gemaakt van het feit dat binnen de categorie van gegevens waarvoor het bevel wordt afgegeven uitsluitend die onderzoeksgegevens die van belang zijn voor het opsporingsonderzoek ter beschikking worden gesteld van het tactische team.
De organisatorische scheiding tussen het technische team en het tactische team behoeft de samenwerking tussen de teams gedurende het opsporingsonderzoek niet te belemmeren. De officier van justitie onder wiens leiding het opsporingsonderzoek plaatsvindt vervult hierbij een schakelfunctie. Afhankelijk van het verloop van het onderzoek kan de grens tussen het technisch optreden en het tactisch optreden verschillen, maar de samenwerking zal dusdanig plaatsvinden dat het tactisch team geen enkele invloed kan uitoefenen op het binnendringen in het geautomatiseerde werk en de plaatsing, inzet en verwijdering van een technisch hulpmiddel.

3.4. Vastlegging van gegevens over de uitvoering van een bevel (logging)
De digitale omgeving waarin het onderzoek in een geautomatiseerd werk plaatsvindt maakt het

mogelijk om gedurende de onderzoeksfase doorlopend en automatisch gegevens vast te leggen over de uitvoering van het bevel van de officier van justitie. Hierdoor kan zowel tijdens de uitvoering van bevel van de officier als na afloop hiervan worden vastgesteld of een handeling of bewerking heeft plaatsgevonden die van invloed is op de betrouwbaarheid en integriteit van de vastgelegde gegevens. Deze vorm van elektronische verslaglegging over de uitvoering van een bevel wordt ook wel aangeduid als "logging".
In hoofdstuk 4 van dit besluit worden regels gesteld over de logging. Gedurende de uitvoering van een bevel worden gegevens over onderzoekshandelingen die worden verricht doorlopend en automatisch worden vastgelegd. Onder de logging van de onderzoekshandelingen valt ook de vastlegging van de gegevens die door een technisch hulpmiddel worden geregistreerd, de zogenaamde bewijslogging. De bewijslogging dient plaats te vinden op een technische infrastructuur van een technisch team. Het functioneren van de technische infrastructuur wordt eveneens doorlopend en automatisch gelogd.
De logging dient zodanig te zijn ingericht dat op basis hiervan kan worden vastgesteld of en zo ja wanneer een onregelmatigheid heeft plaatsgevonden, die van invloed is op de betrouwbaarheid en integriteit van de tijdens de onderzoeksfase vergaarde gegevens. Indien dat het geval is, maakt de opsporingsambtenaar van een technisch team hiervan proces-verbaal op, dat aan de officier van justitie wordt gezonden, zodat de officier van justitie en de rechter kunnen bepalen in hoeverre de geconstateerde onregelmatigheid afbreuk doet aan de bewijskracht van de tijdens het onderzoek vastgelegde gegevens.
Het voorbereidende deel van het onderzoek, het binnendringen in een geautomatiseerd werk, behoeft niet te worden gelogd, omdat de handelingen die in dit deel van het onderzoek plaatsvinden niet van invloed zijn op de betrouwbaarheid en de integriteit van het bewijs. Als in een strafzaak vragen zouden rijzen over de wijze van binnendringen, is het aan de rechter om hierover te oordelen. Zo nodig kan een rechter overgaan tot het horen van de betrokken opsporingsambtenaar of kan hij een deskundige raadplegen.
De logging is ten eerste en vooral bedoeld voor de interne controle van de tijdens de onderzoeksfase verrichte handelingen. Daarnaast maakt de bewijslogging het mogelijk om de met een technisch hulpmiddel geregistreerde gegevens achteraf te verantwoorden in een strafzaak. Die verantwoording vindt plaats aan de hand van de processen-verbaal en andere voorwerpen waaraan gegevens kunnen worden ontleend die voor het onderzoek in de zaak van betekenis zijn (artikel 126aa Sv). De officier van justitie houdt bij het samenstellen van het strafdossier rekening met bijzondere belangen zoals de afscherming van methodieken en middelen. Deze belangen kunnen een minder gedetailleerde verantwoording rechtvaardigen. Als bij het verrichten van onderzoekshandelingen in een geautomatiseerd werk gebruik gemaakt wordt van een gekeurd technisch hulpmiddel zal in het proces-verbaal van de inzet worden verwezen naar het keuringsnummer, waardoor de samenstelling van het hulpmiddel ter bescherming van de opsporingsbelangen, kan worden afgeschermd.
Indien tijdens de behandeling van een strafzaak twijfels zouden rijzen over de betrouwbaarheid en de integriteit van het tijdens het onderzoek vergaarde bewijs, kan de rechter de volledige informatie opvragen of een deskundige raadplegen. Hierbij staat de rechter de procedure zoals omschreven in artikel 187d Sv ter beschikking, waarin de rechter-commissaris kan beletten dat antwoorden op vragen ter kennis komen van de verdachte en diens raadsman, indien er een gegrond vermoeden bestaat dat door de openbaarmaking een zwaarwegend opsporingsbelang wordt geschaad.

3.5. Het doen van onderzoek met een gekeurd technisch hulpmiddel

3.5.1. Algemeen

Het doen van onderzoek in een geautomatiseerd werk met het oog op in het bevel van de officier van justitie opgenomen onderzoeksdoelen kan plaatsvinden met een technisch hulpmiddel. Een technisch hulpmiddel is een sofwareapplicatie die functionaliteiten bevat waarmee gegevens kunnen worden gedetecteerd, geregistreerd en getransporteerd. Het transport van de geregistreerde gegevens vindt plaats naar een technische infrastructuur, een opslaglocatie in beheer van de politie, waarop de gegevens worden vastgelegd. De vastgelegde gegevens kunnen als bewijs dienen in een strafzaak. Gelet hierop is het essentieel dat de gegevens betrouwbaar,

integer en herleidbaar zijn.
In de hoofdstukken 5 tot en met 9 van dit besluit worden regels gesteld over technische hulpmiddelen waarmee onderzoek wordt gedaan in een geautomatiseerd werk. Deze regels hebben ten eerste betrekking op de technische eisen waaraan technische hulpmiddelen moeten voldoen en de voorafgaande goedkeuring hiervan. Ten tweede worden regels gesteld over de toegang tot, plaatsing, inzet en verwijdering van technische hulpmiddelen en de vastlegging van met een technisch hulpmiddel geregistreerde gegevens op een technische infrastructuur binnen de politieorganisatie.
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 en een richtmicrofoon.
Op grond van het wetsvoorstel computercriminaliteit III wordt het mogelijk om deze bevoegdheden uit te oefenen nadat heimelijk en op afstand is binnengedrongen in een geautomatiseerd werk. In het onderhavige besluit worden eisen gesteld aan technische hulpmiddelen die worden gebruikt bij de inzet van de bestaande bijzondere opsporingsbevoegdheden in het kader van een onderzoek in een geautomatiseerd werk. Alsdan en 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.

3.5.2. Technische eisen

Om de betrouwbaarheid en integriteit van technische hulpmiddelen, de betrouwbaarheid en integriteit van de hiermee geregistreerde gegevens en de herleidbaarheid van de gegevens te borgen stelt het besluit diverse technische eisen aan een technisch hulpmiddel. Een technisch hulpmiddel moet in staat zijn om gegevens op zodanige wijze te registreren dat de inhoud identiek is aan de in een geautomatiseerd werk gedetecteerde gegevens. Ook moet een technisch hulpmiddel geregistreerde gegevens kunnen voorzien van de datum en tijd van de registratie. Verder moet een technisch hulpmiddel de geregistreerde gegevens kunnen voorzien van een uniek kenmerk, dat bij vastlegging van de gegevens op de opslaglocatie wordt herkend, zodat de herkomst van de gegevens te allen tijde kan worden vastgesteld.
De integriteit van de met een technisch hulpmiddel vergaarde gegevens, waarmee gedoeld wordt op de zekerheid dat een gegeven niet is gewijzigd of hiervan onbevoegd kennis is genomen, wordt geborgd door eisen te stellen aan de beveiliging van een technisch hulpmiddel en de door een technisch hulpmiddel geregistreerde en getransporteerde gegevens. Naast technische eisen aan het technische hulpmiddel stelt het besluit ook eisen met betrekking tot de kwaliteit van de technische infrastructuur waarop de met een technisch hulpmiddel geregistreerde gegevens worden vastgelegd.
Om de rechtmatigheid van de inzet van een hulpmiddel te kunnen garanderen vereist het besluit dat een technisch hulpmiddel zodanig is ingericht dat het mogelijk is om uitsluitend de in het bevel van de officier van justitie aangegeven functionaliteit(en) van een technisch hulpmiddel in te schakelen en uitsluitend gegevens te detecteren en registeren ten behoeve van deze functionaliteit.

3.5.3. Keuring

Voordat een technisch hulpmiddel wordt ingezet, dient het goedgekeurd te worden door een keuringsdienst. Als bij het verrichten van onderzoekshandelingen gebruik wordt gemaakt van een goedgekeurd hulpmiddel mag er vanuit worden gegaan dat aan de wettelijke eisen is voldaan.
Een onderdeel van de Landelijke eenheid van de Nationale Politie, de keuringsdienst van de Dienst landelijke operationele samenwerking, is momenteel belast met de keuring van de traditionele technische hulpmiddelen die worden ingezet bij stelselmatige observatie, het opnemen van vertrouwelijke communicatie en het opnemen van telecommunicatie. Deze keuringsdienst wordt

eveneens aangewezen voor de keuring van technische hulpmiddelen die gebruikt worden voor het verrichten van onderzoekshandelingen in een geautomatiseerd werk. Het besluit bevat de mogelijkheid om andere organisaties als keuringsdienst aan te wijzen. Om de kwaliteit en consistentie van de keuring te waarborgen stelt een keuringsdienst een keuringsprotocol op. Een keuringsprotocol behoeft de voorafgaande goedkeuring van de Minister van Veiligheid en Justitie. Van de keuring wordt een rapport opgemaakt, waarin bij goedkeuring wordt vermeld dat het technische hulpmiddel voldoet aan de technische eisen die het besluit stelt. Bij de goedkeuring wordt aan het technische hulpmiddel een referentienummer toegekend. Dit referentienummer kan gedurende het opsporingsonderzoek worden gebruikt om het hulpmiddel aan te duiden zodat de samenstelling van het hulpmiddel, ter bescherming opsporingsbelangen, kan worden afgeschermd. De mogelijkheid bestaat om sofwareapplicaties van verschillende producenten te betrekken of deze zelf binnen de politieorganisatie te (laten) ontwerpen, mits aan de wettelijke vereisten voor keuring wordt voldaan. De ervaring leert dat producenten van software veelvuldig gebruik maken van softwareupdates ter verbetering van het product. Indien de werking van een technisch hulpmiddel of een onderdeel hiervan door een softwareupdate zodanig wijzigt dat niet meer wordt voldaan aan de technische eisen vindt herkeuring plaats van het technische hulpmiddel of van het gewijzigde onderdeel hiervan.

3.6. Het doen van onderzoek zonder goedgekeurd technisch hulpmiddel
Het is denkbaar dat bij het verrichten van onderzoekshandelingen technische hulpmiddelen, worden gebruikt die zich naar hun aard niet lenen 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. Indien het onderzoeksbelang dit dringend vordert kan de officier van justitie bepalen dat een niet gekeurd technisch hulpmiddel wordt ingezet. Na afloop van het onderzoek kan alsnog goedkeuring plaatsvinden, tenzij de aard van het hulpmiddel zich naar het oordeel van de officier hiertegen verzet. De betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens zullen dan op andere wijze moeten worden geborgd. Ook als onderzoekshandelingen zonder goedgekeurd hulpmiddel plaatsvinden worden de verrichte onderzoekshandelingen en het functioneren van de technische infrastructuur gelogd.
In bepaalde gevallen kunnen onderzoekshandelingen beter handmatig worden verricht, zodat het gebruik van een technisch hulpmiddel achterwege kan blijven. Hierbij kan worden gedacht aan de situatie dat gegevens direct na het binnendringen kunnen worden ingezien of worden overgenomen ten behoeve van het vaststellen van de identiteit van het geautomatiseerde werk. De vraag of de inzet van een technisch hulpmiddel noodzakelijk is, is onder meer afhankelijk van de aard van de inzet, de aard van het geautomatiseerde werk en de vraag of de gegevens zonder inzet van een technisch hulpmiddel als rechtmatig bewijs kunnen worden aangemerkt. De advisering van de officier van justitie hieromtrent vindt plaats door het technische team.

4. Bewaartermijnen
De gegevens die al dan niet met een technisch hulpmiddel ter uitvoering van een bevel van de officier worden vastgelegd vallen onder een gedifferentieerd regime wat betreft de bewaartermijnen. De processen-verbaal en andere voorwerpen waaraan gegevens kunnen worden ontleend die zijn verkregen door observatie, het opnemen van vertrouwelijke communicatie en het opnemen van telecommunicatie met behulp van een technisch hulpmiddel worden door de officier van justitie, voor zover die niet bij de processtukken zijn gevoegd, ter beschikking gehouden van het onderzoek (artikel 126cc, eerste lid, Sv). Zodra twee maanden zijn verstreken nadat de zaak is geëindigd en de notificatie, bedoeld in artikel 126bb Sv is verricht, doet de officier van justitie de processen-verbaal en andere voorwerpen vernietigen. De procedure is uitgewerkt in het Besluit bewaren en vernietigen niet-gevoegde stukken.
De gegevens die zijn verkregen door de toepassing van de bevoegdheid met het oog op andere onderzoekshandelingen en al dan niet met een technisch hulpmiddel zijn gegenereerd vallen onder het regime van de Wet politiegegevens (Wpg). Afhankelijk van het specifieke doel van de verwerking kan de bewaartermijn verschillen. Doorgaans zullen de gegevens worden verwerkt met het oog op de ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval (artikel 9, eerste lid, Wpg). Zodra de gegevens niet langer noodzakelijk zijn

voor het doel van het onderzoek, worden deze verwijderd of gedurende een periode van maximaal een half jaar bewaard teneinde te bezien of zij aanleiding geven tot een nieuw onderzoek als bedoeld in het eerste lid of een nieuwe verwerking als bedoeld in artikel 10 Wpg. Na afloop van deze termijn worden de gegevens verwijderd (artikel 9, derde lid, Wpg). De situatie dat de gegevens niet langer noodzakelijk zijn voor het doel van het onderzoek zal – in geval van een opsporingsonderzoek dat heeft geleid tot een vervolging – pas optreden op het moment dat de rechter ten aanzien van de zaak onherroepelijk heeft beslist. Als de zaak niet is opgelost en niet is ingezonden aan het openbaar ministerie, wordt het onderzoek meestal wel voortgezet maar op een minder intensief niveau. De gegevens kunnen in dat geval nodig blijven voor het vervolg van het onderzoek en voor het geval dat het team opnieuw bijeen wordt geroepen vanwege nieuwe aanknopingspunten. De gegevens blijven dan doorgaans nodig voor het doel van het onderzoek tot uiterlijk het moment waarop de feiten, waar het onderzoek zich op richt zijn verjaard. Daarna kunnen de gegevens niet meer nodig zijn voor het doel van het onderzoek en moeten zij worden verwijderd (Kamerstukken II 2005/06, 30 327, nr. 3, blz. 45/46). De verwijderde politiegegevens worden gedurende een termijn van vijf jaren bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen en vervolgens gearchiveerd of vernietigd.
De logging wordt bewaard met het oog op de verantwoording van de verrichte onderzoekshandelingen en het functioneren van de technische infrastructuur waarop de met een technisch hulpmiddel geregistreerde gegevens worden vastgelegd. Deze gegevens worden verwerkt met het oog op de opsporing van strafbare feiten en vallen eveneens onder de reikwijdte van de Wpg. Dit betekent dat de gegevens doorgaans moeten worden verwijderd zodra deze niet langer noodzakelijk zijn voor het doel van het onderzoek. Dit geldt in zijn algemeenheid voor de logging van gegevens, dus ook voor de logging met betrekking tot het verrichten van onderzoekshandelingen met het oog op observatie, het opnemen van vertrouwelijke communicatie of het opnemen van telecommunicatie met behulp van een technisch hulpmiddel.

5. Systeemtoezicht
De Inspectie VenJ houdt toezicht op het functioneren van het wettelijke systeem rond de uitvoering van een bevel tot onderzoek in een geautomatiseerd werk. De Inspectie VenJ is belast met het toezicht op de taakuitvoering door de politie op grond van artikel 57, eerste lid, onderdeel d, van de Wet veiligheidsregio's. Artikel 126nba, zevende lid, Sv, (dat van overeenkomstige toepassing is verklaard in de artikelen 126uba/126zpa, derde lid, Sv) bepaalt dat het door de Inspectie uitgeoefende toezicht zich mede uitstrekt over de uitvoering van een bevel tot het binnendringen in een geautomatiseerd werk en onderzoek doen door de opsporingsambtenaren van de bijzondere opsporingsdiensten, bedoeld in artikel 141, onderdeel d, Sv en de buitengewone opsporingsambtenaren, bedoeld in artikel 142, eerste lid, onderdeel b, Sv.
Het toezicht van de Inspectie VenJ heeft betrekking op de naleving van de wettelijke regels die zijn neergelegd in het Wetboek van Strafvordering en het onderhavige besluit en omvat zowel de gevallen die in het kader van de door de officier van justitie ingestelde strafvervolging van een verdachte aan het oordeel van de rechter worden voorgelegd als gevallen die niet tot strafvervolging leiden. Concreet zal het systeemtoezicht van de Inspectie VenJ betrekking hebben op aspecten als de autorisatie van de opsporingsambtenaren voor handelingen ter uitvoering van een bevel van de officier van justitie, de expertise en kennis van de betrokken opsporingsambtenaren, de logging van gegevens over de uitvoering van een bevel, de inzet van een technisch hulpmiddel, de vastlegging van de met een technisch hulpmiddel geregistreerde gegevens op een technische infrastructuur, de beveiliging van gegevens en het gebruik van de gegevens, inclusief de bewaring en vernietiging daarvan. De inspecteurs beschikken over de bevoegdheden voor het toezicht op de naleving op grond van de Algemene wet bestuursrecht (Awb) (artikel 57, derde lid, Wet veiligheidsregio's, artikelen 5:12 tot en met 5:20 Awb).
De Inspectie VenJ werkt op basis van een werkprogramma dat jaarlijks wordt vastgesteld. Voor de invulling van het toezicht zullen naar verwachting de volgende vormen worden gebruikt: doorlichting, thematisch onderzoek en incidentonderzoek. Na afloop van een onderzoek wordt een rapport opgesteld. Het vastgestelde inspectierapport wordt aan de Minister van Veiligheid en Justitie aangeboden en door de Minister openbaar gemaakt.

Om de verhouding tussen taakuitoefening door de Inspectie VenJ en het verstrekkingenregime van de Wpg te verhelderen past dit besluit het Besluit politiegegevens aan. Daarmee wordt de verplichting tot verstrekking van politiegegevens in het kader van de toezichthoudende taak van de Inspectie VenJ expliciet wettelijk vastgelegd.

6. Europeesrechtelijke aspecten

Het vrij verkeer van goederen en diensten binnen de Europese Unie brengt met zich dat lidstaten in de nationale wetgeving geen eisen aan goederen en keuringen mogen stellen die leiden tot beperking van het vrije verkeer tussen de lidstaten. De technische eisen die in het besluit worden gesteld aan de technische hulpmiddelen waarmee onderzoekshandelingen in een geautomatiseerd werk worden verricht en de voorgeschreven keuring kunnen worden aangemerkt als een inbreuk op het vrije verkeer. Daarom is een wederzijdse erkenningsclausule opgenomen voor hulpmiddelen en keuringen.

Dit besluit biedt de mogelijkheid om naast de keuringsdienst van de Landelijke eenheid van de Nationale Politie andere keuringsdiensten aan te wijzen voor de keuring van technische hulpmiddelen. Als van deze mogelijkheid gebruik wordt gemaakt, dan worden hierover bij ministeriële regeling regels gesteld. Afhankelijk van de gekozen systematiek kan sprake zijn van een dienst van algemeen economisch belang of een niet-economische dienst van algemeen belang. Bij het opstellen van de ministeriële regeling zal dan toetsing plaatsvinden aan de daarvoor geldende EU-kaders, zoals de richtlijn 2006/123/EG van het Europees Parlement en de Raad van de Europese Unie van 12 december 2006 betreffende diensten op de interne markt (PbEU L 376) (Dienstenrichtlijn).

Het ontwerpbesluit is op **PM** gemeld aan de Europese Commissie onder richtlijn 2015/1535/EU (richtlijn van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende diensten van de informatiemaatschappij (codificatie van richtlijn 98/34/EG en 98/48/EG, ‘de notificatierichtlijn’)).

7. Financiële gevolgen

Het is de verwachting dat de nieuwe opsporingsbevoegdheid niet leidt tot structurele toename van de totale opsporingsinspanning. De uitvoering van het onderzoek in een geautomatiseerd werk vindt plaats bij een onderdeel van de Landelijke eenheid van de Nationale Politie. De Nationale Politie ontvangt jaarlijks een bijzondere bijdrage van €13,8 miljoen voor de digitale professionalisering en vernieuwing van de organisatie, onder meer ter bestrijding van cybercrime. De aanschaf en implementatie van ICT-hulpmiddelen ter voorbereiding op de invoering van het onderzoek in een geautomatiseerd werk geschiedt uit dit budget. De personeels- en IV-capaciteit en de structurele kosten voor beheer en onderhoud komen ten laste van de algemene begroting van de politie. Aan de begroting van de politie is bij najaarsnota structureel een bedrag toegevoegd voor de aanpak van cybercrime. Voor 2017 bedraagt de bijdrage € 1,4 miljoen, voor 2018 en verdere jaren € 1,5 miljoen. Deze bijdragen zijn bedoeld voor de versterking van personele en materiële capaciteit door opleiding en ICT-middelen en – tools. Voor zover het besluit leidt tot werklastgevolgen bij het openbaar ministerie en de rechtspraak worden de kosten gedekt binnen het reguliere budget.

8. Adviezen

PM.

II. Artikelsgewijze toelichting

Hoofdstuk 1 Algemene bepalingen

Artikel 1 Definities
Artikel 1 bevat een definitiebepaling van een aantal relevante begrippen in het besluit. Het meest gebruikte begrip is het begrip "technisch hulpmiddel" (onderdeel g). Hieronder wordt verstaan: softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel. Onder bevel (onderdeel a) wordt verstaan: een bevel van de officier van justitie als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid, Sv. Op grond van het wetsvoorstel computercriminaliteit III kan het doen van onderzoek al dan niet met een technisch hulpmiddel plaatsvinden. Van doen van onderzoek zonder technisch hulpmiddel is sprake als bij het onderzoek geen gebruik wordt gemaakt van software die gegevens detecteert, registreert en transporteert.
Een "onderzoekshandeling" is een handeling van een opsporingsambtenaar van een technisch team die met het oog op een onderzoeksdoel als bedoeld in de artikelen 126nba, eerste lid, a tot en met e, 126uba, eerste lid, onder a tot en met e, en 126zpa, eerste lid, Sv wordt verricht ter uitvoering van een bevel. Gedurende de uitvoering van een bevel vindt doorlopende en automatische vastlegging van gegevens plaats over de verrichte onderzoekshandelingen.
Met de definitie van "technische infrastructuur" (onderdeel h) wordt gedoeld op de opslaglocatie voor de met een technisch hulpmiddel geregistreerde gegevens. Uit deze definitie, in combinatie met de definitie van "technisch team" (onderdeel i), vloeit voort dat de vastlegging van geregistreerde gegevens dient plaats te vinden op een technische voorziening binnen de politieorganisatie. Deze eis wordt gesteld om de betrouwbaarheid en integriteit van de door een technisch hulpmiddel geregistreerde gegevens te borgen en onbevoegde wijziging of kennisneming hiervan te voorkomen. In de definitie van "technisch team" is de centrale plaatsing van dit team als herkenbaar onderdeel binnen de Landelijke eenheid tot uitdrukking gebracht.

Hoofdstuk 2 Toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijkmaken van gegevens

Artikel 2 Aanwijzing misdrijven
In dit artikel wordt een aantal ernstige misdrijven aangewezen waarvoor de binnendring- en onderzoeksbevoegdheid met het oog op de vastlegging van gegevens en ontoegankelijkmaking van gegevens kan worden toegepast. Het betreft misdrijven die met of met behulp van een geautomatiseerd werk worden gepleegd waarop een wettelijke strafbedreiging van minder dan acht jaren gevangenisstraf staat, maar die niettemin dermate ernstig zijn dat er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders.
De eerste categorie van misdrijven die worden aangewezen zijn computermisdrijven in enge zin, waarbij het misdrijf met een geautomatiseerd werk wordt gepleegd of betrekking heeft op een geautomatiseerd werk. Deze misdrijven zijn verspreid opgenomen in het Wetboek van Strafrecht. Het betreft in de eerste plaats de strafbaarstellingen van computervredebreuk, waaronder het gebruik van een botnet (artikelen 138ab Sr) en van ernstige "spam" of "bombing" (artikel 138b Sr), die zijn opgenomen in de Titel over de misdrijven tegen de openbare orde (Boek II, Titel V). Het wetsvoorstel computercriminaliteit III voegt hieraan strafbaarstellingen inzake het overnemen en helen van gegevens (artikelen 138c en 139g) toe, deze misdrijven worden eveneens aangewezen. Ook de bepalingen uit deze Titel over het aftappen of opnemen van gegevens (artikel 139d) zijn relevant, voor zover het gaat om het aftappen en opnemen van computergegevens. Daarnaast gaat het om de artikelen 161, eerste lid, 161bis en 161sexies, waarin de vernieling van geautomatiseerde werken en werken voor de vitale infrastructuur strafbaar is gesteld. Deze strafbepalingen maken onderdeel uit van Boek II, Titel VII, misdrijven waardoor de algemene veiligheid van personen of goederen in gevaar wordt gebracht. Ook Boek II, Titel XXVII (vernieling) bevat enkele computermisdrijven. Het betreft de artikelen 350a, 350c en 350d (beschadiging van computergegevens), deze misdrijven worden eveneens aangewezen voor de toepassing van de bevoegdheid.

De tweede categorie van misdrijven betreft ernstige commune misdrijven met een grote maatschappelijke impact die in toenemende mate worden gepleegd met behulp van een geautomatiseerd werk. Bij deze vormen van gedigitaliseerde criminaliteit is het geautomatiseerde werk waarvan gebruik wordt gemaakt bij het plegen van het misdrijf vaak het enige aanknopingspunt voor de opsporing. Aangewezen worden diverse ernstige ondermijnende misdrijven die strafbaar zijn gesteld in verschillende titels van het Wetboek van Strafrecht (Boek II, Titel V, misdrijven tegen de openbare orde, Titel VIII, misdrijven tegen het openbaar gezag Titel XII, valsheid in geschrifte, Titel XXXA Witwassen), te weten de rekrutering voor terrorisme (artikelen 131 en 205 Sr), het deelnemen aan een criminele organisatie (artikel 140 Sr), mensensmokkel (artikel 197a Sr) corruptie (artikelen 177, 179, 182, 200 Sr), fraude (artikelen 225, 226, 227, 231, 231a, 232 Sr) en witwassen (artikel 420bis Sr).
Ook spionagemisdrijven (artikelen 98, 98c Sr), waarmee een inbreuk wordt gemaakt op de veiligheid van de staat (Boek II, Titel I), worden in toenemende mate langs digitale weg gepleegd. Hetzelfde geldt voor het plaatsen van een valse bom of het doen van een valse bommelding (artikel 142 Sr, Boek II, Titel V), waarmee een ernstige inbreuk wordt gemaakt op de openbare orde en waardoor overheidsdiensten in hun functioneren worden belemmerd. Ook zedenmisdrijven met minderjarigen (artikelen 240b, 247, 248a en 248e Sr, Boek II, Titel XIV,) en het misdrijf stalking (artikel 285b Sr, Titel XVIII), waarmee een inbreuk wordt gemaakt op de seksuele dan wel persoonlijke levenssfeer van een ander, vinden steeds vaker online plaats.
Voor een effectieve bestrijding van voornoemde ernstige strafbare feiten zijn digitale opsporingsmogelijkheden onontbeerlijk. Door toepassing van de bevoegdheid met het oog het vastleggen dan wel ontoegankelijkmaken van gegevens kan digitaal bewijs worden vergaard voor het gepleegde strafbare feit en kunnen criminele activiteiten worden beëindigd.

Hoofdstuk 3 Deskundigheid van opsporingsambtenaren

Artikel 3 Lidmaatschap van een technisch team
Artikel 3 regelt dat het binnendringen in een geautomatiseerd werk en het al dan niet met een technisch hulpmiddel onderzoek doen is voorbehouden aan de door de korpschef aangewezen opsporingsambtenaren van de politie, de Kmar, de bijzondere opsporingsdiensten en buitengewoon opsporingsambtenaren, bedoeld in artikel 141 Sv onder b, c en d, en 142 Sv, die lid zijn van een technisch team. Door het onderzoek in een geautomatiseerd werk voor te behouden aan deskundigen van een technisch team wordt de kwaliteit en de professionaliteit van dit onderzoek geborgd.
Binnen de Landelijke eenheid worden één of meer technische teams ingericht die kunnen worden belast met het binnendringen in een geautomatiseerd werk en het verrichten van onderzoekshandelingen. Deze teams voeren het onderzoek in een geautomatiseerd werk uit ten behoeve van de politie, de Kmar en de bijzondere opsporingsdiensten. Opsporingsambtenaren kunnen lid worden van een technisch team, indien zij voldoen aan door de Minister van Veiligheid en Justitie bepaalde kwalificaties. De kwalificaties waaraan een lid van een technisch team moet voldoen worden uitgewerkt in een ministeriële regeling. Een lid van een technisch team zal onder meer moeten beschikken over voldoende kennis en vaardigheden met betrekking tot ICT en kennis over het juridisch kader waarbinnen het onderzoek in een geautomatiseerd werk plaatsvindt. Ook vaardigheden met betrekking het opmaken van processen-verbaal zullen deel uitmaken van de opleidingseisen. Het lidmaatschap van een technisch team is een specialistische functie, het doorlopen van de volledige politieopleiding is gelet hierop niet nodig. De leden van het technische team zullen naar verwachting vooral zogenaamde zij-instromers zijn.
De opsporingsambtenaren van een technisch team behoren niet tot het tactische team dat is belast met het tactische onderzoek. Deze functiescheiding vermindert het risico op tunnelvisie.
Het toezicht op de naleving van de deskundigheidseisen maakt onderdeel uit van het systeemtoezicht van de Inspectie VenJ.

Artikel 4 Incidentele samenwerking
Artikel 4 biedt een voorziening voor de incidentele samenwerking tussen opsporingsambtenaren. Een opsporingsambtenaar van de politie, de Kmar, de bijzondere opsporingsdiensten of een buitengewoon opsporingsambtenaar die geen lid is van een technisch team kan door de korpschef

worden aangewezen voor het binnendringen in een geautomatiseerd werk en doen van onderzoek als hij beschikt over specifieke kennis en vaardigheden die nodig zijn voor de uitvoering van een bevel in een individueel opsporingsonderzoek. Hierbij kan worden gedacht aan de situatie dat een opsporingsambtenaar van een bijzondere opsporingsdienst met specifieke kennis op het gebied van digitale fraude wordt toegevoegd aan een technisch team in verband met gewenste technische expertise op dit gebied in een bepaald onderzoek. De korpschef beoordeelt of een opsporingsambtenaar beschikt over voldoende specifieke kennis en vaardigheden voor het onderzoek. De korpschef kan deze bevoegdheid desgewenst mandateren aan het hoofd van het onderdeel van de Landelijke eenheid waar de technische teams worden ondergebracht. Om de kwaliteit en professionaliteit van het onderzoek te borgen bepaalt artikel 4 dat een opsporingsambtenaar die op ad hoc basis deelneemt aan een technisch team gedurende de uitvoering van het onderzoek wordt begeleid door een lid van een technisch team.

Hoofdstuk 4 Geautomatiseerde vastlegging van gegevens over de uitvoering van een bevel (logging)

Artikelen 5 tot en met 7 Vastlegging van gegevens, vaststelling onregelmatigheden en betrouwbaarheid en integriteit gegevens

Artikel 5 bepaalt dat alle onderzoekshandelingen die gedurende de uitvoering van een bevel van de officier van justitie worden verricht en het functioneren van de technische infrastructuur van een technisch team doorlopend en geautomatiseerd worden vastgelegd. Dit wordt ook wel logging genoemd. Er wordt gelogd op het niveau van de autorisatie, op het niveau van de verrichte onderzoekshandelingen en op het niveau van de werking van het systeem. Ter aanvulling op de automatische logging kan ook handmatige verslagging plaatsvinden over de uitvoering van een bevel, bijvoorbeeld in de vorm van een journaal. Zowel onderzoekshandelingen die met een technisch hulpmiddel plaatsvinden als onderzoekshandelingen waarbij de inzet van een technisch hulpmiddel achterwege blijft worden gelogd. Hierdoor zal steeds inzichtelijk zijn welke handelingen gedurende de onderzoeksfase door het technische team zijn verricht en is controle op de uitvoering van het bevel van de officier van justitie mogelijk.

Onder de logging van de onderzoekshandelingen valt ook de vastlegging van gegevens van door een technisch hulpmiddel geregistreerde gegevens, de zogenaamde bewijslogging. De vastlegging van de geregistreerde gegevens dient ingevolge artikel 24 van dit besluit plaats te vinden op een technische infrastructuur van een technisch team. Op grond van artikel 6 moet zowel tijdens de onderzoeksfase als achteraf vastgesteld kunnen worden of zich gedurende de uitvoering van het bevel een onregelmatigheid heeft voorgedaan, die van invloed is op de betrouwbaarheid van de op de technische infrastructuur vastgelegde gegevens. Indien dat het geval is, wordt hiervan proces-verbaal opgemaakt, dat aan de officier van justitie wordt gezonden.

In artikel 7 worden eisen gesteld ter borging van de kwaliteit van de logging. De gelogde gegevens mogen niet mogen worden bewerkt, zijn uitsluitend toegankelijk voor daartoe door de korpschef geautoriseerde ambtenaren en moeten beveiligd zijn tegen wijziging of onbevoegde kennisneming. Het voorbereidende deel van het onderzoek, het binnendringen in een geautomatiseerd werk, behoeft niet te worden gelogd, omdat de handelingen die in dit deel van het onderzoek plaatsvinden niet van invloed zijn op de betrouwbaarheid en de integriteit van het bewijs.

De gelogde gegevens moeten worden verwijderd zodra deze niet langer noodzakelijk zijn voor het doel van het onderzoek. Toezicht op de naleving van de regels over de logging vindt plaats door de Inspectie VenJ.

De logging dient ten eerste en vooral ter interne controle van de uitvoering van het bevel van de officier van justitie. Daarnaast kunnen door middel van de logging de verrichte onderzoekshandelingen worden verantwoord. De gedurende een opsporingsonderzoek verrichte opsporingshandelingen en de hiermee vergaarde gegevens worden neergelegd in een proces-verbaal (artikel 152 Sv). De officier van justitie voegt de processen-verbaal en andere voorwerpen die gegevens bevatten die voor het onderzoek in de zaak van betekenis zijn bij de processtukken (artikel 126aa Sv). In het geval in een strafzaak twijfel ontstaat over de wijze waarop de gegevens zijn verkregen of over de betrouwbaarheid van de verkregen gegevens, bijvoorbeeld op grond van een verweer van de verdachte of diens raadsman, kan aan de hand van de logging hierover verantwoording worden afgelegd.

Hoofdstuk 5 Technische eisen met betrekking tot een technisch hulpmiddel

Hoofdstuk 5 bevat de technische eisen waaraan een technisch hulpmiddel moet voldoen. Als bij de uitvoering van een bevel van de officier van justitie gebruik wordt gemaakt van een goedgekeurd technisch hulpmiddel mag er vanuit worden gegaan dat aan de wettelijke eisen is voldaan. In hoofdstuk 6 van dit besluit worden regels gesteld over de keuringsprocedure.

Artikelen 8 en 9 Gerichte werking, gerichte detectie en registratie
De artikelen 8 en 9 stellen eisen aan de inrichting en werking van een technisch hulpmiddel. De eerste eis betreft de gerichte werking van een technisch hulpmiddel (artikel 8). Het verrichten van onderzoekshandelingen met behulp van een technisch hulpmiddel in een geautomatiseerd werk vindt plaats binnen de grenzen van het bevel van de officier van justitie. Het bevel bevat (onder meer) een aanduiding van de aard en functionaliteit(en) van het technische hulpmiddel. Softwareapplicaties met behulp waarvan onderzoekshandelingen in een geautomatiseerd werk worden verricht beschikken naar hun aard vaak over verschillende functionaliteiten. Om te waarborgen dat de onderzoekshandelingen binnen de grenzen van het bevel van de officier van justitie worden verricht, bepaalt artikel 8 van het besluit dat een technisch hulpmiddel zodanig is ingericht dat de werking ervan kan worden beperkt tot de in het bevel vermelde functionaliteit of functionaliteiten. Hierbij kan worden gedacht aan functionaliteiten als het opnemen van geluid, het maken van screenshots, het vastleggen van toetsaanslagen of het doorzoeken van bepaalde bestandsmappen en het vastleggen van gegevens hieruit.
Bij de keuring wordt getoetst of een technisch hulpmiddel instellingen bevat waarmee de werking van een technisch hulpmiddel kan worden beperkt tot een bepaalde functionaliteit of tot bepaalde functionaliteiten. De keuringsdienst stelt bij de keuring een handleiding op voor het gebruik van een hulpmiddel, waarin wordt aangegeven welke instellingen bij gebruik van een technisch hulpmiddel voor een bepaalde functionaliteit moeten worden aangevinkt. Bij de plaatsing van een technisch hulpmiddel wordt hierover verantwoording afgelegd in een proces-verbaal (artikel 22 van het besluit).
De in artikel 9 gestelde eis ligt in het verlengde van artikel 8. Een technisch hulpmiddel moet in staat zijn uitsluitend gegevens te detecteren en te registreren ten behoeve van de in het bevel vermelde functionaliteit of functionaliteiten. De eis in artikel 8, tweede lid, is overgenomen uit artikel 11 van het Besluit technische hulpmiddelen strafvordering en heeft betrekking op technische hulpmiddelen die worden ingezet ten behoeve van het opnemen van telecommunicatie. Het technische hulpmiddel dient in staat te zijn om uitsluitend van een vooraf opgegeven nummer de telecommunicatie op te nemen.

Artikelen 10, 11 en 12 Betrouwbaarheid en integriteit, herleidbaarheid, datum tijd
De in de artikelen 10 tot en met 12 gestelde technische eisen strekken ertoe de betrouwbaarheid, integriteit en herleidbaarheid van de met een technisch hulpmiddel geregistreerde gegevens te garanderen. Een technisch hulpmiddel detecteert gegevens in het geautomatiseerde werk, registreert de gedetecteerde gegevens en transporteert de gegevens naar de technische infrastructuur van het technisch team. Omdat de met een technisch hulpmiddel vastgelegde gegevens kunnen dienen als bewijs in een strafzaak, is het van essentieel belang dat de betrouwbaarheid en integriteit van de gegevens vaststaan en dat de gegevens herleidbaar zijn. Dit kan allereerst worden bereikt door te eisen dat de inhoud van de gegevens die door een technisch hulpmiddel worden geregistreerd identiek is aan de inhoud van de gegevens die worden gedetecteerd in het geautomatiseerde werk. Dit wordt geregeld in artikel 10, eerste lid. Met gedetecteerde gegevens wordt gedoeld op de gegevens die een technisch hulpmiddel waarneemt in een te onderzoeken geautomatiseerd werk. Een voorbeeld is het lezen van een bestand op een computer van een verdachte. Van geregistreerde gegevens is sprake als het technische hulpmiddel de gedetecteerde gegevens overneemt uit het geautomatiseerde werk. De eis heeft betrekking op de inhoud van de gegevens. Niet is van belang op welke wijze de metadata worden geregistreerd. Als de in het geautomatiseerde werk gedetecteerde gegevens door het technische hulpmiddel in een ander format worden geregistreerd (een voorbeeld is een SMS die op een mobiel apparatuur

als PDU is opgeslagen en die door een technisch hulpmiddel in ASCII coding wordt geregistreerd) zal na de vastlegging van de gegevens op de technische infrastructuur de omzetting van het format met een applicatie moeten worden uitgelokt. Bij de keuring zal worden gekeurd of het technische hulpmiddel een voorziening bevat om de inhoud van de geregistreerde gegevens zichtbaar te maken.
Artikel 10, tweede lid, vereist dat een technisch hulpmiddel beveiligd is tegen wijziging van de werking ervan en tegen de wijziging en kennisneming van geregistreerde gegevens door onbevoegden. Hierbij dient te worden opgemerkt dat in de ICT nooit volledige garanties tegen beïnvloeding van buitenaf kunnen worden gegeven. Wel kan die beïnvloeding zo moeilijk mogelijk worden gemaakt. Bij de keuring wordt getoetst of er beveiligingsmaatregelen aanwezig zijn die beïnvloeding van een technisch hulpmiddel van buitenaf naar de stand van de techniek zo goed mogelijk tegengaan. Hierbij kan worden gedacht aan het aanwezig zijn van authenticatiemaatregelen voor de communicatie met het technische hulpmiddel.
Als een technisch hulpmiddel niet constant met de technische infrastructuur communiceert – het zal in de praktijk regelmatig voorkomen dat een verdachte offline is - dan kan een vorm van tussenopslag nodig zijn. Gelet hierop dient een technisch hulpmiddel beveiligd te zijn tegen wijziging van geregistreerde gegevens en kennisneming hiervan door onbevoegden. Hierbij kan naar de huidige stand van de techniek worden gedacht aan maatregelen als versleuteling van de gegevens met een digitale handtekening. Hierdoor wordt bereikt dat de door een technisch hulpmiddel geregistreerde gegevens na de registratie niet meer leesbaar en toegankelijk zijn.
Om te waarborgen dat de gegevens afkomstig zijn van het ter uitvoering van een bevel van de officier geplaatste technische hulpmiddel wordt in artikel 11 de eis gesteld dat een technisch hulpmiddel een uniek gegeven toevoegt aan de geregistreerde gegevens. Uit dit gegeven moet de relatie met het geplaatste technische hulpmiddel blijken. Hierbij kan worden gedacht aan een code die bij de plaatsing aan het technisch hulpmiddel is toegevoegd. De technische infrastructuur moet in staat zijn om bij de vastlegging van de geregistreerde gegevens het unieke gegeven te herkennen. Op deze wijze kan een herleidbaar gegevensspoor worden gecreëerd.
Artikel 12 vereist dat een technisch hulpmiddel de geregistreerde gegevens voorziet van de datum en tijd van de registratie. Hierdoor wordt inzichtelijk op welk moment een onderzoekshandeling heeft plaatsgevonden. De eis van datum- en tijdregistratie betekent niet dat er doorlopend datum- en tijdregistratie moet plaatsvinden gedurende de inzet van een technisch hulpmiddel. Artikel 12 staat er niet aan de in de weg dat een technisch hulpmiddel uitsluitend gegevens registreert als er gegevens van het te onderzoeken geautomatiseerde werk worden ontvangen. De strekking van de eis is dat zodra er gegevens worden geregistreerd door een technisch hulpmiddel er zekerheid bestaat over de datum en het tijdstip van de gegevensregistratie door het technische hulpmiddel. Door middel van de logging van de onderzoekshandelingen en het functioneren van de technische infrastructuur kan controle plaatsvinden op het functioneren van een technisch hulpmiddel. Indien zich gedurende de inzet van een technisch hulpmiddel onregelmatigheden voordoen die van invloed zijn op de kwaliteit van de vastgelegde gegevens kan hierover verantwoording worden afgelegd aan de hand van de logging.

Artikel 13 Transport geregistreerde gegevens
Op grond van artikel 13, eerste lid, van het besluit dient een technisch hulpmiddel zodanig te zijn ingericht dat geregistreerde gegevens automatisch worden getransporteerd naar een technische infrastructuur, die in beheer is bij een technisch team. Deze eis wordt gesteld om onbevoegde toegang van derden tot de met een technisch hulpmiddel geregistreerde gegevens te voorkomen. De keuring van een technisch hulpmiddel strekt zich uit tot het transport naar de opslaglocatie. De technische infrastructuur waarop de vastlegging van met een technisch hulpmiddel geregistreerde gegevens plaatsvindt wordt niet gekeurd. Om de integriteit van de op de technische infrastructuur vastgelegde gegevens te borgen dienen de geregistreerde gegevens tijdens het transport beveiligd te zijn tegen wijziging en kennisneming door onbevoegden (tweede lid). Bij de beoordeling van deze eis kunnen de wijze van beveiliging van de werking van een technisch hulpmiddel en de wijze van beveiliging van de geregistreerde gegevens worden betrokken.

Hoofdstuk 6 Keuring van een technisch hulpmiddel

Artikelen 14 en 15 Voorafgaande goedkeuring, herkeuring en keuring achteraf
Uitgangspunt is bij de inzet gebruik wordt gemaakt van een vooraf goedgekeurd technisch hulpmiddel. Dit wordt geregeld in artikel 14, eerste lid, van het besluit. Een technisch hulpmiddel kan uitsluitend worden goedgekeurd als het voldoet aan de artikelen 8 tot en met 13 gestelde eisen (tweede lid). Dit wordt beoordeeld tijdens de keuring. Artikel 14, derde lid, bevat regels over de herkeuring van technische hulpmiddelen. Herkeuring is aan de orde als de werking van een gekeurd technisch hulpmiddel of een onderdeel hiervan zodanig wijzigt dat redelijkerwijs kan worden aangenomen dat het hulpmiddel niet langer voldoet aan de in de artikelen 8 tot en 13 gestelde eisen. De herkeuring zal naar zijn aard vooral gericht zijn op de gewijzigde onderdelen van de software, die door de producent meestal in een zogenaamd "change log" worden omschreven. In het geval dat een software update zodanig kort voor de inzet van een technisch hulpmiddel plaatsvindt dat geen herkeuring heeft kunnen plaatsvinden, biedt het besluit de mogelijkheid van herkeuring achteraf (vierde lid).
Van het uitgangspunt van een voorafgaande keuring kan worden afgeweken indien een dringend onderzoeksbelang daartoe noodzaakt. Deze uitzondering is geregeld in artikel 15. Hierbij kan worden gedacht aan de situatie dat 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 nagaan of het beoogde technische hulpmiddel naar verwachting zal voldoen aan de in de artikel 8 tot en met 13 gestelde technische eisen. In het bevel van de officier van justitie wordt expliciet vermeld dat een niet gekeurd technisch hulpmiddel wordt ingezet (tweede lid).
Als hoofdregel geldt dat een technisch hulpmiddel dat niet vooraf is goedgekeurd, na afloop van de inzet alsnog ter keuring aan de keuringsdienst wordt aangeboden (derde lid). Indien naar het oordeel van de officier van justitie de aard van een technisch hulpmiddel zich tegen keuring achteraf verzet, kan hij bepalen dat een technisch hulpmiddel niet ter keuring wordt aangeboden. 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. Indien de officier van justitie besluit om, gelet op de aard van het technische hulpmiddel, keuring achteraf achterwege te laten, dient hij de noodzakelijke procedurele maatregelen te treffen om rechterlijke controle op de inzet mogelijk te maken. Hierbij kan worden gedacht aan een uitgebreide omschrijving van de functionele specificaties van het op maat gemaakte technische hulpmiddel in het proces-verbaal, het vooraf en achteraf maken van een forensische kopie of het audiovisueel vastleggen van het onderzoeksproces. Daarnaast kunnen een digitale kopie van de software en de broncode bij het proces-verbaal worden gevoegd. 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 gegenereerde gegevens. Ook onderzoekshandelingen die zonder gekeurd technisch hulpmiddel worden verricht worden gelogd, evenals het functioneren van de technische infrastructuur. In geval van twijfel kan zo nodig via de logging verantwoording worden afgelegd over de verrichte handelingen en het vergaarde bewijsmateriaal.

Artikelen 16 tot en met 19 Keuringsdienst, keuringsprotocol, keuringsrapport
In de artikelen 16 tot en met 19 van dit besluit wordt de keuringsprocedure omschreven. Artikel 16 stelt regels over de aanwijzing van keuringsdiensten. De keuring van technische hulpmiddelen zal primair worden opgedragen aan een onderdeel van de Landelijke eenheid, thans de keuringsdienst van de Dienst Landelijke Operationele Samenwerking (eerste lid). De keuringsdienst dient een onafhankelijk en objectief oordeel te geven over de ter keuring aangeboden technische hulpmiddelen. Dit dient ook tot uitdrukking te komen in de plaatsing van de keuringsdienst binnen de politieorganisatie. Bij ministeriële regeling kunnen regels worden

gesteld over de aanwijzing van de keuringdienst van de Landelijke eenheid (derde lid).
De mogelijkheid bestaat om een andere organisatie aan te wijzen als keuringsdienst (tweede lid). Als van deze mogelijkheid gebruik wordt gemaakt worden hierover bij ministeriële regeling regels gesteld (vierde lid). Afhankelijk van de gekozen systematiek kan sprake zijn van een dienst van algemeen economisch belang of een niet-economische dienst van algemeen belang. Bij het opstellen van de ministeriële regeling zal toetsing aan de geldende EU-kaders plaatsvinden.
De keuring van technische hulpmiddelen wordt uitgevoerd op basis van een keuringsprotocol waarin de wijze waarop de keuring plaatsvindt wordt vastgelegd (artikel 17). Daarnaast kunnen in het keuringsprotocol de criteria worden opgenomen die bij de keuring worden gehanteerd. Het keuringsprotocol wordt in samenspraak tussen de keuringsdienst en het openbaar ministerie opgesteld. Een keuringsprotocol behoeft voorafgaande goedkeuring van de Minister van Veiligheid en Justitie. Het is niet wenselijk dat de keuringsdiensten bij keuring van soortgelijke technische hulpmiddelen verschillende keuringsprotocollen hanteren. Indien andere keuringsdiensten worden aangewezen, zal de keuringsdienst van de Landelijke eenheid een coördinerende rol worden toebedeeld bij het opstellen en het gebruik van keuringsprotocollen. De keuring is gericht op die onderdelen van het technische hulpmiddel die van belang zijn voor de detectie, registratie en het transport van gegevens naar een technische infrastructuur. Om de consistentie en de kwaliteit van de keuring te waarborgen wordt de keuring uitgevoerd op basis van voornoemd keuringsprotocol.
Artikel 18, eerste lid, bepaalt dat de korpschef een technisch hulpmiddel ter keuring kan aanbieden bij een keuringsdienst. Van de keuring wordt een rapport opgemaakt, waarin de bevindingen van de keuringsdienst worden vastgelegd (tweede lid). De keuring vindt proefondervindelijk plaats. Bij goedkeuring van een technisch hulpmiddel wordt vermeld dat het hulpmiddel voldoet aan de in de artikelen 8 tot en met 13 vermelde eisen (derde lid, onderdeel a). In het keuringsrapport wordt aan een technisch hulpmiddel een uniek keuringsnummer toegekend (derde lid, onderdeel b). In de processen-verbaal die gedurende het opsporingsonderzoek worden opgesteld kan naar dit keuringsnummer worden verwezen. Op deze wijze kan het gebruik van het middel afgeschermd worden ter bescherming van opsporingsbelangen, terwijl de rechter en de verdediging de zekerheid hebben dat het ingezette technische hulpmiddel voldoet aan de wettelijke eisen. Het keuringsrapport bevat verder een omschrijving van de werking van een technisch hulpmiddel en een aanduiding van de functionaliteit of functionaliteiten van het hulpmiddel (derde lid, onderdelen c en d). Bij het opstellen van het rapport haalbaarheidsonderzoek ter advisering van de officier van justitie kan het technische team zich hierop baseren.
In het derde lid, onderdeel e, wordt de mogelijkheid gecreëerd om te voldoen aan een of meer in het besluit gestelde technische eisen via het stellen van procedurele waarborgen bij de keuring. De huidige keuringspraktijk heeft uitgewezen dat hieraan behoefte bestaat. Een voorbeeld betreft het ontbreken van een technisch geborgde datum/tijd functie. Dat kan worden opgelost door in een keuringsrapport verplichte procedurele waarborgen te stellen, waardoor materieel aan de technische eisen kan worden voldaan. In de processen-verbaal over de opsporingshandelingen kan hierover verantwoording worden afgelegd. In het keuringsrapport wordt ook melding gemaakt van relevante informatie met betrekking tot de werking van een functionaliteit of functionaliteiten van een technisch hulpmiddel, zoals relevante informatie ten behoeve van de plaatsing, inzet of verwijdering van het technische hulpmiddel (derde lid, onderdeel f).
Het rapport van een keuringsdienst bevat de periode waarvoor de keuring geldt zolang de werking hiervan ongewijzigd is (derde lid, onderdeel g). Indien de werking van een technisch hulpmiddel of een onderdeel hiervan zodanig wijzigt dat niet meer voldaan wordt aan de in dit besluit gestelde technische eisen, dient herkeuring plaats te vinden (artikel 14, tweede lid). Na afloop van de in het keuringsrapport genoemde periode kan de keuringsdienst besluiten het technische hulpmiddel opnieuw te keuren of de periode waarvoor de keuring geldt te verlengen.
In artikel 19 wordt geregeld dat de keuringsdienst van de Landelijke eenheid een centrale registratie bijhoudt van de eigen keuringsrapporten en, indien aanwezig, van de keuringsrapporten van andere keuringsdiensten.

