Van: 10.2.e **Namens** 10.2.e
Verzonden: woensdag 4 januari 2017 15:49
Aan: 10.2.e @politie.nl>; 10.2.e @politie.nl>
CC: 10.2.e @politie.nl>; 10.2.e @knp.politie.nl>; 10.2.e @politie.nl>
Onderwerp: Actiepunt KMTO n.a.v. NBV 21 december 2016 - CCIII

Beste 10.2.e en 10.2.e

Vanuit de NB Veiligheid van 21 december 2016 is onderstaande actie voortgekomen voor het KMTO.

Wet computercriminaliteit III
Wat: Doorspreken organisatie invoering CCIII
Wie: PC LE
Wanneer: **januari/februari**
Waar: KMT

Theo gaf een korte update rondom de ontwikkelingen CCIII en ging hierbij in op het strategisch en operationeel belang. De KL gaf aan dat er meer aandacht voor dit onderwerp moet zijn en dat we al vroeg in 2017 stil moeten staan bij cyber en de gevolgen die de invoering van CCIII gaan hebben.

Graag ontvang ik een datum waarop dit onderwerp geagendeerd kan worden en informatie over de wijze waarop jullie dit willen inbrengen.
Voor de volledigheid voeg ik een oplegnota voor het KMTO bij.

NB. Het onderwerp Intensivering aanpak cybercrime is op 21 oktober 2016 besproken in het BOO en op 23 november in het KMTO

Met vriendelijke groet,

10.2.e
Adviseur

Politie I Korpsstaf I Afdeling Bestuursondersteuning I 9
Nieuwe Uitleg 1, 2514 BP Den Haag
Postbus 17107 I 2502 CC Den Haag

M 06 10.2.e I E 10.2.e politie.nl
Werkdagen: ma t/m do

Van: 10.2.e
Verzonden: donderdag 5 januari 2017 09:53
Aan: 10.2.e @gelderland-midden.politie.nl>; 10.2.e @politie.nl>
CC: 10.2.e @politie.nl>; 10.2.e @politie.nl>; 10.2.e @politie.nl>
Onderwerp: FW: Actiepunt KMTO n.a.v. NBV 21 december 2016 - CCIII

Hoi 10.2.e en 10.2.e

9 , zie onder het bericht (waarover 10.2.e je eerder ook al mailde) dat CCIII moet worden voorbereid als agendapunt voor een KMTO in januari of februari. Komende vergaderdata KMTO zijn: 18 jan, 1 en 15 feb, 1 mrt.

Graag hoor ik wie dit oppakt en of van mij hierin nog wat wordt verwacht, of dat jullie dit rechtstreeks opnemen met de secretaris KMTO.

Vriendelijke groet,
10.2.e

Van: 10.2.e
Verzonden: dinsdag 10 januari 2017 09:01
Aan: 10.2.e @politie.nl>;10.2.e @gelderland-midden.politie.nl>
CC: 10.2.e @politie.nl>;10.2.e @politie.nl>;
10.2.e @politie.nl>
Onderwerp: Antw: Actiepunt KMTO n.a.v. NBV 21 december 2016 - CCIII

Hallo 10.2.e,

Ik zal bij Theo navraag doen over wat hij wil agenderen en met 10.2.e overleggen over de voorbereiding.

Mochten we nog ondersteuning van jou nodig hebben dan laat ik het weten.

Groet,

10.2.e

From 10.2.e @klpd.politie.nl>
Subject **RE: Antw: Actiepunt KMTO n.a.v. NBV 21 december 2016 - CCIII**
To 10.2.e @politie.nl>,10.2.e @politie.nl>
Date 10 januari 2017 11:36:25 CET

Beste 10.2.e e.a.,

Naar aanleiding van de behandeling van de wet CIII in de Tweede Kamer en de daaropvolgende nationale briefing, waar Theo van der Plas een presentatie over CIII heeft gegeven, heb ik de opdracht van Theo ontvangen met de outlines om een document op te stellen ten behoeve van het KMT. Tijdens de nationale briefing is ook de termijn behandeld door de Korpsleiding, waar ik bij was. Mijn voorstel is om uit te gaan van behandeling in het KMT op 15 februari, zodat we in de voorbereidingen de aanlevertermijnen kunnen halen, want Theo moet zich er ook nog over kunnen buigen. Wij zijn uiteraard op basis van de uitgangspunten en bestaand materiaal aan de slag, m.vr.gr,