Artikel 20 Wederzijdse erkenning
Het beginsel van vrij verkeer van goederen en diensten binnen de Europese Unie brengt met zich

dat lidstaten in de nationale wetgeving geen eisen aan goederen en keuringen mogen stellen die leiden tot beperking van het vrije verkeer tussen de lidstaten. De technische eisen die het besluit stelt aan technische hulpmiddelen en de door het besluit voorgeschreven keuring van technische hulpmiddelen kunnen worden opgevat als een inbreuk op het vrije verkeer. Daarom is in dit artikel een wederzijdse erkenningsclausule opgenomen voor goederen en keuringen.

Hoofdstuk 7 Toegang tot en plaatsing van een technisch hulpmiddel

Artikelen 21 en 22 Toegang en plaatsing van een technisch hulpmiddel
Artikel 21 bepaalt dat de toegang tot technische hulpmiddelen centraal wordt geregistreerd. De korpschef wijst één of meer ambtenaren aan die met de registratie zijn belast. Na vertoon van het bevel van de officier van justitie met daarin een aanduiding van de aard en functionaliteit van het technische hulpmiddel verschaft een met registratie belaste ambtenaar toegang tot een technisch hulpmiddel ten behoeve van de plaatsing ervan. De toegang tot een technisch hulpmiddel wordt verleend voor de periode die nodig is voor de uitvoering van het bevel.
De plaatsing van een technisch hulpmiddel vindt plaats door een opsporingsambtenaar van een technisch team (artikel 22). Dit kan een op grond van de artikelen 3 of 4 van dit besluit aangewezen lid van of deelnemer aan een technisch team zijn.
Het technisch team zal in de praktijk eerst een voorverkenning opstellen. Na analyse daarvan wordt een plan van aanpak voor het binnendringen opgesteld dat wordt getest in een proefopstelling. Nadat is binnengedrongen in het geautomatiseerde werk wordt het technische hulpmiddel geplaatst. Het tweede lid vereist dat bij de plaatsing van een technisch hulpmiddel uitsluitend de in het bevel van de officier van justitie aangeduide functionaliteiten worden ingeschakeld. Hierover dient verantwoording te worden afgelegd in een proces-verbaal. Bij de plaatsing kan het technische hulpmiddel van een uniek gegeven worden voorzien, waarmee de relatie tussen het geplaatste technische hulpmiddel en de met het hulpmiddel vastgelegde gegevens op een technische infrastructuur kan worden aangetoond. De Inspectie VenJ en houdt toezicht op de naleving van de toegang- en plaatsingprocedures en de vereiste autorisaties.

Hoofdstuk 8 Inzet van een technisch hulpmiddel

Artikelen 23 tot en met 27 Inzet van een technisch hulpmiddel en vastlegging van gegevens op een technische infrastructuur
In artikel 23 wordt geregeld dat de inzet van een technisch hulpmiddel plaatsvindt door een opsporingsambtenaar van een technisch team. Van de inzet wordt proces-verbaal opgemaakt. Tijdens de inzet kunnen afhankelijk van de ingeschakelde functionaliteit(en) verschillende soorten gegevens worden geregistreerd. De vastlegging van de geregistreerde gegevens vindt plaats op een technische infrastructuur. Dit betreft een technische voorziening van een technisch team, die is bedoeld voor de vastlegging van de met een technisch hulpmiddel geregistreerde gegevens (artikel 24). Om de betrouwbaarheid, integriteit en herleidbaarheid van de vastgelegde gegevens te borgen stelt het besluit eisen aan de inrichting van de technische infrastructuur waarop de gegevens worden vastgelegd (artikelen 25 tot en met 27 van het besluit). De gegevens mogen niet inhoudelijk worden bewerkt en dienen te worden beveiligd tegen wijziging en kennisneming hiervan door onbevoegden (artikel 25). De vastgelegde gegevens zijn uitsluitend toegankelijk voor de door de korpschef aangewezen ambtenaren. Tactische opsporingsambtenaren hebben geen toegang. De technische infrastructuur moet in staat zijn om het unieke gegeven dat door het technische hulpmiddel aan de geregistreerde gegevens is toegevoegd te herkennen (artikel 26). Zo kan de herkomst van de vastgelegde gegevens worden vastgesteld.
Bij de vastlegging van gegevens op de technische infrastructuur worden de datum en tijd geregistreerd (artikel 27). Hierdoor bestaat zekerheid over de datum en het tijdstip van de vastlegging. Het kan voorkomen dat de datum en tijd in de technische infrastructuur van de politie afwijken van de ingestelde datum en tijd van het te onderzoeken geautomatiseerd werk. Een technisch team heeft geen invloed op de datum en tijd die een verdachte heeft ingesteld in zijn computer of smartphone. Na overlegging van de onderzoeksresultaten door het technische team aan het tactische team kan het tactische team het tijdsverloop reconstrueren.
Via de logging kan controle worden uitgeoefend op de verrichte onderzoekshandelingen en het

functioneren van de technische infrastructuur. Zowel tijdens de uitvoering van een bevel als achteraf moet kunnen worden vastgesteld of wijziging dan wel onbevoegde kennisneming van de ter uitvoering van een bevel vastgelegde gegevens heeft plaatsgevonden. Indien een onregelmatigheid wordt vastgesteld die van invloed is op de kwaliteit van de met een technisch hulpmiddel geregistreerde gegevens dient hiervan proces-verbaal te worden opgemaakt door een opsporingsambtenaar van een technisch team. Dit proces-verbaal wordt aan de officier van justitie gezonden (artikel 6). De Inspectie VenJ houdt toezicht op de naleving van de regels en procedures omtrent de inzet van een technisch hulpmiddel en de vastlegging van gegevens op een beveiligde technische infrastructuur.

Hoofdstuk 9 Verwijdering van een technisch hulpmiddel

Artikelen 28 en 29 Verwijdering van een technisch hulpmiddel, beëindiging transport gegevens
Hoofdregel is dat een technisch hulpmiddel wordt verwijderd uit het te onderzoeken geautomatiseerde werk, nadat het onderzoeksdoel is bereikt of de periode waarvoor het bevel is afgegeven is verstreken (artikel 28). De verwijdering geschiedt door een opsporingsambtenaar van een technisch team. Sommige softwareapplicaties bieden de functionaliteit van een zelfstandige vernietiging van de software na verloop van een bepaalde, vooraf ingestelde, periode.
Vanuit de opsporing bestaat belang bij de verwijdering: bij voorkeur dient te worden voorkomen te dat het gebruik van het technische hulpmiddel bekend wordt. Niettemin kan het voorkomen dat een technisch hulpmiddel niet verwijderd kan worden, bijvoorbeeld omdat voor verwijdering soms meer beheerrechten nodig zijn dan voor de plaatsing. Als het hulpmiddel niet verwijderd kan worden, dan dient het transport van de gegevens te worden beëindigd. Dit wordt geregeld in artikel 29. Van de verwijdering van het technisch hulpmiddel dan wel het stopzetten van het transport van de gegevens wordt proces-verbaal opgemaakt, dat aan de officier van justitie wordt gezonden. Op basis van de logging kan worden gecontroleerd of de ontvangst van gegevens op de technische infrastructuur daadwerkelijk is beëindigd.
Indien de niet of niet volledige verwijdering van een technisch hulpmiddel risico's oplevert voor het onderzochte geautomatiseerde werk stelt het technisch team de officier van justitie hiervan in kennis en stelt het informatie beschikbaar ten behoeve van de volledige verwijdering. De officier van justitie stelt de beheerder van het geautomatiseerde werk daarvan in kennis.
De Inspectie VenJ houdt toezicht op de naleving op de juiste uitvoering van de verwijderingsprocedure.

Hoofdstuk 10 Wijziging overige wet- en regelgeving

Artikel 30 Wijziging Besluit politiegegevens
Artikel 30 strekt tot wijziging van artikel 4:3, eerste lid, van het Besluit politiegegevens. In de Wpg is geregeld dat de politie persoonsgegevens aan derden kan verstrekken met het oog op een zwaarwegend algemeen belang (artikel 18, eerste lid, Wpg). De personen en instanties aan wie, evenals de taak ten behoeve waarvan de politiegegevens worden verstrekt, worden aangewezen bij of krachtens algemene maatregel van bestuur. Dit is uitgewerkt in het Besluit politiegegevens. Om de verhouding tussen de taakuitoefening door de Inspectie VenJ en het verstrekkingenregime van de Wpg te verhelderen wordt artikel 4:3 van het Besluit politiegegevens aangepast en wordt de verplichting tot verstrekking van politiegegevens die worden verwerkt op grond van de artikelen 8, 9, 10 en 13 van de Wpg, ten behoeve van de toezichthoudende taak van de Inspectie VenJ expliciet vastgelegd.
De toezichthoudende taak van de Inspectie VenJ betreft het toezicht op de taakuitvoering door de politie (artikel 57, eerste lid, onderdeel d, Wet veiligheidsregio's) alsmede het onderzoek in een geautomatiseerd werk dat wordt gedaan door de opsporingsambtenaren van de bijzondere opsporingsdiensten en de buitengewone opsporingsambtenaren (artikel 126nba, zevende lid, Sv). De verplichting om gegevens te verstrekken met het oog op de uitvoering van de taken van de Inspectie VenJ omvat de politiegegevens die worden verwerkt ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval en de gegevens die worden verwerkt met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (artikelen 9, eerste lid, en 10, eerste lid, onderdelen a en

c, Wpg). Het gaat hier om zachte gegevens, die binnen de politie worden verwerkt door onder meer de criminele inlichtingeneenheden en de regionale inlichtingendiensten.

Hoofdstuk 11 Inwerkingtreding

Artikelen 31 en 32 Citeertitel en inwerkingtreding
Dit besluit heeft als citeertitel "Besluit onderzoek in een geautomatiseerd werk" en treedt tegelijk in werking met het wetsvoorstel computercriminaliteit III. De datum van inwerkingtreding wordt bepaald op **PM.**

De Staatssecretaris van Veiligheid en Justitie,

Eerste Kamer der Staten-Generaal

0543 1

Vergaderjaar 2016–2017

33 542 Wijziging van het Wetboek van Strafvordering in verband met de regeling van het vastleggen en bewaren van kentekengegevens door de politie

D **BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE**

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 22 mei 2017

Op 8 maart van dit jaar zond ik u de memorie van antwoord ten aanzien van het wetsvoorstel dat strekt tot wijziging van het Wetboek van Strafvordering in verband met de regeling van het vastleggen en bewaren van kentekengegevens door de politie (EK 2016–2017, 33 542, C).

In deze memorie van antwoord heb ik in reactie op een vraag inzake de beveiliging van blanco kentekenplaten vermeld dat het aantal gestolen blanco kentekenplaten is gedaald van 2.439 in 2015 naar 773 in 2016. Deze aantallen zijn naar nu blijkt tot stand gekomen door een foutieve interpretatie van de onderliggende gegevens, en zijn derhalve onjuist. Middels deze brief wil ik dit graag rectificeren. Het aantal gestolen blanco kentekenplaten is in werkelijkheid gedaald van 3.004 in 2015 naar 1.252 in 2016.

De Minister van Veiligheid en Justitie,
S.A. Blok

kst-33542-D
ISSN 0921 - 7371
's-Gravenhage 2017

Eerste Kamer der Staten-Generaal **I**

Vergaderjaar 2016-2017

34 372 Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)

D MEMORIE VAN ANTWOORD

Ontvangen 12 juni 2017

1. Inleiding

Met veel belangstelling heb ik kennisgenomen van de opmerkingen en vragen van de leden van de fracties van de VVD, het CDA, D66, de SP, de PvdA, GroenLinks en de ChristenUnie over dit wetsvoorstel. De ontwikkeling van de informatie- en communicatietechnologie stelt de instanties die zijn belast met de bescherming van burgers tegen criminaliteit, in toenemende mate voor uitdagingen. Recente rapporten onderschrijven de zorg van politie en justitie dat de omvang van cybercrime groeit en dat er behoefte is aan meer bevoegdheden voor de opsporing om de dreiging te adresseren. Voor een schets van de omvang van cybercrime en de onderkenning van de urgentie kan worden gewezen op het rapport van het Rathenau instituut[1], de commissie Verhagen[2], het Cybersecuritybeeld Nederland[3] dat jaarlijks wordt gepubliceerd, en de veiligheidsmonitor[4]. Voor de omvang en urgentie op Europees niveau kan worden gewezen op The Internet Organised Crime Threat Assessment (IOCTA)[5], alsook het Serious and Organised Crime Threat Assessment (SOCTA)[6]. De regering onderkent deze behoefte. Het internet mag geen vrijhaven worden voor criminelen en er moet recht worden gedaan aan slachtoffers. Effectieve handhaving van de rechtsstaat in cyberspace is een voorwaarde voor een veilig internet. Dit wetsvoorstel is hiervoor van essentieel belang. Ik hoop dat met de beantwoording van de vragen ook de bezwaren van de fracties die hun bezorgdheid over dit wetsvoorstel kenbaar hebben gemaakt, onder meer vanwege de proportionaliteit van het wetsvoorstel en de impact op de privacy van burgers, kunnen worden weggenomen.

2. Reikwijdte van het wetsvoorstel

De leden van de fractie van de SP hebben hun teleurstelling uitgesproken over het feit dat de regering twee totaal verschillende problemen, namelijk de toegenomen computercriminaliteit en het gebruik van digitale middelen bij traditionele criminaliteit, heeft proberen te vatten in één

[1] Rathenau instituut (2017) Een nooit gelopen race: Over cyberdreigingen en versterking van de weerbaarheid. Zie in het bijzonder hoofdstuk 2.
[2] Verhagen, H. (2016) Nederland droge digitale voeten: De economische en maatschappelijke noodzaak van meer Cybersecurity. In het bijzonder paragraaf 1.2. over de aantrekkelijkheid van Nederland voor cybercriminelen.
[3] Nationaal Cyber Security Centrum (2016) Cybersecuritybeeld Nederland.
[4] CBS en het ministerie van Veiligheid en justitie (2017) Veiligheidsmonitor 2016.
[5]. Europol (2016) The Internet Organised crime threat assessment.
[6] Europol (2017) Serious and Organised Crime Threat Assessment. met als ondertitel crime in the age of technolology. In het bijzonder in de conclusies op blz. 56, waarin wordt beschreven dat technologie functioneert als katalysator voor criminele activiteiten en daarvoor een bijzonder faciliterende rol vervult.

wetsvoorstel. Zij hebben gevraagd of de regering kan toelichten waarom zij beide terreinen in een wetsvoorstel heeft willen vatten.

Computercriminaliteit heeft niet uitsluitend betrekking op het handelen in de digitale dimensie, en kan niet strikt worden gescheiden van het handelen in de fysieke wereld. Beide dimensies lopen in elkaar over en werken op elkaar in. Voor de aanpak van computercriminaliteit zijn nieuwe bevoegdheden nodig. De ontwikkeling van de informatie- en communicatietechnologie biedt de criminaliteit nieuwe mogelijkheden voor het plegen van strafbare feiten. Deze mogelijkheden hebben betrekking op verschillende aspecten. Dit betreft bijvoorbeeld de verandering in de wijze waarop de burgers met elkaar communiceren. Het verhandelen van goederen en diensten op internet wordt vergemakkelijkt door de mogelijkheden van digitale communicatie, maar heeft een navenant effect op vormen van fraude of zedenmisdrijven. Tevens biedt de informatie- en communicatietechnologie meer mogelijkheden om het handelen af te schermen, zoals het gebruik van encryptie. De nieuwe bevoegdheden zijn daarmee effectief in het digitale en fysieke domein. Tenslotte zijn de strafbaarstellingen niet meer voldoende toegesneden op de technologische ontwikkeling; daarvoor kan worden gewezen op de in dit wetsvoorstel voorgestelde strafbaarstelling van een delict als het overnemen en helen van gegevens. Deze verschillende aspecten hebben een gezamenlijk kenmerk, namelijk dat deze onderdeel vormen van de computercriminaliteit. Zoals eerder aangegeven, lopen beide dimensies in elkaar over. Een drugshandelaar die voor zijn communicatie met anderen gebruik maakt van een speciale telefoon waarmee de communicatie wordt versleuteld, handelt in de fysieke en digitale dimensie. Ditzelfde geldt voor de ‘groomer’ die een afspraak maakt met een minderjarige, met het voornemen tot het verrichten van seksuele handelingen. Het Wetboek van Strafvordering en het Wetboek van Strafrecht zijn tot stand gekomen in een tijd waarin de digitale wereld niet bestond. Dit betekent dat de bevoegdheden en strafbaarstellingen periodiek moeten worden herijkt, zodat de samenleving adequaat kan worden beveiligd tegen het handelen van personen die gebruik maken van de informatietechnologie om criminele activiteiten te plegen waarvan anderen het slachtoffer zijn, om te communiceren met medeplegers en om hun handelen van de buitenwereld af te schermen. De keuze van de regering berust op een inventarisatie van de behoeften bij politie en justitie. Zowel bevoegdheden van de politie en justitie als de strafrechtelijke normstelling hebben geen gelijke tred gehouden met de ontwikkeling van de computercriminaliteit en daarom dient aanpassing plaats te vinden.De regering acht alle onderdelen van het wetsvoorstel van essentieel belang voor de bestrijding van computercriminaliteit.

De leden van de fractie van de SP hebben aangegeven zich zorgen te maken dat de hackbevoegdheid de politie meer digitale mogelijkheden biedt dan er nu in de offlinewereld mogelijk zijn. De leden van deze fractie hebben geen kennis genomen van wetsvoorstellen die het mogelijk maken camera’s te plaatsen in de huizen van verdachte personen, toch is dit naar hun oordeel het effect van het voorstel van de regering.

Het wetsvoorstel introduceert de bevoegdheid tot het op afstand heimelijk binnendringen van een geautomatiseerd werk met het oog op het verrichten van bepaalde onderzoekshandelingen. Hieronder valt de uitvoering van een bevel tot observatie als bedoeld in artikel 126g Sv. De stelselmatige observatie van personen betreft een bestaande opsporingsbevoegdheid. De uitvoering van dit bevel dient plaats te vinden binnen de kaders van artikel 126g Sv. Op basis van deze bevoegdheid is het niet toegestaan heimelijk een woning te betreden of heimelijk een

webcam in een woning aan te zetten. Ook op basis van de voorgestelde bevoegdheid van het op afstand heimelijk binnendringen van een geautomatiseerd werk is dit niet mogelijk.

De noodzaak van de voorgestelde uitbreiding van bevoegdheden is de leden van de fractie van de SP niet helemaal duidelijk. De leden van deze fractie hebben gevraagd of de regering kan aangeven hoe groot het probleem is dat het wetsvoorstel moet oplossen en hoeveel zaken er nu niet opgelost kunnen worden maar met deze wetgeving waarschijnlijk wel zouden worden opgelost.

Door de ontwikkeling van het internet en de technologische vooruitgang wordt de opsporing van strafbare gedragingen in toenemende mate lastig of zelfs onmogelijk. Drie wezenlijke problemen en gebleken knelpunten worden onderscheiden. Het betreft ten eerste de toenemende versleuteling van elektronische gegevens. Via het internet is het eenvoudig om vanuit het buitenland met behulp van een geautomatiseerd werk strafbare feiten in Nederland te plegen terwijl gebruik wordt gemaakt van anonimiseringstechnieken zodat de locatie van verzending wordt verhuld of de boodschap wordt versleuteld. Daardoor is het vaak niet mogelijk met andere middelen, zoals aftappen en opnemen van communicatie of het in beslag nemen van voorwerpen, een dader of een geautomatiseerd werk met daarop bewijsmateriaal, te identificeren en voldoende bewijs te vergaren. Om toch effectief te kunnen opsporen moet het in bepaalde uitzonderlijke gevallen mogelijk zijn om gericht in het betreffende systeem te kunnen binnendringen zodat de gegevens kunnen worden verkregen voordat deze worden versleuteld. Ten tweede vormt het toenemende gebruik van draadloze netwerken, van «hotspots» en allerlei vormen van dynamische IP-adressen een obstakel voor het vergaren van bewijs. Bijvoorbeeld omdat wanneer een internettap op een router geplaatst wordt alleen de in- en uitgaande communicatie kan worden afgetapt, maar de interne communicatie op het netwerk niet kan worden onderschept. Daarnaast wordt door een internettap alle in- en uitgaande communicatie afgetapt, ook van personen in wie de opsporing niet geïnteresseerd is. Door identificatie van een geautomatiseerd werk of van de gebruiker door middel van het binnendringen in het geautomatiseerde werk kan meer gericht onderzoek worden gedaan. De derde ontwikkeling betreft de toenemende opslag van informatie in de cloud. Bestaande bevoegdheden als een netwerkzoeking en doorzoeking ter vastlegging van gegevens gaan er in belangrijke mate van uit dat de gegevens die voor de opsporing van belang zijn, zich bevinden op een bepaalde gegevensdrager die zich op een vaste plaats bevindt. Deze situatie strookt echter steeds minder met de werkelijkheid. Dit belemmert de effectiviteit van traditionele opsporingsbevoegdheden, zoals het aftappen en opnemen van communicatie, het vorderen van gegevens bij aanbieders en het vragen van rechtshulp aan andere landen. Voor toepassing van de huidige bevoegdheden rond de inbeslagneming van geautomatiseerde werken is de plaats waar het geautomatiseerde werk zich fysiek bevindt doorslaggevend. Hieronder wordt, in antwoord op vragen van de leden van de fractie van GroenLinks, nader ingegaan op de noodzaak en de bruikbaarheid van bestaande bevoegdheden.

In de inleiding is reeds ingegaan op de beschikbare rapporten waarin de omvang van computercriminaliteit wordt geschetst. Er wordt niet per zaak geregistreerd welke niet-bestaande bevoegdheden tot een meer effectieve opsporing hadden kunnen leiden. De opsporingsdiensten en het openbaar ministerie houden daarom geen cijfers bij over het aantal gevallen waarin gedurende de afgelopen vijf jaar de voorgestelde bevoegdheid van het op afstand binnendringen in een geautomatiseerd werk had kunnen worden ingezet. Wel kan worden verwezen naar in de nota naar aanleiding van het verslag gegeven voorbeelden van

opsporingsonderzoeken die niet zijn geslaagd omdat de benodigde gegevens in de cloud niet vastgelegd konden worden, omdat de eigenaar van de server niet (tijdig) reageerde op verzoeken of de gegevens inmiddels waren verdwenen (Kamerstukken II 2016/17, 34 372, nr. 6, blz. 15/16).

3. Proportionaliteit en privacy

De leden van de fractie van de VVD hebben gevraagd in hoeverre het wetsvoorstel voldoet aan de vereisten die voortvloeien uit het Europees Verdrag voor de Rechten van de Mens (EVRM), in het bijzonder ten aanzien van het recht op bescherming van de persoonlijke levenssfeer.

Voor de bescherming van grondrechten en het recht op eerbiediging van de persoonlijke levenssfeer is artikel 8 van het Europees Verdrag tot bescherming van Rechten van de Mens en de fundamentele vrijheden (EVRM) van bijzonder belang. De recente jurisprudentie van het Europese Hof tot bescherming van Rechten van de Mens en de fundamentele vrijheden (EHRM) rond het heimelijk vergaren van persoonsgegevens ten behoeve van de opsporing en vervolging van strafbare feiten betreft de arresten in de zaken van Digital Rights Ireland en Seitlinger (zaken C-293/12 en C-294/12), Maximilian Schrems/Data protection Commission (zaak C-362/15), Zakharov tegen Rusland (zaak 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306) en Szabó en Vissy tegen Hongarije (zaak 37138/14). Vooropgesteld moet worden dat deze arresten betrekking hebben op verschillende casus rond het heimelijk verzamelen van persoonsgegevens ten behoeve van zwaarwegende publieke belangen, zoals de bescherming van de nationale veiligheid en de opsporing en vervolging van strafbare feiten. Hier komt bij dat de wettelijke regelingen en systemen rond die casus in de verschillende landen uiteen lopen. Niettemin kunnen uit artikel 8, tweede lid, van het EVRM en de jurisprudentie van het EHRM enkele hoofdlijnen worden afgeleid. Het EHRM toetst een inbreuk op het recht op bescherming van de persoonlijke levenssfeer aan de eisen van legaliteit (voorzienbaarheid bij wet) en noodzakelijkheid. Onder voorzienbaarheid valt niet alleen de vraag of de voorgenomen maatregel is geregeld bij wet, maar ook de vraag of de wet voldoende kwaliteit heeft, dat wil zeggen of de inbreuk voldoende gedetailleerd is uitgewerkt en met effectieve waarborgen is omkleed tegen misbruik. Onder noodzakelijkheid in een democratische samenleving wordt verstaan of de voorgenomen maatregel voldoet aan de vereisten van proportionaliteit (de keuze voor het middel dat in verhouding staat tot het te realiseren doel) en subsidiariteit (de keuze voor het minst ingrijpende middel dat geschikt is om het doel te bereiken), waarbij een beoordeling dient plaats te vinden of de voorgenomen maatregel kan worden gerechtvaardigd door een “pressing social need”.

Het voorliggende wetsvoorstel bevat de nodige waarborgen waarmee tegemoet wordt gekomen aan de vereisten die uit de Europese jurisprudentie voortvloeien. De voorgestelde bevoegdheid tot het op afstand heimelijk binnendringen van een geautomatiseerd werk wordt bij wet vastgelegd. Het belang van de opsporing van ernstige strafbare feiten is erkend als een belang dat de inmenging van het openbaar gezag in het recht op bescherming van de persoonlijke levenssfeer kan rechtvaardigen. Aan het vereiste van de voorzienbaarheid is invulling gegeven door middel van een gedetailleerde wettelijke regeling waarin specifiek is omschreven welke misdrijven aanleiding kunnen geven tot de inzet van de bevoegdheid, een omschrijving van de categorie van personen jegens wie deze bevoegdheid kan worden ingezet en een beperking van de tijdsduur tot vier weken. Hiermee wordt voorzien in een wettelijke regeling die voor de burger voldoende toegankelijk is. De te verrichten onderzoekshandelingen zijn nauwkeurig

omschreven en sluiten merendeels aan bij de bestaande bevoegdheden van het Wetboek van Strafvordering. Het EHRM heeft geoordeeld dat, in het licht van de mogelijkheden van de moderne communicatietechnologie, het vereiste van de "noodzaak in een democratische samenleving" zowel betrekking heeft op de bescherming van de democratische instituties in zijn algemeenheid als op het verkrijgen van vitale informatie in het individuele geval (Szabó en Vissy tegen Hongarije, §73).

Met het vereiste van het dringende opsporingsbelang in combinatie met de ernst van de strafbare feiten wordt uitdrukking gegeven aan het vereiste van een strikte noodzaak tot de inzet van de bevoegdheid, zowel in zijn algemeenheid als in het concrete geval. De voorgestelde maatregel is onvermijdelijk om het hoofd te kunnen bieden aan de ontwikkeling van de cybercrime gedurende de afgelopen jaren. Met dit vereiste wordt tevens tot uitdrukking gebracht dat de voorgestelde bevoegdheid in een concreet onderzoek uitsluitend mag worden ingezet als blijkt dat met de bestaande wettelijke bevoegdheden niet hetzelfde doel kan worden bereikt. Er moet sprake zijn van een misdrijf dat een ernstige inbreuk op de rechtsorde oplevert en waarvoor voorlopige hechtenis mogelijk is. Voor het verrichten van bepaalde onderzoekshandelingen waarbij het geautomatiseerde werk kan worden doorzocht, is een verdenking nodig van een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld of een misdrijf dat bij algemene maatregel van bestuur is aangewezen. Met deze voorwaarden wordt invulling gegeven aan de eisen van legaliteit (voorzienbaarheid) en noodzaak (proportionaliteit). Vooraf wordt de voorgenomen inzet getoetst door de Centrale Toetsingscommissie (CTC) van het openbaar ministerie. Tevens is voorzien in een toetsing door een onafhankelijke rechter, zowel voorafgaand aan de inzet als achteraf ter terechtzitting. Met het wettelijke vereiste van een voorafgaande rechterlijke toetsing wordt het risico van een willekeurige toepassing van de bevoegdheid uitgesloten. De voorgenomen inzet wordt getoetst aan de proportionaliteit en subsidiariteit. De rechterlijke machtiging is gekoppeld aan een periode van vier weken, voor verlenging is rechterlijke instemming nodig. Met het oog op een zorgvuldige toetsing dient de officier van justitie in het bevel een duidelijke omschrijving van de te verrichten onderzoekshandelingen op te nemen, een omschrijving welk deel van het geautomatiseerde werk en welke categorie van gegevens het betreft en een aanduiding van de aard en functionaliteit van het technische hulpmiddel. Het EHRM hecht veel waarde aan onafhankelijk rechterlijk toezicht voor de beoordeling van de rechtmatigheid van de voorgestelde bevoegdheid. Volgens het EHRM vormt rechterlijk toezicht de beste waarborg voor onafhankelijkheid, onpartijdigheid en een degelijke procedure (Zakharov tegen Rusland, §233; Szabó en Vissy tegen Hongarije, §77: "The Court recalls that the rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure."). Het EHRM wijst er verder op dat rechterlijk toezicht het vertrouwen van de burger versterkt dat de rule of law ook geldt in het domein van geheime surveillance. Met het oog op de enorme hoeveelheid informatie die ter beschikking staat aan de autoriteiten en de geavanceerde technieken die deze autoriteiten gebruiken, kan de waarde van onafhankelijk toezicht volgens het EHRM niet overschat worden (Szabó en Vissy tegen Hongarije, §79).

Er is verder voorzien in de nodige waarborgen voor een zorgvuldige uitvoering. De uitvoering van het onderzoek is voorbehouden aan deskundige opsporingsambtenaren die onderdeel vormen van een speciaal team, dat organisatorisch is gescheiden van het tactische team. Er

zullen keuringseisen worden gesteld aan de inrichting en werking van het technische hulpmiddel dat wordt gebruikt voor het detecteren, registreren en transporteren van gegevens. Er wordt voorzien in de geautomatiseerde vastlegging van gegevens over de uitvoering van de onderzoekshandelingen (logging) met het oog op controle op de uitvoering van de bevoegdheid zodat zowel tijdens het onderzoek als op een later moment geen twijfel kan bestaan over de aard en consequenties van de handelingen die zijn verricht bij de uitvoering van het bevel. Dit wordt vastgelegd in het Besluit onderzoek in een geautomatiseerd werk. Op de uitvoering van het onderzoek in een geautomatiseerd werk door de daartoe aangewezen opsporingsambtenaren wordt, aanvullend op de rechterlijke controle, toezicht uitgeoefend door de Inspectie Veiligheid en Justitie. Ten slotte is voorzien in een verplichting tot notificatie van de betrokkene. Hiervoor is aangesloten bij de bestaande regeling voor de notificatie van bijzondere opsporingsbevoegdheden (artikel 126bb Sv). Het EHRM acht het van groot belang dat de betrokkene achteraf op de hoogte kan komen van de geheime surveillance en genoegdoening kan zoeken voor een eventuele inbreuk op zijn privacy (Zakharov tegen Rusland, §234; Szabó en Vissy tegen Hongarije, §86). In het licht van de bestaande en voorgestelde garanties en waarborgen rond de voorgestelde maatregel voldoet deze naar het oordeel van de regering dan ook ruimschoots aan de vereisten die uit het EVRM voortvloeien, in het bijzonder ten aanzien van het recht op bescherming van de persoonlijke levenssfeer.

De leden van de fractie van de VVD hebben gevraagd in hoeverre het wetsvoorstel spoort met de uitgangspunten en vereisten waarin het wetsvoorstel WIV voorziet, en in hoeverre er verschillen bestaan tussen beide wetsvoorstellen op het terrein van de bescherming van de persoonlijke levenssfeer van de burger. De leden van deze fractie hebben tevens gevraagd om, als er verschillen tussen de beide wetsvoorstellen bestaan, een overzicht van de verschillen en of de regering daarbij uitdrukkelijk wil aangeven waarom die verschillen tussen beide wetsvoorstellen bestaan.

Het voorliggende wetsvoorstel beoogt het juridische instrumentarium voor de opsporing en vervolging van computercriminaliteit te versterken. In dat kader wordt voorgesteld een nieuwe bevoegdheid voor de officier van justitie te creëren om onder voorwaarden een geautomatiseerd werk, dat in gebruik is bij een verdachte, op afstand heimelijk binnen te laten dringen door de daartoe aangewezen opsporingsambtenaren met het oog op het verrichten van bepaalde onderzoekshandelingen (onderzoek in een geautomatiseerd werk). Daarbij gaat het deels om reeds bestaande bevoegdheden. Het heimelijk binnendringen in een geautomatiseerd werk is noodzakelijk geworden door de voortschrijdende techniek en het wijdverbreide gebruik van geautomatiseerde werken voor communicatie en de verwerking en opslag van gegevens.

Het wetsvoorstel op de inlichtingen- en veiligheidsdiensten 20xx (Kamerstukken I 2016/17, 34 588, A) voorziet in modernisering van de bevoegdheden van de inlichtingen- en veiligheidsdiensten. Deze modernisering is ingegeven door technologische en maatschappelijke ontwikkelingen, zoals de snelle opkomst en mondiale verspreiding van digitale technologie en het internet, in combinatie met het veranderende dreigingsbeeld.

Een belangrijk verschil tussen het voorliggende wetsvoorstel en het wetsvoorstel Wiv 20xx betreft de reikwijdte. Het voorliggende wetsvoorstel voorziet in opneming in het Wetboek van Strafvordering van een nieuwe bevoegdheid voor de officier van justitie, te weten het bevelen dat een daartoe aangewezen opsporingsambtenaar op afstand heimelijk binnendringt in een geautomatiseerd werk met het oog op het verrichten van bepaalde onderzoekshandelingen. Het

wetsvoorstel Wiv 20xx voorziet in modernisering van de bevoegdheden van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), zodat deze diensten hun wettelijke taken op het gebied van de bescherming van de nationale veiligheid beter kunnen uitvoeren. Dit betreft algemene bevoegdheden inzake de verzameling van gegevens, zoals het al dan niet stelselmatig verzamelen van gegevens over personen uit open bronnen en de raadpleging van informanten, alsmede bijzondere bevoegdheden tot verzameling van gegevens, zoals het observeren en volgen, de inzet van agenten, het onderzoek van besloten plaatsen, van gesloten voorwerpen, aan voorwerpen en DNA-onderzoek, het openen van brieven, het verkennen van en binnendringen in geautomatiseerde werken, het onderzoek van communicatie (gerichte en onderzoeksopdrachtgerichte interceptie van communicatie alsmede het opvragen van communicatiegegevens).

Wat betreft de bescherming van de persoonlijke levenssfeer zijn de uitgangspunten en vereisten waarin de beide wetsvoorstellen voorzien, deels gelijk en deels verschillend. De gelijkenis wordt ingegeven doordat de beide wetsvoorstellen voorzien in bevoegdheden voor de overheid om, met het oog op de bescherming van een algemeen belang, inbreuk te maken op de rechten van burgers. Daarbij geldt voor beide wetsvoorstellen dat het EVRM van toepassing is op de taakuitvoering door de rechtshandhavingsdiensten en de inlichtingen- en veiligheidsdiensten, inclusief de verwerking van persoonsgegevens. Daardoor geldt voor beide wetsvoorstellen dat iedere inzet van bevoegdheden moet voldoen aan de vereisten die voortvloeien uit het EVRM, zoals de eisen van proportionaliteit (het doel moet opwegen tegen de inbreuk op de privacy en deze inbreuk rechtvaardigen) en subsidiariteit (het lichtste middel waarmee het doel kan worden bereikt moet worden gekozen). De verschillen in de uitwerking van die eisen in de beide wetsvoorstellen houden verband met de verschillende wettelijke taken van de desbetreffende overheidsorganen, de toepasselijkheid van de EU-regels en de verschillen in de wijze waarop deze organen in het staatsbestel zijn ingebed.

De wettelijke taken van de politie en het openbaar ministerie hebben betrekking op respectievelijk de uitvoering van de politietaak en de vervolging van strafbare feiten. Er gelden specifieke wetten voor de bescherming van persoonsgegevens. De Wet politiegegevens bevat regels voor de verwerking van persoonsgegevens door een ambtenaar van politie met het oog op de uitvoering van de politietaak als bedoeld in de artikel 3 en 4, eerste lid, PW 2012. De Wet justitiële en strafvorderlijke gegevens bevat regels voor de verwerking van persoonsgegevens door het openbaar ministerie ten behoeve van een strafzaak. De verwerking van persoonsgegevens met het oog op de opsporing en vervolging van strafbare feiten valt onder de reikwijdte van het verdrag betreffende de Europese Unie. Inmiddels hebben de Raad en het Europees Parlement een richtlijn aangenomen die regels geeft over de verwerking van persoonsgegevens ten behoeve van de strafrechtspleging (richtlijn 680/2016). De richtlijn geeft aanleiding tot aanpassing van de Wpg en de Wjsg. De regels van de richtlijn zijn afgeleid van die van de verordening gegevensbescherming (verordening 679/2016). De wettelijke taken van de inlichtingen- en veiligheidsdiensten hebben betrekking op de bescherming van de nationale veiligheid (artikelen 8 en 10 Wiv 20xx). De Europese Unie is niet bevoegd op het gebied van de nationale veiligheid (artikel 4, tweede lid, Verdrag betreffende de Europese Unie). In het wetsvoorstel inlichtingen- en veiligheidsdiensten 20xx is een uitputtende regeling opgenomen voor de verwerking van (persoons)gegevens door de diensten, waaronder een specifieke regeling voor de verstrekking van persoonsgegevens en andere gegevens (par. 3.4. Wiv 20xx)

en een afzonderlijk hoofdstuk over de kennisneming van door of ten behoeve van de diensten verwerkte gegevens (hoofdstuk 5 Wiv 20xx).

Vanwege het onderscheid in de wettelijke taken zijn de rechtshandhavingsdiensten staatsrechtelijk op een andere wijze ingebed dan de inlichtingen- en veiligheidsdiensten. Dit heeft consequenties voor de controle en het toezicht op de inzet van de bevoegdheden door deze overheidsdiensten. De inzet van de bevoegdheid van het onderzoek in een geautomatiseerd werk door de daartoe aangewezen opsporingsambtenaren vindt plaats onder gezag van de officier van justitie. Naast de hiërarchische controle binnen het openbaar ministerie (College van procureurs-generaal en de Procureur-Generaal bij de Hoge Raad) wordt de rechtmatigheid van de inzet van de bevoegdheid in individuele gevallen getoetst door de rechter (de rechter-commissaris en de zittingsrechter). De Inspectie Veiligheid en Justitie is belast met het toezicht op de uitvoering. De Autoriteit persoonsgegevens houdt toezicht op de naleving van de wettelijke regels over gegevensbescherming door de opsporingsinstanties en het openbaar ministerie. Bij klachten over strafvorderlijk optreden kan de Nationale ombudsman voor aanvullende rechtsbescherming zorgen in gevallen waarin de burger geen toegang heeft tot de rechter of een rechter zich niet heeft uitgelaten over een gedraging die een strafvorderlijk aspect kent (artikelen 9:22 en 9:23 Awb). Ten slotte kan het parlement een rol vervullen.

De inzet van de bevoegdheden van de inlichtingen- en veiligheidsdiensten vindt plaats onder verantwoordelijkheid van de Minister van Binnenlandse Zaken en Koninkrijksrelaties, waar het de AIVD betreft, en de Minister van Defensie, ingeval van de MIVD. In het wetsvoorstel Wiv 20xx wordt erin voorzien dat in de gevallen waarbij de minister toestemming dient te verlenen, voorafgaand aan de daadwerkelijke uitoefening van de desbetreffende bevoegdheid de rechtmatigheid van de verleende toestemming wordt getoetst door een onafhankelijke commissie, de Toetsingscommissie inzet bevoegdheden (TIB). Indien de TIB van oordeel is dat de toestemming niet rechtmatig is verleend, vervalt deze van rechtswege. De afdeling toezicht van de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD) is belast met het toezicht op de rechtmatige uitvoering van de Wiv 20xx, waaronder de uitoefening van de bevoegdheden door de inlichtingen- en veiligheidsdiensten. De toezichtsrapporten van de CTIVD worden door de verantwoordelijke minister met diens reactie aan het parlement aangeboden.

De leden van de fractie van het CDA hebben gevraagd hoe de regering de kritiek van de Afdeling advisering van de Raad van State op de proportionaliteit van het voorstel beoordeelt.

De Afdeling advisering van de Raad van State onderschrijft dat bij de bestrijding van ernstige misdrijven binnen de grenzen van het grondwettelijk en verdragsrechtelijk beschermde recht op eerbiediging van de persoonlijke levenssfeer ook van de nieuwe technologische mogelijkheden gebruik moet kunnen worden gemaakt. Het voorstel is in zoverre noodzakelijk. De Afdeling advisering acht echter de voorgestelde bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk onvoldoende gedifferentieerd naar de mate van de ingrijpendheid van die inbreuk op de persoonlijke levenssfeer. Daarmee staat de proportionaliteit van de voorgestelde bevoegdheid, zoals bedoeld in het EVRM, niet vast. Deze bevoegdheid behoeft naar het oordeel van de Afdeling advisering derhalve differentiatie.

De regering is met de Afdeling advisering van oordeel dat het op afstand binnendringen in een geautomatiseerd werk, gevolgd door het doorzoeken van alle gegevens die in dat werk zijn opgeslagen, een meer vergaande inbreuk op de privacy van de betrokkene oplevert dan wanneer het binnendringen wordt gevolgd door het aftappen en opnemen van communicatie of de stelselmatige observatie. Naar aanleiding van het advies van de Afdeling advisering is daarom de voorwaarde voor de inzet van deze bevoegdheid aangescherpt voor de toepassing van onderzoekshandelingen waarbij het geautomatiseerde werk wordt binnengedrongen met het oog op het vastleggen of ontoegankelijk maken van gegevens. Daarbij kunnen gegevens worden doorzocht die in het geautomatiseerde werk worden verwerkt. Voor het verrichten van deze onderzoekshandelingen is een misdrijf vereist dat een ernstige inbreuk op de rechtsorde oplevert en waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld, of een misdrijf dat bij algemene maatregel van bestuur is aangewezen. Beperking van de toepassing tot zeer ernstige misdrijven, waarop gevangenisstraf van acht jaar of meer is gesteld, is echter te beperkend. De bij algemene maatregel van bestuur aan te wijzen misdrijven betreffen bepaalde misdrijven waarop weliswaar geen gevangenisstraf van acht jaar is gesteld maar die naar hun aard worden gepleegd met behulp van een geautomatiseerd werk – het gebruik van een geautomatiseerd werk is dan instrumenteel voor het plegen van het delict – waarbij er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders, en de inzet van andere opsporingsbevoegdheden onvoldoende zicht op resultaat biedt. Dit kan bijvoorbeeld aan de orde zijn bij het ontoegankelijk maken van kinderpornografisch materiaal dat op internet wordt gepubliceerd. Voor het beëindigen van een dergelijke situatie is het van essentieel belang dat op afstand kan worden binnengedrongen in een server om dit materiaal ontoegankelijk te maken. Ook bij de bestrijding van een botnet kan het onvermijdelijk zijn om een server binnen te dringen om de gegevens ontoegankelijk te maken, bijvoorbeeld in de gevallen waarin banken worden belaagd door een zogenaamde DDOS-aanval. Een botnet kan zoveel overlast voor het maatschappelijk verkeer veroorzaken dat de toepassing van de voorgestelde bevoegdheid van het binnendringen van een server of een ander geautomatiseerd werk met het oog op de ontoegankelijkmaking van gegevens aangewezen is, zeker in het licht van de betrekkelijk lichte inbreuk op de bescherming van de persoonlijke levenssfeer die daarbij aan de orde is.

De leden van de fractie van D66 hebben opgemerkt dat het wetsvoorstel een bevoegdheid voor de politie introduceert om binnen te kunnen dringen in elk digitaal apparaat van willekeurige burgers, inclusief toegang tot alle historische en toekomstige gegevens, opgeslagen in randapparatuur en uitgewisseld met verbonden communicatiekanalen. Met de groei van het internet of things zou dit een groeiende lijst (digitale) apparatuur omvatten. De leden van deze fractie hebben erop gewezen dat zowel de Afdeling advisering als het College bescherming persoonsgegevens serieuze kritiek hebben geuit ten aanzien van de door de regering gegeven motivatie, en gevraagd of de regering een nadere toelichting kan geven op de noodzakelijkheid en proportionaliteit en of zij kan onderbouwen waarom een dusdanige verreikende bevoegdheid daadwerkelijk in lijn is met het recht op privacy, zoals beschermd door artikel 8 van het EVRM.

Graag merk ik hierover het volgende op. Er is geen sprake van inzet van de voorgestelde bevoegdheid jegens willekeurige burgers. Het wetsvoorstel koppelt de inzet juist aan een strafrechtelijke relevante verdenking van betrokkenheid van een persoon jegens wie de bevoegdheid kan worden ingezet, bij ernstige strafbare feiten. Het kabinet is zich bewust van de inbreuk op de persoonlijke levenssfeer die de inzet van de voorgestelde bevoegdheid in concrete gevallen met zich mee kan brengen. De inzet van de bevoegdheid vergt daarom

maatwerk, toegesneden op een specifieke situatie. Bij het voorstellen van deze nieuwe bevoegdheid wordt uiteraard rekening gehouden met de privacy van burgers. Het recht op privacy is een belangrijk recht, maar het is geen absoluut recht. In bepaalde gevallen is een inbreuk op dat recht gerechtvaardigd, zoals ten behoeve van de opsporing van strafbare feiten. Een goed voorbeeld is het aftappen en opnemen van communicatie. Ingeval van een absoluut recht op privacy zou dat niet mogelijk zijn. In het voorliggende wetsvoorstel worden de waarborgen van de rechtsstaat uiteraard gerespecteerd. Zo moet het gaan om ernstige strafbare feiten. Het inzetten van deze bevoegdheid is verder pas aan de orde als het onderzoeksbelang dit dringend vereist, er geen andere en minder bezwarende mogelijkheden zijn en als de gevolgen van het optreden in verhouding staan tot het doel. Verder is het binnendringen van een geautomatiseerd werk slechts mogelijk met het oog op het verrichten van bepaalde onderzoekshandelingen. Dit betreft deels bestaande bevoegdheden, zoals het aftappen en opnemen van communicatie en het opnemen van vertrouwelijke communicatie. Dit betreft deels nieuwe bevoegdheden, zoals het vastleggen van opgeslagen gegevens. Inzet van de bevoegdheid vergt een zorgvuldige afweging door het openbaar ministerie, op het niveau van de officier van justitie en op het niveau van het College van procureurs generaal via een verplichte beoordeling door de Centrale Toetsing Commissie. Daarnaast is voorzien in onafhankelijke rechterlijke toetsing, zowel vooraf door een rechter-commissaris als achteraf door de zittingsrechter, zodat een adequate rechterlijke controle verzekerd is. Ten slotte geldt een verplichting tot notificatie van de betrokkene, is voorzien in toezicht door de Inspectie Veiligheid en Justitie en zal periodiek aan de Kamer worden gerapporteerd over de toepassing van de bevoegdheid. Dit betreft het aantal malen dat de bevoegdheid is ingezet en het resultaat van die inzet op het gebied van de strafvervolging. Daarbij zal ook worden ingegaan op de klachten naar aanleiding van de inzet van deze bevoegdheid. Voor de noodzaak voor deze bevoegdheden verwijs ik naar de eerdere beantwoording van een vraag van de leden van de fractie van de SP over hoe groot het probleem is dat dit wetsvoorstel moet oplossen. Voor het antwoord op de vraag hoe de inzet van deze bevoegdheid zich verhoudt met het recht op privacy, zoals beschermd door artikel 8 van het EVRM, wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van de VVD.

De leden van de fractie van de SP hebben opgemerkt dat het binnendringen van een geautomatiseerd werk altijd tot gevolg heeft dat er meer data worden verzameld dan doelmatig gezien nodig is en dat hierdoor ook de privacy van onschuldige burgers wordt bedreigd omdat via het netwerk ook deze in de gaten gehouden kunnen worden. Onder verwijzing naar artikel 3 van de Wet politiegegevens en artikel 8 van het EVRM hebben deze leden gevraagd om een reactie hierop.

Het binnendringen van een geautomatiseerd werk heeft niet altijd tot gevolg dat er meer data worden verzameld dan doelmatig gezien nodig is; de toepassing van de bevoegdheden wordt immers beheerst door de beginselen van proportionaliteit en subsidiariteit. Daarnaast zullen er geen onschuldige burgers via het netwerk in de gaten worden gehouden. De term ‘in de gaten houden’ suggereert een structureel gerichte inzet. Dat is bij onschuldige burgers niet het geval, al kan de verzameling van hun gegevens wel het gevolg zijn van de inzet. De regels rond de inzet van de bevoegdheid zijn er echter juist steeds op gericht om zoveel mogelijk te voorkomen dat gegevens worden verzameld die niet nodig zijn voor het opsporingsonderzoek. Daartoe moet de officier van justitie in het bevel het onderdeel van het geautomatiseerde werk vermelden waartegen het bevel is gericht en ook de functionaliteit die daarbij worden ingezet. Niettemin zal het in de uitvoeringspraktijk onvermijdelijk zijn dat gegevens worden verzameld

van personen die zelf niet bij criminaliteit zijn betrokken. Dat is bij de inzet van traditionele opsporingsmiddelen, als de telefoon- en de IP-tap, niet anders. Bij het aftappen en opnemen van communicatie komen de uitlatingen van gespreksdeelnemers ter kennis van de opsporing en bij de IP-tap betreft dit alle dataverkeer dat van en naar een huisadres of IP-adres gaat, ook het dataverkeer van huisgenoten die de desbetreffende aansluiting gebruiken.

Op grond van de jurisprudentie van het EHRM inzake artikel 8 van het EVRM gelden strenge eisen voor het heimelijk onderscheppen van communicatie van burgers. Voor de vraag of het wetsvoorstel voldoet aan de eisen die daaraan op grond van het EVRM moeten worden gesteld, wordt verwezen naar de eerdere beantwoording in deze paragraaf van een soortgelijke vraag van de leden van de fractie van de VVD.

De leden van de fractie van GroenLinks hebben gevraagd of de regering meent dat het voorgestelde doel, bestrijding van cybercriminaliteit, de voorgestelde middelen heiligt, namelijk de daarmee gepaard gaande inbreuk op individuele grondrechten.

Het wetsvoorstel maakt door de strikte voorwaarden en de diverse waarborgen de inbreuk op de persoonlijk levenssfeer zo klein mogelijk. Zoals hiervoor reeds aan de orde is gekomen, is de regering van oordeel dat de ontwikkeling van computercriminaliteit een ernstige bedreiging vormt van de veiligheid van de Nederlandse samenleving ten aanzien waarvan de opsporingsdiensten nu niet over een gepast antwoord beschikken. Het internet wordt een vrijplaats voor allerlei vormen van ernstige criminaliteit waartegen burgers en bedrijven zich onvoldoende kunnen verweren. Politie en justitie worden ernstig gehinderd in de mogelijkheden om hiertegen op te treden omdat er geen bevoegdheid is om op afstand heimelijk een geautomatiseerd werk binnen te dringen om een einde te maken aan het strafbaar handelen, door gegevens ontoegankelijk te maken, of de daders op te sporen door bewijsmateriaal te verzamelen. Het is vrijwel overbodig te vermelden dat de persoonlijke levenssfeer van de slachtoffers hierbij in het geding is. Het recht op bescherming van de persoonlijke levenssfeer beoogt burgers te vrijwaren tegen ongeoorloofde inmenging van de overheid in hun persoonlijke levenssfeer. Het recht op privacy is echter geen absoluut recht, dit recht dient te worden afgewogen tegen andere zwaarwegende maatschappelijke belangen, zoals het belang van de opsporing en vervolging van ernstige strafbare feiten. Deze balans komt ook tot uitdrukking in de tekst van artikel 8 EVRM. Te dien aanzien kan een vergelijking worden gemaakt met het huisrecht, dat bescherming geniet op grond van artikel 12 van de Grondwet en artikel 8 EVRM. Het huisrecht is echter evenmin een absoluut recht, onder bepaalde omstandigheden en onder bepaalde voorwaarden kan inbreuk worden gemaakt op dit recht. De regering is van oordeel dat met het wetsvoorstel een evenwichtige balans is gevonden tussen de betrokken belangen. Voor de ontwikkeling van de wettelijke voorwaarden is nauw aangesloten bij de criteria voor de toepassing van andere ingrijpende bevoegdheden, zoals de doorzoeking van een woning of de toepassing van bijzondere opsporingsbevoegdheden. Deze waarborgen hebben betrekking op de aard van de strafbare feiten, waarvoor de voorgestelde bevoegdheid kan worden ingezet, de ernst van de verdenking, de mogelijkheid van de inzet van alternatieve bevoegdheden. Hierbij is het vereiste van voorafgaande rechterlijke goedkeuring essentieel.

De voorwaarden die gelden voor de inzet van de voorgestelde bevoegdheid komen overeen met de voorwaarden die gelden voor de inzet van bestaande opsporingsbevoegdheden met een vergelijkbaar indringend karakter. Van een ingrijpende wijziging van de positie van de

verdachte is derhalve geen sprake. De inzet van de bevoegdheid tot het onderzoek in een geautomatiseerd werk is mogelijk als er sprake is van een verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv dat gezien zijn aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert. Dit vereiste geldt ook voor de inzet van andere bijzondere opsporingsbevoegdheden met een heimelijk karakter, zoals de infiltratie (artikelen 126h, 126p en 126ze Sv), het direct afluisteren (artikelen 126l, 126s, en 126zf) of het vorderen van bijzondere persoonsgegevens, bijvoorbeeld gegevens over iemands godsdienst of levensovertuiging, ras of politieke gezindheid (artikelen 126nf, 126uf en 126zn, tweede lid, Sv). Wanneer het geautomatiseerde werk wordt binnengedrongen met het oog op het veiligstellen of ontoegankelijk maken van gegevens geldt overigens voor het verrichten van die onderzoekshandelingen een zwaarder verdenkingscriterium. In dat geval is de verdenking van een misdrijf vereist waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen.

De leden van de fractie van GroenLinks hebben gevraagd waar precies het hiaat zit in de bestaande wettelijke bevoegdheden op dit terrein. De leden van deze fractie hebben tevens gevraagd welke andere mogelijkheden er exact zijn onderzocht en of de regering kan uitleggen waarom deze volgens haar niet voldoen.

De bestaande opsporingsbevoegdheden schieten in toenemende mate tekort om aan wezenlijke problemen en gebleken knelpunten op het gebied van de bestrijding van computercriminaliteit en het vergaren van elektronisch bewijs tegemoet te komen. Ontwikkelingen als de versleuteling van elektronische gegevens, het gebruik van draadloze netwerken en cloudcomputingdiensten dragen hier in belangrijke mate aan bij. Daarnaast kan de voorgestelde bevoegdheid in bepaalde gevallen worden ingezet om de inbreuk op de persoonlijke levenssfeer in het kader van de opsporing zo beperkt mogelijk te houden. De bestaande opsporingsbevoegdheden zijn gebaseerd op het uitgangspunt dat de gegevens die voor de opsporing van belang zijn, zich op een bepaalde gegevensdrager op een bepaalde locatie bevinden. Alsdan kunnen de bestaande bevoegdheden worden ingezet, zoals de doorzoeking van een besloten plaats ter vastlegging van gegevens (art. 125i Sv) of de vordering aan degene die toegang heeft tot bepaalde opgeslagen of vastgelegde gegevens tot verstrekking van die gegevens (art. 126nd/ud Sv). Dit spoort echter niet meer met de werkelijkheid in gevallen waarin smartphones en laptops worden gebruikt of de gegevens zich in de cloud bevinden. Het gebruik van andere, nu al bestaande bevoegdheden, biedt geen soelaas in de zich steeds vaker manifesterende situaties waarin het niet mogelijk is een IP-adres te herleiden tot een specifieke internet dienstverlener, een concreet persoon of een concrete locatie. In die gevallen kunnen de verschillende vorderingen ten aanzien van internet service providers niet worden ingezet omdat niet bekend is aan wie de vordering moet worden verstuurd. Als de locatie van het betreffende geautomatiseerde werk of van de gegevens niet bekend is dan kan evenmin een doorzoeking ter vastlegging van gegevens (artikel 125i Sv) worden uitgevoerd. Ditzelfde geldt voor de andere bevoegdheden tot inbeslagneming van een geautomatiseerd werk of een gegevensdrager (artikelen. 95, eerste lid, 95, eerste lid, 96c, eerste lid, 97 eerste lid, 98, eerste lid, en 99, eerste lid, Sv). Maar ook als de locatie wel bekend is kan de versleuteling van de gegevens de opsporing voor grote problemen plaatsen, aangezien sommige vormen van versleuteling vrijwel niet te kraken zijn. Belangrijk bezwaar van deze bevoegdheden is voorts dat de verdachte doorgaans op de hoogte komt van het feit dat de politie in hem is geïnteresseerd. Dat is doorgaans niet bevorderlijk voor het verdere verloop van het

opsporingsonderzoek, omdat de verdachte alle bewijsmateriaal onmiddellijk zal vernietigen. Het is bijvoorbeeld voorgekomen dat een verdachte van het bezit van kinderpornografie tijdens zijn arrestatie kans zag met zijn voet een schakelaar te bereiken waarmee de stroom van de computer werd afgesloten en de bestanden direct werden gewist. Daardoor ging het bewijsmateriaal verloren. Overigens brengt de inzet van deze bestaande bevoegdheden met zich mee dat politie en justitie kunnen beschikken over alle gegevens die op het geautomatiseerde werk of de gegevensdrager zijn opgeslagen. De wetgever heeft destijds aangegeven dat dit veelal als disproportioneel moet worden aangemerkt in de gevallen waarin een voorwerp in beslag wordt genomen uitsluitend om bepaalde gegevens vast te leggen (Kamerstukken II, 1998/99, 26 671, nr. 3, blz. 19).

Onderzocht is of andere bevoegdheden uitkomst kunnen bieden. Dat lijkt op het eerste gezicht soms het geval, maar bij nadere beschouwing zijn daarbij dikwijls andere zwaarwegende belangen aan de orde. Zo biedt de bevoegdheid tot het opnemen van vertrouwelijke communicatie (artikelen 126l, 126s en 126zf Sv) de mogelijkheid om door middel van een technisch hulpmiddel, zoals een “bug” (een kleine microfoon die opgenomen signalen draadloos verzendt) of een richtmicrofoon, heimelijk vertrouwelijke communicatie op te nemen. Ter uitvoering van de bevoegdheid kan een besloten plaats of een woning worden betreden, zodat het technische hulpmiddel kan worden geplaatst. Deze bevoegdheid biedt echter geen soelaas als de gegevens zijn versleuteld of als de gegevens in de cloud zijn opgeslagen. Verder vormt de noodzaak van fysieke toegang tot de plaats waar het geautomatiseerde werk zich bevindt een grote belemmering voor de opsporing zowel in de gevallen waarin de locatie van het geautomatiseerde werk niet bekend is (terwijl de technische ontwikkelingen het op afstand plaatsen van een “bug” wel mogelijk maken) als in gevallen waarin die locatie wel bekend is, maar de kans bestaat op ontdekking of op onvoorziene omstandigheden ter plaatse. Andere opsporingsbevoegdheden zoals de observatie (artikelen 126g, 126o en 126zd, eerste lid, onderdeel a Sv), het stelselmatig inwinnen van informatie (artikelen 126j, 126qa en 126zd, eerste lid, onderdeel c Sv) of de inkijkoperatie (artikelen 126k, 126r en 126zd, eerste lid, onderdeel d Sv) bieden geen uitzicht op toegang tot gegevens die langs elektronische weg worden verwerkt en bieden dan ook weinig kans op kennisneming van de inhoud van de gegevens die door de verdachte zijn ontvangen of verzonden, of van de communicatie waarbij hij is betrokken.

De leden van de fractie van GroenLinks hebben erop gewezen dat de Afdeling advisering van de Raad van State heeft geoordeeld dat de proportionaliteit van het heimelijk binnendringen in een geautomatiseerd werk onbewezen is gebleven en dat ook andere organisaties stevige kritiek hebben geuit op het wetsvoorstel. De leden van deze fractie hebben opgemerkt dat het College bescherming persoonsgegevens heeft geadviseerd om het wetsvoorstel niet op deze wijze in te dienen omdat het wetsvoorstel een grondwettelijke toetsing niet zou doorstaan. Zij hebben gevraagd wat de verwachting van de regering is ten aanzien van een dergelijke grondwettelijke toetsing van het wetsvoorstel.

Eerder in deze paragraaf is, naar aanleiding van een vraag van de leden van de fractie van de VVD, reeds ingegaan op de vraag in hoeverre het wetsvoorstel voldoet aan de vereisten die voortvloeien uit het EVRM, in het bijzonder ten aanzien van het recht op bescherming van de persoonlijke levenssfeer. Anders dan het College bescherming persoonsgegevens (thans de Autoriteit persoonsgegevens) ziet de regering geen reden waarom de voorgestelde regeling niet zou voldoen aan de vereisten op het gebied van de bescherming van de persoonlijke

levenssfeer, zoals die voortvloeien uit artikel 8 EVRM. Zoals hiervoor aangegeven heeft het advies van de Afdeling advisering van de Raad van State aanleiding gegeven tot aanpassing van het wetsvoorstel.

De leden van de fractie van GroenLinks hebben erop gewezen dat ook de Nederlandse burgerrechtenorganisatie Bits of Freedom het wetsvoorstel te ruim vindt in zijn bevoegdheden. Onder verwijzing naar het voorbeeld van de pacemaker hebben de leden van deze fractie gevraagd waarom, naast de bestaande mogelijkheden en naast de mogelijkheden in de wetten computercriminaliteit I en computercriminaliteit II, nu nog extra bevoegdheden nodig zijn.

Graag benadruk ik nogmaals dat er strikte regels gelden voor de inzet van de bevoegdheid, waaronder het vereiste van een misdrijf waarvoor voorlopige hechtenis is toegelaten. Verder geldt het vereiste van een voorafgaande rechterlijke toetsing. De omschrijving van het begrip geautomatiseerd werk is identiek aan die van het Verdrag van de Raad van Europa (artikel 1: "”computer system’’ means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;"). De definitie van de EU is overigens nog iets ruimer, omdat daarin ook computergegevens zijn betrokken. Het is inherent aan de gehanteerde definitie van geautomatiseerd werk dat de ontwikkeling van apparatuur en systemen die aan die definitie voldoen daarmee ook onder de reikwijdte van de bevoegdheid komen te vallen. De ontwikkeling van het internet of things (waarbij 'slimme apparaten' als koelkasten, navigatiesystemen en thermostaten via het internet worden aangestuurd) kan meebrengen dat die apparaten via het internet kunnen worden binnengedrongen.

Het bij voorbaat uitsluiten van bepaalde geautomatiseerde werken belemmert de opsporing en biedt criminelen meer mogelijkheden de opsporing te ontlopen door juist dergelijke systemen te misbruiken voor het plegen van strafbare feiten. Dat is niet in het belang van de veiligheid van dergelijke systemen. Bovendien staat de techniek niet stil en kent de creativiteit van de misdaad helaas weinig grenzen. De aard van het geautomatiseerde werk zal reden kunnen zijn voor grote terughoudendheid bij de inzet, of bepalend zijn voor het besluit tot de inzet of juist het afzien daarvan. Uiteraard wordt, indien mogelijk, gekozen voor de inzet van minder vergaande bevoegdheden, zoals een vordering van gegevens aan de beheerder van het desbetreffende systeem. De eisen die aan de uitoefening van de bevoegdheid worden gesteld, gecombineerd met het uitgebreide toezicht door zowel de rechter als de Inspectie Veiligheid en Justitie, brengt naar mijn oordeel mee dat er is voorzien in adequate waarborgen tegen oneigenlijk gebruik van de bevoegdheid. Hoewel een pacemaker in beginsel onder de definitie van geautomatiseerd werk valt, zullen hierin naar verwachting geen gegevens te vinden zijn die bijdragen aan de opsporing van ernstige vormen van computercriminaliteit of andere ernstige strafbare feiten. In de praktijk is het tevens moeilijk denkbaar dat er zich een zo zwaarwegend belang voordoet dat het binnentreden van een pacemaker proportioneel zou worden geacht.

De leden van de fractie van GroenLinks hebben gevraagd wat precies de reikwijdte is van deze wet, en of in het wetsvoorstel rekening wordt gehouden met eerdere uitspraken van het Hof van Justitie van de Europese Unie, dat de afgelopen jaren meermalen kritiek op wetten had die de privacy van burgers te veel zouden schenden.

Wat betreft de reikwijdte van de voorgestelde bevoegdheid is nauw aangesloten bij het wettelijke systeem voor de toepassing van andere bijzondere opsporingsbevoegdheden. De

voorgestelde bevoegdheid kan worden toegepast ingeval van (1) verdenking van een ernstig strafbaar feit waarvoor voorlopige hechtenis kan worden toegepast, (2) het vermoeden dat in georganiseerd verband ernstige strafbare feiten worden beraamd of gepleegd die gezien hun aard of samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren, of (3) aanwijzingen van een terroristisch misdrijf. Dit betreft de bestaande criteria voor de toepassing van bijzondere opsporingsbevoegdheden. Daarbij geldt een drempel voor wat betreft de ernst van de strafbare feiten, te weten een misdrijf waarvoor voorlopige hechtenis kan worden toegepast. Verder geldt het vereiste van voorafgaande rechterlijke toestemming.

In antwoord op de vraag over de uitspraken van het Hof van Justitie van de Europese Unie merkt de regering op ervan overtuigd te zijn dat het wetsvoorstel voldoet aan de eisen die daaraan op grond van het Handvest van de grondrechten van de Europese Unie moeten worden gesteld. Voor de toelichting op dit oordeel wordt verwezen naar de eerdere beantwoording in deze paragraaf van een soortgelijke vraag van de leden van de fractie van de VVD.

4. Samenloop bevoegdheden AIVD en MIVD

De leden van de fractie van D66 hebben opgemerkt dat in het wetsvoorstel staat dat de hackbevoegdheid ook ingezet mag worden tegen terrorismedreiging of een internationale cyberdreiging. De leden van deze fractie hebben gevraagd waarom de regering deze bevoegdheid ook wil uitbreiden naar de politie, als de AIVD en MIVD deze bevoegdheid reeds hebben. De leden van deze fractie hebben tevens gevraagd of de regering kan aangeven of dit de afbakening van taken van deze instanties niet juist versnippert en onduidelijker maakt.

De bestrijding van terrorisme is niet alleen relevant in de context van de bescherming van de nationale veiligheid maar eveneens in die van de criminaliteitsbestrijding. Met de Wet terroristische misdrijven van 24 juni 2004 (Stb. 2004, 290) is het materiële strafrecht aangescherpt zodat dit beter is toegesneden op terrorisme en het rekruteren voor de jihad. Daartoe zijn een aantal gedragingen, bij aanwezigheid van het zogenaamde «terroristisch oogmerk», als terroristisch misdrijf strafbaar gesteld. Tevens is de deelneming aan en het leiden van een organisatie die tot oogmerk heeft het plegen van terroristische misdrijven strafbaar gesteld met minimaal acht respectievelijk vijftien jaar gevangenisstraf. Een belangrijke functie van het strafrecht bij terroristische misdrijven ligt in het voorkomen van terroristische aanslagen. Met de wet tot wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven van 20 november 2006 (Stb. 2006, 580) zijn de toepassingsmogelijkheden van bijzondere opsporingsbevoegdheden verruimd ten behoeve van een adequate bestrijding van terroristische misdrijven. In geval van aanwijzingen van een terroristisch misdrijf kunnen bijzondere opsporingsbevoegdheden, zoals de stelselmatige observatie, de pseudokoop en –dienstverlening, de infiltratie en het aftappen en opnemen van communicatie, worden toegepast. Bij ‘aanwijzingen’ van terroristische misdrijven kan het openbaar ministerie al in een vroeg stadium strafrechtelijk ingrijpen. Vanwege de ernst van terroristische misdrijven en hun mogelijke impact op het maatschappelijk leven en de veiligheid van burgers, het hiermee samenhangende zwaarwegende publieke belang om aanslagen te voorkomen en het tekortschieten van de bestaande opsporingsbevoegdheden bij het gebruik van de moderne informatie- en communicatietechnologie (zoals het gebruik van encryptie bij de communicatie met anderen en de opslag van gegevens in de cloud) ligt het

voor de hand dat de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk ook kan worden toegepast ingeval van aanwijzingen van dergelijke misdrijven.

Versnippering in de afbakening van taken van deze instanties vanwege de uitbreiding van deze bevoegdheid naar de politie, zoals gesteld door de leden van de fractie van D66, is niet aan de orde. Het voorkómen van terroristische aanslagen betreft niet een taak die exclusief is toebedeeld aan een bepaalde overheidsorganisatie. Waar de AIVD zich in het kader van de nationale veiligheid – onder meer door het permanent verkennen van tendensen binnen de samenleving – richt op het tijdig onderkennen en zo mogelijk voorkomen van (de realisatie van) terroristische dreigingen, ligt bij de politie en het openbaar ministerie de nadruk op het opsporen en vervolgen van terroristische misdrijven. Dikwijls zal het dan gaan om opsporingsonderzoek naar het voorbereidende stadium van terroristische misdrijven, mede gericht derhalve op het daadwerkelijk voorkomen van terroristische aanslagen, naast – waar mogelijk – het komen tot vervolging. Het voorliggende wetsvoorstel voorziet uitsluitend in aanpassing van de bevoegdheden zodat de bestaande taak beter kan worden uitgevoerd. Voor zover in de praktijk kans zou bestaan op overlap wordt op grond van de Wiv 2002 voorzien in procedures ten behoeve van de afstemming tussen de bescherming van de nationale veiligheid enerzijds en de opsporing van strafbare feiten anderzijds. Als bij de verwerking van gegevens door of ten behoeve van een dienst blijkt van gegevens die tevens van belang kunnen zijn voor de opsporing of vervolging van strafbare feiten, dan kan hiervan mededeling worden gedaan aan de landelijk officier van justitie die is belast met de bestrijding van terroristische misdrijven (artikel 38, eerste lid, Wiv 2002). Andersom zijn de leden van het openbaar ministerie gehouden, door tussenkomst van het College van procureurs-generaal, aan een dienst mededeling te doen van de te hunner kennis gekomen gegevens die zij voor die dienst van belang achten (artikel 61, eerste lid, Wiv 2002). Hierdoor is een goede afstemming tussen de betrokken organen bij de voorkoming en bestrijding van terrorisme verzekerd.

De leden van de fractie van de SP hebben gevraagd waarom de regering met dit wetsvoorstel de bevoegdheid om terroristische aanslagen te voorkomen wil uitbreiden naar de politie, en of het juist is dat de inlichtingendiensten dit tot taak hebben.

Met dit wetsvoorstel wordt geenszins beoogd het werkterrein van politie en justitie uit te breiden . Zoals reeds aangegeven gaat het bij terrorisme om het plegen van de meest ernstige vormen van strafbare feiten. Met behulp van het strafrecht moet daartegen krachtig worden opgetreden en daarmee is gegeven dat ook politie en justitie een belangrijke taak op het terrein van terrorismebestrijding hebben. Dit wetsvoorstel voorziet overigens wel in een uitbreiding van de strafvorderlijke bevoegdheden voor de bestrijding van terrorisme. Voor de redenen die daaraan ten grondslag liggen kan worden verwezen naar mijn eerdere antwoord op een soortgelijke vraag van de leden van de fractie van D66.

De leden van de fractie van de ChristenUnie hebben opgemerkt dat de bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk op dit moment al kan worden toegepast door de AIVD en MIVD, en hebben gevraagd naar de noodzaak van de nieuwe voorgestelde bevoegdheid en de ratio achter de geringe clausulering voor het gebruik daarvan door de opsporingsdiensten.

Voor de noodzaak van de voorgestelde bevoegdheid verwijs ik graag naar de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van D66. De mening dat

de bevoegdheid gering is geclausuleerd wordt dezerzijds niet onderschreven; de bevoegdheid is juist voorzien van strikte waarborgen en garanties, zowel bij de voorbereiding, de uitvoering als de verantwoording daarvan. Voor een nadere toelichting op de strikte clausering verwijs ik naar de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van D66.

De leden van de fractie van de ChristenUnie hebben gevraagd of er andere terreinen zijn dan de opsporing van terroristische misdrijven en kinderpornografie waar de opsporingsdiensten onvoldoende resultaat boeken als gevolg van het ontbreken van de voorgestelde hackbevoegdheden. De leden van deze fractie hebben tevens gevraagd om een nadere cijfermatige onderbouwing van de noodzaak om deze bevoegdheid zo ruim uit te breiden.

De technologische ontwikkelingen gaan zo snel dat bij vele vormen van criminaliteit gebruik wordt gemaakt van het internet of digitale middelen. De bevoegdheid is dan ook zeer belangrijk voor het kunnen blijven bestrijden van computercriminaliteit, waarvan de omvang groeit en de bestrijding steeds gecompliceerder wordt. In deze vorm van criminaliteit komen de encryptieproblemen, afschermingsproblemen alsmede het internationale karakter van de pleegplaatsen en aanwezigheid van bewijsmateriaal in alle indringendheid naar voren, zoals door vele cybersecurity specialisten wordt onderschreven. Voorts is de bevoegdheid van belang voor de bestrijding van de gevestigde georganiseerde criminaliteit. Zoals uit recente onderzoeken is gebleken, is de invoering van het gebruik van encryptietechnieken en andere afschermingmethodieken, waarbij het niet meer goed mogelijk is voor de politie om de inhoud van de communicatie te onderscheppen, gemeengoed geworden. Organisaties worden gefaciliteerd in het zo anoniem mogelijk communiceren, bijvoorbeeld met het oog op het plegen van moorden, drugstransporten, wapenhandel en ondermijnende criminaliteit, zoals witwassen, fraude en corruptie. In dergelijke zaken is het van groot belang om de anonimiseringstechnieken en versleutelingtechnieken te doorbreken. Er zijn geen cijfers te geven over in hoeveel zaken het wel of niet nodig is geweest om deze bevoegdheid te kunnen inzetten. Er wordt niet per zaak geregistreerd welke niet-bestaande bevoegdheden tot een meer effectieve opsporing hadden kunnen leiden.

De leden van de fractie van de ChristenUnie zouden graag inzicht krijgen in hoe vaak de veiligheidsdiensten op dit moment gebruikmaken van de bevoegdheden tot het heimelijk binnendringen van een geautomatiseerd werk en hoe zich dit verhoudt tot het gebruik van dit instrument in de omliggende landen. De leden van deze fractie hebben tevens gevraagd hoe vaak gebruik wordt gemaakt van de bemachtigde gegevens van de veiligheidsdiensten in een strafproces.

Informatie over de mate waarin specifieke bijzondere bevoegdheden worden ingezet geeft inzicht in de werkwijze van de diensten. Dergelijke informatie is staatsgeheim, en kan derhalve uitsluitend vertrouwelijk via de daartoe geëigende kanalen aan de Tweede Kamer, in casu de CIVD, worden verstrekt. Als bij de verwerking van gegevens door of ten behoeve van een dienst blijkt van gegevens die tevens van belang kunnen zijn voor de opsporing of vervolging van strafbare feiten, kan daarvan mededeling worden gedaan aan de Landelijk officier van justitie die is belast met de bestrijding van terroristische misdrijven. De procedure is vastgelegd in artikel 38 Wiv 2002. Het is niet bekend hoe vaak gebruik wordt gemaakt van de gegevens van de veiligheidsdiensten in een strafproces

5. Kwetsbaarheden

De leden van de fractie van het CDA hebben erop gewezen dat in de Tweede Kamer uitgebreid debat is gevoerd over de in dit wetsvoorstel verleende bevoegdheid aan het openbaar ministerie om uitstel te verlenen aan het melden van onbekende kwetsbaarheden aan de producent als de opsporing er zwaarwegend belang bij heeft om deze melding nog uit te stellen. In het wetsvoorstel wordt geen termijn aan het – in beginsel ongeoorloofde - uitstel tot melding van een kwetsbaarheid gesteld. In het debat wordt gewag gemaakt van een termijn van vier weken, maar die termijn kan door de rechter-commissaris steeds weer met vier weken worden verlengd. Het lijkt de leden van deze fractie verstandig om de maximale termijn alsnog in de wet te noemen zodat de onbekende kwetsbaarheid kan worden gerepareerd en zij hebben gevraagd of de regering hier nader op in kan gaan.

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. Deze afweging overstijgt het individuele opsporingsonderzoek en wordt daarom binnen het openbaar ministerie centraal gemaakt. Het wetsvoorstel voorziet in de mogelijkheid voor de officier van justitie om, op grond van een zwaarwegend opsporingsbelang, te bevelen dat het bekend maken aan de producent van een onbekende kwetsbaarheid voor het binnendringen in een geautomatiseerd werk als bedoeld in de artikelen 126nba, 126uba en 126zpa Sv, wordt uitgesteld (artikel 126ffa Sv). Voor het afzien van het 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 aan de interactie tussen officier van justitie en rechter-commissaris gelaten om te komen tot nadere inkadering van de periode van geldigheid van het uitstel. Het ligt echter in de rede 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. De bevoegdheid tot het onderzoek in een geautomatiseerd werk is gekoppeld aan een periode van vier weken, daarna kan het bevel telkens met een periode van vier weken worden verlengd. Dit is vastgelegd in het voorgestelde artikelen 126nba, derde lid, respectievelijk 126uba/zpa, derde lid, Sv. Het ligt in de rede 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.

Een verlenging van de machtiging kan zich bijvoorbeeld voordoen als de melding zou resulteren in het tenietdoen van het heimelijke karakter van het opsporingsonderzoek. Ook kan de onbekende kwetsbaarheid een systeem of computerprogramma betreffen 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. In dergelijke gevallen kan langduriger uitstel van de melding aan de fabrikant aan de orde zijn. Het uitstel wordt dan periodiek door de rechter-commissaris getoetst. Het uitstellen van het delen van informatie over aangetroffen onbekende kwetsbaarheden in wijdverbreide en regulier gebruikte hard- of software ligt uiteraard niet in de rede.

De leden van de fractie van D66 hebben opgemerkt dat de politie gebruik zal maken van niet bekende kwetsbaarheden om in te breken in geautomatiseerde apparatuur. Hiermee houdt de politie naar het oordeel van de leden van deze fractie het bestaan van dergelijke

kwetsbaarheden in stand, waarmee het internet en digitale apparaten onveiliger worden in plaats van veiliger. Deze leden hebben gevraagd waarom de regering niet investeert in het veiliger maken van de digitale wereld in plaats van het financieren en gebruik van niet bekende kwetsbaarheden.

De regering investeert aanzienlijk in het veiliger maken van de digitale wereld. De regering heeft het wetsvoorstel Gegevensverwerking en meldplicht cyber security (Kamerstukken 34 388) aan uw Kamer gezonden. Dit voorstel bevat een meldplicht voor inbreuken op de veiligheid of een verlies van integriteit van elektronische informatiesystemen bij vitale sectoren. Ook wordt informatie en handelingsperspectief geboden aan eindgebruikers via veiliginternetten.nl en de jaarlijkse campagne Alert Online. In aanvulling hierop wordt gestimuleerd om te investeren in het veiliger maken van apparaten en een goede cyber hygiëne. De overheid stimuleert bovendien het verminderen van kwetsbaarheden met het beleid voor 'responsible disclosure'. Naast voorlichting aan haar partners over door derden gemelde kwetsbaarheden zal het Nationaal Cyber Security Centrum van het Ministerie van Veiligheid en Justitie (NCSC) in voorkomende gevallen ontdekte kwetsbaarheden zelf melden aan de fabrikant. De politie zal overigens geen informatie over onbekende kwetsbaarheden inkopen ten behoeve van de inzet van de voorstelde bevoegdheid tot binnendringen in geautomatiseerd werk.

De Nederlandse regering werkt aan een open, vrij en veilig internet. Effectieve handhaving van de rechtsstaat in cyberspace is hiervoor een voorwaarde. Dit wetsvoorstel ziet op het versterken van de opsporing van criminaliteit op internet, zodat kwaadwillenden die het digitale domein misbruiken effectief kunnen worden aangepakt. De overheid investeert bovendien ook op diverse andere manieren in het veiliger maken van het internet en stimuleert dit ook actief. Bij het binnendringen in een geautomatiseerd werk met het oog op het uitvoeren van onderzoekshandelingen zal gebruik worden gemaakt van zowel bekende als onbekende kwetsbaarheden. Er zijn veel bruikbare bekende kwetsbaarheden. Anders dan de vragenstellers veronderstellen zullen niet uitsluitend onbekende kwetsbaarheden worden gebruikt, bekende kwetsbaarheden kunnen naar verwachting in veel gevallen bruikbaar zijn.

De leden van de fractie van de SP hebben geconstateerd dat de hacksoftware door externe partijen ontwikkeld zal worden en dat de politie zonder gedegen kennis eigenlijk niet weet wat zij inkoopt, en gevraagd hoe de regering voorkomt dat de politie schadelijke software inkoopt die weliswaar doet wat het zegt maar tevens informatie over de politie aan derden verschaft.

In het ter uitvoering van het wetsvoorstel opgestelde Besluit onderzoek in een geautomatiseerd werk, waarover uw Kamer bij brief van 10 mei 2017 (Kamerstukken II 2016/17, 34 372, nr. 26) is geïnformeerd, worden verschillende keuringseisen gesteld aan de inrichting en werking van een technisch hulpmiddel dat wordt gebruikt voor het detecteren, registeren en transporteren van gegevens. Eén van de eisen is dat een technisch hulpmiddel beveiligd is tegen wijziging van de werking ervan en tegen wijziging en kennisneming van geregistreerde gegevens door onbevoegden. Ook moet een technisch hulpmiddel in staat zijn om geregistreerde gegevens op zodanige wijze te transporteren dat de gegevens automatisch op een technische infrastructuur binnen de politieorganisatie worden vastgelegd. Met deze eisen wordt voorzien in adequate en effectieve waarborgen tegen willekeurige inmenging en misbruik en worden de betrouwbaarheid en de integriteit van de vastgelegde gegevens verzekerd. Als bij

het onderzoek in een geautomatiseerd werk gebruik wordt gemaakt van een goedgekeurd technisch hulpmiddel, mag er vanuit worden gegaan dat aan de wettelijke eisen is voldaan.

Gedurende de uitvoering van een bevel van de officier van justitie worden doorlopend en automatisch gegevens vastgelegd over de met een technisch hulpmiddel verrichte onderzoekshandelingen en het functioneren van de technische infrastructuur waarop de met een technisch hulpmiddel geregistreerde gegevens worden vastgelegd. Dit wordt ook wel "logging" genoemd. Op deze wijze kan zowel tijdens het verrichten van onderzoekshandelingen als achteraf intern toezicht plaatsvinden binnen de politieorganisatie op de uitvoering van het bevel van de officier van justitie.

Daarnaast houdt de Inspectie Veiligheid en Justitie toezicht op het functioneren van het wettelijke systeem omtrent de binnendring- en onderzoeksbevoegdheid. Dit toezicht heeft onder meer betrekking op aspecten als de inzet van een technisch hulpmiddel, de vastlegging van de met een technisch hulpmiddel geregistreerde gegevens op een technische infrastructuur, de beveiliging van de gegevens en de "logging" over de uitvoering van een bevel.

Bij de leden van de fractie van de SP leeft een grote zorg over het gebruikmaken van de zogenaamde Zero Day-zwaktes. Zij hebben gevraagd hoe de regering erover oordeelt dat dit in de Verenigde Staten heeft geleid tot het seponeren van een zaak van kindermisbruik.

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. Slechts in uitzonderlijke situaties kan, uitsluitend bij een zwaarwegend opsporingsbelang en na accordering van het centraal aanspreekpunt bij het Landelijk Parket, worden besloten om de rechter-commissaris toestemming te vragen om de melding uit te stellen. Overigens is de kans klein dat politie en justitie een onbekende kwetsbaarheid ontdekken die niet eerder reeds is ontdekt en besproken. Vanwege de hiervoor genoemde verplichting die volgt uit het amendement Recourt/Tellegen speelt het al dan niet melden reeds een rol voordat een zaak naar de rechter gaat. De melding van de kwetsbaarheid wordt onafhankelijk getoetst.

De leden van de fractie van de SP hebben gevraagd of het denkbaar is dat de politie een zaak van kindermisbruik (of andere ernstige misdrijven) moet laten varen vanwege het feit dat zij de Zero Day niet wil openbaren. De leden van deze fractie hebben tevens gevraagd hoe de regering oordeelt over de morele kant van de zaak.

Op dit moment ziet de regering geen realistische scenario's waarbij het openbaar ministerie moet besluiten om de vervolging te staken of niet door te zetten vanwege dit dilemma. Dit wordt niet voorzien omdat er rond de inzet van de middelen en de onbekende kwetsbaarheden vele waarborgen worden ingevoerd en vanwege de verplichting die voortvloeit uit het eerdergenoemde amendement Recourt/Tellegen. Mochten er zwaarwegende redenen zijn tot uitstel van de melding, dan worden die onafhankelijk getoetst.

De leden van de fractie van de SP hebben opgemerkt dat de politie op de hoogte is van een zwakte waar vele criminelen gebruik van zullen maken en hebben gevraagd of het niet de taak van de politie is om mensen te beschermen tegen criminaliteit. De leden van de fractie hebben tevens gevraagd of het niet melden van kwetsbaarheden in de beveiliging niet een vorm van meewerken aan de criminaliteit is, en hebben hierover de mening van de regering gevraagd.

In de beantwoording van een eerdere vraag van de leden van de CDA fractie over het opnemen van een maximale termijn is aangegeven dat juist het melden van een onbekende kwetsbaarheid in gevallen het effect zou hebben criminaliteit ongemoeid te laten omdat de opsporing niet kan worden voortgezet. Effectieve handhaving van de rechtsstaat in cyberspace is een voorwaarde voor een veilig internet en van belang voor het recht doen aan slachtoffers. Zoals in antwoord op diverse vragen hierboven is aangegeven levert het voorliggende wetsvoorstel hieraan een belangrijke bijdrage. Daarnaast zijn de inzet en het gebruik van onbekende kwetsbaarheden met diverse waarborgen omkleed en geldt een verplichting tot melden van deze kwetsbaarheden met de mogelijkheid van tijdelijk uitstel. In het licht hiervan ziet de regering niet in waarom deze bevoegdheidsuitoefening zou neerkomen op een vorm van meewerken aan criminaliteit.

De leden van de fractie van de PvdA hebben gevraagd of zij het goed hebben begrepen dat de voorgestelde bevoegdheid voor opsporingsinstanties om onder voorwaarden een geautomatiseerd werk dat in gebruik is bij een verdachte, op afstand heimelijk binnen te dringen impliceert dat de overheid hackkennis op de markt zal gaan verwerven.

De politie zal geen informatie over onbekende kwetsbaarheden inkopen ten behoeve van de inzet van de voorstelde bevoegdheid tot het binnendringen in een geautomatiseerd werk. Wel is het mogelijk dat de politie software aanschaft waarmee in bepaalde gevallen het binnendringen in geautomatiseerd werk wordt uitgevoerd. Niet kan worden uitgesloten dat dergelijke software gebruik maakt van onbekende kwetsbaarheden. Leveranciers van dergelijke software geven hun broncode doorgaans niet prijs. Het heimelijk binnendringen 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. Om hun kennis actueel te houden zullen zij herhaaldelijk cursussen en opleidingen volgen.

De leden van de fractie van de PvdA hebben opgemerkt dat op grond van het voorliggende wetsvoorstel opsporingsinstanties bij het hacken zelfs gebruik mogen maken van onbekende kwetsbaarheden in de software. De leden van deze fractie hebben gevraagd of de regering zo niet het risico loopt mee te werken aan het in stand houden van de markt van onbekende kwetsbaarheden, waarmee veel geld wordt verdiend ten koste van de digitale veiligheid van de Nederlandse burgers.

In aanvulling op de eerdere beantwoording van de vragen van de leden van de fracties van de SP en de PvdA wordt benadrukt dat de politie zich niet begeeft op de markt voor onbekende kwetsbaarheden. De markt voor software ten behoeve van het binnendringen in een geautomatiseerd werk is internationaal van aard en bestaat onafhankelijk van dit wetsvoorstel. De invloed van de Nederlandse opsporingsdiensten op deze markt is gering. Van het in stand houden van de markt door de aanschaf van dergelijke software is dan ook geen sprake.

De leden van de fractie van de PvdA hebben erop gewezen dat de in artikel 126ffa voorgestelde regeling het mogelijk maakt dat die melding op grond van een zwaarwegend opsporingsbelang wordt uitgesteld en dat Bits of Freedom bij brief van 23 februari 2017 een aantal kritische kanttekeningen heeft geformuleerd bij dit artikel. De leden van deze fractie hebben de regering verzocht ten gronde te reageren op de volgende opmerkingen:

1. De opsporingsinstanties zullen veelal gebruikmaken van softwarepakketten die het hacken sterk vergemakkelijken. Volgens Bits of Freedom zullen opsporingsinstanties vaak niet weten van welke kwetsbaarheden daarbij gebruik wordt gemaakt en of deze gemeld moeten worden: "Als de Nederlandse opsporingsdiensten niet weten of zij gebruik maken van onbekende kwetsbaarheden, dan hoeven zij deze ook niet te melden. Wat je niet weet kun je immers niet melden. De meldplicht wordt dan omzeild."

De politie zal geen informatie over onbekende kwetsbaarheden inkopen ten behoeve van de inzet van de voorgestelde bevoegdheid tot het binnendringen in een geautomatiseerd werk. Wel is het mogelijk dat de politie software aanschaft waarmee in bepaalde gevallen het binnendringen in een geautomatiseerd werk wordt uitgevoerd. Niet kan worden uitgesloten dat dergelijke software gebruik maakt van onbekende kwetsbaarheden. Leveranciers van dergelijke software geven hun broncode doorgaans niet prijs. 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.

2. Het is volgens Bits of Freedom zeer aannemelijk dat onbekende kwetsbaarheden gebruikt worden in hacksoftware. Die zullen door het bedrijf dat die software levert, zelf gevonden of ingekocht zijn: "In ieder geval zal de Nederlandse overheid daarmee wel degelijk een bijdrage leveren aan het vercommercialiseren van onze digitale kwetsbaarheid."

Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van de PvdA.

3. Als de betreffende opsporingsinstantie al weet welke onbekende kwetsbaarheden worden gebruikt, dan is het nog maar de vraag of zij dat wel zal melden. Op grond van geheimhoudingsverklaringen die de leverancier van de hacksoftware zal bedingen, zal het de opsporingsinstanties verboden zijn om onbekende kwetsbaarheden bekend te maken, aldus Bits of Freedom.

Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van soortgelijke vragen van de leden van de fractie van de PvdA.

4. Het gebruik van de betreffende hacksoftware is volgens Bits of Freedom omstreden, omdat deze ook zal worden geleverd aan landen die het niet zo nauw nemen met de grondrechten van hun burgers.

Gezien de mogelijkheden om kennis over kwetsbaarheden voor ongewenste doeleinden in te zetten, is de verkoop ervan aan bepaalde partijen onwenselijk. De mogelijkheid tot anonimiteit

op het internet maakt het echter gemakkelijk om heimelijk kennis over kwetsbaarheden aan te bieden en aan te schaffen. Zoals hiervoor is aangegeven is de markt voor software ten behoeve van het binnendringen in een geautomatiseerd werk internationaal van aard en bestaat deze markt onafhankelijk van dit wetsvoorstel. De invloed van de Nederlandse opsporingsdiensten op deze markt is dan ook gering. De verkoop van technologie voor 'intrusion software', die gebruik maakt van kwetsbaarheden, is onderhevig aan exportcontrole op grond van de Europese Dual-use verordening. De Europese Commissie heeft een voorstel gedaan voor de herziening van de bestaande verordening met het doel deze te moderniseren en beter aan te laten sluiten op de internationale ontwikkelingen. De Commissie stelt onder meer voor om de controle van export van cybertoezichttechnologie te intensiveren in relatie tot mensenrechtenschendingen. Nederland is voorstander van het uitbreiden van de reeds bestaande controle op apparatuur voor cybertoezicht met het voorkomen van mensenrechtenschendingen als grondslag. De EU loopt daarmee wereldwijd voorop en het sluit aan bij de bestaande Nederlandse praktijk waarbij mensenrechten als criterium voor exportcontrole wordt toegepast.

5. Het in artikel 126ffa van het wetsvoorstel voorgestelde meldingsregime werkt volgens Bits of Freedom in de praktijk niet, omdat het kan betekenen dat het ene opsporingsteam (gezien het zwaarwegende opsporingsbelang) wel machtiging van de rechter-commissaris krijgt voor uitstel van de melding, terwijl een andere opsporingsteam dat gebruikmaakt van dezelfde onbekende kwetsbaarheid, geen toestemming krijgt (vanwege een geringer opsporingsbelang) en dus de betreffende kwetsbaarheid zou moeten melden, waarna het beveiligingslek gedicht gaat worden. Dat laatste zou echter het werk van het eerstgenoemde opsporingsteam verstoren.

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. In dergelijke gevallen kan het openbaar ministerie, na machtiging van de rechter-commissaris, besluiten de melding van een kwetsbaarheid uit te stellen. Deze afweging overstijgt het individuele opsporingsonderzoek en wordt daarom binnen het openbaar ministerie centraal gemaakt. 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. De opdracht om de kwetsbaarheid te melden komt terecht bij hetzelfde team van de Landelijke eenheid van de Nationale politie. Bij dat team is het overzicht over het gebruik en melden van onbekende kwetsbaarheden.

De leden van de fractie van de PvdA hebben aandacht gevraagd voor de aanschaf en veiligheid van de malware die Nederlandse opsporingsinstanties gaan gebruiken. Met verwijzing naar de brief van Bits of Freedom, waarin wordt gewezen op de Bundestrojaner-affaire en de Verint-zaak, hebben de leden van deze fractie gevraagd hoe de opsporingsinstanties aan de malware komen, of bepaalde voorwaarden voor de aanschaf worden gehanteerd en of de Nederlandse overheid te allen tijde inzicht in de broncode van de malware eist. Ook hebben deze leden gevraagd hoe van derden gekochte malware wordt gecontroleerd op veiligheid, bijvoorbeeld op de aanwezigheid van zogenaamde backdoors.

In de eerdere beantwoording van een vraag van de leden van de fractie van de SP is reeds ingegaan op de vraag hoe de integriteit van het technische hulpmiddel wordt getoetst. In aanvulling daarop kan worden gemeld dat de technische hulpmiddelen waarmee tijdens de onderzoeksfase onderzoekshandelingen in een geautomatiseerd werk worden verricht, kunnen worden betrokken van verschillende producenten of binnen de politieorganisatie zelf worden

ontwikkeld, mits aan de wettelijke vereisten voor keuring wordt voldaan. Voor de selectie van bedrijven geldt de bestaande regelgeving voor inkoop. Overgave van de broncode maakt daar geen deel van uit. Bij de keuring wordt getoetst of een technisch hulpmiddel voldoet aan de technische eisen die zijn neergelegd in het Besluit onderzoek in een geautomatiseerd werk. Een technisch hulpmiddel dient onder meer in staat te zijn om geregistreerde gegevens automatisch naar een technische infrastructuur binnen de politieorganisatie te transporteren en dient beveiligd te zijn tegen wijziging van de werking ervan en wijziging en kennisneming van geregistreerde gegevens door onbevoegde personen. Als een technisch hulpmiddel wordt goedgekeurd door een keuringsdienst, mag er vanuit worden gegaan dat aan de wettelijke eisen wordt voldaan. De keuring van technische hulpmiddelen vindt proefondervindelijk plaats.

De leden van de fractie van de PvdA hebben gevraagd wat de gevolgen zijn van het gebruik van nog onbekende kwetsbaarheden voor de veiligheid van het internet en hoe dit wetsvoorstel zich daarmee verhoudt tot het rapport "De publieke kern van het internet" van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR).

Een belangrijk begrip in het WRR rapport is de publieke kern van het internet, de kernprotocollen die het fundament vormen voor een goed functionerend internet, waaronder in het bijzonder de zogenoemde internet protocol suite of TCP/IP suite. Het kabinet onderschrijft het belang van het behoud van het vrije en open karakter van het internet als platform voor onbelemmerd dataverkeer ter stimulering van economische groei en innovatie. Hier wil het kabinet zich beperken tot het borgen van de juridische kaders van de rechtsstaat en het beschermen van burgerlijke vrijheden. Opgemerkt wordt dat veiligheid en het respecteren van mensenrechten tevens voorwaarden zijn voor economische groei en innovatie.

De overheid heeft de verantwoordelijkheid om haar burgers ook in een online omgeving te beschermen door de bescherming van hun persoonlijke informatie te bevorderen, cybersecurity te bevorderen en cybercriminaliteit en bedreigingen van de nationale veiligheid te bestrijden of te voorkomen. Internationale samenwerking wordt steeds belangrijker om deze belangen te beschermen in een grenzeloze digitale omgeving. Afspraken over samenwerking, (gedrags)normen en standaarden moeten dan ook bij voorkeur in Europees en in breder internationaal verband worden gemaakt. Bovengenoemde belangen vragen om een geïntegreerde benadering. In de optiek van de regering vormen vrijheid en veiligheid geen tegengestelde, maar complementaire belangen. De dynamische balans tussen veiligheid, vrijheid en economische groei wordt tot stand gebracht en in stand gehouden in een constante open dialoog tussen alle stakeholders, zowel nationaal als internationaal. Deze visie op de samenhang tussen veiligheid, vrijheid en economische groei als basis voor beleidsafwegingen is verankerd in de Nationale Cyber Security Strategie 2.0.

In het voorliggende wetsvoorstel is de inzet in het kader van de opsporing alleen mogelijk voor ernstige strafbare feiten en is vooraf toestemming van een rechter-commissaris vereist. De proportionaliteit en subsidiariteit worden zo voorafgaand aan de inzet onafhankelijk getoetst. Net als in de fysieke wereld hebben politie en justitie tot taak de criminaliteit op het internet zoveel mogelijk te voorkómen en op te sporen. 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 hard- of software.

De leden van de fractie van GroenLinks hebben de regering gevraagd om, in plaats van te verwijzen naar haar brief van inmiddels een aantal maanden geleden, in haar beantwoording heel precies in te gaan op het gevaar van het laten voortbestaan van een kwetsbaarheid die mogelijk tot meer slachtoffers van criminaliteit leidt. De leden van deze fractie hebben tevens gevraagd of dit wetsvoorstel juist kwetsbaarheden openhoudt in plaats van ze te dichten, om zo van deze gaten gebruik te kunnen maken tijdens het hacken, en zouden hierop graag een toelichting van de regering ontvangen.

Effectieve handhaving van de rechtsstaat in cyberspace is een voorwaarde voor een veilig internet en van belang voor zowel het terugdringen van het slachtofferschap, als het recht doen aan slachtoffers. Zoals hierboven, in de beantwoording van de vragen van de leden van verschillende fracties, is aangegeven wordt met dit wetsvoorstel beoogd hieraan een belangrijke bijdrage te leveren. Het gebruik van onbekende kwetsbaarheden kan hier onderdeel van zijn. De inzet en het gebruik van onbekende kwetsbaarheden is met diverse waarborgen omkleed. Deze zijn hiervoor aan de orde gekomen, eveneens in antwoord op eerdere vragen hierover van leden van verschillende fracties. Naar die antwoorden wordt op deze plaats kortheidshalve verwezen.

6. Lokpuber en grooming

De leden van de fractie van het CDA hebben gevraagd of het klopt dat poging tot grooming strafbaar blijft in het onderhavige wetsvoorstel. De leden van deze fractie hebben opgemerkt op dat, hoewel daar in de optiek van deze leden inhoudelijk veel voor te zeggen is, poging tot grooming volgens de Afdeling advisering van de Raad van State strafbaarstelling van een ‘poging tot een poging’ is, omdat er volgens staande jurisprudentie nog geen uitvoeringshandeling plaatsvindt. De leden van deze fractie hebben de regering gevraagd juridisch te beargumenteren waarom het advies van de Afdeling advisering niet is gevolgd.

In het advies over het wetsvoorstel (Kamerstukken II 2015/16, 34 372, nr. 4) heeft de Afdeling advisering een opmerking gemaakt over de passage in de memorie van toelichting dat bij wet de strafbaarheid van poging tot grooming niet is uitgesloten. De Afdeling advisering heeft opgemerkt dat het wetsvoorstel geen wijziging aanbrengt die ziet op de strafbaarheid van poging tot grooming, zodat de toelichting op het wetsvoorstel voor het al dan niet strafbaar zijn van poging tot grooming geen bepalende rol kan spelen. Gelet hierop heeft de Afdeling advisering geadviseerd om de bewuste passage te schrappen.

In het nader rapport (Kamerstukken II 2015/16, 34 372, nr. 4) heeft de regering zich op het standpunt gesteld dat voor de strafbaarstelling van een poging tot grooming geen uitdrukkelijke wettelijke regeling noodzakelijk is en heeft de regering nader toegelicht waarom de strafbaarheid van de poging tot grooming niet bij wet is uitgesloten. Gewezen is op artikel 24 van het op 25 oktober 2007 te Lanzarote tot stand gekomen Verdrag van de Raad van Europa inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik (Trb. 2008, 58) (Verdrag van Lanzarote). Dit artikel verplicht tot het strafbaar stellen van poging tot (onder andere) grooming, tenzij een partij zich het recht heeft voorbehouden de poging niet toe te passen (artikel 24, derde lid, van het Verdrag van Lanzarote). Nederland heeft geen gebruik gemaakt van de uitzonderingsmogelijkheid die het verdrag biedt. In het kader van het ratificatietraject van het verdrag is met verwijzing naar artikel 45 Sr opgemerkt dat poging tot het plegen van misdrijven in Nederland strafbaar is (Kamerstukken II 2008/09, 31 808

(R1872), nr. 3; artikelsgewijze toelichting bij artikel 24). In reactie op het advies van de Afdeling advisering is de memorie van toelichting aangevuld met een passage over het ratificatietraject (Kamerstukken II 2015/16, 34 372, nr. 3, blz. 91).

De leden van de fractie van het CDA hebben gevraagd of de regering kan beargumenteren of, en zo ja hoe, het opsporen van pedofielen door middel van een 'virtuele lokpuber' door een (meerderjarige) opsporingsambtenaar tot een eventuele strafbaarstelling van de opgespoorde pedofiel kan leiden. De leden van deze fractie hebben erop gewezen dat de jurisprudentie niet eenduidig is over de strafbaarheid van het ingaan op de lokroep van een virtuele lokpuber waarachter een meerderjarige ambtenaar schuilgaat en vragen of dit in de ogen van de regering strafbaar is.

Op grond van de huidige delictsomschrijvingen in de artikelen 248a Sr (verleiding van een minderjarige) en 248e Sr (grooming) is het niet strafbaar om contact te leggen met iemand die in werkelijkheid geen minderjarige is. Het wetsvoorstel wijzigt deze artikelen waardoor het contact leggen voor seksuele doeleinden met iemand die zich voordoet als een minderjarige alsnog strafbaar wordt. Hierdoor wordt de inzet van de lokpuber, een opsporingsambtenaar die zich voordoet als een kind, bij de opsporing van online verleiding van een minderjarige en grooming mogelijk.

Voor de strafbaarheid van verleiding van een minderjarige tot ontucht is in de eerste plaats vereist dat sprake is van verleiding, misbruik van uit feitelijke verhoudingen voorvloeiend overwicht of misleiding. In de tweede plaats dient de dader de minderjarige dan wel degene die zich als zodanig voordoet door middel van voornoemde middelen opzettelijk te bewegen tot het plegen of dulden van ontuchtige handelingen. In de derde plaats dient het opzet gericht te zijn op het plegen van ontuchtige handelingen of het dulden van zodanige handelingen van de verdachte door de minderjarige of degene die zich als zodanig voordoet.

Voor de strafbaarheid van grooming zijn de volgende elementen essentieel. In de eerste plaats dient de dader door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst in contact te komen met een kind beneden de leeftijd van zestien jaren of met iemand die zich als zodanig voordoet. In de tweede plaats is bij de dader het oogmerk vereist om ontuchtige handelingen te plegen met een persoon die de leeftijd van zestien jaren nog niet bereikt heeft of een afbeelding van een seksuele gedraging te vervaardigen waarbij een persoon die de leeftijd van zestien jaren nog niet bereikt heeft is betrokken. In de derde plaats dient de dader enige handeling te ondernemen gericht op het verwezenlijken van een ontmoeting met een vorenbedoelde persoon.

De leden van de fractie van D66 hebben verwezen naar een recent artikel in de Ars Aequi van mr. dr. K. Lindenberg en opgemerkt dat lokpuberzaken waarbij een opsporingsambtenaar zich op het internet voordoet als jeugdige vooralsnog vaak gedoemd zijn te mislukken, omdat voor de strafbaarheid noodzakelijk is dat de verdachte daadwerkelijk met een minderjarige heeft gecommuniceerd. De leden van deze fractie hebben geconstateerd dat het onderhavige wetsvoorstel het gebruik van de lokpuber mogelijk wil maken door aanvullende strafbaarheid te creëren voor het handelen jegens iemand die zich voordoet als kind. In dit verband hebben zij gevraagd in hoeverre de inzet van de lokpuber in overeenstemming is met het instigatieverbod.

Opsporingsambtenaren kunnen volgens bestendige rechtspraak van de Hoge Raad op basis van algemene taakstellende bepalingen – het betreft de artikelen 3 van de Politiewet 2012 en 141 Sv – onder voorwaarden bevoegd zijn tot het inzetten van lokmiddelen. Eén van de voorwaarden is dat de verdachte door het optreden van de opsporingsambtenaar niet wordt gebracht tot andere handelingen dan die waarop zijn opzet reeds tevoren was gericht (het zogenoemde Tallon-criterium, Hoge Raad 4 december 1979, NJ 1989, 356; zie Hoge Raad 28 oktober 2008, NJ 2009, 224 voor de inzet van een lokfiets). In de praktijk leidt het uitlokkingsverbod ertoe dat een opsporingsambtenaar in beginsel zelf de communicatie niet start, maar afwacht totdat iemand contact met hem legt voor seksuele doeleinden.