10.2.e
9

Politie | Project CCIII
Lookant 1, 3971 PP Driebergen-Rijsenburg
Postbus 100, 3970 AC Driebergen-Rijsenburg
M 06 10.2.e
Email 10.2.e @politie.nl

Van: 10.2.e @politie.nl>
Datum: 13 januari 2017 13:57:53 CET
Aan: 10.2.e @politie.nl>, 10.2.e @klpd.politie.nl>
Onderwerp: Uit het dossier voor de Stas bij TK behandeling

1. Onderzoek in geautomatiseerd werk (126nba Sv)

Factsheet 1.1 Wettelijke regeling en waarborgen

Wettelijke regeling
• Het begrip onderzoek in een geautomatiseerd werk omvat (1) het op afstand heimelijk binnendringen in een geautomatiseerd werk en (2) het verrichten van bepaalde onderzoekshandelingen.
• Het binnendringen van een geautomatiseerd werk vindt plaats ter voorbereiding van het onderzoek al dan niet met een technisch hulpmiddel (met behulp waarvan gegevens kunnen worden vastgelegd).
• De onderzoekshandelingen 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 vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen;
c. de ontoegankelijkmaking van gegevens;
d. de uitvoering van een bevel tot het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie (richtmicrofoon);
e. de uitvoering van een bevel tot stelselmatige observatie.
• Het aftappen, direct afluisteren en de observatie (punten d en e) zijn bestaande Bob-bevoegdheden, het identificatie van het werk of van de gebruiker (punt a), de vastlegging van gegevens (punt b) is nieuw en met de ontoegankelijkmaking van gegevens (punt c) wordt aangesloten bij de bestaande regeling in Sv.

Waarborgen
• Een bevel van de officier van justitie. In het bevel moeten bepaalde gegevens worden opgenomen (misdrijf en feiten en omstandigheden die ten grondslag liggen aan verdenking, zo mogelijk nummer of andere aanduiding waarmee het geautomatiseerde werk kan worden geïdentificeerd (bijv. IP- of MAC-adres, IMEI-nummer), dat de gegevens niet in Nederland zijn opgeslagen, aanduiding technisch hulpmiddel, aanduiding welk deel van het werk het betreft en tijdsduur inzet).
• Toestemming van het College van procureurs-generaal Het College laat zich daarbij adviseren door de Centrale Toetsingscommissie (CTC).
• Vereiste vaneen dringend onderzoeksbelang: hiermee wordt tot uitdrukking gebracht dat de gegevens niet op een minder ingrijpende wijze kunnen worden verkregen, waarbij rekening wordt gehouden met de gevolgen voor het geautomatiseerde werk en de betrokken personen.
• Een voorafgaande machtiging van de rechter-commissaris.
• Voor de bevoegdheden, genoemd in de punten a., d. en e. geldt het vereiste van een feit waarvoor voorlopige hechtenis mogelijk is.
• Voor de vastlegging van gegevens en de ontoegankelijkmaking van gegevens (punten b en c) geldt het vereiste van een feit waarvoor gevangenisstraf van acht jaar of meer kan worden opgelegd of dat bij AMvB is aangewezen.
• Bij AMvB worden aangewezen bepaalde misdrijven die worden gepleegd met behulp van een geautomatiseerd werk en.
• De drempel van acht jaar voor de vastlegging van gegevens en de ontoegankelijkmaking van gegevens is opgenomen n.a.v. advies Raad

van State. In de AMvB worden de delicten opgenomen waarbij het gebruik van een computer instrumenteel is voor het plegen van et delict en waarbij er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders (bijv. gebruik van botnet, aanbieden of verspreiden kinderpornografie of grooming).
• Het binnendringen is beperkt tot de daartoe aangewezen opsporingsambtenaren van het technische team. Dit betreft de door de korpschef aangewezen en ter zake deskundige opsporingsambtenaren die over specialistische kennis beschikken op het gebied van ICT.
• De opsporingsambtenaren van het technische team behoren niet tot het opsporingsteam dat het tactische onderzoek verricht (functiescheiding, vermindert risico tunnelzicht).
• De in het kader van de onderzoekshandelingen verrichte handelingen in geautomatiseerde werk worden gelogd. Daardoor kan later worden nagegaan wat er in dat kader precies is gedaan en kan de integriteit van de bewijsverkrijging worden verzekerd.