De leden van de fractie van de ChristenUnie hebben gevraagd of het voorgestelde artikel 248a Sr ruimte biedt voor anderen dan opsporingsambtenaren om zich voor te doen als een virtuele creatie van iemand die de leeftijd van achttien jaren nog niet heeft bereikt en zo een bijdrage te leveren aan de opsporing. De leden van deze fractie hebben tevens gevraagd of de regering dergelijke initiatieven wenst of dat de opsporing beperkt dient te blijven tot de politie.

Artikel 248a Sr stelt niet als voorwaarde dat een opsporingsambtenaar zich - al dan niet met behulp van een virtuele kindcreatie - voordoet als een minderjarige. In zoverre laat het artikel ruimte voor betrokkenheid van anderen dan opsporingsambtenaren bij de inzet van de lokpuber voor de opsporing van online zedendelicten. De regering is evenwel geen voorstander van burgeropsporing. De opsporing en vervolging van zedenmisdrijven zijn taken voor de politie en het openbaar ministerie. In het bijzonder bij gevoelige misdrijven als zedenmisdrijven dient de opsporing te worden overgelaten aan de opsporingsorganisaties, die beschikken over de benodigde bevoegdheden en expertise. De inzet van lokmiddelen is maatwerk en vraagt om specifieke deskundigheid. Om te voorkomen dat sprake is van ongeoorloofde uitlokking en onrechtmatig verkregen bewijs zal de opsporingsambtenaar die als lokpuber fungeert zich in de praktijk passief opstellen, wachten tot iemand contact legt voor seksuele doeleinden en tijdens die contacten behoedzaam te werk gaan.

De inzet van de lokpuber, een opsporingsambtenaar die zich online voordoet als minderjarige, moet onderscheiden worden van de inzet van een virtuele kindcreatie. Een virtuele kindcreatie is een softwareapplicatie waarin een voorgeprogrammeerd virtueel personage (een “avatar”) wordt gebruikt als lokprofiel om in contact te komen met mensen die webcamseks willen met een minderjarige. Het openbaar ministerie maakt tot nu toe geen gebruik van virtuele kindcreaties bij de opsporing van online zedendelicten, omdat uit praktijkervaringen is gebleken dat uitlokking hierbij onvermijdelijk is. Naar aanleiding van het Sweetieproject van Terres des Hommes, waarin gebruik werd gemaakt van virtuele kindcreaties, heeft het openbaar ministerie enkele tientallen zaken in onderzoek gehad. In geen van de zaken is vervolging ingesteld ter zake van grooming of verleiding van een minderjarige, omdat telkens sprake was van ongeoorloofde uitlokking (zie ook: Aanhangsel Handelingen, 2016/17, nr. 948).

De leden van de fractie van de ChristenUnie hebben gevraagd om uitleg bij de voorgestelde redactie van artikel 248a Sr.

Door de voorgestelde wijziging van artikel 248a Sr wordt verleiding tot ontucht van iemand die zich voordoet als een minderjarige strafbaar. In de eerste plaats is vereist dat sprake is van verleiding (giften of beloften van geld of goed), misbruik van uit feitelijke verhoudingen voorvloeiend overwicht of misleiding. In de tweede plaats dient de dader de minderjarige of

degene die zich als zodanig voordoet door middel van voornoemde middelen opzettelijk te bewegen tot het plegen of dulden van ontuchtige handelingen. In de derde plaats dient het opzet gericht te zijn op het plegen van ontuchtige handelingen of het dulden van zodanige handelingen van de verdachte door de minderjarige of degene die zich als zodanig voordoet. Uit de bewijsmiddelen zal moeten blijken dat er tussen verdachte en de al dan niet zich als zodanig voordoende minderjarige enigerlei voor het plegen dan wel dulden van ontucht relevante interactie is geweest.

De leden van de fractie van de ChristenUnie meenden dat er geen advies aan de Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen is gevraagd over de toepassing van het voornoemde artikel. Gelet op het onderwerp zou een advies volgens de leden van deze fractie in de rede liggen en van meerwaarde zijn bij de beoordeling van het wetsvoorstel. Zij wilden hierop graag de reactie van de regering vernemen.

De Nationaal Rapporteur Mensenhandel en Seksueel Geweld is niet formeel om advies gevraagd over het wetsvoorstel. In haar rapport 'Op goede grond' (2014) gaat de Nationaal Rapporteur in op de voorgenomen wetswijziging met het oog op de inzet van de lokpuber. Zij merkt op dat hoewel een uitbreiding van de strafrechtelijke aansprakelijkheid tot het contact leggen met iemand die zich voordoet als een minderjarige vanuit opsporingsoogpunt wenselijk is, het wel van belang is dat in de toelichting bij het wetsvoorstel expliciet afstand wordt gedaan van de inzet van deze opsporingsmethode door burgers, zoals zelfbenoemde 'pedojagers'.

7. Geautomatiseerd werk

De leden van de fractie van D66 hebben opgemerkt dat de criteria voor de inzet van de hackbevoegdheid hetzelfde zijn als voor de inzet van een telefoon- of internettap en dat deze bevoegdheid vrijwel alle elektronische apparaten omvat (hetgeen met het internet of things de komende jaren alleen maar in omvang zal toenemen). De leden van deze fractie hebben gevraagd of de regering kan uitleggen waarom niet is gekozen voor een lijst met een limitatieve opsomming van specifieke misdrijven waarvoor de bevoegdheid beperkt moet worden en specifieke apparaten die gehackt mogen worden. De leden van de fractie van de SP hebben opgemerkt dat nagenoeg alle apparaten onder de hackbevoegdheid vallen en zouden ook graag een lijst zien van apparaten waarvan de regering van mening is dat deze onder het begrip 'geautomatiseerd werk' vallen.

De bevoegdheid tot het aftappen en opnemen van communicatie (artikelen 126m/t en 126zg Sv) kan worden gebruikt om door middel van een internettap in kaart te brengen welk verkeer met het internet via een router van een thuisnetwerk of een zogenaamde openbare 'hotspot' is waar te nemen. De wettelijke voorwaarden voor de toepassing van deze bevoegdheid zijn deels – voor wat betreft bijvoorbeeld de toepassing van de onderzoekshandelingen van het aftappen en opnemen van communicatie of het opnemen van vertrouwelijke communicatie - gelijk aan die voor de voorgestelde bevoegdheid van het op afstand binnendringen van een geautomatiseerd werk. Het doel van het binnendringen met het oog op het verrichten van die onderzoekshandelingen wijkt in dergelijke gevallen - het aftappen en opnemen van communicatie of het opnemen van vertrouwelijke communicatie - niet af van de bestaande bevoegdheid van het aftappen en opnemen van communicatie of het gebruik van een richtmicrofoon. De bevoegdheid van het op afstand heimelijk binnendringen van een smartphone met het oog op het aftappen en opnemen van communicatie kan onvermijdelijk

zijn om de versleuteling van de communicatie te omzeilen. Om die reden ligt een beperking van de bevoegdheid tot delicten die op een lijst zijn geplaatst, zoals door de leden van de fractie van D66 gesuggereerd, minder voor de hand. Voor de opsporing zou dat een stap terug betekenen in vergelijking met de bestaande bevoegdheden rond het aftappen en opnemen van (vertrouwelijke) communicatie.

De regering is ook overigens geen voorstander van een lijst van specifieke misdrijven waarvoor de bevoegdheid beperkt moet worden. Dit geldt ook voor een eventuele lijst van specifieke apparaten die gehackt zouden mogen worden. In beide gevallen zou dit de opsporing van ernstige strafbare feiten ernstig belemmeren. Zoals in de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van GroenLinks is aangegeven, is niet gekozen voor een limitatieve opsomming van geautomatiseerde werken of voor het uitzonderen van geautomatiseerde werken omdat niet valt te voorzien welke innovaties zich bij diverse apparaten zullen voordoen en welke werkwijzen criminelen zich in de toekomst eigen zullen maken. Bovendien biedt het uitsluiten van bepaalde geautomatiseerde werken criminelen meer mogelijkheden de opsporing te ontlopen door juist dergelijke systemen te misbruiken voor het plegen van strafbare feiten. Dat is niet in het belang van de veiligheid van dergelijke systemen. Indien mogelijk wordt uiteraard gekozen voor de inzet van minder vergaande bevoegdheden, zoals een vordering tot verstrekking van gegevens aan de beheerder van het desbetreffende systeem.

De leden van de fractie van de ChristenUnie hebben geconstateerd dat met de definitie van geautomatiseerd werk in het voorgestelde artikel 80sexies een zeer brede categorie ontstaat omdat naast communicatiemiddelen ook huishoudelijke apparatuur, energiemeters en zelfs apparaten in het menselijk lichaam, zoals de pacemaker, onder deze definitie kunnen vallen. De leden van deze fractie hebben gevraagd of is overwogen een meer limitatieve lijst op te stellen of dat op andere wijze een begrenzing is overwogen. Zij kunnen zich bijvoorbeeld voorstellen dat apparatuur in het menselijk lichaam wordt uitgesloten.

Voor de beantwoording van deze vraag wordt verwezen naar de eerdere beantwoording van soortgelijke vragen van de leden van de fracties van D66 en de SP. In aanvulling daarop kan worden opgemerkt dat, hoewel een pacemaker in beginsel onder de definitie van geautomatiseerd werk valt, hierin naar verwachting geen gegevens te vinden zullen zijn die bijdragen aan de opsporing van ernstige vormen van computercriminaliteit of andere ernstige strafbare feiten. Hier komt bij dat de officier van justitie zal moeten onderbouwen dat het bevel voldoet aan de vereisten van proportionaliteit en subsidiariteit. Het is niet waarschijnlijk dat er zich een geval voordoet waarin de rechter-commissaris het binnendringen in een pacemaker als proportioneel zal beschouwen. In de praktijk is het dan ook moeilijk denkbaar dat er zich een zo zwaar wegend belang voordoet dat het op afstand heimelijk binnendringen van een pacemaker proportioneel zou worden geacht.

8. Toezicht

De leden van de fractie van D66 hebben erop gewezen dat een belangrijk onderdeel van het advies van de Afdeling advisering van de Raad van State het instellen van een orgaan dan wel instantie betrof die belast zou worden met het houden van structureel systeemtoezicht op de toepassing van de nieuw voorgestelde bevoegdheden, met name in de gevallen waarin het gebruik van de bevoegdheden ten aanzien van een geautomatiseerd werk niet tot een

veroordeling door een (straf)rechter heeft geleid. De leden van deze fractie hebben gevraagd of de regering kan uitleggen waarom er geen structureel toezicht in het leven geroepen wordt. De leden van de fractie van de SP hebben eveneens gewezen op het advies van de Afdeling advisering om te voorzien in onafhankelijk toezicht op het binnendringen in de digitale omgeving en gevraagd waarom de regering niet heeft gekozen om deze wetgeving met goed toezicht te omkleden. De leden van de fractie van de PvdA hebben het advies van de Afdeling advisering van de Raad van State aangehaald, waarin de Afdeling heeft geadviseerd te voorzien in structureel systeemtoezicht op de toepassing van opsporingsbevoegdheden waarbij gebruik wordt gemaakt van de informatie- en communicatietechnologie in zaken die niet aan de strafrechter zijn voorgelegd. De leden van deze fractie hebben de regering gevraagd nog eens ten gronde uit een te zetten waarom zij meent dat het niet nodig is het advies van de Afdeling en de daarbij gedane concrete suggesties voor de invulling van dat toezicht op te volgen.

Anders dan de Afdeling advisering is de regering van oordeel dat de bestaande regeling voor de inzet van bijzondere opsporingsbevoegdheden in het Wetboek van Strafvordering, aangevuld met de extra maatregelen op grond van het voorliggende wetsvoorstel, in voldoende waarborgen voorziet om een rechtmatige en zorgvuldige toepassing van de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk te garanderen. Het wetsvoorstel voorziet niet in een bevoegdheid tot het grootschalig verzamelen van informatie over onschuldige burgers; het wetsvoorstel past veeleer in het bestaande systeem van bijzondere opsporingsbevoegdheden waarbij een strafrechtelijke relevante verdenking van betrokkenheid van een persoon bij het beramen of plegen van strafbare feiten aanleiding kan geven tot het heimelijk inzetten van bijzondere opsporingsbevoegdheden ten behoeve van de waarheidsvinding. Hierbij is geen sprake van het grootschalig verzamelen van informatie met betrekking tot onschuldige burgers. Het wettelijk systeem rond de bijzondere opsporingsbevoegdheden is gebaseerd op het uitgangspunt dat het handelen van de opsporingsambtenaar wordt gecontroleerd door de officier van justitie, als leider van het opsporingsonderzoek. De officier van justitie heeft het gezag over de opsporing van strafbare feiten. Die verantwoordelijkheid omvat het toezicht op de rechtmatigheid van het optreden van de opsporingsambtenaar in het kader van de strafrechtelijke handhaving van de rechtsorde. De officier van justitie is lid van het openbaar ministerie en is rechterlijk ambtenaar (art. 1, onderdeel b, Wet RO). De procureur-generaal bij de Hoge Raad waakt over de naleving van de wettelijke voorschriften door het openbaar ministerie. Als de officier van justitie strafvervolging instelt dan wordt het toezicht op de rechtmatigheid van het handelen van de opsporingsambtenaar en de officier van justitie uitgeoefend door de rechter. Dit betreft de rechter die ter terechtzitting oordeelt over het tenlastegelegde. De toepassing van bepaalde bijzondere opsporingsbevoegdheden is vanwege de ernst van de inbreuk op de grondrechten van burgers, zoals het recht op bescherming van de persoonlijke levenssfeer (artikel 10 GW), afhankelijk van een voorafgaande rechterlijke instemming. De officier van justitie is gehouden aan de betrokkene schriftelijk mededeling te doen van de uitoefening van een bijzondere opsporingsbevoegdheid, zodra het belang van het onderzoek dat toelaat (artikel 126bb, eerste lid, Sv). Aldus is de betrokkene in staat zich over het inzetten van de bevoegdheid te beklagen. Voor zover de klacht geen betrekking heeft op een gedraging waarop de rechter toeziet, is de Nationale ombudsman bevoegd de klacht in behandeling te nemen (artikel 9:22 en 9:23 Awb). Tenslotte is de Autoriteit persoonsgegevens belast met het toezicht op de naleving van de wetgeving op het gebied van de bescherming van persoonsgegevens door de rechtshandhavingsdiensten. De Wet politiegegevens en de Wet justitiële en strafvorderlijke

gegevens geven regels met het oog op een zorgvuldige verwerking van persoonsgegevens door ambtenaren van politie en het openbaar ministerie.

Aldus voorziet de regeling rond de inzet van bijzondere opsporingsbevoegdheden in het Wetboek van Strafvordering op dit moment in uitgebreide waarborgen voor een rechtmatige en zorgvuldige inzet van die bevoegdheden. De kern daarvan wordt gevormd door het onafhankelijk toezicht door een rechter. In sommige gevallen, waarbij dit vanwege de inbreuk van de bevoegdheid op de persoonlijke levenssfeer van de betrokkene aan de orde is, is tevens rechterlijke tussenkomst vereist voordat een bijzondere opsporingsbevoegdheid kan worden ingezet. Voor de voorgestelde bevoegdheid van het op afstand heimelijk binnendringen van een geautomatiseerd werk zal aanvullend gelden dat de Centrale Toetsingscommissie van het openbaar ministerie vooraf de voorgenomen inzet toetst. De CTC is een adviesorgaan van het College van procureurs-generaal en zal het College ook adviseren over de voorgenomen inzet van het onderzoek in een geautomatiseerd werk. Aldus is de toestemming nodig van het College voordat deze opsporingsbevoegdheid in een concreet geval kan worden toegepast. Hiermee wordt voorzien in een gedegen toezicht binnen het openbaar ministerie op de voorgenomen inzet van de bevoegdheid. Wat betreft het toezicht achteraf geldt dat, op grond van de Politiewet 2012, de Inspectie Veiligheid en Justitie (VenJ) als rijksinspectie is belast met het toezicht op de kwaliteit van de taakuitvoering van de politie. Dit toezicht betreft de naleving van de wet- en regelgeving rond de toepassing van die bevoegdheden en de kwaliteit van de uitvoering en laat het gezag van de burgemeester en de officier van justitie onverlet. Dit toezicht omvat zowel de gevallen die, in het kader van de door het openbaar ministerie ingestelde strafvervolging jegens een verdachte, aan het oordeel van de rechter worden voorgelegd als de gevallen die niet tot strafvervolging jegens een verdachte leiden. Als rijksinspectie heeft de Inspectie VenJ de ruimte om zelf informatie te verzamelen, daarover een oordeel te vormen, en daarover te rapporteren en te adviseren. Er is dus sprake van onafhankelijke oordeelsvorming. De inspecteurs beschikken over de nodige wettelijke toezichtbevoegdheden op grond van de Algemene wet bestuursrecht.

Het toezicht van de Inspectie VenJ is gericht op het functioneren van het wettelijke systeem rond het onderzoek in een geautomatiseerd werk. Het toezicht heeft betrekking op aspecten als de autorisaties van de bevoegde opsporingsambtenaren voor de uitvoering van het bevel van de officier van justitie voor het onderzoek in een geautomatiseerd werk, de expertise en kennis van de betrokken opsporingsambtenaren, de inzet van het technische hulpmiddel (kwaliteit en betrouwbaarheid), de vastlegging van gegevens over de werking van het technische hulpmiddel en over de toepassing van onderzoekshandelingen in het geautomatiseerde werk (logging), de beveiliging van de vastgelegde gegevens en het gebruik van de gegevens, inclusief de bewaring en vernietiging daarvan.

Gelet op de bestaande structuren en voorzieningen is er geen aanleiding te voorzien in meer aanvullend toezicht. Als, naast de besproken instanties, nog een afzonderlijk orgaan wordt ingericht voor het uitoefenen van toezicht op de voorgestelde bevoegdheid tot het binnendringen van een geautomatiseerd werk, dan zullen de verschillende instanties elkaar eenvoudigweg voor de voeten gaan lopen of op zijn minst dubbel werk verrichten. En als het gaat om eventueel onderzoek door een dergelijk orgaan naar klachten moet worden opgemerkt dat de Nationale ombudsman daartoe thans bevoegd is. Ook op dit punt valt dan ook niet goed in te zien hoe een nieuw toezichthoudend orgaan van toegevoegde waarde zou kunnen zijn.

Dit alles overziend is de regering van oordeel dat in het voorliggende wetsvoorstel is voorzien in adequate en effectieve waarborgen tegen misbruik van de voorgestelde bevoegdheid. Deze waarborgen acht de regering ruimschoots voldoende om een rechtmatige en zorgvuldige toepassing van de bevoegdheden te kunnen garanderen. In aanvulling op het rechterlijk toezicht is op grond van de Politiewet 2012 voorzien in toezicht door de Inspectie VenJ. Op basis van haar wettelijke taak is de Inspectie VenJ de aangewezen instantie voor de uitoefening van het toezicht op de uitvoering van de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk binnen de grenzen van het bevel van de officier van justitie en de machtiging van de rechter-commissaris.

De leden van de fractie van D66 hebben voorts gevraagd of er voldoende toezicht en rechtsbescherming voor de verdachte is en of de privacy van onschuldige derden is gewaarborgd.

Voor het antwoord op de vraag of er voldoende toezicht is wordt verwezen naar hetgeen daarover is opgemerkt in de beantwoording van de soortgelijke vragen van de leden van de fracties van D66, de SP en ChristenUnie. In aanvulling daarop kan worden opgemerkt dat er een notificatieplicht geldt, zodat de betrokkene in kennis wordt gesteld van de inzet van de bevoegdheid tot het op afstand heimelijk binnendringen van een geautomatiseerd werk. Dit betreft de bestaande wettelijke regeling voor de notificatie van bijzondere opsporingsbevoegdheden (artikel 126bb Sv). De privacy van onschuldige derden is zo veel mogelijk gewaarborgd. Dit komt onder meer tot uitdrukking in het vereiste dat het geautomatiseerde werk dat op afstand heimelijk wordt binnengedrongen, bij de verdachte in gebruik moet zijn (artikel 126nba/uba/zpa, eerste lid, Sv). Verder dient de officier van justitie in het bevel een aanduiding van de aard en functionaliteit van het technische hulpmiddel op te nemen dat wordt gebruikt voor de uitvoering van het bevel, en ten aanzien van welke categorie van gegevens aan het bevel uitvoering wordt gegeven (artikel 126nba/uba/zpa, tweede lid, onderdelen d en f, Sv). De toepassing van sommige uitvoeringshandelingen is echter niet bij voorbaat beperkt tot een verdachte. Dit betreft bijvoorbeeld het aftappen en opnemen van communicatie en het opnemen van vertrouwelijke communicatie (artikel 126l/s/zf en 126m/t/zg Sv) die vanwege het belang van de waarheidsvinding ook gericht kunnen zijn op communicatie van een onbekende verdachte of van anderen dan de verdachte. Voorwaarde is dat toepassing van de opsporingsbevoegdheid jegens een persoon nodig is in het belang van het onderzoek. Overigens heeft de inzet van deze bevoegdheden naar zijn aard tot gevolg dat gegevens van derden ter kennis komen van de opsporing. Als het telefoongesprek wordt afgeluisterd of het vertrouwelijke gesprek met een richtmicrofoon wordt opgenomen komt de inbreng van alle gesprekspartners ter kennis van de opsporing. Op grond van de wet gelden specifieke termijnen voor de bewaring en vernietiging van de met behulp van deze bevoegdheden verzamelde gegevens; deze worden vernietigd binnen twee maanden nadat de zaak geëindigd, behoudens gebruik voor ander strafrechtelijk onderzoek (artikel 126cc, tweede lid, Sv).

Onder verwijzing naar het door de Afdeling advisering genoemde probleem van de internationale omgeving hebben de leden van de fractie van de SP de vraag gesteld hoe de rechter zou moeten oordelen als de indringing heeft plaatsgevonden op het terrein van een ander land.

De Nederlandse wet staat niet in de weg aan optreden buiten het Nederlandse grondgebied. Artikel 539a Sv voorziet in een wettelijke basis om opsporingshandelingen te verrichten buiten Nederland, voor zover het volkenrecht en interregionale recht dit toelaten. Op grond van het volkenrecht is het soevereiniteitsbeginsel relevant, dat ertoe strekt dat een staat slechts uitvoerende rechtsmacht mag uitoefenen op het grondgebied van een andere staat met instemming van die staat. Die instemming kan worden verkregen door middel van een verzoek om rechtshulp. Met een rechtshulpverzoek wordt het respect voor de soevereiniteit en de territoriale integriteit van de aangezochte staat tot uitdrukking gebracht, op grond waarvan de aangezochte staat primair zelf bevoegd is om zelf op te treden tegen inbreuken op de rechtsorde die op het eigen grondgebied worden beraamd of gepleegd.

Uit het beginsel van soevereiniteit vloeit voor dat als bekend is, of in de loop van het onderzoek bekend wordt, dat de gegevens zich in een andere rechtsmacht bevinden, een verzoek om rechtshulp aangewezen is. Het soevereiniteitsbeginsel is echter voornamelijk van belang voor de relatie tussen staten en is minder relevant voor de beoordeling van de strafbaarheid van daders. Zo heeft de Hoge Raad geoordeeld dat de vraag of door Nederlandse opsporingsambtenaren het volkenrecht is nageleefd, in die zin dat geen inbreuk is gemaakt op soevereiniteit van de staat binnen de grenzen waarvan is opgetreden, in beginsel in de strafzaak tegen verdachte niet relevant is omdat de belangen die het volkenrecht beoogt te beschermen geen belangen zijn van de verdachte maar van de staat op het grondgebied waarvan buitenlandse opsporingsambtenaren optreden (HR 5 oktober 2010, ECLI: NL: HR: 2010: BL5629 en HR 17 april 2012, ECLI: NL: HR: 2012: BV9070). Op basis van deze jurisprudentie kan worden geconcludeerd dat wanneer Nederlandse opsporingsambtenaren inbreuk zouden maken op de soevereiniteit van een andere staat doordat op afstand heimelijk een geautomatiseerd werk wordt binnengedrongen dat zich op het grondgebied van een andere staat bevindt, dit in de strafzaak tegen de verdachte in beginsel niet relevant is. Daarbij merk ik nog op dat als blijkt dat gegevens zich op het territorium van een andere staat bevinden, een rechtshulpverzoek aangewezen is. Dit komt in paragraaf 11 nader aan de orde, naar aanleiding van een vraag van de leden van de fractie van GroenLinks.

De leden van de fractie van GroenLinks meenden dat onafhankelijk toezicht van fundamenteel belang is voor de Nederlandse rechtsstaat en hebben gevraagd of de regering toezeggingen kan doen over, en zo ja hoe, zij het onafhankelijk toezicht op de hackbevoegdheid wil gaan regelen. De leden van deze fractie hebben tevens gevraagd in hoeverre de in het wetsvoorstel opgenomen toestemming van de rechter-commissaris en controle door de Centrale Toetsingscommissie hiervoor geschikt is.

Voor het antwoord op deze vragen wordt verwezen naar de eerdere beantwoording van soortgelijke vragen van de leden van de fracties van D66, de SP en de PvdA.

De leden van de fractie van de ChristenUnie hebben gevraagd waarom niet is gekozen voor een vorm van onafhankelijk toezicht door een orgaan buiten het Ministerie van Veiligheid en Justitie. De leden van deze fractie hebben tevens gevraagd om een nadere toelichting op welke wijze het structurele toezicht op het gebruik inzichtelijk wordt gemaakt, en op welke wijze het gebruik en de effectiviteit van de inzet zal worden gemonitord.

In de eerdere beantwoording van vragen van de leden van de fracties van de SP, D66 en de PvdA is reeds ingegaan op het toezicht. De inzet van de bevoegdheid stelt hoge eisen aan de

deskundigheid van de betrokken opsporingsambtenaren en vereist een zorgvuldige voorbereiding om te voorkomen dat de inzet mislukt, bijvoorbeeld doordat de verdachte op de hoogte raakt van de activiteiten van politie en justitie en vervolgens bewijsmateriaal vernietigt. De effectiviteit van de inzet zal binnen politie en openbaar ministerie dan ook worden gemonitord zodat een succesvolle inzet van deze bevoegdheid kan worden verzekerd. Verder zal de Kamer in de gelegenheid worden gesteld zich een oordeel te vormen over de inzet van deze bevoegdheid doordat, conform de werkwijze bij het aftappen en opnemen van communicatie, jaarlijks aan de Kamer zal worden gerapporteerd over de inzet van de bevoegdheid (Kamerstukken II 2007/08, 30 517, nrs. 5 en 6). Dit betreft het aantal malen dat de bevoegdheid is ingezet en het resultaat van die inzet op het gebied van de strafvervolging. Daarbij zal ook worden ingegaan op de klachten naar aanleiding van de inzet van deze bevoegdheid (Kamerstukken II 2015/16, 30 372, nr. 3, blz. 40).

9. Begroting

De leden van de fractie van het CDA hebben gevraagd of de regering kan aangeven wanneer de kosten van het nakomen van een vordering tot het verstrekken van gegevens of tot het medewerking verlenen aan het ontsleutelen van gegevens wel en wanneer deze kosten niet worden vergoed, en of deze kosten steeds uit ’s Rijks kas behoren te worden vergoed.

De regeling van artikel 592 Sv past in het systeem dat de kosten die derden moeten maken ten behoeve van het nakomen van een vordering tot verstrekking van gegevens door derden, zoals een aanbieder van een communicatiedienst of een instelling in de financiële sector, op grond van de artikelen 126m, 126n, 126na, 126ua, 126nc tot en met 126ng en 126ni, 126t, 126u, 126uc tot en met 126ug en 126ui, en 126zg, 126zh,126zi, 126zja tot en met 126zo Sv, worden vergoed. Ditzelfde geldt voor de nakoming van een vordering tot ontsleuteling van gegevens, op grond van de artikelen 126nh, 126uh en 126zp Sv. Het gaat daarbij om kosten die verbonden zijn aan een individuele vordering of een individueel verzoek. Kosten die aan de nakoming van de vordering kunnen worden toegerekend in de vorm van extra personeelskosten en extra administratiekosten komen voor vergoeding in aanmerking, voor zover deze kosten inzichtelijk gemaakt worden. Van vergoeding zijn uitgezonderd de kosten die in het kader van de reguliere bedrijfsvoering toch al worden gemaakt.

De leden van de fractie van de ChristenUnie hebben gevraagd op welke wijze de financiële middelen verschuiven binnen het budget van de nationale politie binnen het totaal beschikbare budget. De leden van deze fractie hebben gelezen dat de mate van verschuiving afhankelijk is van de verwachtingen van en ervaring met toepassing van het instrument. Deze leden hebben gevraagd welke verwachting de regering momenteel heeft en ten laste van welke andere inzet dit wetsvoorstel dan bij de invoering zal komen. Ten slotte is gevraagd of voorzien kan worden in enkele scenario’s en een begroting voor de eerste jaren na inwerkingtreding van het wetsvoorstel, en of voor de inzet van deze bevoegdheden extra capaciteit nodig is.

Het is de verwachting dat de nieuwe opsporingsbevoegdheid niet leidt tot structurele toename van de totale opsporingsinspanning en ook dat daarvoor, voor zover nu kan worden overzien, geen extra capaciteit nodig is. Eerder zal sprake zijn van verschuiving van het ene onderzoeksmiddel naar het andere middel. De uitvoering van het onderzoek in een geautomatiseerd werk vindt plaats bij een onderdeel van de Landelijke eenheid van de Nationale politie. De Nationale politie ontvangt jaarlijks een bijzondere bijdrage van € 13,8

miljoen voor de digitale professionalisering en vernieuwing van de organisatie onder meer ter bestrijding van cybercrime. De aanschaf en implementatie van ICT-hulpmiddelen ter voorbereiding op de invoering van het onderzoek in een geautomatiseerd werk geschiedt uit dit budget. De personeels- en IV-capaciteit en de structurele kosten voor beheer en onderhoud komen ten laste van de algemene begroting van de politie. Aan de begroting van de politie is bij najaarsnota structureel een bedrag toegevoegd voor de aanpak van cybercrime. Voor 2017 bedraagt de bijdrage € 1,4 miljoen, voor 2018 en verdere jaren € 1,5 miljoen. Deze bijdragen zijn bedoeld voor de versterking van personele en materiële capaciteit door opleiding en ICT-middelen en tools.

De leden van de fractie van de ChristenUnie hebben gevraagd op welke wijze de extra voorziene structurele last voor de rechtspraak van € 500.000 wordt gedekt in de begroting van het ministerie. De leden van deze fractie misten duidelijkheid over de gevolgen van dit wetsvoorstel voor de begroting van het OM.

De rechtspraak wordt gefinancierd middels outputfinanciering. In het kader van zijn wettelijke adviestaak heeft de Raad voor de rechtspraak een inschatting gemaakt van de gevolgen van nieuwe wet- en regelgeving voor de werklast en organisatie van de rechtspraak. Indien er sprake is van een (verwachte) werklastverzwaring die groter is, kan dit worden meegenomen in de driejaarlijkse onderhandelingen tussen Raad en het Ministerie van Veiligheid en Justitie.

10. Gedelegeerde regelgeving

De leden van de fractie van de VVD hebben geconstateerd dat in een algemene maatregel van bestuur of een OM-aanwijzing toetsingscriteria worden vastgelegd met betrekking tot de opsporingshandelingen die worden verricht indien gegevens niet zijn opgeslagen in Nederland. De leden van deze fractie hebben gevraagd of deze criteria inmiddels zijn opgesteld, en zo ja, wat deze criteria zijn en wanneer de tekst naar verwachting beschikbaar komt.

Het voorliggende wetsvoorstel bevat een facultatieve grondslag om bij algemene maatregel van bestuur nadere regels te stellen over de toepassing van de bevoegdheid tot het doen van onderzoek in een geautomatiseerd werk in gevallen waarin niet bekend is waar de gegevens zijn opgeslagen (artikel 126nba, negende lid, Sv, dat van overeenkomstige toepassing is verklaard in de artikelen 126uba/126zpa, derde lid, Sv). Vooralsnog wordt van deze mogelijkheid geen gebruik gemaakt; de uitwerking hiervan vindt plaats in een aanwijzing van het College van procureurs-generaal.

Het uitgangspunt is dat er rechtshulp wordt gevraagd als de te verrichten opsporingshandelingen betrekking hebben op gegevens die zich op het grondgebied van een andere staat bevinden. Als bekend is dat de gegevens niet in Nederland zijn opgeslagen dient dit in het bevel van de officier te worden vermeld, zodat de rechter-commissaris hierover controle kan uitoefenen.

In uitzonderlijke gevallen kan, onder strikte voorwaarden, zelfstandig worden opgetreden op basis van een zoveel mogelijk stapsgewijze aanpak. In het algemeen zal worden gestart met een beperkte eerste vordering, het bepalen van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker. Als verdergaande handelingen nodig zijn, zal waar mogelijk worden volstaan met het overnemen van de opgeslagen gegevens zodat de beschikkingsmacht van de

rechthebbende niet wordt beperkt. Het optreden in het concrete geval zal aan de hand van criteria worden afgewogen. Deze criteria hebben betrekking op de inspanning die is vereist om de identiteit en locatie van een geautomatiseerd werk te achterhalen, de ernst van het strafbare feit, de mate van betrokkenheid van de Nederlandse rechtsorde (betrokkenheid van Nederlandse slachtoffers of de Nederlandse infrastructuur), de aard van de te verrichten opsporingshandelingen (worden gegevens alleen overgenomen of ook ontoegankelijk gemaakt) en de risico's voor het geautomatiseerde werk. Deze criteria worden uitgewerkt in een OM-Aanwijzing, die in voorbereiding is en voor inwerkingtreding van het wetsvoorstel gereed zal zijn.

De leden van de fractie van het CDA hebben opgemerkt dat het op afstand binnendringen in een geautomatiseerd werk niet alleen mag bij een misdrijf waarop een gevangenisstraf van vier jaar of meer gesteld is, maar ook bij misdrijven die bij algemene maatregel van bestuur worden aangewezen. Dat lijkt de leden van de CDA-fractie ongewenst; zonder tussenkomst van de Staten-Generaal kan de regering hierdoor in beginsel ieder misdrijf via een algemene maatregel van bestuur onder de werking van dit wetsvoorstel brengen. De leden van deze fractie hebben gevraagd waarop juist deze misdrijven worden gekozen en op basis van welke criteria er wordt besloten om eventueel misdrijven toe te voegen. In de optiek van de leden van deze fractie dient een dergelijke algemene maatregel van bestuur ten minste te worden voorgehangen. Deze leden hebben tevens gevraagd of de regering bereid is om een reparatiewetsvoorstel in te dienen, waarin dit wordt geregeld.

Om in een geautomatiseerd werk binnen te kunnen dringen en onderzoek te doen met het oog op de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker en de vastlegging daarvan, met het oog op het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie en met het oog op stelselmatige observatie, moet sprake zijn van een verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv, waarvoor een bevel tot voorlopige hechtenis kan worden gegeven. Een bevel tot voorlopige hechtenis kan worden gegeven in geval van verdenking van een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaren of meer is gesteld of in geval van verdenking van één van de misdrijven, genoemd in artikel 67, eerste lid, onder b en c, Sv, met een lagere wettelijke strafbedreiging.

De voorwaarden voor toepassing van de bevoegdheid tot het binnendringen in een geautomatiseerd werk en doen van onderzoek met het oog op het vastleggen van gegevens of het ontoegankelijk maken van gegevens zijn strikter: in beginsel mag de bevoegdheid met het oog op deze doelen uitsluitend worden toegepast bij een verdenking van een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld. Bij algemene maatregel van bestuur kunnen echter andere misdrijven met een lagere wettelijke strafbedreiging worden aangewezen (artikelen 126nba/126uba/126zpa, eerste lid, onder c, Sv). Deze misdrijven worden aangewezen in het eerdergenoemde Besluit onderzoek in een geautomatiseerd werk. De criteria voor aanwijzing zijn de volgende. Het betreft misdrijven die worden gepleegd met een geautomatiseerd werk (computercriminaliteit in enge zin) en ernstige commune misdrijven die in toenemende mate digitaal worden gepleegd (gedigitaliseerde criminaliteit) waarbij vaak geen ander aanknopingspunt is voor de opsporing dan via het geautomatiseerde werk met behulp waarvan het misdrijf wordt gepleegd. Voorts moet sprake zijn van een duidelijk maatschappelijk belang bij de beëindiging van de strafbare situatie en de vervolging van de daders. Met uitzondering van de computerdelicten in enge zin gaat het bij de

aangewezen misdrijven grotendeels om misdrijven met een strafmaximum van zes jaren gevangenisstraf.

De ontwikkelingen in de cybercriminaliteit gaan snel en de maatschappelijke gevolgen hiervan kunnen groot zijn. Door de aanwijzing van misdrijven bij algemene maatregel van bestuur kan hierop flexibel worden ingespeeld. Indien zich in de toekomst nieuwe vormen van computercriminaliteit en/of ernstige gedigitaliseerde criminaliteit voordoen die voldoen aan voornoemde criteria, kan via wijziging van het Besluit onderzoek in een geautomatiseerd werk de toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijk maken van gegevens worden uitgebreid tot deze misdrijven.

De regering ziet geen aanleiding tot het indienen van een reparatiewetsvoorstel om voorhang van de algemene maatregel van bestuur te regelen en wijst erop dat reeds op andere wijze in de betrokkenheid van het parlement wordt voorzien. Bij de plenaire behandeling van het wetsvoorstel in de Tweede Kamer is toegezegd dat de algemene maatregel van bestuur voorafgaand aan de inwerkingtreding van het wetsvoorstel naar de Kamer wordt gestuurd. Deze toezegging is gestand gedaan bij de eerdergenoemde brief van 10 mei 2017, waarin beide Kamers zijn geïnformeerd over het conceptbesluit onderzoek in een geautomatiseerd werk (Kamerstukken II 2016/17, 34 372, nr. 26).

De leden van de fractie van het CDA hebben gevraagd of de regering met deze leden van mening is dat een eventuele uitbreiding van het wetsvoorstel met andere misdrijven in het geheel niet bij algemene maatregel van bestuur geregeld kan worden, maar bij wet moeten worden vastgelegd.

Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van deze fractie.

De leden van de fractie van de PvdA hebben opgemerkt dat het wetsvoorstel op verschillende plaatsen delegatiebepalingen bevat en zij hebben gevraagd of zij het goed begrijpen dat het hierbij steeds gaat om het Besluit technische hulpmiddelen strafvordering.

Het wetsvoorstel bevat een aantal grondslagen om bij of krachtens algemene maatregel van bestuur regels te stellen over de uitoefening van de binnendring- en onderzoeksbevoegdheid. Het betreft ten eerste de grondslag om de inzet van de bevoegdheid voor het doen van onderzoek voor bepaalde onderzoeksdoelen mogelijk te maken bij verdenking van bij algemene maatregel van bestuur aangewezen misdrijven (artikelen 126nba/126uba/126zpa, eerste lid, Sv). Het betreft ten tweede de mogelijkheid om nadere regels te stellen over de deskundigheid en autorisatie van de bij het onderzoek in een geautomatiseerd werk betrokken opsporingsambtenaren, de samenwerking met andere opsporingsambtenaren en de geautomatiseerde vastlegging van gegevens ter uitvoering van een bevel van de officier van justitie (artikel 126nba, achtste lid, onder a en b, Sv). Ten derde kunnen nadere regels gesteld worden over verschillende aspecten met betrekking tot het doen van onderzoek met behulp van een technisch hulpmiddel (artikel 126ee Sv). Omwille van de overzichtelijkheid vindt de uitvoering van deze bepalingen plaats in een nieuw besluit, het eerdergenoemde Besluit onderzoek in een geautomatiseerd werk. Net als het Besluit technische hulpmiddelen strafvordering zal dit besluit gebaseerd zijn op het uitgangspunt dat de gegevens die met een technisch hulpmiddel worden vastgelegd betrouwbaar, integer en herleidbaar dienen te zijn.

De leden van de fractie van de PvdA hebben gevraagd op welke termijn de tekst van de lagere regelgeving (waaronder in ieder geval voornoemd Besluit) beschikbaar zal zijn, of er een voorhangprocedure zal plaatsvinden en of de desbetreffende regelgeving ter internetconsultatie zal worden aangeboden.

Hiervoor is, in antwoord op een soortgelijke vraag van de leden van de fractie van het CDA, aangegeven dat bij de eerdergenoemde brief van 10 mei 2017 aan beide Kamers is toegezonden het conceptbesluit onderzoek in een geautomatiseerd werk. Het conceptbesluit is inmiddels ook voor internetconsultatie aangeboden door middel van plaatsing op de website www.internetconsultatie.nl.

11. Internationale aspecten

De leden van de fractie van de VVD hebben gevraagd naar het tijdpad voor de paraplu-afspraken met andere staten waarbij Nederlandse opsporingsambtenaren toegang krijgen tot geautomatiseerde werken die zich buiten Nederland bevinden of buitenlandse opsporingsambtenaren zich onbedoeld op een Nederlandse server of net bevinden. De leden van deze fractie hebben tevens gevraagd of de regering binnen een termijn van één jaar de Kamer kan informeren over de voortgang van deze paraplu-afspraken en de inhoud daarvan. Deze leden hebben voorts gevraagd of de regering hen kan informeren over de stand van zaken en ontwikkelingen om te komen tot internationale regels met het oog op de bestrijding van internationale computercriminaliteit, en of de regering van plan om in dezen initiatieven te ontwikkelen, mede met het oog op de belangrijke positie die Nederland inneemt op het terrein van de handhaving van de internationale rechtsorde.

Zoals in de eerdere beantwoording van vragen van de leden van de fracties van GroenLinks en de ChristenUnie in paragraaf 3 is aangegeven, bestaat er behoefte aan internationale afspraken inzake het vergaren van bewijs (E-evidence) vanwege het open internationale karakter van het internet. Op de Global Conference on CyberSpace in 2015 is dit onderwerp geagendeerd, vervolgens zijn cybersecurity en de aanpak van cybercrime als prioriteiten benoemd tijdens het Nederlandse EU-voorzitterschap en zijn in juni 2016 door de JBZ-Ministers Raadsconclusies aangenomen over criminal justice in cyberspace. Deze conclusies zien op:

- het ontwikkelen van een gezamenlijk EU-kader voor verzoeken aan private partijen voor het verkrijgen van bepaalde typen data. Hierbij wordt gestreefd naar synergie met de formulieren en instrumenten die binnen de Europese Unie voor rechtshulp al eerder zijn ontwikkeld en gangbaar zijn;

- het stroomlijnen en versnellen van de bestaande procedures voor wederzijdse rechtshulp en wederzijdse erkenning binnen de Europese Unie en met derde landen, onder andere door digitalisering van verzoeken en automatische vertaling hiervan, alsook het vergroten van kennis en vaardigheden van hen die in de lidstaten deze verzoeken behandelen;

- het herijken van de afspraken ten aanzien van handhavende rechtsmacht door te bezien welke onderzoekshandelingen onder welke voorwaarden mogen worden ingezet in cyberspace in de gevallen waarin het huidige kader nog niet voorziet, onder andere wanneer de locatie van

elektronisch bewijs of de oorsprong van een cyber aanval (nog) niet bekend of redelijkerwijs niet bekend te maken is.

In vervolg op de Raadsconclusies wordt onder regie van de Commissie, in nauwe samenwerking met lidstaten en met andere zowel nationale als Europese instituties, uitvoering gegeven aan de in de Raadsconclusies genoemde actiepunten. In de Raadsconclusies wordt de Commissie verzocht over de resultaten van het proces inzake handhavende rechtsmacht te rapporteren aan de JBZ-raad in juni 2017.

Er wordt binnen de Raad voor Europa ook gesproken over een additioneel protocol bij het Cybercrimeverdrag uit 2001(Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Trb. 2002, 18 en Trb. 2004, 290). Dit verdrag heeft tot nog toe het meest ruime toepassingsbereik en bevat bepalingen over geharmoniseerde strafbaarstellingen, strafprocessuele bevoegdheden (zoals bevriezing van gegevens) en internationale samenwerking. Op dit moment hebben 52 landen dit verdrag geratificeerd (de landen die lid zijn van de Raad van Europa, met uitzondering van Rusland, en landen zoals VS, Canada, Australië, Japan, Sri Lanka, Paraquay, de Dominicaanse republiek en Senegal). Als model law zijn elementen van het verdrag gebruikt in ongeveer 60 andere landen. Op 16 september 2016 heeft de Cloud Evidence Group, een subgroep van het comité van verdragspartijen van het Cybercrimeverdrag, zijn eindrapport uitgebracht. Het eindrapport bevat diverse aanbevelingen voor het versterken van de mogelijkheden voor toegang tot digitaal bewijs in de cloud ten behoeve van strafrechtelijke handhaving. Eén van de aanbevelingen betreft het voorbereiden van een concept voor een additioneel protocol bij het verdrag. Tijdens de bijeenkomst van het comité van verdragspartijen op 14 en 15 november 2016 heeft het comité bij consensus besloten dat er in beginsel een noodzaak is voor een additioneel protocol. Ten behoeve van een formeel besluit van het comité om een conceptprotocol op te stellen bij de volgende bijeenkomst van het comité in juni 2017, is de Cloud Evidence Group verzocht Terms of Reference voor een dergelijk proces uit te werken. Deze Terms of Reference worden in juni verwacht. Op het verdere verloop van de discussie over dit onderwerp kan echter niet worden vooruit gelopen.

De leden van de fractie van GroenLinks hebben gevraagd hoe het wetsvoorstel zich verhoudt tot de huidige regels op het gebied van internationale samenwerking ten aanzien van cybercriminaliteit. Tevens hebben de leden van deze fractie gevraagd wanneer er precies gebruik gemaakt kan worden van de voorgestelde grensoverschrijdende bevoegdheid en of het gebruikelijke rechtshulpverzoek niet volstaat voor dit soort gevallen.

Het wetsvoorstel brengt geen verandering in de bestaande regels voor de internationale samenwerking. Een belangrijke bron voor dergelijke regels ten aanzien van cybercriminaliteit wordt gevormd door het eerdergenoemde Cybercrimeverdrag. Met de Wet computercriminaliteit II is dit verdrag in de Nederlandse wetgeving geïmplementeerd. Ter uitvoering van dit verdrag zijn een aantal gedragingen in de Nederlandse wetgeving strafbaar gesteld, zoals de wederrechtelijke toegang tot computersystemen, de wederrechtelijke onderschepping van computergegevens en de verstoring van computersystemen. Tevens zijn de bevoegdheden van politie en justitie op basis van de Nederlandse wetgeving aangepast, zoals die inzake de tijdelijke ‘bevriezing’ van bepaalde opgeslagen gegevens, het doorzoeken van computers en computergegevens en de verstrekking van verkeersgegevens. Deze regels worden op geen enkele wijze door dit wetsvoorstel aangetast.

De voorgestelde bevoegdheid dient om op afstand heimelijk binnen te kunnen dringen in een geautomatiseerd werk. Internet is niet gebonden aan de landsgrenzen; bij de uitvoering van de bevoegdheid zullen dan ook geautomatiseerde werken kunnen worden benaderd die zich in het buitenland bevinden. Zoals in de memorie van toelichting en de nota naar aanleiding van het verslag uiteen is gezet, is een rechtshulpverzoek aangewezen als blijkt dat gegevens zich op het territorium van een andere staat bevinden (Kamerstukken II 2016/17, 34 372, nr. 3, par. 2.8.3. en nr. 6, blz. 94/95). Diverse landen, waaronder Nederland zelf, hebben ten behoeve van de snelle afhandeling van rechtshulp in cybercrimezaken een 24/7 contactpunt ingericht. Wanneer gegevens in de Cloud zijn opgeslagen of het internetgedrag van personen is gericht op het niet kunnen achterhalen van een geografische plaats (bijv. het gebruik anonimiseringssoftware zoals TOR) dan bestaat er geen wetenschap van de locatie van de herkomst of opslag van gegevens. Er kan dan geen rechtshulpverzoek aan een ander land worden gericht. Vooralsnog kunnen die gegevens ook binnen Nederland worden opgeslagen en verwerkt. Onder omstandigheden kan dit betekenen dat op afstand heimelijk wordt binnengedrongen in een geautomatiseerd werk bijvoorbeeld een server, met het oog op het verrichten van bepaalde onderzoekshandelingen waarvan niet bekend is of gegevens worden opgeslagen en verwerkt in Nederland of daarbuiten. Als wetenschap bestaat dat de gegevens niet in Nederland zijn opgeslagen dan moet dat in het bevel worden vermeld, zodat het aspect van de inbreuk op de soevereiniteit van een andere staat onderwerp vormt van een expliciete afweging van de officier van justitie en de rechter-commissaris. Indien in het verdere verloop van het onderzoek duidelijkheid ontstaat over de feitelijke locatie van de gegevens en die locatie in een andere land is dan wordt zo snel mogelijk alsnog een rechtshulpverzoek gedaan en aan de bevoegde buitenlandse autoriteiten verantwoording afgelegd over het handelen en de daaraan ten grondslag liggende afwegingen.

De leden van de fractie van GroenLinks hebben gevraagd hoe de onderhandelingen in EU-verband en in de Raad van Europa over een helder grensoverschrijdend juridisch kader verlopen.

Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van de VVD.

12. Overige

De leden van de fractie van de VVD hebben gevraagd hoe en waar gegevens worden opgeslagen die beschikbaar komen in het kader van het binnendringen in een geautomatiseerd werk op grond van de wet.

Gedurende het opsporingsonderzoek in het kader waarvan onderzoek wordt verricht in een geautomatiseerd werk, is er sprake van een strikte taakverdeling en functiescheiding. De uitvoering van een bevel tot onderzoek in een geautomatiseerd werk is voorbehouden aan daartoe aangewezen opsporingsambtenaren van een technisch team, vanwege hun specialistische kennis en vaardigheden op het terrein van informatie- en communicatietechnologie. Binnen de Landelijke eenheid van de Nationale politie worden één of meer technische teams ingericht. De gegevens die tijdens het onderzoek in een geautomatiseerd werk met een technisch hulpmiddel zijn geregistreerd, worden automatisch vastgelegd op een technische voorziening bij het betreffende technische team. De vastgelegde gegevens zijn uitsluitend toegankelijk voor door de korpschef aangewezen ambtenaren. De

technische infrastructuur is beveiligd tegen wijziging van de vastgelegde gegevens en tegen kennisneming door onbevoegden. Op basis van het bevel worden de vastgelegde gegevens door het technische team beschikbaar gesteld aan het tactische team dat is belast met het operationele onderzoek. De beschikbaar gestelde gegevens worden door het tactische team opgeslagen ten behoeve van het onderzoek.

De leden van de fractie van de VVD hebben gevraagd op welke wijze daarbij een onderscheid wordt gemaakt tussen gegevens die nodig zijn voor de vaststelling van ernstige strafbare feiten en zogenoemde bijvangst. De leden van deze fractie hebben verder gevraagd of de gegevens die als bijvangst gelden worden vernietigd, en zo ja, wanneer en hoe, en zo nee, op welke juridische grondslag de bijvangst wordt opgeslagen.

Hierboven is opgemerkt dat de resultaten van het onderzoek door het technische team ter beschikking worden gesteld aan het tactische team. Zo nodig kan het technische team op basis van technische criteria zorgdragen voor voorafgaande filtering van de onderzoeksgegevens, zodat binnen de categorieën van gegevens die in het bevel van de officier zijn opgenomen uitsluitend de gegevens die van belang zijn voor het opsporingsonderzoek ter beschikking komen van het tactische team. De verzamelde gegevens vallen onder een gedifferentieerd regime wat betreft de bewaartermijnen. De processen-verbaal en andere voorwerpen waaraan gegevens kunnen worden ontleend die zijn verkregen door observatie met behulp van een technisch hulpmiddel dat signalen registreert, het opnemen van vertrouwelijke communicatie en het aftappen en opnemen van communicatie worden door de officier van justitie, voor zover die niet bij de processtukken zijn gevoegd, ter beschikking gehouden van het onderzoek (artikel 126cc, eerste lid, Sv). Zodra twee maanden zijn verstreken nadat de zaak is geëindigd en de notificatie, bedoeld in artikel 126bb Sv is verricht, doet de officier van justitie de processen-verbaal en andere voorwerpen vernietigen. De procedure is uitgewerkt in het Besluit bewaren en vernietigen niet-gevoegde stukken.

De gegevens die zijn verkregen door de toepassing van de bevoegdheid met het oog op andere onderzoekshandelingen vallen onder het regime van de Wet politiegegevens. Afhankelijk van het specifieke doel van de verwerking kan de bewaartermijn verschillen. Doorgaans zullen de gegevens moeten worden verwijderd zodra deze niet langer noodzakelijk zijn voor het doel van het onderzoek, of gedurende een periode van maximaal een half jaar bewaard teneinde te bezien of zij aanleiding geven tot een nieuw onderzoek. Na afloop van deze termijn worden de gegevens verwijderd (artikel 9, vierde lid, Wpg). De verwijderde politiegegevens worden gedurende een termijn van vijf jaren bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen, en vervolgens gearchiveerd of vernietigd (artikel 14 Wpg).

De leden van de fractie van de VVD hebben gevraagd of bijvangst van fiscale aard wordt doorgestuurd naar de Belastingdienst. De leden van deze fractie hebben tevens gevraagd op grond van welke nationale en internationale rechtsregels, uitspraken en arresten, daaronder begrepen van internationale gerechtshoven, fiscale gegevens die kwalificeren als bijvangst dienen te worden doorgespeeld naar de Belastingdienst – eventueel naar de Belastingdienst van een andere staat – bijvoorbeeld onder de toepassing van een EU-verordening, verdrag of overeenkomst tot fiscale gegevensuitwisseling.

Het openbaar ministerie heeft de verantwoordelijkheid om een effectieve bijdrage te leveren aan een rechtvaardige en veilige samenleving. Het verstrekken van strafvorderlijke informatie aan anderen – binnen de geldende wettelijke kaders – kan daartoe een belangrijke bijdrage leveren. De Wet justitiële en strafvorderlijke gegevens biedt een wettelijke grondslag voor de verstrekking van strafvorderlijke gegevens aan personen of instanties voor buiten de strafrechtspleging gelegen doeleinden (artikel 37f Wjsg). Het verstrekken van strafvorderlijke gegevens is alleen mogelijk als het past binnen de taakuitoefening van het openbaar ministerie en voor zover dit noodzakelijk is wegens een zwaarwegend algemeen belang. Daarbij doet niet terzake op grond van welke specifieke opsporingsbevoegdheid de gegevens zijn verkregen; als de gegevens onderdeel vormen van het strafdossier dan kunnen deze op grond van de wet aan andere personen of instanties worden verstrekt. Het beleid terzake is uitgewerkt in de Aanwijzing verstrekking van strafvorderlijke gegevens voor buiten de strafrechtspleging gelegen doeleinden (Aanwijzing wet justitiële en strafvorderlijke gegevens; Stcrt. 2013, 32596).In voorkomende gevallen kunnen de gegevens uit het stafdossier ook aan de Belastingdienst worden verstrekt (Aanwijzing Wet justitiële en strafvorderlijke gegevens, punt 3, onder c). Wanneer een zaak is geëindigd met een sepot of een vrijspraak of wanneer nog geen definitieve vervolgingsbeslissing is genomen, geldt als uitgangspunt dat geen informatie wordt verstrekt tenzij er sprake is van een zwaarwegend belang dat de verstrekking in dat geval rechtvaardigt.

De leden van de fractie van de VVD hebben opgemerkt dat wanneer er bij de provider/aanbieder en de officier van justitie verschil van inzicht bestaat over het ontoegankelijk maken van gegevens in een geautomatiseerd werk, er een formele procedure in gang wordt gezet die mogelijk veel tijd in beslag kan nemen. De leden van deze fractie hebben gevraagd op welke manier wordt gewaarborgd dat deze procedurele route zo spoedig mogelijk verloopt, juist met het oog op de potentiële dreiging die met deze informatie verbonden kan zijn wanneer de informatie voor derden beschikbaar blijft op het net.

Een bevel van de officier van justitie aan de aanbieder tot het ontoegankelijk maken van gegevens betreft een ingrijpende beslissing omdat grondrechten van burgers, zoals de vrijheid van meningsuiting, hierbij kunnen zijn betrokken. Daarom is een voorafgaande rechterlijke toetsing vereist. Gekozen is voor een schriftelijke machtiging van de rechter-commissaris wegens het niet voldoen aan een ambtelijk bevel of het plegen van of deelnemen aan een strafbaar feit in verband met het verspreiden van de desbetreffende gegevens. De officier van justitie behoeft daarvoor niet te wachten op een definitieve beslissing van de rechter naar aanleiding van de ingestelde strafvervolging. Het zou dan enkele maanden of langer kunnen duren voordat er een definitieve uitspraak van de rechter is. De regeling is echter voorzien van de nodige waarborgen voor een zorgvuldige toepassing. Zo dient de rechter-commissaris de aanbieder in de gelegenheid te stellen te worden gehoord. Vanwege de mogelijk verstrekkende consequenties van een bevel tot ontoegankelijkmaking van gegevens staat voor de belanghebbende, waaronder degene tot wie het bevel is gericht, de mogelijkheid open van beklag bij de raadkamer van de rechtbank op grond van de bestaande beklagregeling voor inbeslaggenomen voorwerpen (artikel 552a Sv). Vanwege het spoedeisende karakter van de beslissing beslist de rechtbank zo spoedig mogelijk. Deze procedure kan binnen een kort tijdsbestek worden doorlopen. De regering is van mening dat hiermee een goed evenwicht is gevonden tussen de betrokken belangen.

De leden van de fractie van het CDA hebben opgemerkt dat de bewoordingen van de aanleiding tot het mogen binnendringen in een geautomatiseerd werk in de verschillende wetsartikelen

verschillend worden omschreven en hebben gevraagd of de regering de logica van de verschillende formuleringen kan uitleggen. Verder hebben de leden van deze fractie gevraagd of men in het ene geval eerder mag binnendringen dan in het andere geval en zo ja, wat de verschillen zijn en waarom deze zijn gemaakt.

De bewoordingen van de aanleiding tot het mogen binnendringen in een geautomatiseerd werk zijn in de verschillende wetsartikelen verschillend omschreven vanwege de verschillende verdenkingscriteria die van toepassing zijn. Dit onderscheid vloeit voort uit de systematiek van de Wet bijzondere opsporingsbevoegdheden waarmee (onder meer) Titel IVA van het Eerste Boek van het Wetboek van Strafvordering is gewijzigd. De Wet bijzondere opsporingsbevoegdheden vormt een apart regime voor het onderzoek naar georganiseerde criminaliteit (Kamerstukken II 1996/97, 25 403, nr. 2). Later is, met Titel VB, een afzonderlijk regime ingevoegd voor de opsporing van terroristische misdrijven (Kamerstukken II 2004/05, 30 164, nr. 2).

De voorgestelde bevoegdheid vertoont inhoudelijk overeenkomsten met de bijzondere opsporingsbevoegdheden van Titel IVA van het Eerste Boek van het Wetboek van Strafvordering en wordt – net als de in die titel genoemde bevoegdheden - heimelijk toegepast zonder dat de betrokkene daar weet van heeft. Daarom is gekozen voor plaatsing in die titel. Het is van belang dat de bevoegdheid van het onderzoek in een geautomatiseerd werk ook kan worden toegepast bij het onderzoek naar de georganiseerde criminaliteit en terroristische misdrijven. Daarom wordt voorgesteld deze bevoegdheid tevens op te nemen in de desbetreffende titels van het Eerste Boek.

In titel IVA is als criterium voor de toepassing van de opsporingsbevoegdheden opgenomen de verdenking van een misdrijf. In titel V van het Eerste Boek is als verdenkingscriterium opgenomen: een redelijk vermoeden op grond van feiten of omstandigheden dat in georganiseerd verband misdrijven als omschreven in artikel 67, eerste lid, Sv worden beraamd of gepleegd die gezien hun aard of samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren. Bij enkele in titel V geregelde bevoegdheden, namelijk het aftappen en opnemen van communicatie en het opnemen van vertrouwelijke communicatie, is de kring van personen beperkt tot personen ten aanzien van wie een redelijk vermoeden bestaat dat zij betrokken zijn bij het in georganiseerd verband beramen of plegen van ernstige misdrijven. Zij behoeven geen verdachte te zijn in de zin van artikel 27 Sv, maar zij dienen wel een meer dan toevallige betrokkenheid te hebben bij het criminele handelen van de groepering, die bijvoorbeeld blijkt uit meer dan incidentele contacten met de criminele organisatie of haar leden. In Titel VB van het Eerste Boek is voor de opsporingsbevoegdheden als verdenkingscriterium opgenomen: aanwijzingen van een terroristisch misdrijf. Van aanwijzingen is sprake indien de beschikbare informatie feiten en omstandigheden bevat die erop duiden dat daadwerkelijk een terroristisch misdrijf zou zijn of zal worden gepleegd. Anders dan bij de opsporing op basis van Titel IV is bij terroristische misdrijven niet vereist een ‘redelijk vermoeden’ van een strafbaar feit, aanwijzingen zijn voldoende.

De leden van de fractie van het CDA hebben gewezen op het gestelde in artikel II, onder X, onder punt 9 van het wetsvoorstel, op grond waarvan het gerecht het bevel kan opheffen als het de klacht gegrond acht. Volgens de leden van deze fractie zou hier geen sprake moeten zijn van ‘kunnen’ maar van ‘moeten’. De leden van deze fractie hebben gevraagd aan welke

gevallen de regering denkt waarbij – ondanks de gegrondheid van het beklag – het bevel toch niet zou moeten of mogen worden opgeheven.

In het voorliggende wetsvoorstel wordt voorgesteld de regeling over het beklag tegen inbeslagneming, in artikel 552a Sv, uit te breiden met de mogelijkheid dat belanghebbenden zich kunnen beklagen over een bevel tot het ontoegankelijk maken van gegevens, bedoeld in artikel 125p Sv. Als het gerecht het beklag gegrond acht dan kan het gerecht het bevel geheel of gedeeltelijk opheffen. Niet uitgesloten is dat het gerecht het beklag van een belanghebbende gegrond acht omdat het belang van de belanghebbende om over de gegevens te kunnen beschikken prevaleert boven het belang van de officier van justitie om de gegevens ontoegankelijk te houden, in afwachting van een definitieve beslissing van de rechtbank, op grond van artikel 354 of artikel 552fa Sv. Daarbij kan het gerecht termen aanwezig zien om de ontoegankelijkmaking van de gegevens overigens te handhaven. Dit kan aan de orde zijn als het gaat om kinderpornografisch materiaal en de ouders of hulpverleners kennis willen nemen van de beelden om hulp of ondersteuning te kunnen bieden aan het slachtoffer. De rechter heeft dan de keuze tussen gehele of gedeeltelijke opheffing van de ontoegankelijkmaking van de gegevens.

De leden van de fractie van de SP wilden graag weten wat artikel 125p Sv extra beoogt in vergelijking tot artikel 54a Sr, omdat ook met dit laatste artikel kon worden bevolen websites met bijvoorbeeld materiaal van seksueel misbruik van kinderen offline te halen. Zij hebben gevraagd of de regering kan uitleggen waarom artikel 125p Sv nodig is.

Met het voorgestelde artikel 125p Sv wordt een afzonderlijke en zelfstandige bevoegdheid voor de officier van justitie geïntroduceerd om bij verdenking van een strafbaar feit waarvoor voorlopige hechtenis is toegestaan een tussenpersoon te bevelen terstond alle maatregelen te nemen die redelijkerwijs gevergd kunnen worden om gegevens ontoegankelijk te maken. De regeling is bedoeld als aanvulling op de bestaande vrijwillige Notice and take down (NTD) gedragscode, die zich richt op tussenpersonen die in Nederland een openbare telecommunicatiedienst op het internet leveren. De bevoegdheid is van belang in gevallen waarin de tussenpersoon niet bereid is op basis van de gedragscode de gegevens ontoegankelijk te maken, bijvoorbeeld als de officier van justitie en de tussenpersoon van mening verschillen of de vrijheid van meningsuiting in het geding is. Daarnaast kan het bevel ook worden gericht aan tussenpersonen die de gedragscode niet hebben ondertekend, waarbij te denken valt aan hosting providers en beheerders van een website.

De leden van de fractie van de SP hebben begrepen dat content die offline is gehaald binnen afzienbare tijd weer online kan komen. De leden van deze fractie hebben gevraagd of zinsnede "[...] of nieuwe strafbare feiten te voorkomen" in artikel 125p, tweede lid, onder b, van het wetsvoorstel suggereert dat een internetserviceprovider die het materiaal offline heeft gehaald aansprakelijk is als het materiaal daarna opnieuw op internet verschijnt.

Op grond van het voorgestelde artikel 125p, eerste lid, Sv dient de aanbieder van een communicatiedienst alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om gegevens ontoegankelijk te maken ter beëindiging van een strafbaar feit of ter voorkoming van strafbare feiten. In bepaalde gevallen is het technisch niet goed mogelijk om de gegevens effectief ontoegankelijk te maken, bijvoorbeeld als gegevens op de een of andere manier zijn gedupliceerd en ook nog op andere gegevensdragers staan. De verplichting tot het

ontoegankelijk maken is, evenals in het huidige artikel 54a Sr het geval is, geclausuleerd. In het voorgestelde artikel 125p, derde lid, Sv wordt artikel 125o, tweede en derde lid, Sv van overeenkomstige toepassing verklaard. Daarmee wordt onder het ontoegankelijk maken van gegevens hetzelfde verstaan als in artikel 125o, tweede lid, Sv, te weten: het treffen van maatregelen ter voorkoming dat de beheerder van een geautomatiseerd werk of derden verder van die gegevens kennisnemen of gebruikmaken, alsmede ter voorkoming van de verdere verspreiding van die gegevens. De ontoegankelijkmaking van de gegevens kan plaatsvinden door de desbetreffende gegevens te verwijderen, dan wel de toegang daartoe te blokkeren. Blokkering kan aan de orde zijn als de gegevens niet kunnen worden verwijderd, zodat de gegevens voor de gebruikers niet raadpleegbaar zijn. Om aan het bevel tot ontoegankelijkmaking te voldoen dient de blokkering voort te duren zolang de gegevens worden aangeboden. Dit laat de situatie onverlet dat dezelfde gegevens op een andere plaats op het internet toegankelijk worden of nog blijken te zijn, omdat ze bijvoorbeeld in eerdere instantie zijn gedupliceerd (in de techniek aangeduid als 'mirror'). Voor een dergelijke toegankelijkheid kan de provider niet verantwoordelijk worden gehouden, tenzij de provider hiervan expliciet op de hoogte is. Op grond van artikel 54a Sr blijft vervolging van een tussenpersoon die een communicatiedienst aanbiedt bij een strafbaar feit dat met gebruikmaking van die dienst wordt begaan, achterwege als de tussenpersoon voldoet aan een bevel als bedoeld in artikel 125p Sv.

De leden van de fractie van de ChristenUnie hebben gevraagd om een reflectie op het feit dat Nederland bovenmatig vaak gebruik maakt van telefoon- en gegevenstaps, mede in het licht van de uitwerking op de veiligheid voor Nederlandse burgers vergeleken met andere EU-burgers. De leden van deze fractie hebben tevens gevraagd welke verwachting de regering heeft van het gebruik van de voorgestelde bevoegdheid en of deze zich zal ontwikkelen tot een ultimum remedium of juist tot een gangbaar gebruikte opsporingsbevoegdheid.

Enkele jaren geleden is door het WODC een onderzoek verricht om een beter zicht te verkrijgen op het feitelijke gebruik van de telefoon- en internettap bij de opsporing en vervolging in strafzaken, mede in het licht van de wijze waarop dat in enkele ons omringende landen gebeurt. Dit onderzoek beoogde een beeld te geven van de wettelijke kaders en het gebruik van de telefoon- en internettap in de opsporing in Nederland en enkele ons omringende landen, te weten Engeland en Wales, Zweden en Duitsland. In het rapport getiteld 'Het gebruik van de telefoon- en internettap in de opsporing', dat bij brief van 23 mei 2012 aan uw Kamer is aangeboden (Kamerstukken II, 2011/12, 30517, nr. 25) wordt vastgesteld dat het heersende beeld is dat er in Nederland veel wordt getapt. Het aantal taps op vaste lijnen is in Nederland al jaren stabiel, maar de opkomst van de mobiele telefoon heeft geresulteerd in een flinke toename van het aantal taps. Hierbij passen enkele belangrijke kanttekeningen. In de eerste plaats blijkt uit de cijfers van het rapport dat het aantal taps slechts een klein percentage betreft van het totale aantal telefoonaansluitingen in Nederland. De toename van het aantal telefoontaps vanaf 1998 is toe te schrijven aan de opkomst van de mobiele telefonie. Daar het aantal taps op vaste lijnen ongeveer gelijk is gebleven, kan hieruit worden opgemaakt dat het aantal telefoontaps het stijgende aantal mobiele telefoons op de voet is gevolgd (blz. 81). Ook in Duitsland is een dergelijke ontwikkeling kenbaar, in het rapport wordt melding gemaakt van een stijging van het aantal tapbevelen in dat land van 6.391 tot 39.200 in de periode van 1998 tot en met 2007. Dit betreft een toename van ruim 600 % (blz. 242). In de tweede plaats worden door de verdachten/gebruikers dikwijls meerdere nummers gebruikt. Om verdachten telefonisch toch te kunnen blijven volgen, moet dan steeds een nieuw tapbevel worden

aangevraagd. In het rapport wordt melding gemaakt van meerdere nummers per verdachte, in dat kader wordt melding gemaakt van een zaak waarbij bij iemand thuis 150 verschillende telefoons en 380 SIM-kaarten zijn gevonden; op grond van de huidige regeling zijn dan in ieder geval 380 verschillende tapbevelen en machtigingen vereist (blz. 129). Ook uit de Engelse tapstatistieken kan worden afgeleid dat personen frequent wisselen van toestel en van nummer, aangezien het aantal tussentijdse mutaties van de lopende bevelen veel groter is dan het aantal tapbevelen (blz. 259). De onderzoekers geven aan dat overwogen zou kunnen worden om over te stappen naar een tapbevel dat gekoppeld is aan een persoon in plaats van aan een telefoonnummer of telefoontoestel, een werkwijze die ook in een aantal onderzochte landen wordt gebezigd. In de derde plaats wordt in andere landen gekozen voor de inzet van verderstrekkende bevoegdheden. Op dit punt zijn er verschillen in de keuzes die worden gemaakt. Volgens de onderzoekers is dit voor een groot deel te verklaren door het feit dat er tussen de onderzochte landen een verschil van perceptie bestaat als het gaat om de zwaarte van de verschillende opsporingsmiddelen, zoals infiltratie door undercoveragenten.

De onderzoekers concluderen dat een vergelijking van cijfers over de inzet van taps in de onderzochte landen niet één op één is te maken. Taps worden in andere landen anders geregistreerd en de rechtsstelsels verschillen van elkaar. In het algemeen kan worden geconcludeerd dat de telefoontap in Nederland frequenter wordt ingezet dan in de andere onderzochte landen. Daar staat tegenover dat in Nederland op nummer wordt getapt, niet op de persoon, waardoor het aantal taps aanzienlijk hoger is dan het aantal personen van wie de communicatie wordt afgetapt, en dat andere bijzondere opsporingsmiddelen, mede vanwege het verhoogde risico voor de betrokken opsporingsambtenaren, juist minder vaak worden ingezet dan in het buitenland.

De regering verwacht niet dat de voorgestelde bevoegdheid zich zal ontwikkelen tot een gangbaar gebruikte opsporingsbevoegdheid. Daarvoor zijn verschillende redenen. In de eerste plaats gelden er strikte wettelijke voorwaarden voor de inzet van deze bevoegdheid. Dit betreft onder meer het criterium van het dringende opsporingsbelang en een voorafgaande machtiging van de rechter-commissaris. Bij de toetsing van de voorgenomen inzet door in eerste instantie de officier van justitie en vervolgens de rechter-commissaris, vormt de invulling van het criterium van het dringende opsporingsbelang, aan de hand van een beoordeling van de proportionaliteit en subsidiariteit, een essentieel bestanddeel. Indien er andere, minder ingrijpende middelen zijn waarmee het doel bereikt kan worden en het onderzoek het toelaat (denk hierbij aan gevaarzetting en risico’s bij het te laat kunnen ingrijpen), zoals het vorderen van gegevens bij dienstverleners, het plaatsen van een tap, het doen van een doorzoeking, inbeslagneming of een bevriezingsbevel, zal eerst daarvoor moeten worden gekozen. In de tweede plaats betreft dit 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, het technische team, dat organisatorisch is gescheiden van het tactische team dat is belast met het tactische opsporingsonderzoek en dat kan worden belast met de uitvoering van een bevel van de officier van justitie tot het op afstand binnendringen van een geautomatiseerd werk. In de derde plaats betreft dit een bevoegdheid waarvan de inzet een zorgvuldige voorbereiding vergt vanwege mogelijke beveiligingsmaatregelen rond het geautomatiseerde werk en de noodzaak om heimelijk te opereren. Voorkomen moet worden dat de betrokkene er van op de hoogte raakt dat opsporingsambtenaren op afstand zijn binnengedrongen in het geautomatiseerde werk dat bij

hem in gebruik is en maatregelen treft om het opsporingsonderzoek te frustreren. Ieder geautomatiseerd werk is vanuit technisch oogpunt echter anders en dit betekent dat de methode voor het binnendringen nauwkeurig moet worden afgestemd op het geautomatiseerde werk in kwestie. De noodzaak van een zorgvuldige voorbereiding komt eveneens tot uitdrukking in de procedure die voorschrijft dat de voorgenomen inzet wordt voorgelegd aan de Centrale Toetsingscommissie, die het College van procureurs-generaal adviseert over de voorgenomen inzet van een aantal bijzondere opsporingsmethoden. In het licht van deze omstandigheden ligt een al te gemakkelijke inzet van deze bevoegdheid bepaald niet voor de hand.

De leden van de fractie van de ChristenUnie hebben voorts gevraagd hoe de leeftijdsgrenzen in de voorgestelde artikelen 248a Sr en 248e Sr zich verhouden tot de leeftijdsgrens van 21 jaar in het wetsvoorstel regulering prostitutie en bestrijding misstanden seksbranche.

De in de zedenwetgeving en het wetsvoorstel regulering prostitutie en bestrijding misstanden seksbranche (Wrp) gestelde leeftijdsgrenzen dienen beschouwd te worden in het licht van de door deze wetgeving beschermde belangen. De zedenwetgeving beschermt kinderen tegen inbreuken op hun lichamelijke en seksuele integriteit en doorkruising van hun seksuele ontwikkeling door het plegen van ontucht met een kind strafbaar te stellen. Er zijn verschillende niveaus van strafrechtelijke bescherming al naar gelang de leeftijd van een kind. De grens voor seksuele meerderjarigheid is in beginsel op zestien jaren gesteld. Ontucht met een kind beneden de leeftijd van zestien jaren is strafbaar. In artikel 248e Sr, waarin grooming strafbaar is gesteld, wordt aangesloten bij deze leeftijdsgrens. In bepaalde omstandigheden strekt de strafrechtelijke bescherming tegen ontucht zich uit tot de leeftijd van achttien jaren. Dit is het geval in artikel 248a Sr, waarin kinderen tot en met de leeftijd van achttien jaren beschermd worden tegen seksuele verleiding.

Prostitutie is een legale beroepsactiviteit. Aan de in de Wrp opgenomen minimumleeftijd van 21 jaren voor de uitoefening van prostitutiewerkzaamheden ligt de doelstelling ten grondslag om jeugdige personen buiten de prostitutie te houden. Aangenomen wordt dat personen op de leeftijd van 21 jaren meer levenservaring hebben, weerbaarder zijn en de tijd hebben gehad om als volwassene na te denken over de zwaarte en risico’s van het prostitutievak. Ook is er een grotere kans dat personen op deze leeftijd een vervolgopleiding hebben gevolgd waarmee kennis en vaardigheden zijn opgedaan waardoor er een mogelijk alternatief voor sekswerk aanwezig is.

De leden van de fractie van de ChristenUnie hebben tevens gevraagd met welke reden in het voorgestelde artikel 248a Sr wordt gekozen voor een objectivering van de leeftijdsaanduiding.

Het huidige artikel 248a Sr dat verleiding van een minderjarige strafbaar stelt, bevat de bestanddelen “persoon waarvan hij weet of redelijkerwijs moet vermoeden dat deze de leeftijd van achttien jaren nog niet heeft bereikt”. Het gaat hier om zogenaamde subjectieve bestanddelen: er is opzet dan wel schuld ten aanzien van de leeftijd van de minderjarige vereist. Uit de jurisprudentie kan worden afgeleid dat dit delictsbestanddeel aan een veroordeling wegens artikel 248a Sr in de weg staat indien de verdachte iemand die zich als minderjarige voordoet verleidt tot ontucht. Hierdoor is de opsporing van dit strafbare feit met behulp van een lokpuber niet mogelijk.

Het wetsvoorstel breidt de strafrechtelijke aansprakelijkheid uit tot verleiding van iemand die zich voordoet als een persoon die de leeftijd van achttien jaren nog niet heeft bereikt. Het is niet goed denkbaar dat een verdachte weet dan wel redelijkerwijs dient te vermoeden dat hij met iemand die zich voordoet als een minderjarige te maken heeft. Daarom is het schuldverband ten aanzien de leeftijd geschrapt. Voor gedragingen waarbij iemand daadwerkelijk een minderjarige verleidt wordt

evenmin opzet of schuld op de leeftijd vereist. Het gebruik van geobjectiveerde leeftijden komt vaker voor in de zedentitel, bijvoorbeeld in artikel 247 Sr waarin het plegen van ontucht met een persoon beneden de leeftijd van zestien jaren strafbaar is gesteld.

De leden van de fractie van de ChristenUnie hebben ook gevraagd of de nieuwe invulling van artikel 248a Sr gevolgen heeft voor de interpretatie van de daaropvolgende artikelen en in het bijzonder artikel 248b Sr. De leden van deze fractie hebben tevens gevraagd of 'ontucht plegen' in dit artikel door het voorgestelde artikel 248a Sr in het vervolg ook met een webcam of ander technisch hulpmiddel kan plaatsvinden.

In zowel het huidige artikel 248a Sr als het voorgestelde artikel 248a Sr wordt het opzettelijk bewegen van een minderjarige tot het plegen van ontuchtige handelingen strafbaar gesteld. Handelingen die op afstand via een webcam worden verricht kunnen ook nu al een strafbare gedraging opleveren. Het openbaar ministerie gebruikt artikel 248a Sr regelmatig voor de opsporing en vervolging van digitale kinderlokkers die online kinderen aanzetten tot het zich naakt te tonen voor een webcam of tot het verrichten van seksuele handelingen. Doordat de inzet van de lokpuber op dit moment niet mogelijk is vindt de opsporing van deze strafbare feiten vaak achteraf plaats, als het leed al is geschied. Vaak gaat het om verdachten die zoveel mogelijk kinderen tegelijk benaderen en veel schade aanrichten. In verschillende zaken hebben veroordelingen plaatsgevonden (recent: Rechtbank Amsterdam, 16 maart 2017, ECLI:NL:RBAMS:2017:1627).

Het plegen van ontucht *met* iemand is in artikel 248a Sr geen voorwaarde voor strafrechtelijke aansprakelijkheid; in een aantal andere artikelen in de zedentitel, waaronder het door de leden van de fractie van de ChristenUnie genoemde artikel 248b Sr, wordt dit wel vereist. In het WODC-onderzoek "Herziening van de zedendelicten" is het systematische vraagstuk in hoeverre voor "ontucht plegen *met*" fysiek contact nodig is aan de orde gesteld. Op dit moment wordt een wetsvoorstel tot modernisering van de zedentitel van het Wetboek van Strafrecht voorbereid. Doel is onder meer om digitaal gepleegde zedenmisdrijven een duidelijke plaats te geven in het wettelijke kader.

De Staatssecretaris van Veiligheid en Justitie,

K.H.D.M. Dijkhoff

Van: 10.2.e @politie.nl]
Verzonden: dinsdag 13 juni 2017 15:41
Aan: 10.2.e - BD/DRC/CV
Onderwerp: FW: Deskundigenbijeenkomst privacy Eerste Kamer

Zojuist ontvangen.

Gr.

10.2.e

Van: 10.2.e BD/DRC/CV
Verzonden: dinsdag 13 juni 2017 15:54
Aan: 10.2.e - BD/DRC/CV; 10.2.e - BD/DRC/CV
CC: 10.2.e - BD/DRC/CV
Onderwerp: FW: Deskundigenbijeenkomst privacy Eerste Kamer

TI, verdere info over de hoorzitting. Het heet ook nu: deskundigenbijeenkomst privacy!

9

Met vriendelijke groet,
10.2.e
Beleidsadviseur
M 06 10.2.e
10.2.e @minvenj.nl

From: 10.2.e BD/DRC/CV
Sent: dinsdag 13 juni 2017 16:52:42
To: 10.2.e (LP Rotterdam)';10.2.e @om.nl
Cc: 10.2.e BD/DGPOL/PBT/PT; 10.2.e - BD/DRC/CV
Subject: FW: Deskundigenbijeenkomst privacy Eerste Kamer

Dag 10.2.e ,

Ziehier de laatste info van de EK. Behalve de procedurele info in de mail, zit er w.b. ANPR ook een bijlage bij (brief van mijn hand) over rectificatie van cijfers. Deze brief kan dus ook besproken worden, al lijkt het me voor de EK niet bijster interessant. Als je hier meer over wilt weten, dan is het denk ik handig dat we even bellen.

De korte versie is: bij het opstellen van de memorie van antwoord hebben we uit twee hoeken cijfers gekregen. Die cijfers weken van elkaar af, maar dat hebben we niet gezien. We hebben toen een van
de beide sets cijfers in de Kamerstukken opgenomen, en die cijfers bleken onjuist. Overigens bleek ook de andere set aangeleverde cijfers niet geheel juist.

groeten

10.2.

Van: 10.2.e . - BD/DGPOL/PBT/PT 10.2.e @minvenj.nl>
Verzonden: dinsdag 13 juni 2017 17:27
Aan: 10.2.e
CC: 10.2.e BD/DGPOL/PBT/PT
Onderwerp: FW: Deskundigenbijeenkomst privacy Eerste Kamer
Bijlagen: Informatie Nationale Politie.pdf; Programma deskundigenbijeenkomst privacy.pdf; EK 34372, C.pdf; EK 33542, D.pdf; EK 34372, D.pdf

Oa een bijlage waarin het programma van 20/6 is opgenomen, incl namen v vertegenwoordigers vd diverse organisaties. Zet jij het door naar de betrokkenen en evt andere geïnteresseerden 9 etc etc)?

10.2.e
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
10.2.e @minvenj.nl
06 10.2.e

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Dubbel zie docs. 675, 676, 677, 678, 679

Onderwerp
Consultatie Ontwerpbesluit Onderzoek in Geautomatiseerd Werk

Adresregels
Aan de Staatssecretaris van Veiligheid en Justitie
Dr. K.H.D.M. Dijkhoff
Tav Directie Wetgeving en Juridische zaken
Directeur Wetgeving en Juridische Zaken
Mr. A.G. van Dijk
Postbus 20301
2500 EH Den Haag

Organisatieonderdeel
Portefeuillehouder Digitalisering en Cybercrime
Programma CCIII

Behandeld door
10.2.e

Functie
Operationeel Specialist

Telefoon
10.2.e

E-mail
10.2.e @politie.nl

Ons kenmerk
Klik hier als u tekst wilt invoeren.

Uw kenmerk
2068042

In afschrift aan
Klik hier als u tekst wilt invoeren.

Datum
14 juni 2017

Bijlage(n)
0

Pagina
1

Geachte Excellentie,

Van het door u bij brief van 10 mei jl. ter consultatie aangeboden Ontwerpbesluit Onderzoek in een geautomatiseerd werk (hierna: het Ontwerpbesluit), heb ik met belangstelling kennis genomen.

Voor het feit dat de Politie in ruime mate betrokken heeft mogen zijn bij de besprekingen over de totstandkoming van dit Ontwerpbesluit zeg ik u dank.

Niettemin nopen de tekst van het Ontwerpbesluit en de daarbij behorende Nota van Toelichting (hierna: de NvT) mij tot het maken van de volgende opmerkingen.

In hoofdstuk 4 (Geautomatiseerde vastlegging van gegevens over de uitvoering van een bevel) van het Ontwerpbesluit worden regels gesteld over logging. De politie is vanuit het perspectief van transparantie voorstander van het op een adequate en toetsbare manier uitvoeren van de logging. Dit om 12-14 door de Officier van Justitie en de Rechter Commissaris vooraf mogelijk te maken en daarnaast toezicht achteraf op de uitgevoerde handelingen door de Inspectie Veiligheid en Justitie (IV&J) en de rechter mogelijk te maken.

Met opmerkingen [A1]: 12-14

Logging
Uit de NvT is niet duidelijk op te maken welke verschillende vormen van logging gegenereerd worden op de technische infrastructuur van de politie en hoe deze verschillende vormen van logging in verhouding tot elkaar staan. Ter illustratie volgen hieronder een aantal zinsneden uit de NvT:

1. Zowel tijdens de uitvoering van het bevel van de officier van justitie als na afloop hiervan kan worden vastgesteld of een handeling of bewerking heeft plaatsgevonden die van invloed is op de betrouwbaarheid en integriteit van de vastgelegde gegevens (pagina 12).
2. De logging is ten eerste bedoeld voor interne controle van de tijdens de onderzoeksfase verrichte handelingen (pagina 12).
3. Daarnaast maakt de bewijslogging het mogelijk om de met een technische hulpmiddel geregistreerde gegevens achteraf te verantwoorden in een strafzaak (pagina 12).
4. Er wordt gelogd op het niveau van autorisatie, op het niveau van de verrichte onderzoekshandelingen en op het niveau van de werking van het systeem (pagina 19).
5. De gelogde gegevens moeten worden verwijderd zodra deze niet langer noodzakelijk zijn voor het doel van het onderzoek(pagina 19).

Bovenstaande punten, in combinatie met de verdere tekst in de NvT, maken niet helder welke vorm van logging dient voor bewijsvergaring en welke voor interne controle. Ook wordt niet duidelijk wat het onderscheid is tussen de verschillende vormen van logging die plaatsvinden op de technische infrastructuur van de politie. Dit is wel noodzakelijk om helderheid te verschaffen over het doel van de verschillende vormen van logging.

Voorgesteld wordt een duidelijker onderscheid van de verschillende vormen van logging op te nemen in de NvT Het onderscheid in onderstaande vormen van logging is in de cybersecurity wereld een herkenbaar en gebruikelijk onderscheid:

1. Inzetlogging

Inzetlogging heeft betrekking op alle logging die specifiek wordt uitgevoerd om de verrichte handelingen vast te leggen. Dit betreft niet alleen het (automatisch) vastleggen van het beeldscherm en de toetsaanslagen van de opsporingsambtenaar, maar ook het vastleggen van de communicatie tussen de technische infrastructuur en het geautomatiseerde werk, het vastleggen van gebruikte scripts, software versies en het journaal van de opsporingsambtenaar. Logging zal zoveel mogelijk geautomatiseerd plaatsvinden. Niet alles kan automatisch worden vastgelegd; procedures zullen ervoor moeten zorgen dat dat wat niet automatisch vastgelegd kan worden, handmatig vastgelegd wordt.

2. Systeemlogging

Systeemlogging wordt voornamelijk gebruikt voor het signaleren, onderzoeken en verhelpen van problemen m.b.t. veiligheid, betrouwbaarheid en beschikbaarheid in de technische infrastructuur van de politie. De politie maakt hierbij gebruik van standaard protocollen. Hierdoor kan het voorkomen dat niet alle logregels worden afgeleverd. Systeemlogging wordt automatisch door alle gebruikte systemen gegenereerd, centraal verzameld en vastgelegd. De centraal verzamelde systeemlogging bevat logregels van alle systemen binnen de technische infrastructuur. Veel systemen binnen de technische infrastructuur van de politie worden voor de uitvoering van meerdere bevelen tegelijkertijd gebruikt, waardoor afzonderlijke logregels niet aan een specifiek bevel kunnen worden toegewezen.

De gegevens worden wel bewaard om aan de eisen van transparantie te kunnen voldoen. Indien tijdens de behandeling van een zaak of tijdens audits van de Inspectie V&J vermoedens zijn van ongeautoriseerde toegang tot systemen en/of oneigenlijk gebruik van systemen dat heeft kunnen leiden tot het in twijfel trekken van de verrichte handelingen en het hiermee vergaarde bewijs, zullen de logregels ten tijde van het uitvoeren van het betreffende bevel separaat veiliggesteld worden.

Met opmerkingen [A2]: Is veilgstellen wel een handige term? Ik denk dat wordt bedoeld: onderzocht kunnen worden?

3. Authenticatie- en Authorisatielogging

Authenticatie- en authorisatielogging zijn een subcategorie van systeemlogging. Daarmee zijn zij onderhevig aan de beperkingen van systeemlogging. Echter doordat authenticatie- en autorisatielogging van groot belang zijn voor de controle op de toegang tot een technisch hulpmiddel, 12 -14 aflevering van deze logregels moet gegarandeerd zijn.

Met opmerkingen [A3]: 12-14

Componentkeuring

Voor de keuring van technische hulpmiddelen kan keuring van afzonderlijke componenten de keuring aanzienlijk eenvoudiger maken. Dit kan bijvoorbeeld gelden als de toevoeging van een component voor een specifiek apparaat niet direct leidt tot een complete herkeuring van het technische hulpmiddel, aangezien deze toevoeging niet leidt tot een wijziging van de functionaliteit van het technisch hulpmiddel. Het is uitdrukkelijk niet de bedoeling dat met deze vorm van componentkeuring een nieuw technisch hulpmiddel wordt samengesteld. In de NvT is niet opgenomen dat een dergelijke

componentkeuring is toegestaan. De politie is voorstander van het opnemen van een dergelijke componentkeuring, aangezien hierdoor een snellere (her)keuring kan plaatsvinden. Dat is in het belang van een effectieve opsporing in een zeer dynamische en veranderlijke digitale wereld.

Functionaliteiten
Artikel 8 van het Ontwerpbesluit bepaalt dat een technisch hulpmiddel zodanig is ingericht dat de werking ervan kan worden beperkt tot de in het bevel vermelde functionaliteit of tot bepaalde functionaliteiten. De Keuringsdienst stelt daaropvolgend een handleiding op voor het gebruik van het hulpmiddel, waarbij wordt aangegeven welke instellingen bij gebruik moeten worden aangevinkt. De politie is de mening toegedaan dat dit artikel de mogelijkheid openhoudt om in bepaalde gevallen een technisch hulpmiddel in te zetten, ook indien de werking vanuit de aard van het hulpmiddel niet volledig beperkt kan worden tot het tot de in het bevel vermelde functionaliteit of functionaliteiten. De beperking tot de in het bevel genoemde gegevens kan dan plaatsvinden door een filtering door het technische team, alvorens de data wordt overgedragen aan het tactische onderzoeksteam. Het bevel biedt, in combinatie met de functiescheiding, waarborgen dat geen andere informatie dan waartoe het bevel strekt, zal worden gebruikt. Vanzelfsprekend zal hiervan ook proces-verbaal worden opgemaakt.

Met opmerkingen [A4]: Goed om aan te geven hoe we het gaan interpreteren. Is dit afgestemd met het OM?

Opnemen communicatie
Artikel 9 lid 2 stelt dat het opnemen van telecommunicatie beperkt is tot een nummer. Dit is technisch vaak niet mogelijk. Digitale communicatievormen lopen steeds minder via de traditionele nummers. De term nummer is daardoor niet toekomstbestendig. 12-14

Met opmerkingen [A5]: 12-14

Verwijdering van een technisch hulpmiddel
In artikel 28 van het Ontwerpbesluit worden regels gesteld over het verwijderen van een technische hulpmiddel. Uit dit artikel en de bijbehorende passages in de NvT wordt niet duidelijk op welke gronden tot verwijdering over kan worden gegaan. De politie adviseert een passage op te nemen in het Ontwerpbesluit waarin wordt aangegeven op basis van welke bevoegdheid over gegaan kan worden tot het verwijderen van een technisch hulpmiddel na afloop van een bevel tot binnendringen. Opname in het bevel tot binnendringen dat het bevel ook het verwijderen van het technisch hulpmiddel bevat kan hierover al duidelijkheid verschaffen.

Met opmerkingen [A6]: Is dit afgestemd met het OM?

187d Sv procedure
In de NvT wordt melding gemaakt van de mogelijkheid tot de inzet van de artikel 187d Sv procedure. De politie is verheugd dat deze procedure is opgenomen in het Ontwerpbesluit. Hiermee kan geheimhouding van gebruikte middelen worden bewerkstelligd, wat vanuit tactisch perspectief noodzakelijk is. De politie vertrouwt er op dat er naast deze procedure nog voldoende waarborgen in het rechtsproces zijn ingebouwd om deze geheimhouding in stand te houden. Daarnaast wordt geadviseerd om in de definitieve tekst van het Ontwerpbesluit aansluiting te zoeken bij de geheimhoudingsprocedures zoals die ook gelden binnen het WOD-domein (Werken on Dekmantel).

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,

E.S.M. Akerboom

korpschef

Onderwerp
Consultatie Ontwerpbesluit
Onderzoek in Geautomatiseerd
Werk

Datum
14 juni 2017

Pagina

Klik hier als u tekst wilt invoeren.
Klik hier als u tekst wilt invoeren. Klik hier als u tekst wilt invoeren.

Onderwerp
Consultatie Ontwerpbesluit Onderzoek in Geautomatiseerd Werk

Klik hier als u tekst wilt invoeren.
www.politie.nl

Datum
14 juni 2017

Pagina
5 van 5

Van: 10.2.e - BD/DRC/CV 10.2.e @minvenj.nl]
Verzonden: woensdag 14 juni 2017 12:31
Aan: 10.2.e (Landelijk Parket Rotterdam) 10.2.e @om.nl>; 10.2.e @politie.nl>
CC: 10.2.e . - BD/DCS/ACSB 10.2.e @nctv.minvenj.nl>; 10.2.e - BD/DRC/CV 10.2.e @minvenj.nl>; 10.2.e - BD/DRC/CV 10.2.e @minvenj.nl>; 10.2.e - BD/DRC/CV 10.2.e @minvenj.nl>; 10.2.e - BD/DRC/CV 10.2.e @minvenj.nl>

Onderwerp: RE: Mogelijke vragen voor Pol, OM en NCSC

Hallo 10.2.e en 10.2.e

Ik had nog even wat vragen opgesteld, ter info hieronder.

De deskundigenbijeenkomst heet officieel: deskundigenbijeenkomst privacy

Bij de vraag of er voldoende privacywaarborgen zijn kom je al snel op een politiek vlak. Als ik met jullie mee mag denken, zou ik beantwoording langs onderstaande lijn voorstellen:

12-14

[redacted]

POL: INZET

-Hoe verwerft u expertise?
-Wordt het middel van tevoren gekeurd?
-aankoop software, hoe weten we of er een onbekende kwetsbaarheid in zit?
kunnen we dat komen te weten?
zou u het nodig vinden om te weten of er een onbekende kwetsbaarheid in zit?
-Hoe bruikbaar zijn bekende kwetsbaarheden, heeft u onbekende kwetsbaarheden echt nodig?
-privacy: wat is het voordeel van de scheiding van het tactisch en technisch team.
-Hoe wordt de data verzameling ingeperkt tot de verdachte?
-Is dit geen efficiency maatregel voor minder politie inzet?
-Hoe is het toezicht geregeld?
-Hoe verschaft u transparantie over uw werkwijze?
-Bent u klaar op dag 1 om met de inzet te beginnen?

Vragen die de EK mee heeft gestuurd:

- Wat is de impact van de onderwerpen van thema 1 en thema 2 op de uitvoerbaarheid en handhaafbaarheid van de wetsvoorstellen?
- Is de deskundigheid en accountability bij de actoren die de wetsvoorstellen moeten uitvoeren en handhaven up-to-date?
- Welke overige problemen voorziet u in de uitvoerbaarheid en handhaafbaarheid van de wetsvoorstellen?

OM: beslissing tot inzet, melden kwetsbaarheid

-Wat is een zwaarwegend opsporingsbelang?
-Wat is het afwegingskader voor het melden van een onbekende kwetsbaarheid?
-Waarom kunt u niet meer uit de weg met bestaande opsporingsmiddelen?
-De bevoegdheden van de opsporing nemen toe om gelijke tred te houden met de digitalisering, zou privacy waarborgen niet moeten toenemen om gelijke tred te houden met de bevoegdheden van de opsporing?
-Welke toets of de grondrechten van verdachten zijn gewaarborgd is er wanneer een zaak niet voor de rechter komt?
-Hoe vindt toezicht plaats op uw werkwijze?
-Hoe verschaft u transparantie over uw werkwijze?
-Bent u klaar op dag 1 om te beginnen?

Vragen die de EK mee heeft gestuurd:
- Wat voegen deze wetsvoorstellen toe aan de al bestaande wet- en regelgeving?
- Wordt er al voldoende en effectief gebruikgemaakt van instrumentaria in de bestaande wet- en regelgeving, met voldoende deskundig personeel?
- Wat zijn de grenzen aan de noodzaak van de wetgeving, aangezien deze de grondrechten van burgers aantast? Hoe zwaarwegend is het belang?

NCSC: dreiging in het veld
-Wat zijn de meest prangende dreigingen?
-Worden kwetsbaarheden vanuit de industrie sowieso gepatchd? Zijn gebruikers accuraat in het updaten?
-zijn bekende kwetsbaarheden dan niet nog op grote schaal bruikbaar?
-Hoe beoordeelt u de noodzakelijkheid van voorgestelde bevoegdheden?
-Hoe groot is het risico voor onbekende kwetsbaarheden voor de veiligheid van het internet?
-moeten deze dan niet ten alle tijden zo snel mogelijk worden gedicht?
-Vindt u de opsporing voldoende uitgerust om de digitale dreigingen tegen te gaan?

Vragen die de EK mee heeft gestuurd:
- Wat voegen deze wetsvoorstellen toe aan de al bestaande wet- en regelgeving?
- Wordt er al voldoende en effectief gebruikgemaakt van instrumentaria in de bestaande wet- en regelgeving, met voldoende deskundig personeel?
- Wat zijn de grenzen aan de noodzaak van de wetgeving, aangezien deze de grondrechten van burgers aantast? Hoe zwaarwegend is het belang?

Ik ben uiteraard beschikbaar voor eventuele verdere vragen.

Met vriendelijke groet,

10.2.e
Beleidsadviseur

M 06 10.2.e
10.2.e @minvenj.nl

Van: Plas, Theo van der (T.G.)10.2.e @politie.nl>
Wanneer: 15 juni 2017 10:00:00 CEST
Vereist:10.2.e @politie.nl>,10.2.e @politie.nl>, 10.2.e @politie.nl>,10.2.e @politie.nl>, 10.2.e @politie.nl>
Onderwerp: Gezamenlijk Voorbereiding ronde tafel EK 20/6
Locatie: Driebergen, F6

Ik plan de ochtend in ivm de voorbereiding.

Van: 10.2.e
Verzonden: donderdag 15 juni 2017 10:55
Aan: Plas, Theo van der (T.G.); 10.2.e 10.2.e 10.2.e
Onderwerp: Aantekeningen ronde tafel

Pitch:

Algemene inleiding, daarna twee hoofdstukken. Een voor CCIII en een voor ANPR.

Politie maakt inbreuk.
Politie is voor encryptie en bescherming van de privacy, maar moet kunnen optreden als criminelen er misbruik van maken, om de veiligheid te waarborgen.
Hoogst mogelijke strafvorderlijke randvoorwaarden.
Andere waarborgen. Trits van middelen die we gebruiken van social media tot bekende en onbekende kwetsbaarheden. Andere waarborgen zoals functiescheiding, beveiliging data, WPG etc...

Uitvoerbaarheid en randvoorwaarden voor waarborgen privacy is belangrijkste lijn.
Afweging tussen veiligheid en privacy. Balans is nodig. Communicerende vaten.

Vragen de we verwachten:
Financiering
0 days
Heeft de politie voldoende Expertise
Hoeveel zaken
Is de politie er klaar voor, hoeveel zaken kan zij draaien.-is aan om, ultimum remedium. Gata dit in de toekomst

Maakt de politie het internet onveilig (dit is een belangrijk argument van Google en Microsoft)
Door achterhouden onbekende kwetsbaarheden. Vaak zijn het al bestande kwetsbaarheden. Op termijn ga je melden.
Software bedrijven maken slechte software met veel kwetsbaarheden vanwege economische belangen. Daar ligt de primaire verantwoordelijkheid.

De schending van de privacy van eenverdahcte is met deze methode veel kleiner dan bij ander middelen.

Wannacry voorbeeld, dat gaat hier ook gebeuren. Antwoord is dat wij meldingsplicht hebben. Dat is aan de officier/RC.
De exploit was al bekend en door Microsoft gepatineerd twee maanden voor Wannacry. Dus allen bedrijven en burgers die niet gepacteerd hebben zijn slachtoffer geworden.

Nog opsturen/ voorbereiden
Encryptiestandpunt
Onbekende kwetsbaarheden standpunt
Position Paper NCTV
Amendement -ultimum remedium

Rapport CTIVD- hebben we de genoemde waarborgen ingebouwd. verschil met dienst. Logging.

Besluit - wordt meegenomen inde reactie
Consultatiereactie concept van[9] hierop

Dossier minister met schema-voor welke feiten welke bevoegdheid.
Spreektekst

Voorbeelden van ontoegankelijk maken of overnemen![7-12]
Wat Inge heeft gezegd over of we dit al een keer hebben toegepast.

Standpunten van andere partijen.
KPN: binnendringen hoeft niet gelogd te worden. Iet openbaar maar wel controleerbaar door inspectie.

Opbouw van middelen voor binnendringen:[7-12] (hier ook proportionaliteit/ subsidiariteit.)
Politie moet over volledig pallet kunnen beschikken om haar taak uit te kunnen voeren.
Elke zaak is maatwerk.

Hoe zit het in België. Voorbeelden uit andere landen? Aantallen keren toegepast.
BKA mag in hele beperkte gevallen, veiligheid tegen de staat, terrorisme.
UK?

Kunnen we een botnet platleggen.[7-12].

Rechtsmacht in het buitenland. Je kunt starten maar[7-12]

[7-12] **is geen alternatief voor dit wetsvoorstel**
[7-12]

Van: 10.2.e
Verzonden: donderdag 15 juni 2017 11:42
Aan: Plas, Theo van der (T.G.); 10.2.e 10.2.e 10.2.e 10.2.e 10.2.e
Onderwerp: Antw: Gezamenlijk Voorbereiding ronde tafel EK 20/6

Inleidende tekst voorstel

De samenleving verandert. De grenzen van de stad en het land begrenzen de criminaliteit niet meer. De grenzen van de fysieke wereld begrenzen de criminaliteit evenmin. De bevoegdheden van de politie dienen aan te sluiten op deze verandering, zodat zij haar taak, de daadwerkelijke handhaving van de rechtsorde, kan waarmaken. De wet computercriminaliteit 3 geeft ons die mogelijkheden in de virtuele wereld. De 28 dagen database ANPR versterkt onze mogelijkheden op criminaliteit met een mobiel karakter.

Aanvullende vraag
Waar gaat de privacydiscussie elkaar raken?

Waarborgen benoemen

Stukken tbv ANPR even bij elkaar aanleveren:
Wetsvoorstel
AmvB
Beantwoording kamervragen
Ijsselland arrest
Position paper.
Kamervragen

Met vriendelijke groet

10.2.e

Zakelijk: 06 10.2.e
Privé : 06- 10.2.e

Van: 10.2.e
Verzonden: donderdag 15 juni 2017 13:39
Aan: Plas, Theo van der (T.G.); 10.2.e 10.2.e ; 10.2.e
Onderwerp: Brief kwetsbaarheden en encryptie
Bijlagen: tk-kwetsbaarheden-in-hardware-en-software.pdf; Kabinetsstandpunt_encryptie.pdf

Beste Theo,

Bijgaand de brief over kwetsbaarheden en de brief over encryptie als achtergrondinformatie.

Groet,
10.2.e

Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de
Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

Directoraat-Generaal Rechtspleging en Rechtshandhaving
DRC / C&V

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/venj

Ons kenmerk
2008352

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

Datum 8 november 2016
Onderwerp Kwetsbaarheden in hardware en software

De afgelopen jaren is het parlement enkele keren geïnformeerd over het gebruik van kwetsbaarheden in hardware en software door de overheid.[1] In het algemeen overleg cyber security op 20 januari jl. heeft de Staatssecretaris van Veiligheid en Justitie naar aanleiding van een vraag van het lid Verhoeven (D66) toegezegd een brief te sturen over het gebruik van onbekende kwetsbaarheden in hardware en software. Naar aanleiding van die toezegging sturen wij u deze brief.