Van: 10.2.e
Verzonden: vrijdag 13 januari 2017 14:05
Aan: 10.2.e 10.2.e
CC: 10.2.e
Onderwerp: Antw: Uit het dossier voor de Stas bij TK behandeling

Beste 10.2.e

Wat jij zegt klopt formeel conform alle stukken. Dat wordt mij ook bevestigd door de jurist en 10.2.e Maar de beeldvorming is dat het gaat om delicten 8 jaar, maar dat gaat over de verdere opsporingshandelingen, zeg maar het vergaren van vastgelegde gegevens. Voor id,ovc en lokatie is 4 jaar. Mijn punt was even de beeldvorming die gaat ontstaan en in een nu.nl artikel is dat onderscheid zo moeilijk te maken en uit te leggen. Bovendien komt er dan een heleboel tekst die niet van de journalist is, maar misschien dat hij zelf het onderscheid wel wil maken, hij heeft immers een dossier, gr 10.2.e

Van: 10.2.e
Verzonden: vrijdag 20 januari 2017 15:56
Aan: Plas, Theo van der (T.G.) 10.2.e @politie.nl>; 10.2.e
@politie.nl>
CC: 10.2.e @politie.nl>; 10.2.e
@politie.nl>; 10.2.e @klpd.politie.nl>; 10.2.e
@klpd.politie.nl>
Onderwerp: Eerste concept hoofdlijnennotitie CCIII tbv KMT 15 februari

Beste Theo en 10.2.e

Bijgaand een eerste concept van de hoofdlijnennotitie CCIII tbv het KMT op 15 februari. Deze is opgesteld naar aanleiding van de discussie in de Nationale Briefing van 21 december en ons overleg op 9 januari. We hopen hiermee aan de vraag van de Korpschef te kunnen voldoen.

Graag horen wij jullie reactie en opmerkingen, zodat we deze kunnen verwerken in een volgende versie.

Op 31 januari zal 10.2.e de inhoud nog persoonlijk met je bespreken.