De samenleving digitaliseert en de afhankelijkheid van het internet groeit. Dat biedt grote maatschappelijke en economische voordelen. Tegelijk zijn er zorgen over de mogelijkheid voor bedrijven, burgers en de overheid om op een veilige manier gebruik te kunnen blijven maken van het internet. Veilige computersystemen zijn daarvoor een voorwaarde, en voor het vertrouwen daarin is het van belang het aantal kwetsbaarheden in computersystemen te verminderen. Tegelijk is het voor de veiligheid, zowel fysiek als in de digitale wereld, van belang dat de daders van criminaliteit, terrorisme en spionage worden aangepakt. Daarvoor is het noodzakelijk dat de overheid onderzoek doet in computersystemen, onder meer via het internet. In het streven naar een open, vrij en veilig internet dient aan de diverse belangen recht te worden gedaan. Deze belangen zijn in de meeste gevallen met elkaar in overeenstemming, maar het komt ook voor dat een belangenafweging noodzakelijk is, bijvoorbeeld tussen veiligheid en vrijheden, of tussen verschillende veiligheidsbelangen. Het kabinet

[1] Eerste Kamer, vergaderjaar 2014–2015, CVIII, N
Eerste Kamer, vergaderjaar 2014–2015, CVIII, O
Eerste Kamer, vergaderjaar 2014–2015, CVIII, G
Antwoorden van de Staatssecretaris van Veiligheid & Justitie op Kamervragen van het lid Oosenbrug (PvdA), 3 juli 2015, aanhangsel ah-tk-201420152773
Antwoorden van de Staatssecretaris van Veiligheid & Justitie op Kamervragen van de leden Verhoeven en Hachci (beiden D66), 3 juli 2015, aanhangsel ah-tk-201420152772

Directoraat-Generaal Rechtspleging en Rechtshandhaving
DRC / C&V

Datum
8 november 2016

Ons kenmerk
2008352

hecht dan aan een zorgvuldige afweging die per geval wordt gemaakt. Deze brief behandelt eerst het bestaan van bekende en onbekende kwetsbaarheden en het verhelpen daarvan. Vervolgens wordt de relatie met nationale veiligheid en de opsporing van strafbare feiten behandeld, met bijzondere aandacht voor de bevoegdheid tot binnendringen in geautomatiseerd werk en de daarbij behorende voorwaarden en waarborgen. Tot slot wordt aandacht besteed aan de internationale markt voor kennis over kwetsbaarheden.

Bekende en onbekende 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" 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".

Het bestaan, de ontdekking en het verhelpen van kwetsbaarheden
Kwetsbaarheden ontstaan bij het produceren van hard- en software, bijvoorbeeld door programmeerfouten of door beperkte aandacht voor veiligheid bij het ontwerp. Hard- en software worden vaak vanwege concurrentieoverwegingen snel op de markt gebracht. Bovendien zijn de omvang en complexiteit van software fors toegenomen. Veel gebruikte applicaties hebben tegenwoordig tientallen miljoenen regels broncode. Kwetsbaarheden zijn daarom talloos en wijdverbreid.

De risico's van specifieke kwetsbaarheden kunnen sterk verschillen. Bij de fabrikant onbekende kwetsbaarheden en het gebruik daarvan krijgen vaak de meeste aandacht in de media, bijvoorbeeld als het software betreft die zeer veel wordt gebruikt. In andere gevallen betreft het zeer specifieke systemen en zijn de kwetsbaarheden vaak lastig te gebruiken. In dergelijke gevallen brengen de kwetsbaarheden vaak minder maatschappelijke risico's met zich mee. Ook reeds bekende kwetsbaarheden kunnen grote risico's met zich mee brengen. Deze zijn vaak bij een grotere groep mensen bekend en kunnen door personen met kwade bedoelingen gemakkelijker worden opgezocht en ingezet.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
DRC / C&V

Datum
8 november 2016

Ons kenmerk
2008352

Veel kwetsbaarheden worden snel nadat ze worden ontdekt gemeld bij de fabrikant. Steeds vaker stimuleren fabrikanten het melden van kwetsbaarheden door het bieden van financiële vergoedingen. Tevens maken veel fabrikanten regelmatig een nieuwe versie of update van hun product, waarmee de op dat moment bekende kwetsbaarheden worden verholpen. Soms duurt het echter lang voordat een fabrikant een update beschikbaar stelt, en soms gebeurt dat in het geheel niet. Het beschikbaar stellen van updates om kwetsbaarheden weg te nemen, is niet verplicht en kan veel tijd en kosten met zich mee brengen. Daarnaast blijken veel eindgebruikers niet of niet direct alle voor hen beschikbare updates te installeren, of ze doen dit niet op de juiste manier. Het gevolg is dat vele systemen niet alleen onbekende kwetsbaarheden bevatten, maar ook kwetsbaarheden die reeds langer bij de fabrikant bekend zijn.

De overheid stimuleert het melden van kwetsbaarheden, onder meer met het beleid voor *responsible disclosure*. Naast voorlichting aan haar partners over door derden gemelde kwetsbaarheden zal het Nationaal Cyber Security Centrum van het Ministerie van Veiligheid en Justitie (NCSC) in voorkomende gevallen ontdekte kwetsbaarheden zelf melden aan de fabrikant. Ook heeft het kabinet het wetsvoorstel Gegevensverwerking en meldplicht cyber security aan het parlement gestuurd. Dit voorstel bevat een meldplicht voor inbreuken op de veiligheid of een verlies van integriteit van elektronische informatiesystemen bij vitale sectoren.

De nationale veiligheid en de opsporing van strafbare feiten
Criminelen, terroristen en buitenlandse inlichtingendiensten en krijgsmachten maken voor hun activiteiten steeds vaker gebruik van het internet. Die activiteiten zijn zonder onderzoek te doen in het digitale domein steeds lastiger te onderkennen of te bewijzen. Voor een effectieve opsporing, het tegengaan van spionage, verstoring en sabotage, en het waarborgen van de nationale veiligheid is onderzoek in het digitale domein noodzakelijk. Daarvoor zijn in de wet verschillende bevoegdheden opgenomen voor de daarmee belaste diensten. Voorbeelden uit de opsporing zijn het vorderen van gegevens en het onderzoek aan een geautomatiseerd werk tijdens een doorzoeking of na inbeslagname. Dergelijke bevoegdheden zijn voor de inlichtingen- en veiligheidsdiensten vastgelegd in de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) en voor de opsporing in het Wetboek van Strafvordering (WvSv). De Wiv 2002 bevat de bevoegdheid tot binnendringen in een geautomatiseerd werk voor de AIVD en de MIVD ten behoeve van de nationale veiligheid. Het wetsvoorstel Computercriminaliteit III bevat wijzigingen in het WvSv voor een bevoegdheid tot

Directoraat-Generaal Rechtspleging en Rechtshandhaving
DRC / C&V

Datum
8 november 2016

Ons kenmerk
2008352

binnendringen in geautomatiseerd werk voor vooraf bepaalde opsporingsdoeleinden, voorzien van specifieke voorwaarden en waarborgen.

Technische mogelijkheden
Er zijn verschillende technieken beschikbaar die het binnendringen in een geautomatiseerd werk mogelijk maken. Er zijn vele soorten geautomatiseerde werken en de beveiliging ervan kan vele vormen hebben. Bij de keuze van een methode om het werk binnen te dringen zijn, naast noodzaak, proportionaliteit en subsidiariteit, aspecten als de effectiviteit van de inzet, de kans op onderkenning en het risico op gevolgschade van belang. Of het gebruik van een kwetsbaarheid de meest aangewezen methode is, wordt per geval bepaald.

De inzet van wettelijke bevoegdheden voor de nationale veiligheid
Om een zorgvuldige afweging te kunnen maken over de inzet van de genoemde bevoegdheden, is elke bevoegdheid in de desbetreffende wet van specifieke voorwaarden en waarborgen voorzien. Dat geldt ook voor de bevoegdheid tot binnendringen in een geautomatiseerd werk in de Wiv 2002. De bevoegdheid mag alleen worden ingezet in het kader van de nationale veiligheid. De inzet van deze bevoegdheid wordt altijd getoetst aan de eisen van noodzaak, proportionaliteit en subsidiariteit. De inzet moet proportioneel zijn ten opzichte van het doel en het potentiele risico op onbedoelde effecten. Bovendien is de inzet alleen geoorloofd als niet met een minder ingrijpend middel hetzelfde doel kan worden bereikt. De bevoegdheid mag alleen worden ingezet indien vooraf toestemming is verleend door de Minister van Binnenlandse Zaken en Koninkrijksrelaties voor de AIVD of de Minister van Defensie voor de MIVD. Daarnaast ziet de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) toe op de rechtmatigheid van de taakuitvoering van de AIVD en de MIVD. Met het komende voorstel voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten beoogt de regering de waarborgen betreffende de inzet van deze bijzondere bevoegdheid verder te versterken.

Op 16 december 2014 heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties mede namens de Minister van Defensie het parlement geïnformeerd over de omgang met kwetsbaarheden op internet door de AIVD en de MIVD.[2] De diensten kunnen bij de inzet van bijzondere bevoegdheden kwetsbaarheden in de digitale beveiliging van een target onderkennen en gebruiken. Indien de AIVD of de MIVD in het kader van hun wettelijke

[2] kenmerk 2014Z23370 en Eerste Kamer, vergaderjaar 2014–2015, CVIII, G

Directoraat-Generaal Rechtspleging en Rechtshandhaving
DRC / C&V

Datum
8 november 2016

Ons kenmerk
2008352

taakuitvoering stuiten op een kwetsbaarheid die de belangen van gebruikers van het internet kan schaden, zullen deze diensten belangendragers informeren. Veelal zal het de fabrikant van de hardware of software betreffen en/of een specifieke groep gebruikers die een groot risico loopt.

Er kunnen echter wettelijke bepalingen (de wettelijke plicht tot het beschermen van bronnen, actueel kennisniveau) of operationele redenen zijn die het melden van kwetsbaarheden (tijdelijk) in de weg staan. In dergelijke gevallen wordt het belang van informatieverstrekking afgewogen tegen het belang van geheimhouding en bronbescherming. Voorbeelden van situaties waarin het belang van het melden van een bij de fabrikant onbekende kwetsbaarheid mogelijk niet opweegt tegen andere zwaarwegende belangen zijn de inzet in een gewapend conflict, zwaarwegende belangen voor de nationale veiligheid of als de kennis van een kwetsbaarheid onder voorwaarde van geheimhouding met de Nederlandse overheid is gedeeld. Geconstateerde kwetsbaarheden hoeven niet noodzakelijkerwijs betrekking te hebben op een groot deel van de gebruikers van het internet. Sommige kwetsbaarheden betreffen zeer specifieke systemen. Als het zwaarwegend belang tijdelijk van aard is, dan zal de kwetsbaarheid daarna alsnog worden gemeld.

De inzet van wettelijke bevoegdheden voor de opsporing van strafbare feiten
In het wetsvoorstel Computercriminaliteit III is de inzet in het kader van de opsporing alleen mogelijk voor een beperkt aantal ernstige strafbare 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 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

Directoraat-Generaal Rechtspleging en Rechtshandhaving
DRC / C&V

Datum
8 november 2016

Ons kenmerk
2008352

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.

De internationale markt voor kennis over kwetsbaarheden
Op internet kan kennis over kwetsbaarheden in hardware en software worden gekocht. Het opdoen van kennis over kwetsbaarheden en de verkoop hiervan is niet verboden. Het beperken van onderzoek naar kwetsbaarheden wordt niet wenselijk geacht. Fabrikanten stimuleren steeds vaker het melden van kwetsbaarheden door het bieden van financiële vergoedingen. Dergelijke kennis kan bijdragen aan de veiligheid van systemen en van het gebruik ervan.

Gezien de mogelijkheden om kennis over kwetsbaarheden voor ongewenste doeleinden in te zetten, is de verkoop ervan aan bepaalde partijen onwenselijk. De mogelijkheid tot anonimiteit op het internet maakt het echter gemakkelijk om heimelijk kennis over kwetsbaarheden aan te bieden en aan te schaffen, waardoor het lastig is deze markt aan controle te onderwerpen. Wel is de verkoop van zogenaamde *intrusion software* die gebruik maakt van kwetsbaarheden in bepaalde omstandigheden onderhevig aan exportcontrole. Zoals gemeld in de antwoorden op vragen van de leden Oosenbrug (PvdA) en Verhoeven (D66) van 28 augustus 2015 hecht de regering aan beperking van de uitvoer van ICT-goederen en -software naar regimes met een slechte staat van dienst op het gebied van mensenrechten.[3] De Europese Commissie heeft inmiddels een voorstel gedaan voor herziening van de dual use-verordening waarmee het toezicht op de internationale handel in goederen voor tweeërlei gebruik (dual use) wordt geregeld.

Conclusie
Het kabinet bevordert een vrij, open en veilig internet. Het beperken van kwetsbaarheden in hardware en software is daarvoor van belang. De overheid bevordert het melden van kwetsbaarheden, onder meer met het beleid voor

[3] Antwoorden van de Staatssecretaris van Veiligheid & Justitie op Kamervragen van de leden Oosenbrug (PvdA) en Verhoeven (D66), 28 augustus 2015, aanhangsel ah-tk-201420153199

Directoraat-Generaal Rechtspleging en Rechtshandhaving
DRC / C&V

Datum
8 november 2016

Ons kenmerk
2008352

responsible disclosure. Het kabinet heeft tegelijk tot taak om binnen de wettelijke kaders de nationale veiligheid te waarborgen en strafbare feiten op te sporen, in de digitale en in de fysieke wereld. Daarvoor is toegang tot digitale informatie noodzakelijk, waarbij in bepaalde gevallen kan worden gekozen voor het binnendringen in een geautomatiseerd werk. Het gebruik van kwetsbaarheden is daarbij één van de technische mogelijkheden om de bevoegdheid tot binnendringen uit te voeren. Deze bevoegdheid is alleen onder strenge, bij wet bepaalde voorwaarden toegestaan en is met specifieke waarborgen omkleed. De noodzaak, proportionaliteit en de subsidiariteit zijn leidend bij de afweging tot inzet. De waarborgen verzekeren een zorgvuldige afweging van de betrokken belangen.

De Staatssecretaris van Veiligheid en Justitie,

K.H.D.M. Dijkhoff

De Minister van Binnenlandse Zaken en Koninkrijksrelaties

R.H.A. Plasterk

De Minister van Defensie

J.A. Hennis-Plasschaert

Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 383

BRIEF VAN DE MINISTERS VAN VEILIGHEID EN JUSTITIE EN VAN ECONOMISCHE ZAKEN

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 4 januari 2016

Kabinetsstandpunt Encryptie

Hierbij sturen wij u het kabinetsstandpunt toe over encryptie. Hiermee wordt tegemoet gekomen aan de gedane toezeggingen tijdens het AO Telecomraad van 10 juni 2015 (Kamerstuk 21 501-33, nr. 552) en AO JBZ-Raad van 7 oktober 2015 (Kamerstuk 32 317, nr. 357).

Inleiding

Encryptie, ook wel versleuteling, is in toenemende mate eenvoudig te verkrijgen en gebruiken en maakt daarmee steeds vaker onderdeel uit van het reguliere dataverkeer. Door de overheid, bedrijven en burgers wordt encryptie steeds meer toegepast om de vertrouwelijkheid en integriteit van hun communicatie en opgeslagen data te beschermen. Dat is belangrijk voor het vertrouwen van mensen in digitale producten en diensten en voor de Nederlandse economie in het licht van de zich snel ontwikkelende digitale maatschappij. Tegelijkertijd vormt encryptie een belemmering voor het verkrijgen van informatie die noodzakelijk is voor opsporings-, inlichtingen- en veiligheidsdiensten wanneer kwaadwillenden (zoals criminelen en terroristen) hiervan gebruikmaken. De recente aanslagen in Parijs, waarbij mogelijk gebruik is gemaakt van versleuteling van de communicatie door de terroristen, leiden tot de gerechtvaardigde vraag wat er nodig is om opsporings-, inlichtingen- en veiligheidsdiensten goed zicht te bieden en laten houden op aanslagplanning.

De in de vorige alinea beschreven tweeledigheid was eveneens te horen in het publieke debat van de afgelopen maanden over de dilemma's rondom het gebruik van encryptie. Ook uw Kamer heeft over dit onderwerp gesproken. Tijdens het AO Telecomraad is gevraagd wat het Kabinet gaat doen aan het stimuleren van sterke encryptie. Daarnaast is vanuit de Tweede Kamer gevraagd om te komen met een kabinetsstandpunt rond encryptie.

kst-26643-383
ISSN 0921 - 7371
's-Gravenhage 2016

Hierna wordt ingegaan op het belang van encryptie voor de systeem- en informatiebeveiliging van de overheid en bedrijven, en voor de grondwettelijke bescherming van de persoonlijke levenssfeer en het communicatiegeheim. Daarnaast wordt het belang van opsporing van ernstige misdrijven en bescherming van de nationale veiligheid geschetst. Tot slot wordt na weging van de belangen gekomen tot een conclusie.

De Nederlandse situatie kan hierbij niet los worden gezien van de internationale context. Sterke encryptiesoftware is in toenemende mate wereldwijd beschikbaar of al geïntegreerd in producten of diensten. Gelet op de brede beschikbaarheid en toepassing van geavanceerde encryptietechnieken en het grensoverschrijdende karakter van het dataverkeer is het handelingsperspectief op nationaal niveau beperkt.

Belang van encryptie voor de overheid, bedrijven en burgers

Cryptografie speelt een sleutelrol in de technische beveiliging in het digitale domein. Veel cybersecuritymaatregelen in organisaties leunen sterk op de toepassing van encryptie. De veilige opslag van wachtwoorden, het beschermen van laptops tegen verlies of diefstal en het veilig bewaren van backups zijn moeilijker zonder het gebruik van encryptie. Het afschermen van gegevens die verstuurd worden via internet, bij internetbankieren bijvoorbeeld, is alleen mogelijk met behulp van encryptie. Door de verbondenheid van systemen, wereldwijde vertakkingen en verschillende routes die communicatie kan afleggen, is het risico op onderschepping, inbreuk, inzage of wijziging van informatie en communicatie altijd aanwezig.

De overheid communiceert in toenemende mate digitaal met de burgers en verleent diensten waarbij vertrouwelijke gegevens worden uitgewisseld, zoals het gebruik van DigiD of het doen van belastingaangifte. Zoals in het Regeerakkoord is geformuleerd moeten vanaf 2017 burgers en bedrijven hun overheidszaken volledig digitaal kunnen regelen. De overheid heeft hierbij de plicht om te zorgen dat deze gegevens tegen kennisneming door derden zijn beveiligd; encryptie is hiervoor onontbeerlijk. Ook de bescherming van de communicatie binnen de overheid is van encryptie afhankelijk zoals bij de beveiliging van diplomatiek berichtenverkeer en militaire communicatie.

Voor bedrijven is encryptie essentieel om bedrijfsinformatie veilig te kunnen bewaren en versturen. Het kunnen gebruiken van encryptie versterkt de internationale concurrentiepositie van Nederland en draagt bij aan een aantrekkelijk vestigings- en innovatieklimaat voor onder andere startups, datacentra en cloudcomputing. Vertrouwen in veilige communicatie en opslag van data is essentieel voor de (toekomstige) groeipotentie van de Nederlandse economie, die vooral zit in de digitale economie.

Encryptie ondersteunt de eerbiediging van de persoonlijke levenssfeer en het communicatiegeheim van burgers doordat het hen een middel biedt om de vertrouwelijkheid en integriteit van persoonsgegevens en communicatie te beschermen. Dit is ook belangrijk voor de uitoefening van de vrijheid van meningsuiting. Het stelt bijvoorbeeld burgers, maar ook beroepen met een belangrijke democratische functie zoals journalisten, in staat om vertrouwelijk te communiceren.

Encryptie stelt derhalve alle betrokkenen in staat de vertrouwelijkheid en integriteit van communicatie te waarborgen en zich beter te weren tegen bijvoorbeeld spionage en cybercriminaliteit. Hierbij zijn fundamentele rechten en vrijheden, veiligheids- en economische belangen gebaat.

Encryptie en de opsporings-, inlichtingen- en veiligheidsdiensten

De bevoegdheden en middelen die de diensten tot hun beschikking hebben, moeten toegerust zijn op de huidige en toekomstige digitale realiteit. Met effectieve, rechtmatige toegang tot gegevens bevorderen de opsporings-, inlichtingen- en veiligheidsdiensten de veiligheid van de digitale en de fysieke wereld. Encryptie vormt waar het toegepast wordt door kwaadwillenden een belemmering voor de opsporings-, inlichtingen- en veiligheidsdiensten bij de toegang tot die gegevens. Zij ervaren deze belemmeringen bijvoorbeeld wanneer zij onderzoek doen naar de verspreiding en opslag van kinderporno, bij de ondersteuning van militaire missies in het buitenland, het tegengaan van cyberaanvallen of wanneer zij zicht willen krijgen en houden op het voorbereiden van aanslagen door terroristen. Criminelen, terroristen en tegenstanders in gewapende conflicten zijn zich er vaak van bewust dat zij op enig moment de aandacht van de diensten kunnen trekken en hebben tegenwoordig eveneens beschikking over geavanceerde encryptiemethoden die lastig te omzeilen of doorbreken zijn. Het gebruik van dergelijke methoden vereist weinig technische kennis, aangezien encryptie vaak integraal deel uitmaakt van de internetdiensten waarvan ook zij gebruik kunnen maken. Dat bemoeilijkt, vertraagt, of maakt het onmogelijk om (tijdig) inzicht te verkrijgen in de communicatie ten behoeve van de bescherming van de nationale veiligheid en de opsporing van strafbare feiten. Tevens kan het onderzoek ter zitting en de bewijsvoering voor een veroordeling ernstig worden gehinderd.

Het recht op eerbiediging van de persoonlijke levenssfeer en het communicatiegeheim van burgers

Het toepassen van encryptie helpt burgers zoals eerder werd opgemerkt, bij het borgen van de persoonlijke levenssfeer en de vertrouwelijkheid van hun communicatie. De hierboven genoemde rechtmatige toegang tot gegevens en communicatie door opsporings-, inlichtingen- en veiligheidsdiensten vormt evenwel een inbreuk op de vertrouwelijke communicatie van burgers.

Vertrouwelijkheid van communicatie raakt aan de grondwettelijk geregelde eerbiediging van de persoonlijke levenssfeer en aan het recht op bescherming van het brief-, telefoon- en telegraafgeheim (hierna: «het communicatiegeheim»). Deze grondrechten zijn verankerd in respectievelijk artikel 10 en artikel 13 Grondwet. Daarnaast zijn deze fundamentele rechten vastgelegd in artikel 8 EVRM en artikel 7 en artikel 8 EU-Handvest (voor zover Unierecht wordt geraakt).

De bescherming van grondrechten is van toepassing op de digitale wereld. De hiervoor genoemde grondrechtelijke- en internationaalrechtelijke bepalingen bieden samen het kader om onwettige inbreuken tegen te gaan. De genoemde rechten zijn niet absoluut, hetgeen inhoudt dat beperkingen zijn toegestaan voor zover deze voldoen aan de vereisten die de Grondwet en het EVRM (en voor zover het Unierecht betreft, het EU-Handvest) stellen. Een inbreuk is toelaatbaar wanneer deze een legitiem doel dient, bij wet is geregeld en de beperking voorzienbaar en kenbaar is. Daarnaast dient de beperking noodzakelijk te zijn in een democratische samenleving. Tot slot dient de inbreuk proportioneel te zijn, dat wil zeggen dat het door de overheid nagestreefde doel proportioneel dient te zijn in relatie tot de inbreuk op de persoonlijke levenssfeer en/of het communicatiegeheim.

Deze vereisten bieden het kader waarbinnen de afweging gemaakt kan worden tussen de bij encryptie in het geding zijnde belangen, zoals het

recht op de persoonlijke levenssfeer en het communicatiegeheim, de openbare en nationale veiligheid en het voorkomen van strafbare feiten. Voorgaand afwegingskader is voor zover het de bijzondere bevoegdheden van de inlichtingen- en veiligheidsdiensten betreft overigens ook neergelegd in de Wet op de inlichtingen- en veiligheidsdiensten 2002 (artikelen 18 en 31 van de Wiv 2002). De medewerkingsverplichtingen inzake decryptie die zijn opgenomen in de Wiv (artikelen 24, derde lid en 25, zevende lid van de Wiv 2002) en in het WvSv (artikel 126m, zesde lid, van het WvSv), kunnen worden ingeroepen indien de daaraan gekoppelde bijzondere bevoegdheden na een afweging in voormelde zin worden uitgeoefend.

Afweging en conclusie

Het breken van de versleuteling is tegenwoordig in steeds minder gevallen mogelijk. Daarnaast is de mogelijkheid om gegevens in onversleutelde vorm te vorderen bij een dienstverlener, minder vaak beschikbaar. In toenemende mate worden bij moderne toepassingen van encryptie de gegevens nog slechts in versleutelde vorm door dienstverleners verwerkt. Gelet op het belang van de opsporing en vervolging van strafbare feiten en de belangen die zijn gemoeid met de nationale veiligheid, nopen deze ontwikkelingen tot het zoeken naar nieuwe oplossingen.

Op dit moment is er geen zicht op mogelijkheden om in algemene zin, bijvoorbeeld via standaarden, encryptie producten te verzwakken zonder daarmee de veiligheid van digitale systemen die van encryptie gebruik maken te compromitteren. Door bijvoorbeeld een technische ingang in een encryptie product te introduceren die het voor opsporingsinstanties mogelijk zou maken versleutelde bestanden in te zien, kunnen digitale systemen kwetsbaar worden voor bijvoorbeeld criminelen, terroristen en buitenlandse inlichtingendiensten. Dit zou onwenselijke gevolgen hebben voor de beveiliging van gecommuniceerde en opgeslagen informatie, en de integriteit van ICT-systemen, die in toenemende mate van belang zijn voor het functioneren van de samenleving.

Bij de uitvoering van hun wettelijke taken zijn de opsporings-, inlichtingen- en veiligheidsdiensten deels afhankelijk van samenwerking met aanbieders van ICT-producten en -diensten. Gegeven deze afhankelijkheid, is overleg nodig met aanbieders over effectieve gegevensverstrekking bij gebruik van hun diensten door kwaadwillenden, met inachtneming van ieders rol en verantwoordelijkheden en de wettelijke kaders.

Gegeven de voorgaande afweging komen we tot de volgende conclusie:

Het kabinet heeft tot taak de veiligheid van Nederland te waarborgen en strafbare feiten op te sporen. Het kabinet onderstreept hierbij de noodzaak tot rechtmatige toegang tot gegevens en communicatie. Daarnaast zijn overheden, bedrijven en burgers gebaat bij maximale veiligheid van de digitale systemen. Het kabinet onderschrijft het belang van sterke encryptie voor de veiligheid op internet, ter ondersteuning van de bescherming van de persoonlijke levenssfeer van burgers, voor vertrouwelijke communicatie van overheid en bedrijven, en voor de Nederlandse economie.

Derhalve is het kabinet van mening dat het op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland. In de internationale context zal Nederland deze conclusie en

de afwegingen die daaraan ten grondslag liggen uitdragen. Ten aanzien van het stimuleren van sterke encryptie zal de Minister van Economische Zaken opvolging geven aan de strekking van het amendement (Kamerstuk 34 300 XIII, nr.10) op de begroting van het Ministerie van Economische Zaken.

De Minister van Veiligheid en Justitie,
G.A. van der Steur

De Minister van Economische Zaken,
H.G.J. Kamp

Van: 10.2.e
Verzonden: donderdag 15 juni 2017 13:45
Aan: Plas, Theo van der (T.G.); 10.2.e 10.2.e 10.2.e 10.2.e
Onderwerp: 'Eerste Kamer moet wetsvoorstel over hacken door politie opschorten' | Artikel gedeeld via FD.nl
Bijlagen: HFD_20170615_0_011_019.pdf

De discussie is geopend… Dit is een van de deelnemers aan de hoorzitting as dinsdag…

Groet,
10.2.e

Ik las dit artikel via https://fd.nl en wil het graag met u delen:
https://fd.nl/opinie/1205740/eerste-kamer-moet-wetsvoorstel-over-hacken-door-politie-opschorten

Eerste Kamer moet wetsvoorstel over hacken door politie opschorten

Hacken verenigt telefoontap, huiszoeking en heimelijke observatie in één digitale variant

ILLUSTRATIE: HEIN DE KORT VOOR HET FINANCIEELE DAGBLAD

Axel Arnbak

Zonder specifieke wettelijke bevoegdheid hacken Nederlandse opsporingsdiensten computers in binnen- en buitenland. In ieder geval sinds het Bredolab-incident in 2010. Even lang al probeert het ministerie van Veiligheid en Justitie een wet langs de Staten-Generaal te loodsen die deze inzet van overheidsdwang moet legaliseren. Iedereen vindt dat internetcriminaliteit moet kunnen worden aangepakt en toch stuit de voorgestelde hackbevoegdheid al jaren op stevige kritiek uit alle hoeken van de samenleving.

Tot veler frustratie hielp coalitiepartner PvdA eind 2016, vlak voor de verkiezingen, de VVD alsnog aan een meerderheid in de Tweede Kamer voor de hackwet. Nu moet de Eerste Kamer constitutionele chocola maken van de controversiële wet. Juist de senaat, de grondrechtenwaakhond van ons staatsbestel, moet het hoofd koel houden en de hackbevoegdheid pas goedkeuren als het kabinet de talloze onbeantwoorde vragen en aanzienlijke bezwaren wegneemt.

Op het eerste gezicht klinkt het logisch de politie een hackbevoegdheid toe te kennen, vooral gelet op soms geavanceerde en vaak weerzinwekkende vormen van cybercrime. Maar de hackbevoegdheid is een ongekend verregaande vorm van overheidsdwang. Hacken verenigt namelijk de telefoontap, huiszoeking, heimelijke observatie, infiltrant en zo'n beetje het hele analoge arsenaal van de politie in één digitale equivalent. Politiek en samenleving debatteren dus scherp over de impact op individuele privacy, collectieve cybersecurity en geopolitieke verhoudingen.

De principiële privacybezwaren zijn evident en het kabinet deed hier en daar al wat water bij de wijn. Toch blijft het universele karakter van de hackwet problematisch voor het parlementaire debat. Want hoe verhoudt de hackwet zich tot haar fysieke evenknieën? En is het, in lijn met de voorstellen van de Tilburgse hoogleraar Bert-Jaap Koops, niet tijd voor een nieuw digitaal huisrecht voor computersystemen en clouds, waarin administratie, brieven en fotoboeken handig bij elkaar staan opgeslagen? Eén hack kan alle digitale kroonjuwelen ineens prijsgeven.

Het Wetboek van Strafvordering heeft zich in twee eeuwen ontwikkeld tot een elegante catalogus, waarbij per dwangmiddel de privacyschending en waarborgen genuanceerd zijn afgewogen. Voor zulke vragen heeft de Eerste Kamer onvoldoende tijd. Rechters, die de inzet van hacken in individuele gevallen vooraf moeten goedkeuren, klagen terecht dat het aan tijd en budget ontbreekt om die taak te vervullen. De Raad voor de Rechtspraak pleit dan ook voor een nieuw toezichtsorgaan dat de inzet van de hackbevoegdheid naast individueel ook integraal toetst.

Politie heeft met een hackwet belang bij kwetsbare ICT-systemen

De impact van de hackwet op cybersecurity is zowel fascinerend als zorgelijk. De samenleving kan niet zonder veilige ICT, maar de politie heeft met een hackwet belang bij kwetsbare systemen. De Amerikaanse overheid ligt op dit gebied al jaren in de clinch met Apple en WhatsApp, omdat de iPhone en de app de cybersecurity van burgers 'te goed' beschermen. Inmiddels kun je als hacker meer dan $ 1 mln verdienen door een nog onbekende kwetsbaarheid in het besturingssysteem van de iPhone te ontdekken en te verkopen aan digitale wapenhandelaren. Zij maken vervolgens peperdure hackingtools voor onze politie. Zo stimuleert de hackwet een cultuur van onveiligheid.

De geopolitieke dimensie is nog ingewikkelder. Net als analoge wapenhandelaren leveren digitale collega's hun waar vaak aan onfrisse regimes. Zo publiceerde WikiLeaks al in 2014 dat de Nederlandse politie dezelfde FinFisher-spyware heeft ingekocht als kwade regimes in Bahrein, Pakistan en Oeganda. De hackwet verbiedt het inkopen van kwetsbaarheden, maar zegt niets over zakendoen met kwestieuze wapenhandelaren. Daarnaast bevat de hackwet geen verbod op hacken over de grens. Behalve als een schending van soevereiniteit, zien China, Rusland en Iran de hackwet ook als uitnodiging hier te komen hacken. Activisten en R&D-intensieve bedrijven zijn daar niet bepaald blij mee.

De Eerste Kamer heeft dus nog een stevig debat over de wenselijkheid en de uitvoerbaarheid van de hackwet te voeren. In de Tweede Kamer kon de wet nog overleven dankzij politieke opportuniteit. De Eerste Kamer doet er goed aan de hackwet op te schorten, totdat de essentiële vragen en aanzienlijke bezwaren zijn geadresseerd.

Axel Arnbak is advocaat bij De Brauw Blackstone Westbroek en onderzoeker aan het Instituut voor Informatierecht (UvA). Reacties: @axelarnbak. Dit artikel is een verkorte bewerking van een lezing in de Eerste Kamer tijdens de 'Deskundigenbijeenkomst privacy' op 20 juni a.s.

Van: 10.2.e
Verzonden: donderdag 15 juni 2017 13:55
Aan: Plas, Theo van der (T.G.); 10.2.e 10.2.e 10.2.e PMM)
Onderwerp: Motie Recourt over gebruik kwetsbaarheden/software
Bijlagen: tten_door_opsporingsinstanties_van_onbekende_kwetsbaarheden_of_software_die_daarvan_gebruikmaakt.pdf

We hadden het even over ultimum remedium.

In deze motie wordt aangegeven dat onbekende kwetsbaarheden of software alleen in uiterste gevallen mag worden gebruikt. Geen gebruik van ultimum remedium dus in de stukken… Ook niet voor de inzet van de binnendring bevoegdheid.

Groet,
10.2.e

Tweede Kamer der Staten-Generaal

0701 2

Vergaderjaar 2016–2017

34 372 Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)

Nr. 23 **MOTIE VAN HET LID RECOURT**

Voorgesteld 13 december 2016

De Kamer,

gehoord de beraadslaging,

constaterende dat op grond van het voorliggend wetsvoorstel opsporingsinstanties gebruik mogen maken van kwetsbaarheden in geautomatiseerde werken;

van mening dat de overheid de veiligheid en integriteit van geautomatiseerde werken moet stimuleren, zoals door het bevorderen van responsible disclosure en door het stimuleren van derden om op uitnodiging van soft- of hardwarefabrikanten te zoeken naar kwetsbaarheden;

verzoekt de regering, te bewerkstelligen dat opsporingsinstanties onbekende kwetsbaarheden of software die daarvan gebruikmaakt alleen in het uiterste geval zullen inzetten,

en gaat over tot de orde van de dag.

Recourt

kst-34372-23
ISSN 0921 - 7371
's-Gravenhage 2016

Van: 10.2.e
Verzonden: donderdag 15 juni 2017 13:57
Aan: Plas, Theo van der (T.G.); 10.2.e 10.2.e 10.2.e , 10.2.e
Onderwerp: Standpunt KPN op het besluit onderzoek in geautomatiseerd werk (internetconsultatie)
Bijlagen: 2017.05.29 - Consultatie voorontwerp binnendringen geautomatiseerd werk reactie KPN (1).pdf

Ter informatie.
Gr.
10.2.e

Reeds beoordeeld, zie doc. 668

Reeds beoordeeld, zie doc. 668

Reeds beoordeeld, zie doc. 668

Reeds beoordeeld, zie doc. 668

Reeds beoordeeld, zie doc. 668

Van: 10.2.e
Verzonden: donderdag 15 juni 2017 14:54
Aan: Plas, Theo van der (T.G.); 10.2.e 10.2.e 10.2.e ; 10.2.e
Onderwerp: Wanneer, waarvoor en hoe binnendringen
Bijlagen: Binnendringen.docx

Beste Theo,

Op anderhalf a4'tje het wanneer, waarvoor en hoe binnendringen geprobeerd uit te leggen. Ik hoop dat dit helpt, mocht je meer nodig hebben, dan hoor ik dat graag!

Groet,

10.2.e

10.2.e
9

Politie | Project CCIII

Hoofdstraat 54, 3972 LB Driebergen-Rijsenburg
Postbus 100, 3970 AC Driebergen-Rijsenburg
M: +31 (0)6 10.2.e
E: 10.2.e @politie.nl

Binnendringen

Onderzoeksdoelen

- Vaststelling en vastlegging kenmerken geautomatiseerd werk of gebruiker;
- Stelselmatige observatie (art. 126g Sv);
- Opnemen van (vertrouwelijke) communicatie (art. 126l Sv);
- Vastlegging opgeslagen gegevens;
- Ontoegankelijkmaking van gegevens.

Voorwaarden

- Verdenking artikel 67 lid 1 Sv feit voor,
    - Vastelling en vastlegging kenmerken Geautomatiseerd werk of gebruiker
- Verdenking misdrijf 8 jaar of meer voor,
    - Vastleggen gegevens
    - Ontoegankelijkmaking gegevens
- Of aanvullende misdrijven
    - Misdrijven benoemd in Besluit Onderzoek in Geautomatiseerd Werk (opgesteld door OM en MVenJ, zonder bemoeienis van politie)
        - Schending of bemachtiging staatsgeheim (Sr 98.1 en 98.2 en 98c.1)
        - Opruiing (131.1 en 131.2 Sr.)
        - Computervredebreuk (138ab lid 1-3 Sr)
        - Spam of bombing (138b lid 1-3 Sr)
        - Heling niet openbare gegevens (138c Sr) **(NIEUW in CCIII)**
        - Gegevens opnemen, aftappen (139c.1 Sr)
        - Plaatsen opname-, tap- afluisterapparatuur (139d, id 1-3 Sr)
        - Openbaar maken afbeelding (139g.1) **(NIEUW IN CCIII)**
        - Deelnemen criminele organisatie (140.1 Sr)
        - Valse bom(melding) (142a.1 en 2)
        - Belemmering herstel waterstaatswerk (160 Sr)
        - Vernieling waterkering of waterlozing, elektriciteitswerk, telecomwerk (161 aanhef, en onder 1;161bis aanhef, 1en2, 16sexies aanhef, 1 Sr)
        - Poging tot omkoping ambtenaren (177.1-2 Sr)
        - Mensensmokkel (197a Sr.1-2)
        - Wegmaken bewijsstukken (200.1 Sr)
        - Werven voor vreemde krijgsdienst of strijd (205.1 en 3 Sr)
        - (Gekwalificeerde) Valsheid in geschrift en valse opgave authentieke akte (225,1 en 2, 226.1 en 227.1 Sr)
        - Vals reisdocument of identiteitsbewijs (231.1-2 Sr)
        - Valse biometrische of persoonlijke gegevens (231a.1-2 Sr)
        - Valse betaalpas (232.1-2 Sr)
        - Kinderporno (240b.1 Sr)
        - Ontucht beneden 16 of onmachtige (247 Sr)
        - Verleiding minderjarige (248a Sr)
        - Grooming (248e Sr) **(NIEUW IN CCIII)**
        - Stalking (285b Sr)
        - Computergegevens veranderen of vernielen (350a.1-3 Sr)
        - Vernielen telecommunicatiewerk of technisch hulpmiddel daarvoor vervaardigen (350c.1 en 350d Sr)
        - Ambtelijke corruptie (363.1-2 Sr)
        - Witwassen (420bis.1 Sr)
- Bevel OvJ, na machtiging RC
- Toetsing door CTC
- Max 4 weken (verlengbaar)

Binnendringen

- 7-12
-
-
-

Van: 10.2.e
Verzonden: donderdag 15 juni 2017 15:00
Aan: Plas, Theo van der (T.G.); 10.2.e 10.2.e 10.2.e 10.2.e
Onderwerp: Bewaartermijnen en WPG
Bijlagen: Bewaartermijnen en WPG.docx

Beste Theo,

Bijgevoegd a4'tje komt uit de nota van toelichting op het ontwerpbesluit. Dit geeft een beeld over de bewaartermijnen en WPG. Het regiem is duidelijk beschreven en voldoet dus aan de WPG.

Groet,

10.2.e

Bewaartermijnen

De gegevens die al dan niet met een technisch hulpmiddel ter uitvoering van een bevel van de officier worden vastgelegd vallen onder een gedifferentieerd regime wat betreft de bewaartermijnen. De processen-verbaal en andere voorwerpen waaraan gegevens kunnen worden ontleend die zijn verkregen door observatie, het opnemen van vertrouwelijke communicatie en het opnemen van telecommunicatie met behulp van een technisch hulpmiddel worden door de officier van justitie, voor zover die niet bij de processtukken zijn gevoegd, ter beschikking gehouden van het onderzoek (artikel 126cc, eerste lid, Sv). Zodra twee maanden zijn verstreken nadat de zaak is geëindigd en de notificatie, bedoeld in artikel 126bb Sv is verricht, doet de officier van justitie de processen-verbaal en andere voorwerpen vernietigen. De procedure is uitgewerkt in het Besluit bewaren en vernietigen niet-gevoegde stukken.

De gegevens die zijn verkregen door de toepassing van de bevoegdheid met het oog op andere onderzoekshandelingen en al dan niet met een technisch hulpmiddel zijn gegenereerd vallen onder het regime van de Wet politiegegevens (Wpg). Afhankelijk van het specifieke doel van de verwerking kan de bewaartermijn verschillen. Doorgaans zullen de gegevens worden verwerkt met het oog op de ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval (artikel 9, eerste lid, Wpg). Zodra de gegevens niet langer noodzakelijk zijn voor het doel van het onderzoek, worden deze verwijderd of gedurende een periode van maximaal een half jaar bewaard teneinde te bezien of zij aanleiding geven tot een nieuw onderzoek als bedoeld in het eerste lid of een nieuwe verwerking als bedoeld in artikel 10 Wpg. Na afloop van deze termijn worden de gegevens verwijderd (artikel 9, derde lid, Wpg). De situatie dat de gegevens niet langer noodzakelijk zijn voor het doel van het onderzoek zal – in geval van een opsporingsonderzoek dat heeft geleid tot een vervolging – pas optreden op het moment dat de rechter ten aanzien van de zaak onherroepelijk heeft beslist. Als de zaak niet is opgelost en niet is ingezonden aan het openbaar ministerie, wordt het onderzoek meestal wel voortgezet maar op een minder intensief niveau. De gegevens kunnen in dat geval nodig blijven voor het vervolg van het onderzoek en voor het geval dat het team opnieuw bijeen wordt geroepen vanwege nieuwe aanknopingspunten. De gegevens blijven dan doorgaans nodig voor het doel van het onderzoek tot uiterlijk het moment waarop de feiten, waar het onderzoek zich op richt zijn verjaard. Daarna kunnen de gegevens niet meer nodig zijn voor het doel van het onderzoek en moeten zij worden verwijderd (Kamerstukken II 2005/06, 30 327, nr. 3, blz. 45/46). De verwijderde politiegegevens worden gedurende een termijn van vijf jaren bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen en vervolgens gearchiveerd of vernietigd.

De logging wordt bewaard met het oog op de verantwoording van de verrichte onderzoekshandelingen en het functioneren van de technische infrastructuur waarop de met een technisch hulpmiddel geregistreerde gegevens worden vastgelegd. Deze gegevens worden verwerkt met het oog op de opsporing van strafbare feiten en vallen eveneens onder de reikwijdte van de Wpg. Dit betekent dat de gegevens doorgaans moeten worden verwijderd zodra deze niet langer noodzakelijk zijn voor het doel van het onderzoek. Dit geldt in zijn algemeenheid voor de logging van gegevens, dus ook voor de logging met betrekking tot het verrichten van onderzoekshandelingen met het oog op observatie, het opnemen van vertrouwelijke communicatie of het opnemen van telecommunicatie met behulp van een technisch hulpmiddel.

From 10.2.e @politie.nl>
Subject FW: Mogelijke vragen voor Pol, OM en NCSC
To "Plas, Theo van der (T.G.)" 10.2.e @politie.nl>, 10.2.e @klpd.politie.nl>, 10.2.e @politie.nl>, 10.2.e @politie.nl>
Date 15 juni 2017 15:43:38 CEST

Beste allemaal,

Deze mail van 10.2.e vond ik nog in mijn mailbox. Volgens mij hebben wij zijn punten al wel redelijk besproken en wordt er een gedeelte al meegenomen in de spreektekst.
Ik ga nog even wat QenA's opzoeken, @10.2.e als jij daar mee kunt helpen zou dat heel mooi zijn!

Groet,

10.2.e

Elevator Pitch CCIII en ANPR, deskundigenbijeenkomst privacy Eerste Kamer

<u>Kernboodschap</u>: Onze samenleving digitaliseert steeds sneller, en dat geldt ook voor de criminaliteit. Criminelen worden mobieler en maken handig gebruik van steeds nieuwe mogelijkheden om anoniem te blijven en hun communicatie te versleutelen, waardoor ze buiten schot kunnen blijven. Opsporing en rechtshandhaving komen daardoor steeds meer onder druk te staan. De 28 dagen database ANPR versterkt onze mogelijkheden op criminaliteit met een mobiel karakter. De nieuwe wet CCIII is een nieuw en noodzakelijk wapen voor de politie in onze rechtsstaat om de missie van de politie 'waakzaam en dienstbaar' daadwerkelijk invulling te kunnen blijven geven.

Geachte voorzitter, geachte leden van vaste Kamercommissie Veiligheid en Justitie, geachte deelnemers aan deze discussie,

Allereerst wil ik u danken dat ik hier namens de ~~nationale~~ politie onze visie mag geven op de twee voorliggende wetsvoorstellen. Ik zal hier voor zowel ANPR als de wet Computercriminalteit III het woord ~~zal~~ voeren. In mijn functie van programmadirecteur Digitalisering & Cybercrime ben ik namelijk verantwoordelijk voor de implementatie van zowel de wet Computercriminaliteit III, als de ANPR wetgeving.

Elevator Pitch CCIII en ANPR, deskundigenbijeenkomst privacy Eerste Kamer

Kernboodschap: Onze samenleving digitaliseert steeds sneller, en dat geldt ook voor de criminaliteit. Criminelen worden mobieler en maken handig gebruik van steeds nieuwe mogelijkheden om anoniem te blijven en hun communicatie te versleutelen, waardoor ze buiten schot kunnen blijven. Opsporing en rechtshandhaving komen daardoor steeds meer onder druk te staan. De 28 dagen database ANPR versterkt onze mogelijkheden op criminaliteit met een mobiel karakter. De nieuwe wet CCIII is een nieuw en noodzakelijk wapen voor de politie in onze rechtsstaat om de missie van de politie 'waakzaam en dienstbaar' daadwerkelijk invulling te kunnen blijven geven.

Geachte voorzitter, geachte leden van vaste kamercommissie Veiligheid en Justitie, geachte deelnemers aan deze discussie,

Allereerst wil ik u danken dat ik hier namens de nationale politie onze visie mag geven op de twee voorliggende wetsvoorstellen. Onderling hebben mijn collega en ik afgesproken dat ik hier voor ANPR en de wet Computercriminalteit III het woord zal voeren. In mijn functie van programmadirecteur Digitalisering & Cybercrime ben ik namelijk verantwoordelijk voor de implementatie van zowel de wet Computercriminaliteit III, als de ANPR wetgeving. Vanuit mijn jarenlange ervaring in de opsporing en Intelligence met allerlei vormen en ontwikkelingen op het gebied van ernstige criminaliteit wil ik beginnen met twee praktijkvoorbeelden die het belang van beide wetsvoorstellen illustreren.

Onlangs deden wij een inval bij een verdachte van kinderporno. Tijdens de inval bleek dat de verdachte zoals we vaak zien een 'kill switch' had, waarmee met één handeling alle bewijs voor ons als politie door hem ontoegankelijk kon worden gemaakt door versleuteling. En daarmee hoogstwaarschijnlijk ook nog steeds beschikbaar zou blijven voor andere kinderporno-afnemers. Doortastend optreden wist dit deze keer maar net te voorkomen. Er zijn echter ook gevallen bekend waar me minder geluk hebben gehad. In deze gevallen kan de bevoegdheid tot binnendringen de zekerstelling van het bewijs en verstoring van het kinderporno netwerk wel mogelijk maken.

Een heel ander voorbeeld, met betrekking tot de bevoegdheid van de bewaarplicht ANPR.

Criminelen, die met explosieven geldautomaten opblazen, met geen enkel gevoel voor eventuele slachtoffers onder bewoners, zijn moeilijk te pakken. Tegelijkertijd weten we ook dat ze niet alleen in de nacht van de ramkraak bij de geldautomaat komen en dat ze het ook niet bij 1 ramkraak laten Opgeslagen passages van ANPR kunnen we correleren bij meerdere ramkraken, daarmee komt een dadergroep in beeld en krijgen we de mogelijkheid in te grijpen of het bewijs rond te krijgen.

Met opmerkingen [10.2.e1]: m.i. goed voorbeeld, wellicht kan de tekst iets eenvoudiger. Bijvoorbeeld: Het wetsvoorstel ANPR maakt het mogelijk om nieuwe verbanden te leggen met eerdere voertuigbewegingen. Daardoor kunnen we ramkraken stoppen of de daders opsporen.

Met opmerkingen [10.2.e2]: Mogelijk kun je dit voorbeeld op deze wijze beneden gebruiken niet hier. Tenzij hier een angst aanwezig is dat dit datamining genoemd wordt. Ik vind dat natuurlijk niet. Correleren is geen datamining. Je gaat namelijk gericht op zoek. Op basis van locatie, het voltrokken feit, tijdstip etc.

Dit geldt net zo goed voor terrorisme:. Was een Duitse of Belgische aanslagpleger net voor de aanslag ook in ons land? Alleen door de tijdelijke opslag van passagegegevens is dit vast te stellen.

Voordat ik dieper op de inhoud van beide wetsvoorstellen in ga, wil ik hier toch ook benoemen dat naast de bevoegdheid tot het op afstand kunnen binnendringen, het wetsvoorstel CCIII ook wetswijzigingen op het terrein van online handelsfraude, heling van gegevens, ontoegankelijk maken en het corrumperen en grooming bevat. De collega's van het OM zijn hier in hun bijdrage ook al op ingegaan. Deze voorgestelde wijzigingen zijn voor de politie minstens zo belangrijk!

Deze wijzigen maken het voor burgers, bedrijven en overheid eenvoudiger om aangifte te doen van deze vormen van criminaliteit, terwijl ook de opsporing en de bewijslast om uiteindelijk tot een veroordeling bij de rechter te kunnen komen wordt vergemakkelijkt.

Ik vervolg mijn betoog. In de context van ons werk zie ik 4 samenhangende ontwikkelingen: digitalisering, mobilisering, versleuteling en anonimisering. Onze samenleving verandert ingrijpend en steeds sneller onder invloed van digitalisering. De grenzen van de gemeente en het land begrenzen de criminaliteit niet meer. De grenzen van de fysieke wereld begrenzen de criminaliteit evenmin. De mobiliteit neemt toe, zowel in fysieke zin als in de digitale wereld. Criminaliteit verandert sterk doordat vrijwel elke vorm van criminaliteit inmiddels een digitale component heeft én er steeds nieuwe vormen van criminaliteit ontstaan in de vorm van cybercrime.

Anonimisering en versleuteling zijn de nieuwe en laagdrempelige standaarden in digitale communicatie, die door de overheid, door burgers en private en

publieke instanties in Nederland en in Europa, als een belangrijk onderdeel van onze privacy en als vanzelfsprekend worden aangemerkt.

Ook criminelen maken daarvan echter steeds vaker gebruik, waardoor hun communicatie verborgen blijft en ze buiten schot blijven van politie en justitie. De recente Ennetcom zaak, waarbij criminelen communiceerden met versleutelde telefoons, maakt nog eens duidelijk dat wij als politie steeds vaker essentieel bewijs in strafrechtelijke onderzoeken naar ernstige zaken als liquidaties, drugshandel en afpersing missen. En ook niet meer kunnen volgen hoe deze criminele wereld er uit ziet en deze dus ook niet goed kunnen bestrijden.

Traditionele methoden als interceptie zullen door toenemend gebruik van versleuteling steeds minder als bewijs dienen. Zo dreigen wij als politie met lege handen te komen staan. Opsporing en rechtshandhaving komen steeds meer onder druk te staan.

Voor het bestrijden van zware en georganiseerde misdaad is het noodzakelijk om zicht te blijven houden op de communicatie van criminelen die ernstige feiten plegen. De bevoegdheid tot binnendringen uit de wet computercriminaliteit III is daarvoor noodzakelijk omdat op die manier kennis genomen kan worden van de inhoud van berichten voordat deze worden versleuteld!

Deze bijeenkomst vandaag staat in het teken **van privacy**. Ik wil daar nader op ingaan.

Wij zijn er als politie, om uw grondrechten te beschermen en voor de veiligheid van onze samenleving. Als bewaker van de rechtsstaat hechten wij als politie grote waarde aan het recht op privacy. Soms kunnen en moeten wij echter een inbreuk maken op individuele grondrechten, omdat andere, zwaarder wegende belangen van de samenleving als geheel dat eisen. Het Wetboek van Strafvordering kent politie en het OM daartoe gelimiteerde en afgewogen bevoegdheden toe. Wij moeten die bevoegdheden proportioneel toepassen en alleen als er geen andere wegen meer openstaan (subsidiariteit)

Met opmerkingen [10.2](3): Blijkt dit niet voldoende uit de woorden gelimiteerd e afgewogen? De termen proportionaliteit en subsidiariteit komen verderop ook terug. Kan hier m.i. worden weggelaten.

U weet dat tijdens een doorzoeking van een woning er grondig en uitgebreid het hele huis wordt doorzocht. Dat heeft een grote impact op de verdachte en

diens eventuele partner en kinderen. In de digitale omgeving kunnen we met de nieuwe bevoegdheid juist *heel precies en nauwkeurig zoeken*. We doen uitvoerig vooronderzoek en leggen over elke stap verantwoording af. Met de nieuwe bevoegdheid tot binnendringen kan *chirurgisch* worden ingegrepen en zo precies mogelijk bij bewijs worden gekomen. Of kan precies die interventie worden gedaan die in een geval van kindermisbruik, ontvoering of terrorisme noodzakelijk is.

Met opmerkingen 10.2.e (4]: En nauwkeurig?

Dames en heren, ik ken geen énkele andere bevoegdheid, die met zoveel **waarborgen** is omgeven als de nieuwe bevoegdheid van heimelijk binnendringen in een geautomatiseerd werk:

- Die zich beperkt tot *zeer ernstige strafbare feiten*;
- die plaats vinden met een geautomatiseerd werk dat *in gebruik is bij een verdachte*;
- Waar de inzet nauwgezet geformuleerd wordt in een *bevel*;
- Dat vooraf wordt *getoetst op proportionaliteit en subsidiariteit* door de *rechter-commissaris, de officier van justitie en via de centrale toetsingscommissie door het college van PG's*;
- Waar een nauwgezette logging plaatsvindt van alle onderzoekshandelingen;
- En een inzet kent middels *gekeurde* technische hulpmiddelen.

Met opmerkingen 10.2.e 5]: Formulering van position paper aanhouden

Als laatste is daar natuurlijk de *toets van de rechter bij een rechtszaak en onafhankelijk toezicht door de Inspectie Veiligheid en Justitie achteraf*, met transparante en openbare rapportage. Deze buitengewoon hoge eisen zijn naar mijn mening terecht, omdat het om ingrijpende bevoegdheden gaat. Bevoegdheden die echter absoluut noodzakelijk zijn voor goed politiewerk van vandaag en morgen!

Tenslotte is het in internationaal opzicht belangrijk om de verhouding tot ons omringende landen te noemen. In Europa is al een vergelijkbare wetgeving CC III in werking in landen als Groot-Brittannië, Duitsland, België, Frankrijk, Denemarken en Noorwegen. Ook voor de internationale samenwerking in de bestrijding van grensoverschrijdende criminaliteit is het cruciaal dat Nederland in staat wordt gesteld om hieraan te blijven bijdragen.

Vandaag spreken we ook over het wetsvoorstel ANPR. In de context van een veranderende wereld is aanpassing van onze wettelijke mogelijkheden ook op dit gebied een Must. Ook hier spelen het maatschappelijk belang, de noodzaak van het gebruik en de privacy-aspecten.

Dit voorstel geeft de politie de mogelijkheid om achteraf beter te onderzoeken wat er in de aanloop naar een delict heeft plaatsgevonden. Het wetsvoorstel biedt de mogelijkheid om na een delict zicht te krijgen op de daders, de routes die gevolgd zijn en eventuele mededaders. Dat geldt niet alleen voor plofkraken, maar ook bijvoorbeeld bij .

ernstige geweldsmisdrijven. Indien een gedeelte van een kenteken wordt herkend kan in de opgeslagen passagegegevens worden gezocht op deze combinatie. Ook kan worden bekeken welke voertuigen op het moment van het delict in de buurt waren waarmee gerichter worden gezocht, wat ook de overlast voor de bewoners van Nederland beperkt. Dan hoeft niet iedereen, zoals nu is gebeurd bij de recente moordzaken op 2 jonge meisjes, worden ondervraagd die wel eens in de betrokken omgeving komt maar kan het opsporingsonderzoek veel gerichter plaatsvinden. Ook maakt dit wetsvoorstel het mogelijk bij gijzelingen en ontvoeringen op basis van opgeslagen kentekenpassages het juiste kenteken, sneller ter beschikking te hebben van de politie en direct in referentielijsten van ANPR te plaatsen waarmee real time de beweging van het voertuig kenbaar wordt voor de politie.

Deze directe opvolgactie, waarbij de daders kort na het delict gelokaliseerd kunnen worden, is van groot belang voor de heterdaadkracht van de politie. De opslag van ANPR passages, die op basis van een bevel van de OVJ doorzocht kunnen worden, geeft de politie die mogelijkheid. Niet alleen gericht op de directe daders, maar ook op mededaders. Dit is een krachtig en noodzakelijk middel in de strijd tegen criminaliteitsvormen met een mobiel karakter.

Met opmerkingen 10:2:6 (6): Heterdaadkracht gebruiken?

De politie is zich zeer bewust van de zorgvuldigheidseisen die gesteld worden aan de registratie en het gebruik van deze passagegegevens. Daartoe is een groot aantal waarbrogen in de wet opgenomen:

ANPR wordt steeds met voorafgaande toestemming van een Officier van Justitie, na een toets op proportionaliteit en subsidiariteit, ingezet. De bevraging vindt plaats door een opgeleide en geautoriseerde opsporingsambtenaar, die geen lid

is van het opsporingsteam en die de uitkomst nog eens checkt met de aanvraag voordat deze aan het team wordt verstrekt.

Elke bevraging wordt gelogd en is daarmee controleerbaar en transparant. Door de ingebouwde horizonbepaling van 3 jaar voor het wetsvoorstel ANPR is de democratische controle op de naleving van deze voorwaarden gewaarborgd.

De invoering van beide wetten vereist zorgvuldigheid. De politie bereidt zich hier programmatisch en op landelijk niveau op voor. Hiertoe heb ik een CC III programma-organisatie ingericht waarbij eigen specifieke deskundigheid en externe expertise bij elkaar wordt gebracht. Er wordt gezorgd voor een strikte scheiding tussen het technische team dat geautomatiseerde werken binnendringt en doorzoekt, en de tactische opsporingsteams die ondersteuning vragen. Digitaal rechercheren is vakwerk. Daarom worden alleen goed opgeleide, deskundige en gecertificeerde medewerkers aangewezen en ingezet. We zullen in afstemming met het OM de inzet van deze bevoegdheid tot binnendringen stapsgewijs opbouwen.

Datzelfde geldt ook voor de invoering van de ANPR-wetgeving worden De noodzakelijke voorbereidingen voor de implementatie worden getroffen. Met aandacht voor de opgenomen waarborgen zoals de noodzakelijke logging en de functiescheiding tussen geautoriseerde bevrager en opsporingsteam.

Dames en heren, ik kom tot een afronding. Criminelen maken gebruik van alle voor hen beschikbare methoden. Op dit moment staan we als politie naar mijn mening op forse achterstand. U staat voor de belangrijke afweging of u een politie wilt die -als het écht moet- kan doordringen tot de diepste lagen van ernstige criminaliteit. Zonder de bevoegdheid en het vermogen om op afstand binnen te dringen en waar nodig gegevens ontoegankelijk te maken, halen we die achterstand nooit meer in. En zonder passagegegevens is onze heterdaadkracht in de aanpak van ernstige vormen van criminaliteit beperkt. De huidige bevoegdheden schieten simpelweg te kort.

De wetsvoorstellen CCIII en ANPR zijn voor ons een nieuw en noodzakelijk instrument om onze missie ‘waakzaam en dienstbaar’ voor de veiligheid van onze samenleving invulling te kunnen blijven geven.

12-14

Ik dank u voor uw aandacht.

Met opmerkingen 10.2.e 7]: 12-14

Met opmerkingen 10.2.e (8]: 12-14

Voordat ik dieper op de inhoud van beide wetsvoorstellen in ga, wil ik hier benoemen dat naast de bevoegdheid tot het op afstand kunnen binnendringen, het wetsvoorstel CCIII ook wetswijzigingen op het terrein van online handelsfraude, heling van gegevens, ontoegankelijk maken en het corrumperen en grooming bevat. De collega's van het OM zijn hier in hun bijdrage ook al op ingegaan. Deze voorgestelde wijzigingen zijn voor de politie minstens zo belangrijk als de bevoegdheid tot binnedringen~~1~~.

Met opmerkingen 10.2.6 (1): 12-14

Deze wijzigingen maken het voor burgers, bedrijven en overheid eenvoudiger om aangifte te doen van deze vormen van criminaliteit, terwijl ook de opsporing en de bewijslast om uiteindelijk tot een veroordeling bij de rechter te kunnen komen wordt vergemakkelijkt.

Vanuit mijn jarenlange ervaring in de Opsporing en Intelligence met ~~-~~allerlei vormen van ernstige criminaliteit wil ik beginnen met twee praktijkvoorbeelden die het belang van beide wetsvoorstellen illustreren.

Onlangs deden wij een inval bij een verdachte van kinderporno. Tijdens de inval bleek dat de verdachte zoals we vaak zien een 'kill switch' had, waarmee met één handeling alle bewijs voor ons als politie door hem ontoegankelijk kon worden gemaakt door versleuteling. En het materiaal hoogstwaarschijnlijk nog steeds beschikbaar zou blijven voor andere kinderporno-afnemers. Doortastend optreden wist dit

deze keer maar net te voorkomen. We hebben soms helaas minder succes.

In dit soort gevallen kan de bevoegdheid tot binnendringen de zekerstelling van het bewijs en verstoring van het kinderporno netwerk ~~wel~~ met een grotere kans op succes mogelijk maken.

Met opmerkingen 10.2.6 **(2]:** Het was in het voorbeeld ook mogelijk, dus 'wel' klopt hier niet.

Een ander voorbeeld, nu met betrekking tot de bevoegdheid van de bewaarplicht ANPR.

Criminelen, die met explosieven geldautomaten opblazen, met geen enkel gevoel ~~bij~~ voor eventuele slachtoffers onder bewoners, zijn moeilijk te pakken. Tegelijkertijd weten we ook dat ze niet alleen in de nacht van de ramkraak bij de geldautomaat komen. Het wetsvoorstel ANPR maakt het mogelijk om nieuwe verbanden te leggen met eerdere voertuigbewegingen. Daardoor kunnen ~~we ramkraken stoppen en~~ daders opsporen en ramkraken stoppen.

Met opmerkingen 10.2.6 **(3]:** Invoegen: Maar al eerder een voorverkenning doen?

Dit geldt net zo goed voor terrorisme: Was een Duitse of Belgische aanslagpleger net voor de aanslag ook in ons land? Alleen door de tijdelijke opslag van passagegegevens is dit vast te stellen.

In de context van dit politiewerk zie ik 4 samenhangende ontwikkelingen: digitalisering, mobilisering, versleuteling en anonimisering. Onze samenleving verandert ingrijpend en steeds sneller onder invloed van digitalisering. De grenzen van de gemeente en het land begrenzen de criminaliteit niet meer. De grenzen van de fysieke wereld begrenzen de criminaliteit

evenmin. De mobiliteit neemt toe, zowel in fysieke zin als in de digitale wereld. Criminaliteit verandert sterk doordat vrijwel elke vorm van criminaliteit inmiddels een digitale component heeft én er steeds nieuwe vormen van criminaliteit ontstaan in de vorm van cybercrime.

Anonimisering en versleuteling zijn de nieuwe en laagdrempelige standaarden in digitale communicatie, die door de overheid, door burgers en private en publieke instanties in Nederland en in Europa, als een belangrijk onderdeel van onze privacy en als vanzelfsprekend worden aangemerkt.

Ook criminelen maken daarvan echter steeds vaker gebruik, waardoor hun communicatie verborgen blijft en ze buiten schot blijven van politie en justitie.

Traditionele methoden als interceptie zullen door toenemend gebruik van versleuteling steeds minder als bewijs kunnen dienen. Zo dreigen wij als politie met lege handen te komen staan. Opsporing en rechtshandhaving komen dus steeds meer onder druk.

Voor het bestrijden van zware en georganiseerde misdaad is het dan ook noodzakelijk om zicht te blijven houden op de communicatie van criminelen die ernstige feiten plegen. De bevoegdheid tot binnendringen uit de wet computercriminaliteit III is daarvoor nodig omdat op die manier kennis genomen kan worden van de inhoud van berichten *voordat* deze worden versleuteld!

Deze bijeenkomst vandaag staat in het teken van **privacy**. Ik wil daar nader op ingaan.

Wij zijn er als politie, om uw grondrechten te beschermen en voor de veiligheid van onze samenleving. Als bewaker van de rechtsstaat hechten wij als politie grote waarde aan het recht op privacy. Soms kunnen en moeten wij echter een inbreuk maken op individuele grondrechten, omdat andere, zwaarder wegende belangen van de samenleving als geheel dat eisen. Het Wetboek van Strafvordering kent politie en het OM daartoe gelimiteerde en afgewogen bevoegdheden toe.

U weet dat tijdens een doorzoeking een woning grondig en uitgebreid wordt doorzocht. Dat heeft een grote impact op de verdachte en diens eventuele partner en kinderen. In de digitale omgeving kunnen we met de nieuwe bevoegdheid juist *heel precies zoeken*. We doen uitvoerig vooronderzoek en leggen over elke stap verantwoording af. Met de nieuwe bevoegdheid tot binnendringen kan *chirurgisch* worden ingegrepen en zo precies mogelijk bij bewijs worden gekomen. Of kan precies die interventie worden gedaan die in een geval van kindermisbruik, ontvoering of terrorisme noodzakelijk is.

Dames en heren, ik ken geen énkele andere bevoegdheid, die met zoveel **waarborgen** is omgeven als de nieuwe bevoegdheid van heimelijk binnendringen in een geautomatiseerd werk:

- Die zich beperkt tot *zeer ernstige strafbare feiten*;

- die plaats vinden met een geautomatiseerd werk dat *in gebruik is bij een verdachte*;
- Waar de inzet nauwgezet geformuleerd wordt in een *bevel*;
- Dat vooraf wordt *getoetst op proportionaliteit en subsidiariteit* door de *rechter-commissaris op vordering van~~,~~ de officier van justitie en ~~via de~~ door de centrale toetsingscommissie moet worden goedgekeurd.~~ door het college van PG's;~~*
- Waar een nauwgezette logging plaatsvindt van alle onderzoekshandelingen;
- En een inzet kent middels *gekeurde* technische hulpmiddelen.
- Door *geautoriseerd en opgeleid personeel*
- Binnen een van het tactische team afgescheiden *uitvoerend technisch team*

Als laatste is daar natuurlijk de *toets van de rechter bij een rechtszaak en onafhankelijk toezicht achteraf door de Inspectie Veiligheid en Justitie*, met transparante en openbare rapportage. Deze buitengewoon hoge eisen zijn naar mijn mening terecht, omdat het om ~~ingrijpende~~ een ingrijpende ~~bevoegdheden~~ bevoegdheid gaat. Een ~~B~~bevoegdheden die echter absoluut noodzakelijk ~~zijn~~ is voor goed politiewerk van vandaag en morgen!

Tenslotte is het in internationaal opzicht belangrijk om de verhouding tot ons omringende landen te noemen. In Europa

Met opmerkingen 10.2.6 (4): Formulering van position paper aanhouden

Met opmaak: Lettertype: 18 pt

is al een vergelijkbare wetgeving CC III in werking in landen als Groot-Brittannië, Duitsland, België, Frankrijk, Denemarken en Noorwegen. Ook voor de internationale samenwerking in de bestrijding van grensoverschrijdende criminaliteit is het cruciaal dat Nederland in staat wordt gesteld om hieraan te blijven bijdragen.

Met opmerkingen 10.2.6 (5): ??

Met opmerkingen 10.2.6 (6): Dit was toch niet vergelijkbaar?

Vandaag spreken we ook over het wetsvoorstel ***ANPR***. In de context van de veranderende wereld is aanpassing van onze wettelijke mogelijkheden ook op dit gebied een Must. Ook hier spelen het maatschappelijk belang, de noodzaak van het gebruik en de privacy-aspecten.

Dit voorstel geeft de politie de mogelijkheid om achteraf beter te onderzoeken wat er in de aanloop naar een delict heeft plaatsgevonden. Het wetsvoorstel biedt de mogelijkheid om na een delict zicht te krijgen op de daders, de routes die gevolgd zijn en eventuele mededaders.

Ik noemde u al de ram-en plofkraken. Maar dit geldt ook voor de mobiele bendes, die door heel Nederland en Europa, soms zeer gewelddadig inbreken. Na de inbraak kunnen we met deze wet zien waar het voertuig recent is geweest, en daarmee in welke omgeving de verdachte tijdelijk verblijft of zijn vluchtplaats is.

~~Of~~En bij gijzelingen en ontvoeringen~~, waar~~ is het mogelijk ~~is~~ op basis van opgeslagen kentekenpassages het juiste kenteken, sneller ter beschikking te hebben van de politie, direct in

referentielijsten van ANPR te plaatsen en daarmee real time de beweging van het voertuig te onderkennen.

Deze directe opvolgacties, waarbij de daders kort na het delict gelokaliseerd kunnen worden, is van groot belang voor de heterdaadkracht van de politie in haar strijd tegen criminaliteitsvormen met een mobiel karakter.

De politie is zich zeer bewust van de *zorgvuldigheidseisen* die gesteld worden aan de registratie en het gebruik van deze passagegegevens. Daartoe is ook hier een groot aantal waarborgen in de wet opgenomen:

Een ANPR-verzoek wordt steeds met voorafgaande toestemming van een Officier van Justitie, na een toets op proportionaliteit en subsidiariteit, uitgevoerd. De bevraging vindt plaats door een opgeleide en geautoriseerde opsporingsambtenaar, die geen lid is van het opsporingsteam en die de uitkomst nog eens dubbelcheckt met de aanvraag.

Elke bevraging wordt gelogd en is daarmee controleerbaar en transparant. Door de ingebouwde horizonbepaling van 3 jaar voor het wetsvoorstel ANPR is de democratische controle op de naleving van deze voorwaarden gewaarborgd.

De invoering van beide wetten vereist zorgvuldigheid. De politie bereidt zich hier programmatisch en op landelijk niveau op voor. Hiertoe heb ik een CC III programma-organisatie ingericht ~~waarbij~~ waarin eigen specifieke deskundigheid en

externe expertise bij elkaar wordt gebracht. Er komt een strikte scheiding tussen het technische team dat geautomatiseerde werken binnendringt en doorzoekt, en de tactische opsporingsteams die ondersteuning vragen.

Digitaal rechercheren is vakwerk. Daarom worden alleen goed opgeleide, deskundige en gecertificeerde medewerkers aangewezen en ingezet. We zullen in afstemming met het OM de inzet van deze bevoegdheid tot binnendringen stapsgewijs opbouwen.

Datzelfde geldt ook voor de invoering van de ANPR-wetgeving worden. De noodzakelijke voorbereidingen voor de implementatie van alle waarborgen worden getroffen.

Dames en heren, ik kom tot een afronding. Criminelen maken gebruik van alle voor hen beschikbare methoden. Op dit moment staan we als politie naar mijn mening op forse achterstand. U staat voor de belangrijke afweging of u een politie wilt die -als het écht moet- kan doordringen tot de diepste lagen van ernstige criminaliteit. Zonder de bevoegdheid en het vermogen om op afstand binnen te dringen en waar nodig gegevens ontoegankelijk te maken, halen we die achterstand nooit meer in. En zonder passagegegevens is onze heterdaadkracht in de aanpak van ernstige vormen van criminaliteit beperkt. De huidige bevoegdheden schieten simpelweg te kort.

De wetsvoorstellen CCIII en ANPR zijn voor ons een nieuw en noodzakelijk instrument om onze missie ‘waakzaam en

dienstbaar’ voor de veiligheid van onze samenleving invulling te kunnen blijven geven.

Ik dank u voor uw aandacht.

Van: 10.2.e
Verzonden: maandag 19 juni 2017 10:57
Aan: 10.2.e Plas, Theo van der (T.G.); 10.2.e 10.2.e
Onderwerp: spreektekst 10.2.e morgen
Bijlagen: Spreektekst OM - Bijeenkomst EK 18 juni 2017.def.doc

Hoi,

Bij deze de goedgekeurde spreektekst van 10.2.e morgen.

Gr.
10.2.e

Groet,
10.2.

Dinsdag 20 juni 2017, commissie Veiligheid en Justitie (V&J)

"Deskundigenbijeenkomst wetsvoorstellen ANPR en computercriminaliteit III"

Blok 1 - Thema: *Noodzaak en belang van de voorgestelde wetgeving*

Spreektekst Openbaar Ministerie CCIII *(833 woorden = 6.24 min)*

Geachte leden van de commissie voor Veiligheid en Justitie,

Dank voor de uitnodiging om namens het openbaar ministerie in te gaan op het belang van het wetsvoorstel computercriminaliteit III. Mijn naam is Martijn Egberts. Ik ben de Landelijk officier van justitie Cybercrime. Naast mij zit Mèlanie Nijenhuis, informatie officier bij het Landelijk Parket en zij zal zo dadelijk een toelichting geven op de wet ANPR. Na onze inleidingen beantwoorden wij graag eventuele vragen.

Ik begin met een toelichting op de wet CCIII. Een belangrijk en noodzakelijk wetsvoorstel. Dagelijks zie ik vanuit de praktijk dat de bestaande bevoegdheden voor de opsporing steeds minder effectief worden.

Zonder wettelijke grondslag mag het openbaar ministerie geen inbreuken maken op iemands privéleven. Dat klinkt logisch en dat is het ook. De andere kant van de medaille is echter dat met die wettelijke grondslagen het openbaar ministerie in staat moet zijn om haar taken betreffende de opsporing, vervolging en preventie van criminaliteit, goed te kunnen vervullen. Als technologie de wereld verandert, zullen bevoegdheden moeten mee veranderen om te voorkomen dat er een vrijplaats komt voor criminaliteit.

We zien steeds vaker situaties waarbij cyber criminaliteit in materiële- en zelfs fysieke zin gevolgen heeft. Recent kon u zien dat een wereldwijde aanval met het Wannacry randsomware ervoor zorgde dat afdelingen van ziekenhuizen moeten sluiten en bedrijven ontwricht werden. De opsporingsmogelijkheden van politie en OM worden steeds minder effectief om dergelijke aanvallen op te sporen, als er geen moderne bevoegdheden beschikbaar komen. Ik, en mijn collega's binnen politie en openbaar ministerie, hebben steeds vaker het gevoel te vechten met onze handen op onze rug.

Een van de belangrijkste redenen hiervoor is het gemak waarmee criminelen technisch hoogwaardige versleutelingstechnieken gebruiken en zich succesvol online anoniem kunnen bewegen. Dit maakt deze daders onzichtbaar voor de opsporingsdiensten. De gevolgen van deze daders zijn echter níet onzichtbaar voor de burgers die het slachtoffer worden van ransomware, van kinderporno van liquidaties of van drugshandel.

De vraag in welke opsporingsonderzoeken er doelbewuste afscherming wordt tegengekomen moet haast omgekeerd gesteld worden, er is feitelijk geen enkel cybercrime onderzoek waarbij dit niet het geval is. Zelfs in veel reguliere opsporingsonderzoeken zijn afscherming en versleuteling aan de orde van de dag.

Een bekend en effectief voorbeeld van afscherming begint vaak bij het gebruik van volstrekt legitieme Virtual Private Networks (VPN). Een dienst waarmee een versleutelde verbinding wordt opgezet met een server waar dan ook ter wereld, waarbij niet je eigen ip-adres, maar dat van de VPN-aanbieder zichtbaar wordt. Omdat deze aanbieders in het algemeen niet registreren welke klanten op welk moment van hun ip-adressen gebruik maken, kan er dus geen koppeling

plaatsvinden. In de bijlage van de position paper is de werkwijze van een VPN- dienst opgenomen en waarom deze dienst de opsporing bemoeilijkt. Deze VPN diensten worden in onderzoeken naar terrorisme, kinderporno en cybercrime veel teruggezien.

Een ander voorbeeld is The Onion Browser (TOR) waarmee het darkweb toegankelijk wordt. Deze dienst is ook niet ontworpen voor crimineel gebruik, maar er wordt inmiddels veelvuldig misbruik van gemaakt om zo anoniem mogelijk drugs, wapens en cybercrimetools te verkopen en kopen. Niet alleen zijn daarbij de bezoekers niet te achterhalen, maar ook de websites die zij bezoeken staan op zogenaamde TOR hidden servers die vrijwel niet te lokaliseren zijn.

Alle bovenstaande voorbeelden van afscherming zijn uiteraard niet illegaal om te gebruiken. Integendeel, veel van deze diensten en producten dragen bij aan een veiligere digitale infrastructuur. Echter, de criminelen maken dankbaar gebruik van deze diensten waardoor regelmatig de bestaande opsporingsbevoegdheden niet meer toereikend zijn om ernstige feiten, zoals terreur, kinderporno, cybercrime en georganiseerde misdaad op te sporen.

Om beter te kunnen optreden tegen criminelen die gebruik maken van genoemde afschermingstechnieken is de bevoegdheid nodig om heimelijk op afstand een geautomatiseerd werk te betreden en zeer gericht die data veilig te stellen die relevant is voor het onderzoek. Deze mogelijkheid, zal alleen worden ingezet bij verdenking van ernstige strafbare feiten en pas na een professionele toetsing binnen het OM en na een afweging door een onafhankelijke RC.

Het wetsvoorstel beperkt zich niet enkel tot de bevoegdheid om op afstand een geautomatiseerd werk te betreden. De wet stelt ook de heling van digitale gegevens strafbaar. Door het strafbaar stellen van het wederrechtelijk overnemen en het voorhanden hebben of bekend maken van door misdrijf verkregen gegevens, worden gedragingen strafbaar die kunnen worden beschouwd als «heling» van gegevens. Dit voorstel voorziet in een betere strafrechtelijke bescherming van computergegevens.

Ook is in het wetsvoorstel voorgesteld de strafbaarstelling van het verleiden van minderjarigen tot ontucht en grooming te verruimen. Met de term grooming wordt gedoeld op het ongewenst benaderen van kinderen op het internet, bijvoorbeeld in chatrooms, met het oogmerk om ontuchtige handelingen met hen te plegen.

U zult vandaag verschillende standpunten horen. Ik hoop dat u, op het moment dat u over deze wet een afweging moet maken, zich rekenschap geeft van de noodzaak voor politie en openbaar ministerie om bewijs te kunnen vergaren om misdrijven succesvol te vervolgen. Iets dat zonder deze wet in toenemende mate onmogelijk wordt.

= EINDE =

A. Actie- besluitenlijst driehoeksoverleg CCIII

A: actuele lijst
B: afgewikkelde actiepunten
C: genomen besluiten

A	Actiepunt	Wie	Status	Datum
1	**Hoofdlijnennotitie CCIII v. 04**			
	Het BOO is op 12 mei 2017 akkoord gegaan met de notitie. Eigenlijk zou het KMT nog voor het zomerreces een besluit moeten nemen, i.v.m. de doorlooptijden (werving, selectie, screening e.d.). Als dat niet lukt komt realisatie van de vereiste bezetting per 1 januari 2018 in gevaar. Gewenste routing: direct naar het KMTO. En een afzonderlijke afstemming met het hoofd bedrijfsvoering, voordat de nota naar het KMTO gaat. 9 en 9 gaan proberen dit te realiseren.	Theo 10.2.e 10.2.	Actie Actie	12.07.2017
2	**Vacatures en werving**			
	De korpsleiding heeft ingestemd met werving 7-12 fte HBO voor de LE, waarva 7-12 voor DLOS. 7-12 vacatures voor CCIII maken deel uit van 7-12 De werving wordt in gang gezet, waarbij werving van een teamleider CCIII (OS niveau 11) prioriteit heeft. Realisatie van de werving geschiedt door de taakgroep mens.	Marjolein Aannemer taakgroep mens	Besluit Actie	19.06.2017 15.07.2017
3	**Personeel**			
a	**Participatie operationeel jurist in CCIII**			
	10.2.e heeft zich als jurist teruggetrokken uit CCIII. Zijn expertise en zijn inzet in de juridische werkgroep zijn nodig voor het programma. Marjolein heeft een mail gestuurd naar 9 en zal dit verder afhechten naar zijn leidinggevende, 9	Marjolein	Actie	29.04.2017
	20170619 update: De programmaleiding CCIII acht de inhoudelijke participatie van 10.2.e van belang voor het programma, als lid van de taakgroep Juridisch en als operationeel jurist bij oefeningen en inzet. Officiële standpunten van de politie naar buiten en naar andere organisatie-onderdelen worden door de driehoek c.q. de programmaleiding uitgedragen en niet door individuele medewerkers.	Marjolein	Besluit	19.06.2017

4	**Presentatie CCIII in** 7-12			
	Enkele deelnemers van het 7-12 zijn not amused over het advies van het BOO 7-12 f.t.e. te leveren ten behoeve van de landelijke CCIII voorziening. Er wordt ruimte gepland in het 7-12 voor de zomervakantie (7-12 juli) voor een bredere presentatie en dialoog over CCIII. Marjolein vraagt aan het 7-12 om te participeren in de taakgroepen CCIII. 9 levert daarvoor een korte memo aan.	Marjolein 10.2.e Marjolein 10.2.e	Actie Afgerond	19.06.2017 21.06.2017
5	**Ontwikkeling wetgeving**			
a	Op 20 juni vindt de deskundigenbijeenkomst in de EK plaats. Theo spreekt namens de NP. Het programmateam heeft een positionpaper, spreektekst en Q&A's voorbereid en er heeft een oefensessie plaatsgevonden ter voorbereiding.	Theo Programmateam CCIII	Afgerond Afgerond	20.06.2017
b	**Consultatiereactie Besluit Onderzoek Geautomatiseerd Werk**			
	Het programmateam CCIII heeft een afgestemde conceptreactie opgesteld. De driehoek gaat akkoord met het politiestandpunt over het besluit. Er volgt nog een laatste inbrengmogelijkheid. De definitieve reactie zal door het CCIII team op 23 juni ter goedkeuring worden aangeboden aan de driehoek. 9 zal zorgdragen voor doorzenden aan het ministerie via de juridische staf politie.	Driehoek 10.2.e	Besluit	19.06.2017 22.06.2017
6	**Screening**			
	Op advies van de AIVD besluit de driehoek dat voor alle medewerkers van CCIII de zwaarste vorm van screening (A-screening) geldt. Dit geldt ook voor eventueel ingehuurde medewerkers.	Driehoek	Besluit	19.06.2017
7	**Keuring**			
a	**Personeel**			
	20170425 update: Marjolein gaat het gesprek met 10.2.e aan over de externe verkenning en zal hem ook verzoeken het auditrapport aan ons ter beschikking te stellen.	Marjolein	Actie	

	20170619 update: Alleen het hoofd KD is officieel geplaatst; de overige medewerkers zijn HPK. Er zijn twee vacatures, die officieel eerst intern moeten worden opengesteld. De KD heeft afgelopen 17 jaar goed gepresteerd op analoog terrein maar beschikt onvoldoende over deskundigheid en capaciteit die nodig is voor keuring digitale TH. De kwaliteit van de KD vormt voor CCIII een hoog (politiek) afbreukrisico. Daarom is de keuring binnen de scope van het programma gebracht. Deskundigheid van medewerkers KD is een absoluut vereiste. Voorgesteld wordt de mogelijke invulling van vacatures KD te betrekken bij het besluit over externe keuring.	Marjolein	Informatie Besluit	15.07.2017
b	**Externe verkenning keuring**			
	20170619: Het NFI heeft zich teruggetrokken als externe keuringsdienst, zodat alleen TNO overblijft. Het conceptvoorstel van TNO ziet er goed uit maar moet verder worden uitgewerkt. De definitieve conceptofferte wordt in week 26 verwacht, en wordt met een advies van het programmateam voorgelegd aan de driehoek.	10.2.e	Actie	
	Er zijn veel afhankelijkheden van invloed op de doorlooptijd bij een besluit om met een externe partij in zee te gaan, waaronder: - Inwerkingtreding van het BOGW - Screening van medewerkers - Aanwijzing door de minister als KD - Inrichten testomgeving lab - Aanschaffen TH - Inkoopprocedures intern Daardoor is start met een gekeurd TH niet haalbaar op 1 januari 2017. Met gefaseerde en uitgekiende planning zou een eerste gekeurd TH medio 2018 beschikbaar zijn. Dit heeft consequenties voor het aantal/ soort zaken dat het CCIII team kan draaien. Goed verwachtingenmanagement is noodzakelijk. 9 bereidt mogelijke besluitvorming voor met TNO. Onderwerp agenderen in begeleidingscommissie.	Marjolein 10.2.e	actie	17.07.2017
6	**Meerjarenbegroting**			

	De driehoek neemt kennis van de concept begroting. Opgemerkt wordt dat in deze begroting nog geen kosten voor huisvesting zijn opgenomen. Ook voor huisvesting zullen de kosten hoog zijn (niveau meldkamer +) De inkoop van soft- en hardware zou via heimelijke inkoop moeten gebeuren. Gevraagd wordt om in de begeleidende notitie verder in te gaan op de volgende vragen: 1. Waarom zijn de kosten van software zo hoog? 2. Is het mogelijk om kostenefficiënt samen te werken met andere partijen als AIVD en defensie? 3. Wat is de ROI van CCIII, wat levert het op? (businesscase)	10.2.e 10.2.e	Actie	01.07.2017
7	**Versterking programma-organisatie CCIII**			
	Uit de mijlpalenplanning wordt duidelijk dat er veel werk te verzetten is. 10.2.e werkt in afstemming met 9 en 10.2.e een voorstel uit voor versterking van de programma-organisatie. Dit wordt volgende keer besproken en geagendeerd voor de volgende begeleidingscommissie.	10.2.e	Actie	01.07.2017
8	**Begeleidingscommissie**			
a	9 heeft n.a.v. nationale briefing kort met 10.2.e van PDC gesproken. Marjolein zal 10.2.e ook benaderen met verzoek deelname in de begeleidingscommissie en om inzet van personeel uit de disciplines HR, huisvesting, communicatie en financiën in het programma te bewerkstelligen.	10.2.e	Actie	10.05.2017
b	Het conceptverslag van de begeleidingscommissie van 1 juni jl. wordt met dank aan 10. goedgekeurd en kan worden verspreid aan de leden.	Driehoek	Besluit	19.06.2017

B. Afgehandelde actiepunten driehoeksoverleg CCIII

B	Actiepunt	Wie	Status	Datum
	Portefeuillehouder digitaal opsporen			
	Marjolein gaat deze rol vanuit het 7-12 landelijk invullen. Biedt mogelijkheden tot synergie met CCIII.	Marjolein	Mededeling	12.04.2017
	Programma aanpak			
	Theo verzoekt de programma-aanpak CCIII af te stemmen 10.2.e en 10.2.e	10.2	Actie	01.05.2017
	Scrumteams			
	De inzet van scrumteams wordt verwerkt in de programmaorganisatie CCIII. Behoefte van CCIII is breed inzetbare scrummers, op de gehele bedrijfsvoeringskant van CCIII. 10.2.e heeft dit ingebracht bij 10.2.e en 10.2.e . CCIII betaalt en bepaalt. Theo stuurt hierop aan via 10.2.e	10.2.e Theo	Afgehandeld Afgehandeld	25.04.2017 25.04.2017
	Hoofdlijnennotitie CCIII v. 04			
	Theo zal de notitie afstemmen met Willem Woelders en toelichten in het BOO van 12 mei 2017. 10.2. en 10. worden per omgaande gevraagd om een laatste reactie. Stukken worden op 5 mei aangeleverd aan BOO.	Theo 10.2.e	Afgerond Afgerond	25.04.2017
	Personeel			
	DLOS 7-12 vacatures openstellen d.m.v. vacatureruimte. Programma levert de profielen hiervoor aan. Medewerkers die al werkzaam zijn in het lab worden uitgenodigd mee te solliciteren c.q. hun informele aanstelling wordt geformaliseerd. Een van de vacatures is de rol van teamleider lab. De urgentie om deze vacature open te stellen wordt gedeeld. Zo mogelijk wordt de openstelling van deze vacature naar voren getrokken.	10.2.e	Afgerond	29.04.2017
	20170425 update: Marjolein zet de openstelling van de 10 vacatures DLOS in werking met de P&O adviseur 10.2.e	Marjolein	Afgerond	25.04.2017
	10.2.e leidt de juridische werkgroep en vertegenwoordigt de juridische discipline in de begeleidingsgroep.	10.2.e	Besluit	25.04.2017
	Mijlpalenplanning CCIII			
	De driehoek gaat akkoord met de planning en besluit: - Deze te presenteren in de volgende begeleidingsgroep. - Leden van de begeleidingsgroep waar mogelijk een actieve rol te laten vervullen in de realisatie.	Driehoek	Besluit	25.04.2017

	9 heeft op basis van onderzoek en de risico analyse een globale mijlpalenplanning opgesteld en gepresenteerd. Deze voldoet aan de behoefte om inzicht van de driehoek. Uit de planning wordt duidelijk dat: - er veel werk is verzet, maar ook nog veel moet gebeuren - er vele afhankelijkheden zijn in de realisatie van CCIII, die gevolgen hebben voor de planning - Het realisatieplan CCIII geen blauwdruk is die op 1 juli klaar is, maar een groeidocument met een plateauplanning 10.2.e stuurt een foto van de mijlpalenplanning toe aan de driehoek.	10.2.e 10.2.e	Afgerond Afgerond	25.04.2017
	Keuring			
	20170425 update: Met TNO staat inmiddels een afspraak. NFI wordt op 26 april een eerste reactie op de vraag verwacht.	10.2.e	Actie	19.05.2017
	Ontwikkeling wetgeving			
	10.2.e stuurt update rond van ontwikkelingen rond het besluit CCIII. Feedback politie is niet verwerkt door ministerie. OM is betrokken via begeleidingscommissie. Theo vertegenwoordigt de NP bij de discussie in de Eerste Kamer. 10.2.e en 10.2.e ondersteunen daarbij. Verwachte datum behandeling is 15 mei.	10.2.e Theo 10.2.e	Afgehandeld	25.04.2017
	20170425 update: Het lukt waarschijnlijk niet meer om de feedback van de politie voor de formele consultatie in te brengen. Het ontwerp besluit bevat fouten en onderdelen die het voor de politie moeilijk maken. Theo van der Plas doet nog een laatste poging om dit via 9 onder de aandacht te brengen van de directie wetgeving van V&J.	Theo	Afgerond	29.04.2017
	Theo verzoekt om 10.2.e actief te blijven informeren door het programma CCIII. Afgesproken wordt dat 10.2.e en 10.2. elkaar over en weer actief informeren.	10.2.e 10.2.	Afgerond	29.04.2017
	Screening			
	Tot heden is A-screening vereiste voor CCIII. AIVD zet in op P-screening. We verifiëren de wenselijkheid bij 10.2.e /lid begeleidingscommissie namens AIVD, en komen met een advies.	10.2	Afgerond	29.04.2017
	20170425 update: 10.2. heeft afstemming gehad met de AIVD en de risico's van een lagere screeningseis voor CCIII nogmaals uitgebreid onder de aandacht gebracht. ondanks toezending van alle informatie en het VIK-rapport, heeft CCIII geen "status aparte" gekregen. VIK vraagt nu een officiële bevestiging van de AIVD.	10.2	Afgerond	10.05.2017
	Begeleidingscommissie			
	Documentatie programma CCIII in 7-12			

	10.2.e laat de risico analyse en het governance model zien, die in mindmap vorm zijn weergegeven. 7-12 is al op politiesystemen aanwezig. Veilige toegang tot de vertrouwelijke bestanden moet nog worden geregeld, dan is het ook beschikbaar voor alle betrokkenen in het programma.	10.2.e	Afgerond	10.05.2017
	Planning driehoeksoverleggen			
	Driehoeksoverleggen worden vierwekelijks ingepland. Tussentijds worden korte bilaterale overleggen tussen opdrachtnemer en programmamanagement ingepland.	Marjolein	Afgerond	01.05.2017

C. Besluiten driehoeksoverleg CCIII

C	Actiepunt	Wie	Status	Datum
1	**Governance CCIII**			
	De driehoek is akkoord met de rol- en taakverdeling governance CCIII, overeenkomstig de notitie en besluit deze vast te stellen. Theo vervult de rol van opdrachtgever, Marjolein die van opdrachtnemer, 9 die van programmamanager en 10.2.e die van plv. Programmamanager. De planning wordt in de notitie als volgt verhelderd: Het programma transformeert het huidige laboratorium naar een werkende proefopstelling op 1 januari 2018, en levert CCIII als nieuwe werkende voorziening op 1 januari 2019 op en draagt het dan over aan de staande organisatie. Dit wordt in de mijlpalenplanning en het realisatieplan uitgewerkt. Wij doen ook een voorstel voor professionalisering van de programmaorganisatie CCIII.	Theo, 10.2.e 10.2.e	Besluit	12.04.2017
2	**Hoofdlijnennotitie CCIII v. 04**			
	Driehoek is akkoord met de notitie. Doel is commitment te verwerven van korpsleiding op de koers en invulling te geven aan werving personeel.	Driehoek	Besluit	25.04.2017
3	**Organisatorische inbedding CCIII**			
	Het lab met de uitbreiding met personeel van DLOS en de eenheden blijft in afwachting van een daarover te nemen definitief besluit, organisatorisch ingebed in de sector DLOS, rechtstreeks onder leiding van Marjolein.	Marjolein	Besluit	25.04.2017
4	**Keuring**			
	De driehoek besluit conform beslisadvies d.d. 6 april 2017 om een verkenning uit te voeren naar de mogelijkheden om de keuring uit te besteden, en geeft daarvoor opdracht aan het programma. Opties worden verkend en zo mogelijk voorzien van kostenplaatje aan driehoek voorgelegd.	10.2.e	Besluit	29.04.2017
5	**Begeleidingscommissie**			

	Voorstel voor samenstelling begeleidingscommissie is akkoord. Vaste leden kunnen worden vervangen. Marjolein Smit voorzitter 10.2.e FIOD 10.2.e KMar 10.2.e AIVD 10.2.e 7-12 10.2.e 10.2.e DICT 10.2.e IM 10.2.e OM 10.2.e 7-12 10.2.e DLR 10.2.e programma CCIII 10.2.e programma CCIII 10.2.e programma CCIII	Marjolijn		19.06.2017
	10.2.e zal de vergaderingen van de begeleidingscommissie notuleren.	Marjolein	Besluit	19.06.2017

From 10.2.e @politie.nl>
Subject **Hoofdlijnennotitie CCIII**
To 10.2.e @politie.nl>
Date 22 juni 2017 10:36:48 CEST

Ho 10.2.e

Afgelopen maandag hebben wij in het Driehoeksoverleg CCIII (Theo, Marjolein, programma) kort gesproken over de hoofdlijnennotitie.

Met Theo en Marjolein hebben we afgesproken dat we de notitie niet langs het BBVO laten gaan, maar rechtstreeks naar het KMTO.

Wel moeten we even een overleg inplannen met 10.2.e (achternaam ben ik even kwijt) om over de bedrijfsvoeringsaspecten te praten voordat het KMTO plaatsvindt.

Kun jij misschien nagaan wanneer we het stuk kunnen agenderen op het KMTO? Dan kunnen we dat proces namelijk ook in gang zetten.

Dank alvast!
Groet,
10.2.e

Van: 10.2.e via YouTube [mailto:10.2.e @youtube.com]
Verzonden: vrijdag 23 juni 2017 12:58
Aan: 10.2.e @politie.nl>
Onderwerp: 10.2.e sent you a video: "Deskundigenbijeenkomst wetsvoorstellen vastleggen kentekengegevens en computercriminaliteit"

10.2.e has shared a video with you on YouTube

Deskundigenbijeenkomst wetsvoorstellen vastleggen kentekengegevens en computercriminaliteit

by EersteKamer

De Eerste Kamercommissie voor Veiligheid en Justitie organiseerde op dinsdag 20 juni 2017 een deskundigenbijeenkomst over de wetsvoorstellen Vastleggen en bewaren kentekengegevens door politie (33542) en Computercriminaliteit III (34372). In de bijeenkomst kwamen achtereenvolgens drie thema's aan de orde, te weten:
- noodzaak en belang van de voorgestelde wetgeving
- te respecteren privacywetgeving, databescherming en Europees kader, en
- uitvoerbaarheid en handhaafbaarheid.

From 10.2.e ' <10.2.e @politie.nl>

Subject **FW: 10.2.e sent you a video: "Deskundigenbijeenkomst wetsvoorstellen vastleggen kentekengegevens en computercriminaliteit"**

To 10.2.e " <10.2.e @politie.nl>, 10.2.e '
<10.2.e @klpd.politie.nl>, 10.2.e ' <10.2.e @politie.nl>, 10.2.e '
<10.2.e @politie.nl>, 10.2.e " <10.2.e @politie.nl>, 10.2.e '
<10.2.e @politie.nl>, "Plas, Theo van der (T.G.)" <10.2.e @politie.nl> Date 23 juni 2017 12:59:44 CEST

Beste allemaal,

Bijgaand de video van de bijeenkomst van afgelopen maandag. Alvast een goed weekend!

10.2.e

Van: 10.2.e @eerstekamer.nl>
Verzonden op: vrijdag 23 juni 2017 1:57 p.m.
Aan: "Plas, Theo van der (T.G.)" 10.2.e @politie.nl>,"10.2.e @politie.nl>
Onderwerp: Conceptverslag deskundigenbijeenkomst privacy

Geachte heer Van der Plas, geachte heer 10.2.e ,

Bijgaand treft u het conceptverslag aan van de deskundigenbijeenkomst privacy. Desgewenst kunt u correcties in de weergave van uw woorden aanbrengen. Ik verzoek u deze correcties **uiterlijk vrijdag 7 juli 2017 om 18.00 uur** aan mij door te geven. Hebben wij op het moment van het verstrijken van de correctietermijn geen reactie van u vernomen, dan gaan wij ervan uit dat u instemt met de weergave van uw woorden. Wanneer u correcties aanbrengt, gelieve dit duidelijk in de tekst aan te geven.

Het conceptverslag is opgesteld door de Dienst Verslag en Redactie (DVR) van de Tweede Kamer. Bij de beoordeling van correctievoorstellen hanteert de DVR het criterium 'gezegd is gezegd'. Correcties die een inhoudelijke wijziging van het gesproken woord tot gevolg hebben, zijn dan ook niet toegestaan. De DVR hanteert tevens als regel dat het schrappen of het toevoegen van tekst of tekstgedeelten ter verduidelijking van hetgeen is gezegd, niet is toegestaan. U kunt dus in beperkte mate wijzigingen aanbrengen.

Mocht u over het bovenstaande nog vragen hebben, dan hoor ik dat graag.

Ik dank u nogmaals hartelijk voor uw waardevolle bijdrage. De commissie V&J kijkt terug op een interessante en geslaagde bijeenkomst.
Met vriendelijke groet,

10.2.e
9

Eerste Kamer *der Staten-Generaal*
Binnenhof 22
Postbus 20017
2500 EA Den Haag
M +31 (0)6 10.2.e
F +31 (0)70 10.2.e
E
10.2.e @eerstekamer.nl **I**
www.eerstekamer.nl

Van: 10.2.e
Verzonden: vrijdag 23 juni 2017 14:36
Aan: 10.2.e ; 10.2.e 9
Onderwerp: Fwd: Conceptverslag deskundigenbijeenkomst privacy
Bijlagen: Conceptverslag deskundigenbijeenkomst privacy.docx

Ter info.
Gr
10.2.e

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Zie opmerking bij document 718 (en 720)

Van: 10.2.e
Verzonden: vrijdag 23 juni 2017 16:39
Aan: Plas, Theo van der (T.G.); Smit-Arnold Bik, Marjolein (C.P.M.)
CC: 10.2.e 10.2.e); 10.2.e 10.2.e
); 10.2.e 10.2.e 10.2.e 10.2.e
Onderwerp: Definitief concept consultatiereactie Besluit Onderzoek in Geautomatiseerd Werk
Bijlagen: Consultatiereactie BOGW def concept 23-06-2017.docx

Beste Theo en 10.2.e

Bijgaand treffen jullie aan het definitieve concept voor de consultatiereactie op het Besluit Onderzoek in Geautomatiseerd Werk.

Hierin is geprobeerd om alle opmerkingen zo goed als mogelijk te verwerken. Uiteindelijk zal niet iedereen het met elk punt eens zijn, maar naar de mening van het programma CCIII is dit op dit moment het meest haalbare. Alle belangrijke punten zijn volgens ons hierin benoemd.

Voor wat betreft de punten die niet zijn overgenomen of anders zijn verwoord dan in de reacties die we hebben ontvangen, kunnen we uitleggen waarom dit is gebeurd.

Voordat deze versie de lijn in gaat richting de KC, hoor ik graag of jullie akkoord zijn met dit stuk. Ik heb met 10.2.e afgesproken dat hij en 10.2.e er maandag ook nog naar kijken. Pas na verwerking van eventuele opmerkingen van jullie kant en na jullie akkoord zal het stuk door 10.2.e verder het proces worden doorgeleid.

Rest mij jullie een goed weekend te wensen. Het was weer een interessante week!

Met vriendelijke groet,
10.2.e

Onderwerp
Consultatie Ontwerpbesluit Onderzoek in Geautomatiseerd Werk

Adresregels
Aan de Staatssecretaris van Veiligheid en Justitie
Dr. K.H.D.M. Dijkhoff
Directie Wetgeving en Juridische Zaken
Directeur Wetgeving en Juridische Zaken
Mr. A.G. van Dijk
Postbus 20301
2500 EH Den Haag

Organisatieonderdeel
Portefeuillehouder Digitalisering en Cybercrime
Programma CCIII

Behandeld door
10.2.e

Functie
Operationeel Specialist

Telefoon
06-10.2.e

E-mail
10.2.e@politie.nl

Ons kenmerk
Klik hier als u tekst wilt invoeren.

Uw kenmerk
2068042

In afschrift aan
Klik hier als u tekst wilt invoeren.

Datum
23 juni 2017

Bijlage(n)
0

Pagina
1

Geachte Excellentie,

Van het door u bij brief van 10 mei jl. ter consultatie aangeboden Ontwerpbesluit Onderzoek in een geautomatiseerd werk (hierna: het Ontwerpbesluit), heb ik met belangstelling kennis genomen.

Voor het feit dat de Politie in ruime mate betrokken heeft mogen zijn bij de besprekingen over de totstandkoming van dit Ontwerpbesluit zeg ik u dank.

Niettemin nopen de tekst van het Ontwerpbesluit en de daarbij behorende Nota van Toelichting (hierna: de NvT) mij tot het maken van de volgende opmerkingen.

1. Logging

In hoofdstuk 4 (Geautomatiseerde vastlegging van gegevens over de uitvoering van een bevel) van het Ontwerpbesluit worden regels gesteld over logging. De politie is vanuit het perspectief van transparantie voorstander van het op een adequate en toetsbare manier uitvoeren van de logging. Dit om toezicht achteraf op de uitgevoerde handelingen door de Inspectie Veiligheid en Justitie (IV&J) en de rechter mogelijk te maken.

Uit de NvT is niet duidelijk op te maken welke verschillende vormen van logging gegenereerd worden op de technische infrastructuur van de politie en hoe deze verschillende vormen van logging in verhouding tot elkaar staan. Ter illustratie volgen hieronder een aantal zinsneden uit de NvT:

1. Zowel tijdens de uitvoering van het bevel van de officier van justitie als na afloop hiervan kan worden vastgesteld of een handeling of bewerking heeft plaatsgevonden die van invloed is op de betrouwbaarheid en integriteit van de vastgelegde gegevens (pagina 12).
2. De logging is ten eerste bedoeld voor interne controle van de tijdens de onderzoeksfase verrichte handelingen (pagina 12).
3. Daarnaast maakt de bewijslogging het mogelijk om de met een technische hulpmiddel geregistreerde gegevens achteraf te verantwoorden in een strafzaak (pagina 12).
4. Er wordt gelogd op het niveau van autorisatie, op het niveau van de verrichte onderzoekshandelingen en op het niveau van de werking van het systeem (pagina 19).
5. De gelogde gegevens moeten worden verwijderd zodra deze niet langer noodzakelijk zijn voor het doel van het onderzoek(pagina 19).

Bovenstaande punten, in combinatie met de verdere tekst in de NvT, maken niet helder welke vorm van logging dient voor bewijsvergaring en welke voor interne controle. Ook wordt niet duidelijk wat het onderscheid is tussen de verschillende vormen van logging die plaatsvinden op de technische infrastructuur van de politie. Dit is wel noodzakelijk om helderheid te verschaffen over het doel van de verschillende vormen van logging.

Voorgesteld wordt een duidelijker onderscheid van de verschillende vormen van logging op te nemen in de NvT. Hierbij valt te denken aan de volgende vormen:

a) Inzetlogging

Inzetlogging heeft betrekking op alle logging die specifiek wordt uitgevoerd om de verrichte handelingen vast te leggen. Dit betreft niet alleen het (automatisch) vastleggen van het beeldscherm en de toetsaanslagen van de opsporingsambtenaar, maar ook het vastleggen van de communicatie tussen de technische infrastructuur en het geautomatiseerde werk, het vastleggen van gebruikte scripts, software versies en het journaal van de opsporingsambtenaar. Logging zal zoveel mogelijk geautomatiseerd plaatsvinden. Niet alles kan automatisch worden vastgelegd; procedures zullen ervoor moeten zorgen dat dat wat niet automatisch vastgelegd kan worden, handmatig vastgelegd wordt. Uiteindelijk zal alleen de inzetlogging die betrekking heeft op een technisch hulpmiddel aan het strafdossier worden toegevoegd.

b) Systeemlogging

Systeemlogging wordt voornamelijk gebruikt voor het signaleren, onderzoeken en verhelpen van problemen m.b.t. veiligheid, betrouwbaarheid en beschikbaarheid in de technische infrastructuur van de politie. Systeemlogging wordt automatisch door alle gebruikte systemen gegenereerd, centraal verzameld en vastgelegd. De politie maakt voor systeemlogging gebruik van standaard protocollen. Hierdoor kan het voorkomen dat niet alle logregels bij de centrale verzameling worden afgeleverd. De centraal verzamelde systeemlogging bevat logregels van alle systemen binnen de technische infrastructuur. Veel systemen binnen de technische infrastructuur van de politie worden voor de uitvoering van meerdere bevelen tegelijkertijd gebruikt, waardoor afzonderlijke logregels niet aan een specifiek bevel kunnen worden toegewezen.