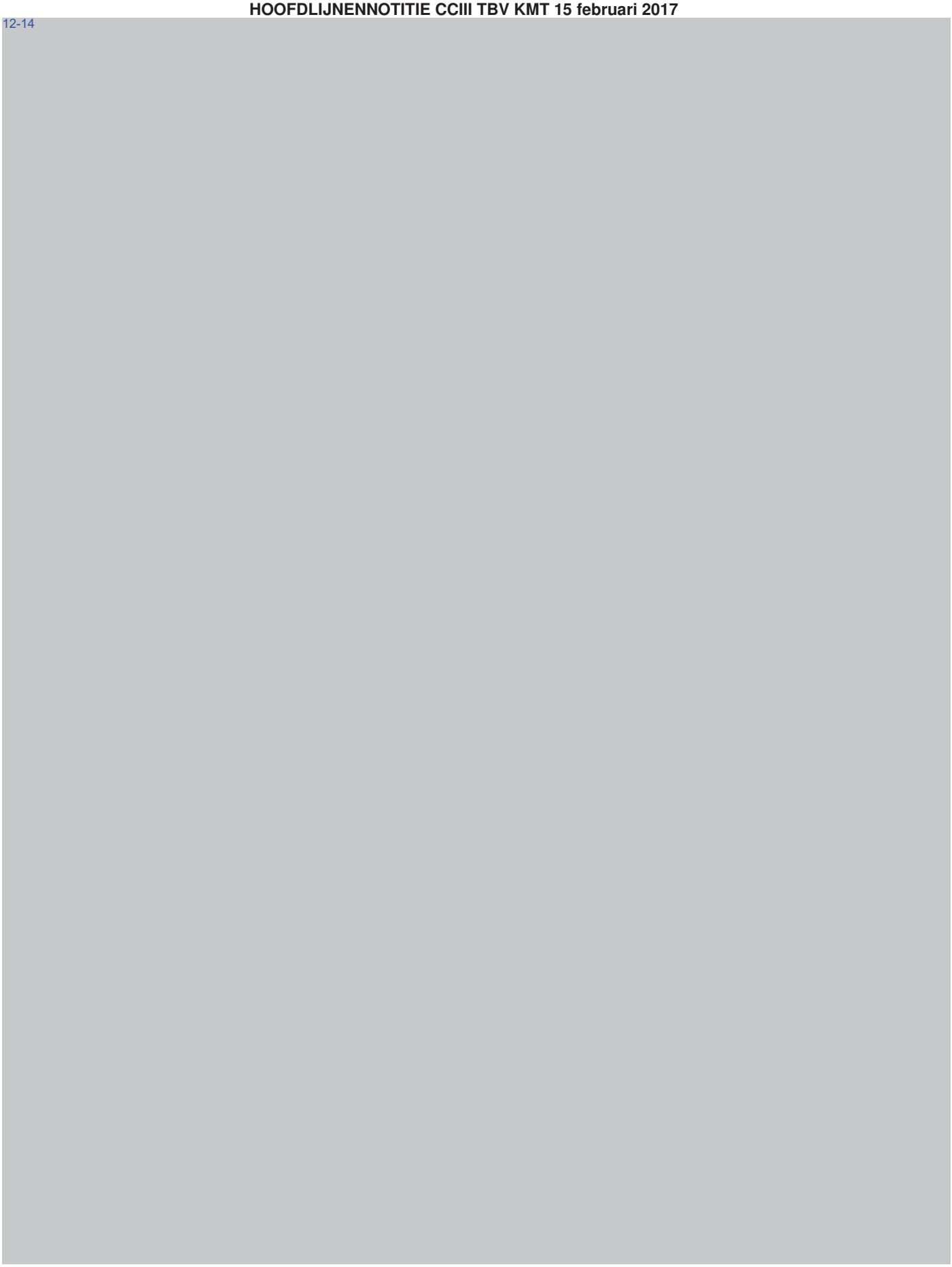
Het zou mooi zijn als we jullie reactie voor die datum kunnen ontvangen.

Met vriendelijke groet,

10.2.e

HOOFDLIJNENNOTITIE CCIII TBV KMT 15 februari 2017

12-14



12-14

12-14

12-14

12-14

Van: 10.2.e
Verzonden: maandag 23 januari 2017 15:32
Aan: 10.2.e @politie.nl>; 10.2.e @gelderland-midden.politie.nl>; 10.2.e @politie.nl>
CC: 10.2.e @politie.nl>; 10.2.e @politie.nl>; 10.2.e @politie.nl>
Onderwerp: RE: Actiepunt KMTO n.a.v. NBV 21 december 2016 - CCIII

Beste 10.2.e en allen,

Het project CCIII heeft in de persoon van 10.2.e het concept document aangeleverd bij de portefeuillehouder Theo van der Plas.
Bij mijn weten is hij kortstondig met verlof.
Maar ik neem aan dat zodra hij zijn licht erover heeft doen schijnen, wij nader geinformeerd worden over de vorm en verdere procedure?
Wij gaan inmiddels uit van een vastgestelde datum 15-2.
Als er anderszins nog iets moet gebeuren op dit punt vanuit het project hoor ik dat graag, m.vr.gr,

10.2.e
9

Politie | Project CCIII
Lookant 1, 3971 PP Driebergen-Rijsenburg
Postbus 100, 3970 AC Driebergen-Rijsenburg
M 06 10.2.e
Email 10.2.e @politie.nl

From: 10.2.e
Sent: Wednesday, January 25, 2017 09:23 AM

To: 10.2.e ;10.2.e
Cc: 10.2.e 10.2.e 10.2.e

Subject: RE: Actiepunt KMTO n.a.v. NBV 21 december 2016 - CCIII

Hoi 10.2.e

Eerder gaf jij aan dat jij agendering kon regelen. Maar ik weet niet of jij dit al hebt aangemeld voor KMTO van 15 februari. Laat je dit even weten? Dan weet ik ook of ik daar nog iets voor moet doen.

Vriendelijke groet,

10.2.e

Van: 10.2.e
Verzonden: woensdag 25 januari 2017 18:09
Aan: 10.2.e @politie.nl>; 10.2.e @klpd.politie.nl>; 10.2.e @gelderland-midden.politie.nl>
CC: 10.2.e @politie.nl>; 10.2.e @politie.nl>; 10.2.e @politie.nl>
Onderwerp: Re: Actiepunt KMTO n.a.v. NBV 21 december 2016 - CCIII

Hi 10.2.e,

Theo zou nog met Jannine afstemmen of het rechtstreeks naar KMT gaat of via BOO en BBVO. Ik heb nog geen tergkoppeling gehad en hij is nu met verlof. Daarvan is de agendering afhankelijk.

@10.2.e weet jij misschien of ze dit hebben afgestemd?

Met vriendelijke groet,

10.2.e

Staf Korpsleiding Politie
Directie Operatien

Verzonden vanaf mijn Blackberry

Van: 10.2.e
Verzonden: donderdag 26 januari 2017 14:20
Aan: 10.2.e Plas, Theo van der (T.G.)
CC: 10.2.e 10.2.e 10.2.e ; 10.2.e ; 10.2.e 10.2.e
Onderwerp: RE: Eerste concept hoofdlijnennotitie CCIII tbv KMT 15 februari

Hallo 10.2.e ,

Dank voor het stuk. Een goed basis, waarin veel belangrijke punten aan de orde komen. Ik heb het doorgenomen en heb best veel opmerkingen gemaakt, maar opbouwend bedoeld. Hebben jullie de check gedaan of alle elementen terugkomen in jullie portfolio startdocument? Dat is immers de bassi voor de implementatie.

Vooral de gevraagde besluitvorming die jullie hebben opgenomen moeten we nog goed afstemmen. Dit is ook het belangrijkste deel van de oplegger. Ik denk dat we die nog moeten aanscherpen.
Daar zal ik zoals beloofd bij meehelpen.
Maak jij daar een eerste opzet voor, in ieder geval voor de basisonderdelen zoals een samenvatting van het stuk ed?
Dan vullen we samen oa. de gevraagde besluitvorming verder in.

Een belangrijk ander aandachtpunt is wanneer het implementatieplan klaar is. Jullie noemen nu rond de zomer. Dat is echt te laat als we dan nog KMT besluitvorming moeten hebben en feitelijk pas echt gaan implementeren. Om dat te versnellen is recent de goedkeuring bevestigd voor de inhuur.
Goed daar volgende week met Theo naar te kijken.

Ik stel voor dat we volgende week verder afstemmen als jullie naar mijn opmerkingen hebben kunnen kijken. Theo is deze week op vakantie en zal waarschijnlijk volgende week reageren. In ieder geval hebben jullie een afspraak staan om eea. door te nemen, dus dat is mooi.

Groet en fijn weekend,

10.2.e

Van: 10.2.e
Verzonden: donderdag 26 januari 2017 14:50
Aan: 10.2.e @knp.politie.nl>; 10.2.e @politie.nl>
CC: 10.2.e @politie.nl>; 10.2.e @politie.nl>;10.2.e @klpd.politie.nl> Onderwerp: Agendering Hoofdlijnennotitie CCIII voor KMT

Hallo collega's,

In de NB van december 2016 is gesproken over de Wetgeving Computercriminaliteit III en wat dit betekent voor de politie. Erik Akerboom heeft toen de pfh Digitalisering en Cybercrime de opdracht gegeven een hoofdlijnennotitie te maken voor CCIII en die te agenderen in het KMT.

Er wordt nu aan die notitie gewerkt met op dit moment als richtdatum agendering op 15 februari. Kunnen jullie dit onderwerp voorlopig op de agenda zetten van het KMT voor 15/2?
Klopt het dat de aanleverdatum voor de stukken dan 6/2 is?

Er wordt nog afgestemd of misschien vooraf nog het BOO meegenomen wordt. Zodra ik daar meer over weet zal ik jullie daarover informeren en kunnen we kijken naar passende data.

Groet,

10.2.e

Van: 10.2.e
Verzonden: donderdag 26 januari 2017 14:54
Aan: 10.2.e @politie.nl>10.2.e @politie.nl>; 10.2.e @politie.nl>
CC: 10.2.e @politie.nl>10.2.e @politie.nl>; 10.2.e @politie.nl>
Onderwerp: RE: Actiepunt KMTO n.a.v. NBV 21 december 2016 - CCIII

Beste 10.2.e en allen,

Als ik in alle bescheidenheid de mail lees van mevrouw 10.2.e dan constateer ik in dezelfde bescheidenheid dat die precies past bij het verloop van de discussie in de Nationale Briefing. Het gezelschap was zeer belangstellend voor dit onderwerp en wilde daar in het KMT over spreken. De KC zelf drong aan op spoed en uiteindelijk zijn we uitgekomen op 15 februari. Vorige week hebben wij na opdracht en aanwijzingen van de portefeuillehouder Theo van der Plas een concept aangeleverd. Hij zal zich erover buigen en dan kan het document denk ik zo snel mogelijk door.
Ik heb totaal geen verstand van de procedures en eventuele procesgang via andere gremia. Dus ik heb daar geen oordeel over, maar gaat dat niet vertragend werken? Dat lijkt mij in deze casus wellicht niet handig? m.vr.gr,

10.2.e
9

Politie | Project CCIII
Lookant 1, 3971 PP Driebergen-Rijsenburg
Postbus 100, 3970 AC Driebergen-Rijsenburg
M 06 10.2.e
Email 10.2.e @politie.nl

From 10.2.e @knp.politie.nl>
Subject **RE: Agendering Hoofdlijnennotitie CCIII voor KMT**
To 10.2.e @politie.nl>
Date 26 januari 2017 15:00:01 CET

Hoi 10.2.e

Ik zal het op 15 februari agenderen, maar Erik Akerboom is dan niet aanwezig. Dit is misschien niet handig, maar dat laat ik aan jullie over. Wie gaat het onderwerp dan toelichten tijdens het KMTO?
Aanleverdatum voor 15/2 is dinsdag 7/2.

Als het eerst nog in het BOO moet, dan wordt de planning anders, nl:
BOO 17/2 – aanleveren 7/2
KMTO 1/3 – aanleveren 21/2

De stukken voor BOO 3/2 zijn namelijk vanmiddag rees verzonden.

Voldoende info zo? Anders hoor ik het wel!

Groet,
10.2.e

Met vriendelijke groet,
9
Adviseur

Politie I Korpsstaf I Afdeling Bestuursondersteuning I9
Nieuwe Uitleg 1, 2514 BP Den Haag
Postbus 17107 I 2502 CC Den Haag
M 06 10.2.e I E: 10.2.e @politie.nl
Werkdagen: ma t/m do

From 10.2.e
Subject **RE: Actiepunt KMTO n.a.v. NBV 21 december 2016 - CCIII**
To 10.2.e @politie.nl>, 10.2.e @politie.nl>, 10.2.e @klpd.politie.nl>
Date 26 januari 2017 15:01:50 CET

Hallo 10.2.e

Ik weet niet op welke mail je doelt, maar ik denk dat je het hebt over de vraag of we eerst naar het BOO gaan voor het KMT. Dit is iets waar Theo zelf nog naar wilde kijken met Jannine. Theo zit zelf in dit overleg van de hoofden operatien en dat fungeert als adviesorgaan van het KMT.
Als hiervoor wordt gekozen is dat juist om beter resultaat te halen en niet om te vertragen.

Jullie maken in je stuk een vergelijking met de cyberteams en dat zo'n besluit voor CCIII ook mooi zou zijn.

Om die cyberteams te bereiken hebben we onder andere: diverse strategische sessies, overleg met 9 en bespreking in BOO gehad, voordat uiteindelijk KMT besloot.

Dit is dus echt een shortcut in vergelijking met dat proces, ook al nemen we wel alleen BOO mee.

Groet,
10.2.e

Nadelen niet mogen hergebruiken Technische Hulpmiddelen met onbekende kwetsbaarheden

12-14

12-14

Nadelen niet mogen hergebruiken Technische Hulpmiddelen met onbekende kwetsbaarheden

12-14

12-14

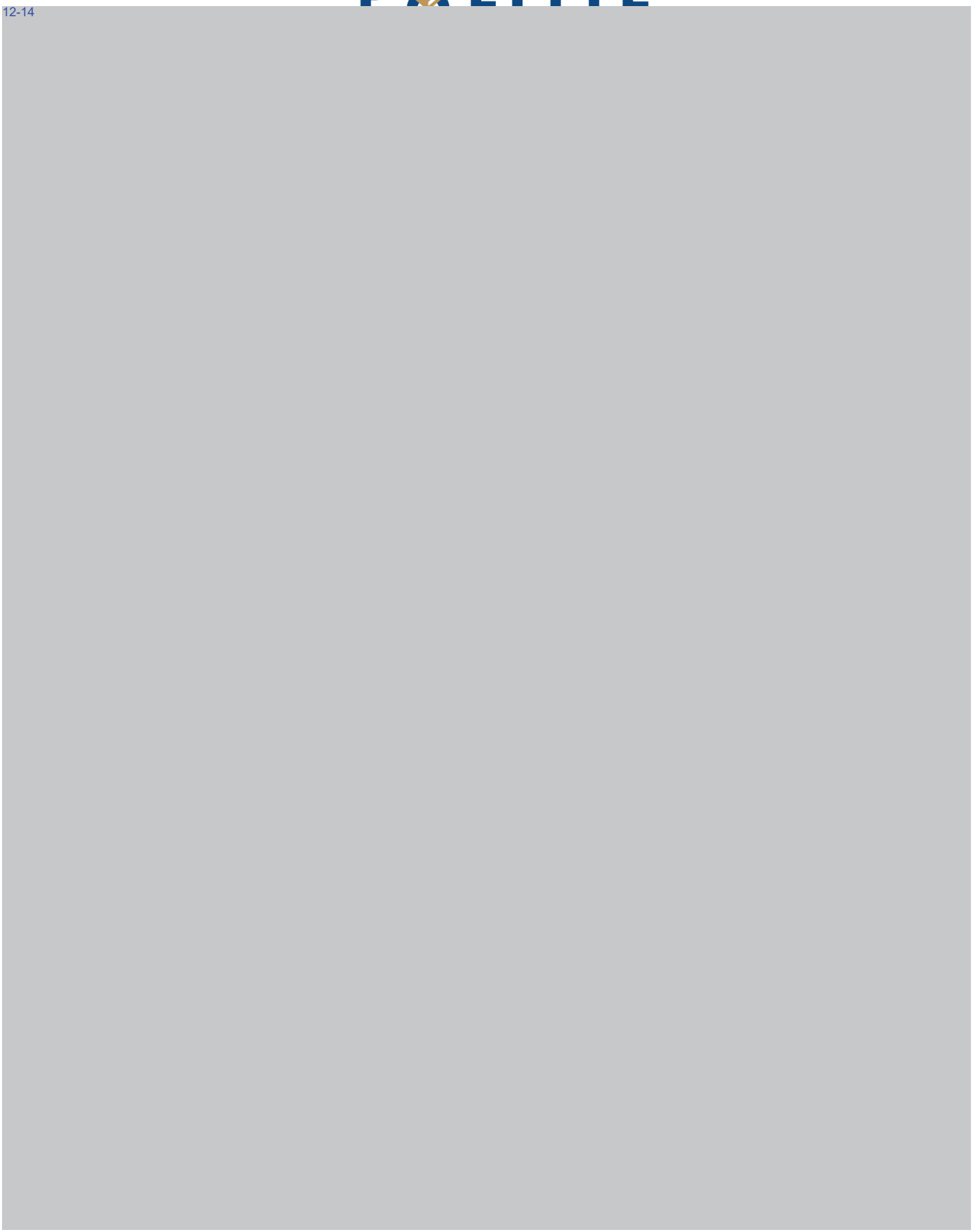
12-14

12-14

[redacted]