De gegevens worden wel bewaard om aan de eisen van transparantie te kunnen voldoen. Indien tijdens de behandeling van een zaak of tijdens audits van de Inspectie V&J vermoedens zijn van ongeautoriseerde toegang tot systemen en/of oneigenlijk gebruik van systemen dat heeft kunnen leiden tot het in twijfel trekken van de verrichte handelingen en het hiermee vergaarde bewijs, zullen de logregels ten tijde van het uitvoeren van het betreffende bevel separaat veiliggesteld kunnen worden.

c) Authenticatie- en Authorisatielogging

Authenticatie- en authorisatielogging zijn een subcategorie van systeemlogging. Daarmee zijn zij onderhevig aan de beperkingen van systeemlogging. Echter doordat authenticatie- en autorisatielogging van groot belang zijn voor de controle op de toegang tot een technisch hulpmiddel, is het noodzakelijk de authenticatie- en authorisatielogging die betrekking heeft tot de toegang tot een technisch hulpmiddel apart uit te voeren. De aflevering van deze logregels moet gegarandeerd zijn. De technische infrastructuur bij de politie wordt zodanig ingericht dat dit mogelijk is.

d) Bewijslogging

In de NvT wordt melding gemaakt van bewijslogging. Het gaat hier dan om de vastlegging van de door een technisch hulpmiddel geregistreerde gegevens. Naar de mening van de politie gaat het hier om het opslaan van bewijs. Het verdient aanbeveling om in de NvT helderheid te verschaffen of met bewijslogging inderdaad het opslaan van bewijs wordt bedoeld.

2. Componentkeuring

Voor de keuring van technische hulpmiddelen kan keuring van afzonderlijke componenten de keuring aanzienlijk eenvoudiger maken. Dit kan bijvoorbeeld gelden als de toevoeging van een component voor een specifiek apparaat niet direct leidt tot een complete herkeuring van het technische hulpmiddel, aangezien deze toevoeging niet leidt tot een wijziging van de functionaliteit van het technisch hulpmiddel. Het is uitdrukkelijk niet de bedoeling dat met deze vorm van componentkeuring een nieuw technisch hulpmiddel wordt samengesteld. In de NvT is niet opgenomen dat een dergelijke componentkeuring is toegestaan. De politie is voorstander van het opnemen van een dergelijke componentkeuring, aangezien hierdoor een snellere (her)keuring kan plaatsvinden. Dat is in het belang van een effectieve opsporing in een zeer dynamische en veranderlijke digitale wereld.

3. Keuring achteraf

De betreffende artikelen in het Ontwerpbesluit en de toelichting in de NvT laten de mogelijkheid open dat er inzetten gaan plaatsvinden met zowel geen keuring vooraf als geen keuring achteraf, beide ter beoordeling van de Officier van Justitie. Theoretisch zou dit kunnen leiden tot het nooit keuren van een hulpmiddel. De politie is de mening toegedaan dat de hoofdregel moet zijn inzet met een vooraf gekeurd technisch hulpmiddel. Dit mede gelet op de nadruk tijdens de wetsbehandeling op de keuring en het onafhankelijke toezicht. Slechts in uitzonderlijke gevallen kan keuring achteraf plaatsvinden.

4. Functionaliteiten

Artikel 8 van het Ontwerpbesluit bepaalt dat een technisch hulpmiddel zodanig is ingericht dat de werking ervan kan worden beperkt tot de in het bevel vermelde functionaliteit of tot bepaalde functionaliteiten. De Keuringsdienst stelt tijdens de keuring een handleiding op voor het gebruik van het hulpmiddel, waarbij wordt aangegeven welke instellingen bij gebruik moeten worden aangevinkt. De politie is de mening toegedaan dat dit artikel de mogelijkheid openhoudt om in bepaalde gevallen een technisch hulpmiddel in te zetten, ook indien de werking vanuit de aard van het hulpmiddel niet volledig beperkt kan worden tot het tot de in het bevel vermelde functionaliteit of functionaliteiten. Bij functionaliteiten valt dan te denken aan bijvoorbeeld camera, microfoon en gps-module. Een nadere inperking binnen zo'n functionaliteit is technisch moeilijk uit te voeren. De beperking tot het overdragen van de in het bevel genoemde gegevens kan dan plaatsvinden door een filtering op basis van technische criteria door het technische team, alvorens de data wordt overgedragen aan het tactische onderzoeksteam. Het bevel biedt, in combinatie met de functiescheiding, waarborgen dat geen andere informatie dan waartoe het bevel strekt, zal worden gebruikt. Vanzelfsprekend zal hiervan ook proces-verbaal worden opgemaakt.

Met opmerkingen 12-14

Met opmerkingen [12-14 .

5. Opnemen communicatie

Artikel 9 lid 2 stelt dat het opnemen van telecommunicatie beperkt is tot een nummer. Dit is technisch vaak niet mogelijk. Digitale communicatievormen lopen steeds minder via de traditionele nummers. De term nummer is daardoor niet toekomstbestendig. Voorgesteld wordt om het Ontwerpbesluit een meer neutralere formulering wordt opgenomen waardoor het artikel meer toekomstbestendig is.

Met opmerkingen 12-14

Met opmerkingen 12-14

6. Verwijdering van een technisch hulpmiddel

In artikel 28 van het Ontwerpbesluit worden regels gesteld over het verwijderen van een technische hulpmiddel. Uit het artikel en de bijbehorende passages in de NvT wordt niet duidelijk op welke gronden tot verwijdering over kan worden gegaan. De politie adviseert een passage op te nemen in de NvT waarin wordt aangegeven op basis van welke bevoegdheid over gegaan kan worden tot het verwijderen van een technisch hulpmiddel na afloop van een bevel tot binnendringen. Hierbij valt te denken aan het opnemen van een passage waarin wordt aangegeven dat in het bevel tot binnendringen een termijn van maximaal 3 weken wordt opgenomen waarbinnen het technisch hulpmiddel na afloop van

Onderwerp
Consultatie Ontwerpbesluit Onderzoek in Geautomatiseerd Werk

Datum
23 juni 2017

Pagina
4 van 5

het bevel tot binnendringen wordt verwijderd, met daarbij een proces verbaal van redenen waarom verwijdering niet mogelijk was binnen het oorspronkelijke bevel en dat het nieuwe bevel alleen geldt voor binnendringen met als doel het verwijderen van het technisch hulpmiddel.

7. Geheimhouding

In het Ontwerpbesluit worden veel regels gesteld met als doel de uitvoering van de wet zo transparant mogelijk te maken, bijvoorbeeld door uitgebreide logging. De Keuringsdienst wordt volledig ingelicht en meegenomen in het gehele proces, de Inspectie Veiligheid en Justitie onbelemmerde toegang tot alle relevante informatie en de rechter of een gespecialiseerde Rechter Commissaris zal volledig op de hoogte worden gebracht van alle relevante informatie. Hoewel de politie een voorstander is van deze transparantie mag dit er niet toe leiden dat informatie over de gebruikte middelen, de werkwijze en/of de tactische mogelijkheden van het technisch team, zoals mede in de logging is vastgelegd, openbaar worden gemaakt. De in de NvT vermelde mogelijkheid tot het inzetten van 187d Sv procedure kan door de rechter gebruikt worden om deze geheimhouding te bewerkstelligen. Om een voldoende mate van geheimhouding te kunnen garanderen moet echter aansluiting worden gezocht bij de geheimhoudingsprocedures zoals die ook gelden binnen het WOD-domein (Werken Onder Dekmantel). Ik adviseer om in de definitieve tekst van de Ontwerpbesluit deze aansluiting te zoeken.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,

E.S.M. Akerboom

korpschef

Onderwerp
Consultatie Ontwerpbesluit
Onderzoek in Geautomatiseerd Werk

Klik hier als u tekst wilt invoeren.
www.politie.nl

Datum
23 juni 2017

Pagina
5 van 5

Van: 10.2.e
Verzonden: woensdag 28 juni 2017 16:27
Aan: Plas, Theo van der (T.G.); 10.2.e
Onderwerp: FW: Hoofdlijnennotitie CCIII tbv BOO 12 mei
Bijlagen: FORMAT OPLEGNOTA BOO CCIII 28 april 2017.doc; hoofdlijnennotitie voorziening tot binnendringen v0.5.pdf

Hoi Theo,

Dit is de versie die naar het BOO is gezonden.

Met vriendelijke groet,
10.2.e

OPLEGNOTA BREED OPERATIEN OVERLEG (BOO)

Agendapunt: < in te vullen door secretaris > **Datum:** < in te vullen door secretaris >

Onderwerp: **Hoofdlijnennotitie CCIII**

Aangeboden door

☐ **Lid KL, referent** <naam invullen>
☑ **Politiechef: J. van den Berg**
☐ **Directeur:** <naam invullen>
☐ **Programmamanager:** <naam invullen>

Steller: 10.2.e , 0610.2.e

☑ **Opinievormend** ☑ **Ter implementatie** ☐ **Ter kennisname**

Gevraagd

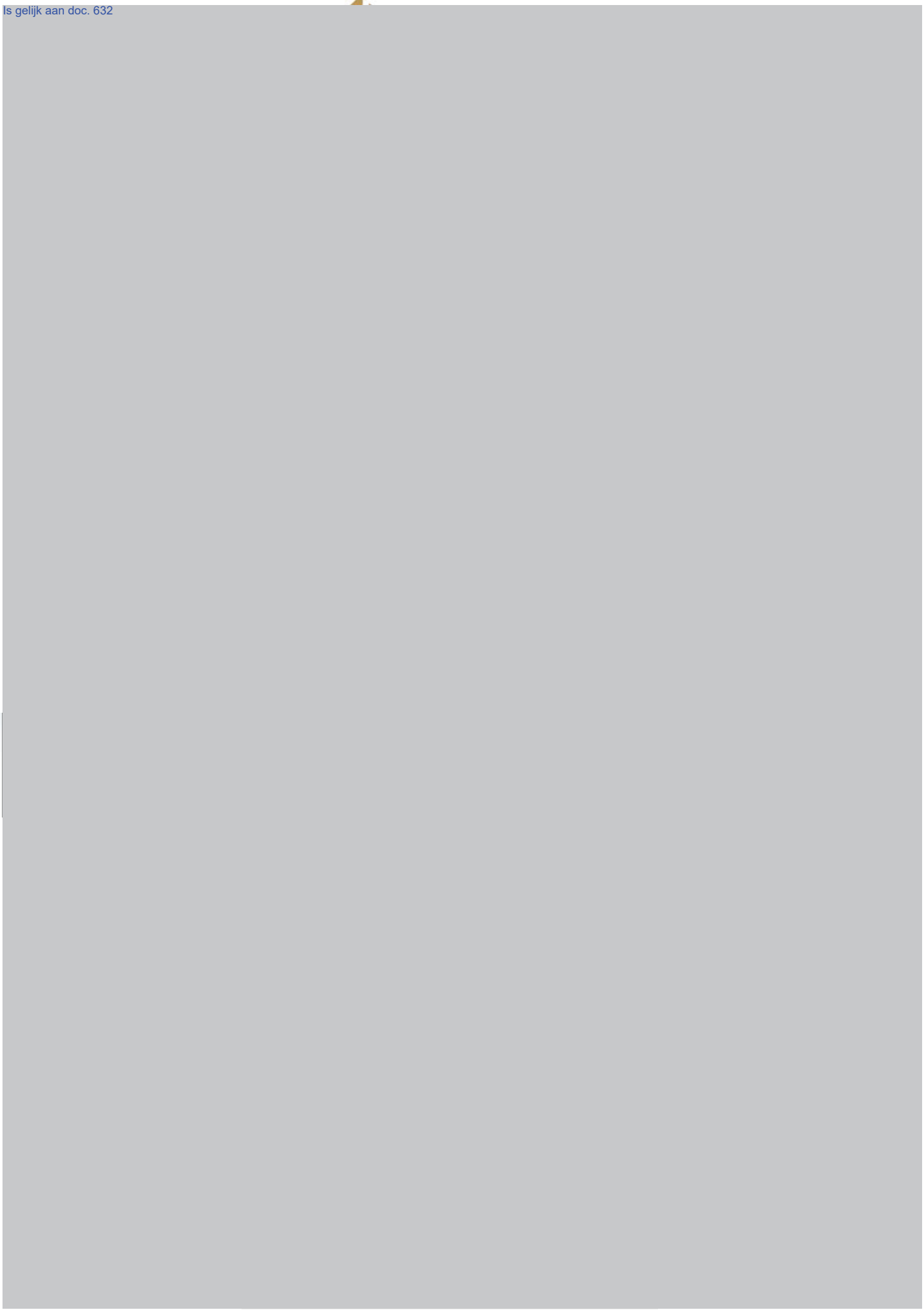
Zie voor def. versie doc. 745

Zie voor def. versie doc. 745

Zie voor def. versie doc. 745

Zie voor def. versie doc. 745

Is gelijk aan doc. 632



Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632

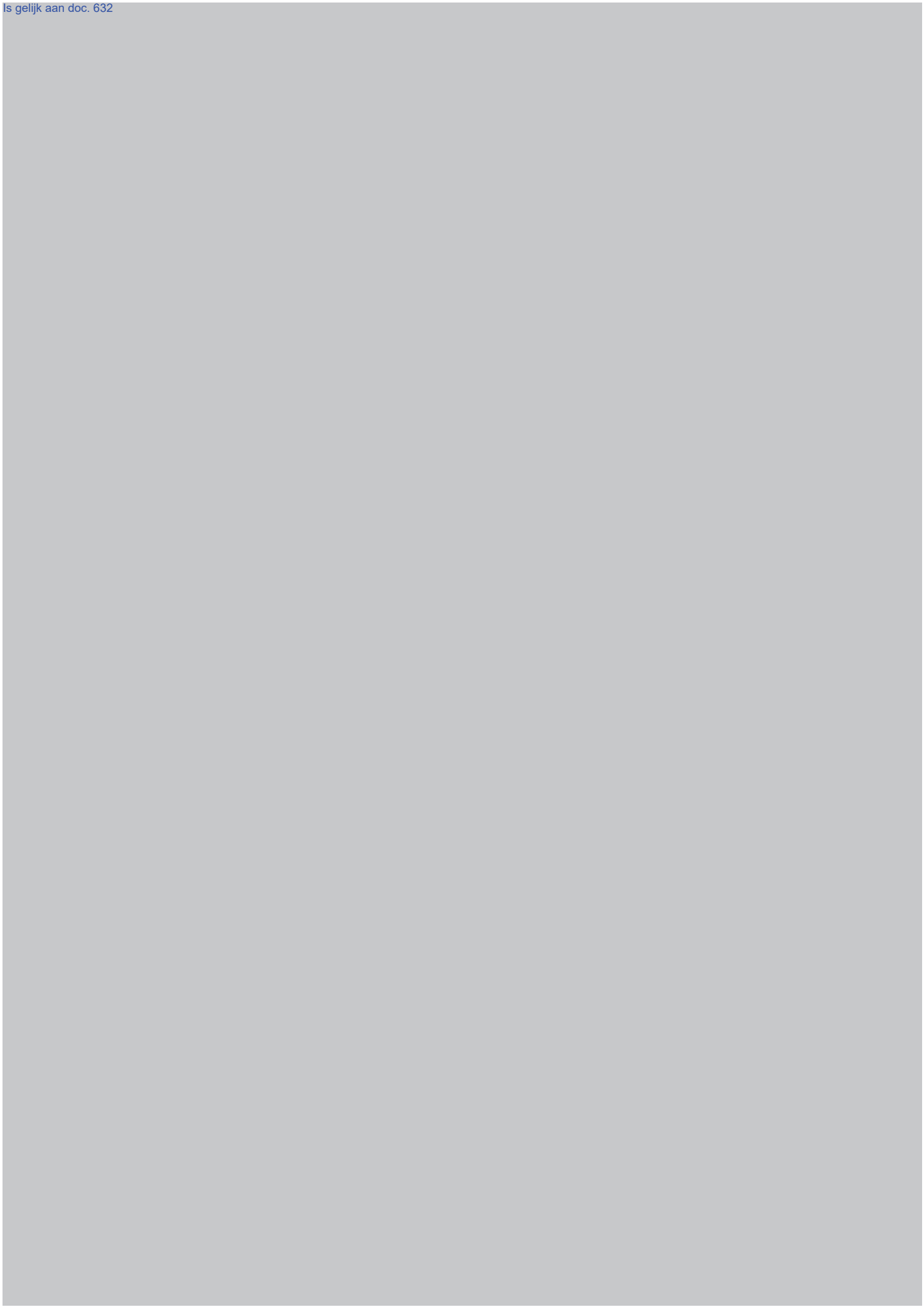
Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632



Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632

Is gelijk aan doc. 632

Van: 10.2.e
Verzonden: woensdag 28 juni 2017 16:31
Aan: Plas, Theo van der (T.G.); 10.2.e
Onderwerp: FW: Acties/Afspraken BOO 12 mei, inzake 'Hoofdlijnennotitie Computercriminaliteit III'

Dit is uiteindelijk in het verslag gekomen.

Gr.

10.2.e

Van: 10.2.e
Verzonden: woensdag 28 juni 2017 18:13
Aan: 10.2.e @politie.nl>
Onderwerp: Definitief verslag BOO 12 mei

Hoi 10.2.e ,

Heb jij voor mij toevallig het definitieve verslag van het BOO van 12 mei?

Dank je wel alvast!
Met groet,
10.2.e

Van: 10.2.e **Namens** 10.2.e
Verzonden: donderdag 29 juni 2017 10:03
Aan: 10.2.e @politie.nl>
Onderwerp: RE: Definitief verslag BOO 12 mei

Hoi 10.2.e

Hierbij!

Groet,
10.2.e

Besluitenlijst BREED OPERATIONEEL OVERLEG (BOO)

Datum: 12 mei 2017

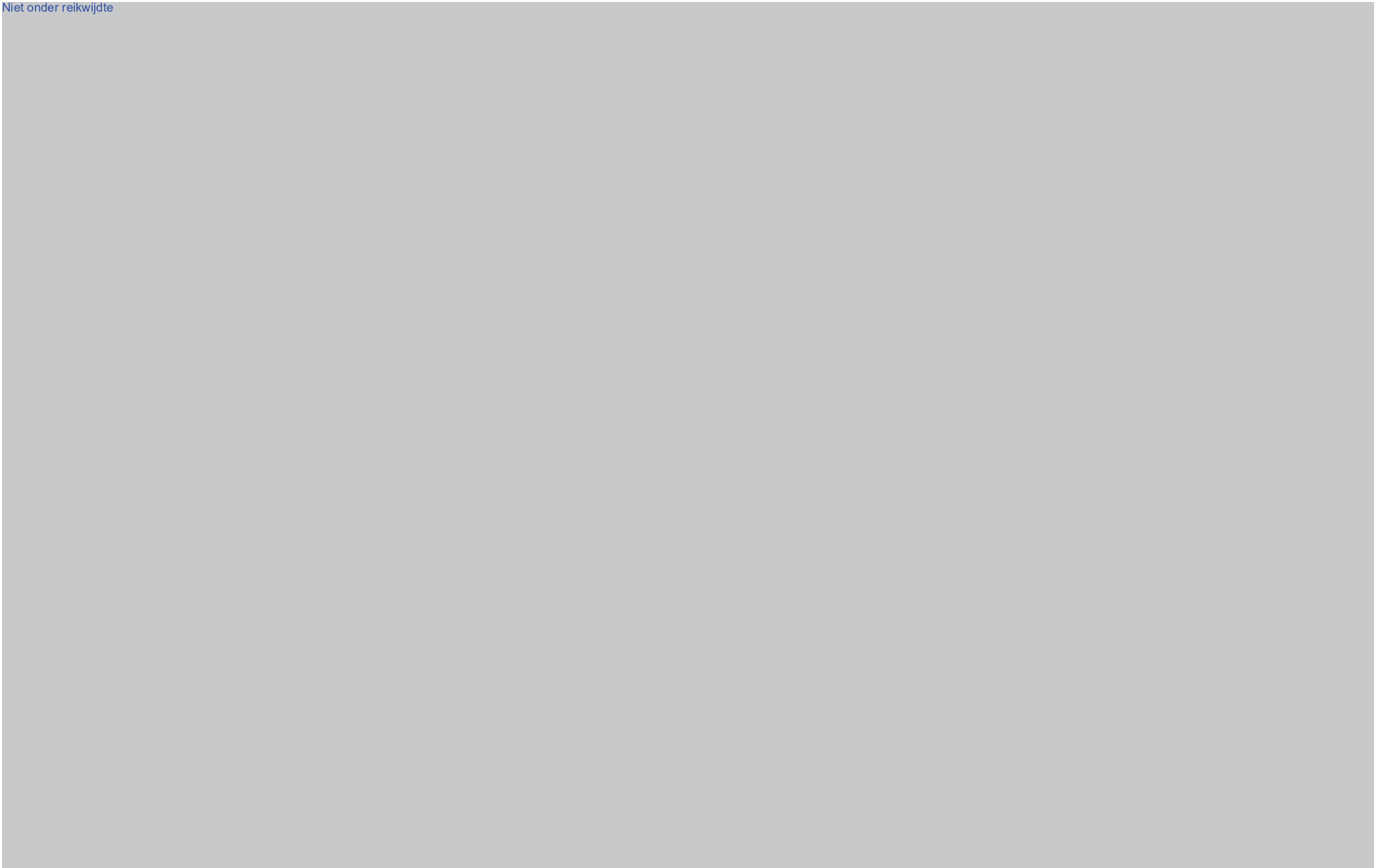
Aanwezigen: mw. Huyzer, (voorzitter), 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e 10.2.e dhr. Woelders, 10.2.e en 10.2.e (verslag)

Afwezigen: 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e , 10.2.e

Gasten: 10.2.e t, 10.2.e , 10.2.e (directie Finance & Control), 10.2.e en 10.2.e (bij agendapunt 4) en 10.2.e (bij agendapunt 5)

Pnt	Verantwoordelijke	Onderwerp	Besluit	Toelichting
Ter informatie				
1	10.2.e	Opening		De voorzitter opent de vergadering om 9:00 uur
2	Niet onder reikwijdte			

Niet onder reikwijdte



	Niet onder reikwijdte			
Ter b				
3				
4				
5	Dhr. Van der Plas	Hoofdlijnennotitie Computercriminaliteit III	Het BOO neemt kennis van: - de notitie over het programma CCIII en specifiek de implementatie van de bevoegdheid tot 'heimelijk op afstand binnendringen in een geautomatiseerd werk'; - de fasering die in het programma is aangebracht in een fase 1 van experimenteren (tot 1 juli) die leidt tot een	10.2.e en 10.2.e sluiten aan om dit agendapunt toe te lichten. De achtergrond en komende tijdlijn wordt benoemd. De HRM-component ligt vandaag voor. Gevraagd wordt een keuze te maken tussen 2 scenario's: 1. de Landelijke Eenheid wer7-12 fte voor de centrale voorziening. Vanuit de eenheden wordt daarnaast formatieruimte ter grootte v7-12 fte afgeroomd ten behoeve van de Landelijke Eenheid; 2. de Landelijke Eenheid wer7-12 fte voor de centrale voorziening. Vanuit de eenheden wordt daarnaast in tota7-12 fte door een

			nader onderbouwd realisatieplan voor fase 2 (vanaf 1 juli), waarin de PIOFACH aspecten concreet zijn uitgewerkt. Dit definitieve realisatieplan wordt voor 1 juli aan het KMT ter besluitvorming voorgelegd; - de keuze om de voorziening in ieder geval voorlopig centraal in te richten, vanwege de politiek-bestuurlijke gevoeligheden rond deze bevoegdheid en vanwege de complexiteit en potentieel hoge kosten van de implementatie; - het feit dat er op dit moment in fase 1en 2 onvoldoende capaciteit beschikbaar is in de voorziening om de benodigde experimenten uit te voeren die noodzakelijk zijn om tijdig een voldoende onderbouwd plan van aanpak voor de implementatie op te kunnen stellen; - het feit dat het lab CCIII in eerste instantie als een Eigen Beheerde Organisatie (EBO) is ingericht en dat de definitieve voorziening CCIII in de toekomst zal worden ingepast in de infrastructuur van de Nationale Politie. Het BOO maakt de keuze voor scenario 2: *"De Landelijke Eenheid wel* 7-12 *fte voor de centrale voorziening. Vanuit de Eenheden wordt daarnaast in totaal* 7-12 *fte door een gekwalificeerde medewerker tewerkgesteld bij de voorziening. Hiermee wordt, gezamenlijk met de partners, een voorziening van* 7-12 *gecreëerd. Na 2 jaar keren de medewerkers terug naar hun eenheid, waardoor de kennisontwikkeling van de eenheden een impuls krijgt. Het is dus lonend om te investeren voor de eenheden. Terugkeer zal gefaseerd plaatsvinden om een braindrain van de nieuwe eenheid te voorkomen".*	gekwalificeerde medewerker tewerkgesteld bij de voorziening. Er wordt kort gediscussieerd over de keuze voor deze 7-12 de vraag of er formatieruimte is geclaimd per wet en de scenario's. Het BOO is akkoord met scenario 2, 12-14 Na de zomer ziet het BOO deze koers graag terug op de agenda. **Actie: dhr. v.d. Plas** Daarnaast wordt aandacht gevraagd voor de werving van het personeel. Een helder profiel voor de medewerker is belangrijk. Geadviseerd wordt 7-12 hierin mee te nemen. Afgesproken wordt het onderwerp Cyber ieder kwartaal te agenderen voor het BOO. Op deze manier kan het BOO aangehaakt blijven bij de ontwikkelingen op dit gebied, zoals de ervaringen van de cyberteams welke al in werking zijn. **Actie: dhr. v.d. Plas / secretaris BOO**

			12-14 [redacted] Na de zomer komt deze koers op de agenda van het BOO. Het BOO besluit op basis van bovenstaande keuze dat: - het sectorhoofd van de DLOS van de Landelijke Eenheid de opdracht krijgt om de voorziening op basis van deze notitie en het realisatieplan in te richten en tot werking te brengen; - er gestart wordt met de centrale werving. Eenheden (incl. DLOS) te vragen vacatureruimte ter beschikking te stellen; - daartoe een landelijke wervingscampagne wordt gestart, waarbij medewerkers van de eenheden mee kunnen solliciteren.	
6	Niet onder reikwijdte	[redacted]		

7	Niet onder reikwijdte
8	
Ter	
9	
10	

Actiepuntenlijst BOO

nr.:	Oorsprong:	Verantwoordelijke:	Onderwerp:	Toelichting:	status / deadline:
1.	BOO 20160617	Niet onder reikwijdte			
2.	BOO 20160617				
3.	BOO 20170331				
4.	BOO 20170512	Dhr. v.d. Plas	CCIII	Een visie ontwikkelen met een nadere duiding en koers hoe we duurzaam tot stand kunnen brengen dat de medewerkers terugkeren naar de eenheden	
5.	BOO 20170512	Dhr. v.d. Plas	Cyber	Cyber ieder kwartaal op agenda BOO – zo kan het BOO aangehaakt blijven bij de ontwikkelingen op dit gebied	augustus 2017
6.	BOO 20170512	Niet onder reikwijdte			
7.	BOO 20170512				

Van: 10.2.e
Verzonden: donderdag 29 juni 2017 10:12
Aan: Plas, Theo van der (T.G.) 10.2.e @politie.nl>; 10.2.e
@politie.nl>
Onderwerp: FW: Definitief verslag BOO 12 mei

Hoi 10.2.e

Hierbij het verslag van 12 mei.

Gr.
10.2.e

Is gelijk aan doc. 727

Is gelijk aan doc. 727

Is gelijk aan doc. 727

Is gelijk aan doc. 727

Is gelijk aan doc. 727

Is gelijk aan doc. 727

Van: 10.2.e
Verzonden: donderdag 29 juni 2017 13:50
Aan: 10.2.e
CC: 10.2.e 10.2.e 10.2.e 10.2.e
Onderwerp: tekstvoorstel

Opvolgingsmarkering: Opvolgen
Markeringsstatus: Gemarkeerd

Hoi 10.2.e

Zoals afgesproken hierbij een tekstvoorstel. Ik neem 10.2. en 10.2 meteen even mee in de cc.

Tekstvoorstel:

Laat maar even weten of dit zo kan.

Met vriendelijke groet,
10.2.e

Van: 10.2.e
Verzonden: donderdag 29 juni 2017 18:06
Aan: 10.2.e @politie.nl>
Onderwerp: Antw: tekstvoorstel

Ik kijk morgen gelijk even 10.2.e r.

Ik had bij lezing eerste doc vanuit mijn inhoudelijk lekenperspectief een paar vragen die jij wellicht zo kan verduidelijken

12-14

Tot zover mijn tekstopmerkingen, de twee punten van onderstaande mail kijk ik morgenochtend na

Groet, 10.2.e

From 10.2.e @politie.nl>
Subject **RE: Antw: tekstvoorstel**
To 10.2.e @politie.nl>
Date 30 juni 2017 11:03:08 CEST

Hoi 10.2.e

Dank voor je opmerkingen. Ik zal hieronder je vragen zo goed als mogelijk proberen te beantwoorden.

Groet,
10.2.e

Versterking programma-aanpak CCIII

Auteur: Programmateam CCIII

Status: concept

Versie: 0.8

Datum: 4 juli 2017

Rubricering: Groen-Politie Intern

Toelichting voor gebruik van rubricering:

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.6	27.06 2017	Eerste bespreekconcept voor programmamanagement.	
0.8	04.07.2017	Verwerking commentaar CCIII programmateam	

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie
0.6	27.06.2017	Programmaleiding CCIII en wnd. Teamleider lab CCIII	
0.8	04.07.2017	CCIII programmaleiding, wnd. teamleider lab en sleutelfiguren	

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

12-14

Opdracht Digitalisering en Cybercrime: Eigentijds politiewerk in het digitaal domein

1. Aanleiding

Nederland digitaliseert in hoog tempo. Dat biedt grote kansen voor onze economie en maatschappelijke ontwikkeling, maar brengt tegelijkertijd een toenemende dreiging mee van cybercrime en gedigitaliseerde criminaliteit. Deze dreiging is inmiddels ook realiteit gebleken als we bv. kijken naar de groei van Ransomware en naar concrete aanvallen zoals Wannacry en NotPetaya.
De politie moet mee veranderen. Dat vereist de komende tijd een extra inspanning van de organisatie en medewerkers en het vereist een andere relatie met onze burgers, onze partners en uiteindelijk ook met criminelen.

Dit is een eerste aanzet, die na de opdracht in een programmaplan zal worden omgezet.

2. De opgave

Huidige situatie: context
De context van deze opdracht ligt in de snelle digitalisering van de samenleving en de kansen en bedreigingen die dit voor de politie met zich meebrengt. Het adaptief vermogen van de politie om te ontdekken wat de politietaak moet zijn en dit te vertalen naar een handelingsperspectief binnen de organisatie, met publieke en private partners en burgers, vraagt echt een andere manier van werken. Gelet op dit domein is een belangrijk kenmerk van handelen om “er gewoon in te gaan staan” en van daar uit te ontwikkelen. Dat mechanisme is nog niet sterk aanwezig in de organisatie, waardoor er in afstemming van alle partijen, in vertaling naar consequenties of in wijze van werken nog veel te doen is.
We moeten onze organisatie aanpassen. Dat geldt voor onze manier van werken, onze HRM-processen, de IV-organisatie, maar het geldt ook voor leiderschap en diversiteit van onze collega’s. Overigens zijn wij daar niet uniek in, dit is ook bij andere partijen of organisaties het geval.

Huidige situatie: organisatieontwikkeling
Voor de start van de NP was het Programma Aanpak Cybercrime (PAC) al diverse jaren bezig met de aanpak van cybercrime en de gevolgen van digitalisering voor de politieorganisatie. Er is een groot aantal initiatieven opgestart, waaronder IRN en het LMIO, die nu nog van grote waarde zijn voor de organisatie.
Met de start van de NP en de portefeuille Digitalisering en Cybercrime is meer focus gekomen in de aanpak en hebben diverse intensiveringen plaatsgevonden.

Onder de huidige portefeuille Digitalisering en Cybercrime valt een aantal projecten en programma’s.

1. Cybercrime; met als deelonderwerpen:
    a. Bewustwording
    b. Intake en screening
    c. Informatiepositie
    d. Gereserveerde capaciteit
    e. Kennis en kunde
    f. Samenwerking
    g. Samenbrengen van deze speerpunten
2. Social-media
3. Digitaal Opsporen
4. Sensing
5. Computercriminaliteit III
6. Vrijwilligers in het cyberdomein
7. Innovatieprojecten in relatie tot digitalisering en cybercrime

Deels zijn deze te herleiden tot het ondersteunen van het bestaande proces, deels te herleiden op innovatie of nieuwe thema’s. Allen hebben gemeen dat zij (deels) gefinancierd worden vanuit de portefeuillegelden.

Op het gebied van cybercrime is het THTC in 2015 op sterkte gekomen voor de aanpak van High Tech Cybercrime. In 2016 werd de massaliteit en ontwikkelingssnelheid van cybercrime onderkend, waarop er versnelling en verbreding werd ingezet. Tegelijk zien we dat de rest van de organisatie is achtergebleven wat heeft geleid tot de cybercrimestrategie en het plan van aanpak, die in november 2016 zijn vastgesteld in het KMT.

Het doel van deze cybercrimestrategie is om te komen tot verhoogde weerbaarheid van de Nederlandse samenleving tegen cybercrime in 2020. De basis vormt een aantal uitgangspunten, zoals het vergroten van de weerbaarheid en het vertrouwen in het digitale domein als cruciaal voor de economie; het principe van eigen verantwoordelijkheid van burger, bedrijf en overheid; van de rechten van burgers op privacy en vrijheid; van het basisprincipe dat opsporing niet de oplossing is voor het probleem, maar een middel is om de rechtsstaat te borgen, straffeloosheid in het digitale domein te voorkomen en specifieke criminaliteit te doen stoppen.
De strategie om te komen tot dit doel verloopt langs zes lijnen, waaraan in samenhang wordt gewerkt. Dit zijn het vergroten van bewustwording, het verbeteren van intake en screening, het creëren van een informatiepositie op dit domein, gereserveerde capaciteit voor de bestrijding, het vergroten van kennis en kunde en tenslotte de samenwerking met (inter) nationale private en publieke partners, wetenschap en uiteraard de burger in de samenleving.
Cybercrime kan gezien worden als een concreet vliegwiel dat de organisatie kan helpen de omslag te maken die noodzakelijk is in een steeds meer gedigitaliseerde maatschappij. Tegelijk is het gezien de sterk toenemende dreiging operationeel absoluut noodzakelijk grote stappen te maken.

Dat gaat niet vanzelf. De aansluiting met de buitenwereld heeft nog niet in de breedte tot goede samenwerkingsverbanden geleid. Vaak is die bereidheid er wel en wordt zelfs verwacht dat de politie de samenwerking zoekt.

Op het gebied van digitalisering heeft de pf de afgelopen jaren vooral ingezet op het verder brengen van de organisatie op diverse actuele thema's die om aandacht vroegen. Denk hierbij aan: Digitale opsporing, social media, inzet van sensoren, invoering van heimelijk binnendringen (CC III).

Tegelijk is de constatering dat dit eigenlijk vooral noodzakelijk achterstallig onderhoud is en dat we op deze manier het huidige tempo van de digitalisering niet bijhouden en eerder achter komen te liggen. Ook omdat we niet snel genoeg innoveren, ontwikkelen, implementeren en borgen. Zelfs de eerder genoemde successen uit de PAC tijd(IRN en LMIO) zijn nog steeds niet geborgd.

De opgave
Met de snelheid waarin we nu werken en veranderen lopen we in een maatschappij die steeds sneller digitaliseert risico's, maar vooral laten we ook kansen liggen die digitalisering biedt voor onze operationele taakstelling.

Er is daarom een *turnaround* nodig naar het concept van *Think big, act small, scale fast*.
Er is een begin gemaakt, maar vraagt een hoog tempo in doorontwikkeling van gedeelde beelden, opvattingen, besluitvorming en realisatie. In samenhang met partners en publiek.

Welke rol hebben we hierin? Hoe pakken we die op en wat is de verhouding met andere publieke of private partijen? Wat mag van de burger zelf verwacht worden? Pakken we alle aangiften bijvoorbeeld aan, gaan we tegenhouden /verstoren/interveniëren? Stappen we mee in preventie en tegenhouden?
Of van heel ander orde: wat doen we bij economische spionage? Dit zijn allemaal voorbeelden van vraagstukken die nog niet beantwoord zijn.

Cybercrime en digitalisering zijn dan ook nog geen vast onderdeel van de werkprocessen en wordt nog als een nieuw werkgebied beschouwd. Teveel hoor je nog dat we ons in de digitale wereld gaan begeven, terwijl die er natuurlijk gewoon al is en wij er al deel van uitmaken. Het is ook geen naar toe bewegen, het is gaan doen.
De politie kan in de digitaliserende wereld haar plaats niet zelfstandig innemen. Er is altijd sprake van een "license to operate", de legitimiteit van ons optreden. Dat vereist verbinding met burgers en partners, verbinding met de politiek-bestuurlijke context en met ons gezag. Met oog voor veiligheid en voor privacy, in een goede balans. En een veranderstrategie die hierbij aansluit.

3. Opdrachtformulering

De opdracht luist:

1. **Stimuleer de organisatieontwikkeling dusdanig dat digitalisering en cybercrime een normaal onderdeel vormt van de politie(taak), waarbij we als politie flexibiliteit ontwikkelen om de steeds sneller veranderende vraag van de omgeving en van de eigen organisatie te vertalen naar een**

effectieve inzet met nieuwe interventiemethoden: soms met eigen inzet, soms met publiek-privaat partnerschap en soms bewust niet.

2. **Stimuleer, initieer en sluit aan bij een vernieuwende werking in organisatieverandering, die tegemoet komt aan de noodzakelijke flexibiliteit in de aanpak van cybercrime en gedigitaliseerde criminaliteit.**
3. **Maak daarbij gebruik van de in de huidige portefeuille D en C lopende programma's en projecten en ondersteun deze ontwikkeling, ook als die vanuit de lijn wordt ingezet**
4. **Werk toe naar een meerjarenplanning van het programma , die ook integraal financieel is onderbouwd en dekking heeft. Stel daarbij een mijlpalenplanning op voor het programma (inclusief de huidige portefeuilleonderdelen), zodat ook de voortgang van het programma en de resultaten inzichtelijk zijn**
5. **Verbind de politiewereld met de externe omgeving, zowel publiek-privaat als met de wetenschap**
6. **Maak bij de uitwerking en realisatie gebruik van talenten en van ervaring van medewerkers en doe dit o.a. in de vorm van een netwerkorganisatie en van een klankbordgroep**
7. **Bouw en onderhoud een nationaal en internationaal netwerk van stakeholders en belanghebbenden, in nauwe afstemming met de lijn, dat fundamenteel bijdraagt aan de ontwikkeling van digitalisering en cybercrime**
8. **Maak daarbij expliciet verbinding met het internationaal speelveld, samen met de lijn, en stimuleer de participatie aan internationale politieorganisaties als Europol en Interpol**
9. **Stel voor hoe de positionering van de politie moet zijn – stapsgewijs – en beschouw digitalisering en cybercrime zowel als dreiging als kans, in de consequenties en mogelijkheden voor het politiewerk.**
10. **Creëer het verhaal - *The Bigger Picture* - zodat er een eenduidig, korpsbreed, gedragen verhaal op digitalisering en cybercrime ontstaat, dat door elke medewerker van ons korps kan worden begrepen en verteld.**

4. Voorgenomen aanpak:

Het realiseren van deze opdracht vraagt voor de komende twee jaar een permanente, versnelde ontwikkeling van een onderdeel van ons vak. We staan in de wereld, zijn er onderdeel van en luisteren wat de omgeving en onze collega's daarvan ervaren en voorzien. Daar passen we onze organisatie op aan, onze werkprocessen, onze mensen en onze relaties naar publieke en private partijen. De politie bereidt zich daar ook op voor met de strategievorming 2020-25. Hierbij wordt aansluiting gezocht.

Andere vormen van werken, scrumteams en geconcentreerde inzet van bijvoorbeeld recherchekundigen met meer focus en snelheid in realisatie en opbrengst voor het werk, de operatie. Andere externen betrekken in tijdelijke constructies van arbeid, die bijvoorbeeld voor 5 jaar bij ons werkzaam zijn en dan weer de organisatie verlaten. Expertise en kennis kan alleen op die manier onze organisatie blijvend van meest recente kennis en inzichten verrijken.
De veranderstrategie van deze nieuwe manier van werken kan als een katalysator werken voor de politie. Juist op dit werkveld zal dit resultaat te zien geven. Het is hoogstwaarschijnlijk de enige manier waarop digitalisering en cybercrime met de juiste snelheid en vorm tot een normaal onderdeel van de politieorganisatie kan komen.

Dat vraagt iets van onze interne organisatie en van onze verbinding met de externe omgeving. Het vraagt om:
- de ontwikkelthema's cyber te benoemen en van alle kanten te steunen: van uitvoering tot de top en van lijn tot en met staf en PDC;
- connectiviteit met de COR en met de vakbonden: hoe doen we dit samen? Ook zij zijn zich bewust van de consequenties die cybercrime en digitalisering hebben op de arbeidsverhouding van nu en in de toekomst;
- participatie van collega's, dwars door de organisatie heen, die aan de uitwerking en uitvoering van het programma deelnemen.;
- draagvlak en participatie van partners en publiek-private verbinding en het verbeteren van de relatie met bestuursorganen en maatschappelijke instanties;
- het in verbinding brengen en stimuleren van digitalisering en cybercrime elementen in andere portefeuilles, die voor de korpsverandering van belang zijn. Daarin zit ook een belangrijk timingselement, flexibiliteit en een prioritering van bijvoorbeeld portfolio en IV-portfolio.

Een voorbeeld van dat laatste is het *programma herijking opsporing*, waar digitalisering en vernieuwing een belangrijk element is. In het Koersdocument Naar een Toekomstbestendige Opsporing en Vervolging staan richtinggevende principes en ideeën die in de uitwerking van de portefeuille Digitalisering en Cybercrime centraal staan. Daardoor is een verbinding noodzakelijk, zodat de programma's elkaar versterken.

Een aantal van de huidige thema's in de portefeuille vraagt om herijking. Kunnen deze al voor een deel aan de lijnorganisatie worden overgedragen en welke moeten juist een extra stimulans krijgen? Waar moet de energie op zitten en welke vragen meer om beheer dan ontwikkeling? Afhankelijk van de fasering van het thema zal hier de komende tijd, ook in het licht van de ontwikkelthema's, een keus in gemaakt worden en het tempo hieraan worden bijgesteld

5. Ontwikkelthema's korpsniveau Digitalisering en Cybercrime

Cybercrime en digitalisering kent een aantal thema's die – in het licht van wat hierboven is gesteld - verdere uitwerking vereisen. Ik noem er hier enkele, maar dit vereist verdere uitwerking in het programmaplan:

1. **Positionering** van de politie en management van verwachtingen, inclusief het vormen van een boegbeeldfunctie, zowel intern als extern.
2. **Bewustwording** en kennis vergroten: *what business are we in?*
3. **Weerbaarheid** vergroten bij burgers, private en publieke partijen, en als politie een eigenstandige rol innemen om dit te bereiken.
4. **Samenhang**: met andere programma's en portefeuilles, maar ook de samenwerking met wetenschap en partners, nationaal en internationaal.

Wat is ons verhaal? The bigger picture.
Er is op dit moment geen eenduidig, korpsbreed, gedragen verhaal op digitalisering en cybercrime. Op onderdelen is een strategie vastgesteld - recent nog op cybercriminaliteit – maar het grotere verhaal is niet gemaakt en daardoor ook niet voor iedereen binnen en buitende organisatie te begrijpen en na te vertellen.
Dat zal zeker geen statisch verhaal kunnen zijn, maar ook dat kan de kern zijn; wat we wel en niet doen, waar we aan werken, wat we doen en willen bereiken.
Uiteraard zal dit worden afgestemd met de strategische visievorming 2020-2025.

6. Governance:

Besluitvorming Korpsleiding en politiechefs
De besluitvorming over het beleid rond digitalisering en cybercrime vindt langs de normale lijn plaats: in KL en KMT. Om in het KMT de juiste besluitvorming te laten plaatsvinden, zal de KL- referent of de politiechef LE (afhankelijk van de reikwijdte van het gevraagde) de te nemen besluiten indienen.

Stuurgroep op het programma D en C:
Gelet op het brede strategisch belang en de verbinding met de ontwikkeling van het korps, wordt een strategische stuurgroep ingesteld op het programma. De stuurgroep staat onder leiding van de plv. KC als opdrachtgever en ziet toe dat het programma de juiste thema's omvat, de koppeling heeft naar korpsontwikkelingen en het juiste tempo en opbrengsten kent. Deelnemers zijn senior users en senior suppliers: Dick Heerschop, Henk De Jong, Jannine v.d. Berg, PJ Aalbersberg, Gerrit den Uyl/Joop de Schepper.

Vision Board: advisering
Voor de totale ontwikkeling van digitalisering en cybercrime is het voorstel om in een visionboard de ontwikkeling te laten voeden. Deelnemers vanuit de wetenschap, het bedrijfsleven, politiek en bestuur dragen bij tijdens diner pensant, thema-meetings en workshops.

Programmateam:
Het programmateam bestaat niet alleen uit een klein aantal mensen, dat vast hiervoor werkzaam is. De kracht en de werking van het programma moet ook komen van collega's, uit de eigen organisatie, die hieraan deelnemen. In het programmaplan/roadmap zal dit verder worden uitgewerkt, in verschillende vormen en stijlen.

Klankbordgroep:
Om inzichten van medewerkers mee te kunnen nemen in het programma wordt een klankbordgroep ingericht.

Verantwoordingslijnen Digitalisering en Cybercrime: sturing en verantwoording

Momenteel wordt de Governance in het korps rond portefeuilles herzien. Er zijn twee verantwoordingslijnen voor de programmadirecteur:

1. voor de huidige portefeuillewerkzaamheden Digitalisering en Cybercrime loopt die naar de (plv) politiechef LE V.d. Berg/Woelders
2. voor organisatievraagstukken die de portefeuille overstijgend zijn loopt die naar de plv. KC Van Essen.

Uiteindelijk komen beide verantwoordingslijnen samen bij de plv. KC, die ook als referent optreedt voor de portefeuille van Digitalisering en Cybercrime van de LE, als van de organisatieontwikkeling Digitalisering en cybercrime. Hij treedt ook op als rechtstreeks aanspreekpunt namens de KL. Die positionering in de Kl is zowel extern als intern van belang, vanwege de keuze om Digitalisering en Cybercrime als een strategisch thema aan te wijzen.

Bij deze governance beschrijving is uitgegaan van de huidige governance. Na besluitvorming over de nieuwe korps governance door de KL wordt de governance van het programma opnieuw vastgesteld.

7. Programmateam: werking

Om het programma Digitalisering en Cybercrime succesvol te laten zijn, is het noodzakelijk om een flexibele werkvorm te kiezen. Een klein programmateam met inzet van politie-en recherchekundigen, in combinatie met ervaren, innovatieve collega's, die met gebruikmaking van een grote netwerkorganisatie de ontwikkeling energie geven en tastbare resultaten van vooruitgang kunnen laten zien. Binnen die netwerkorganisatie zal een beroep worden gedaan op alle geledingen van de organisatie om een bijdrage te leveren.

De uitwerking van het programmaplan/roadmap hiervan zal de volgende stap zijn. Daarin zal ook de scope worden beschreven, de tijdsindicatie en de doelen/resultaten die behaald gaan worden.

Er zal een monitoringsysteem worden verbonden aan het programma, zodat er driemaandelijks een zo Smart mogelijk voortgangsgesprek over de voortgang, de resultaten en de benodigde resources en support kan worden gehouden.

Voor de verbinding met de portfoliowerking binnen het korps zal er een relatie worden gelegd met de Directie Operatien, zodat onderdelen die passen in de werking hierin kunnen worden opgenomen.

Stilstand is op dit moment natuurlijk geen optie. Het werk en de ontwikkeling gaat in hoog tempo door.

Theo van der Plas

Concept komt overeen met def. versie. Zie doc. 741.

Concept komt overeen met def. versie. Zie doc. 741.

Concept komt overeen met def. versie. Zie doc. 741.

Concept komt overeen met def. versie. Zie doc. 741.

Concept komt overeen met def. versie. Zie doc. 741.

Concept komt overeen met def. versie. Zie doc. 741.

Concept komt overeen met def. versie. Zie doc. 741.

Concept komt overeen met def. versie. Zie doc. 741.

Concept komt overeen met def. versie. Zie doc. 741.

Concept komt overeen met def. versie. Zie doc. 741.

Concept komt overeen met def. versie. Zie doc. 741.

Concept komt overeen met def. versie. Zie doc. 741.

Concept komt overeen met def. versie. Zie doc. 741.

Concept komt overeen met def. versie. Zie doc. 741.

Concept komt overeen met def. versie. Zie doc. 741.

Concept komt overeen met def. versie. Zie doc. 741.

Concept komt overeen met def. versie. Zie doc. 741.

Concept komt overeen met def. versie. Zie doc. 741.

Organisatieonderdeel Staf Korpsleiding
Behandeld door Korpsstaf, Directie Operatien en project CC III Landelijke eenheid

Postadres Postbus 17107
2502 CC Den Haag
Bezoekadres Nieuwe Uitleg 1
2514 BP Den Haag.
Telefoon 088-10.2.e
E-mail 10.2.e @knp.politie.nl

Ons kenmerk KNP2017-0021103
Uw kenmerk 2068042
In afschrift aan -
Datum 6 juli 2017
Bijlage(n) 0
Pagina

VERZONDEN 10 JULI 2017

Aan de Staatssecretaris van Veiligheid en Justitie
Directie Wetgeving en Juridische Zaken
t.a.v. mevr. mr. A.G. van Dijk, directeur
Postbus 20301
2500 EH Den Haag

Onderwerp consultatieadvies ontwerp-Besluit onderzoek in geautomatiseerde werken

Excellentie,

Van het door u bij brief van 10 mei jl. ter consultatie aangeboden Ontwerpbesluit Onderzoek in een geautomatiseerd werk (hierna: het Ontwerpbesluit) heb ik met belangstelling kennis genomen.

Allereerst wil ik mijn waardering uitspreken voor het doorlopen proces, waarin de politie betrokken is geweest in de fase van preconsultatie van dit ontwerpbesluit. De tekst van het Ontwerpbesluit en de daarbij behorende concept voor de concept Nota van Toelichting (hierna: de NvT) geven aanleiding tot het maken van de volgende opmerkingen.

1. Lidmaatschap technisch team

In het Ontwerpbesluit wordt in artikel 3 het lidmaatschap van een technisch team geregeld. In het Ontwerpbesluit is opgenomen dat de korpschef deze leden van het technisch team aanwijst. Ik heb echter geen bevoegdheid opsporingsambtenaren van de Koninklijke Marechaussee (KMar) en van de bijzondere opsporingsdiensten (BOD) aan te wijzen als lid van het technisch team. Deze bevoegdheid ligt bij het bevoegd gezag van de KMar en de BOD zelf. Geadviseerd wordt om in het besluit de bevoegdheid om leden aan het technisch team toe te wijzen toe te delen aan de daarvoor aangewezen verantwoordelijken bij de KMar en de BOD.
In het algemene deel in de NvT is opgenomen dat de bevoegdheid tot binnendringen in een geautomatiseerd werk voor de KMar en de Bijzondere Opsporingsdiensten in ieder geval in de beginfase door de politie kan worden uitgevoerd. De politie zal middels convenanten aan deze samenwerking vormgeven.

2. Logging

In hoofdstuk 4 van het Ontwerpbesluit worden regels gesteld over logging. De politie hecht vanuit het perspectief van transparantie aan een adequate en toetsbare manier uitvoeren van de logging. Dit om toezicht achteraf op de uitgevoerde handelingen door de Inspectie Veiligheid en Justitie (IV&J) en de rechter mogelijk te maken.

Uit de huidige tekst van de NvT is nog onvoldoende te herleiden welke verschillende vormen van logging gegenereerd worden op de technische infrastructuur van de politie. Ook kan worden verduidelijkt hoe deze verschillende vormen van logging in verhouding tot elkaar staan. Ter illustratie volgen hieronder een aantal zinsneden uit de NvT: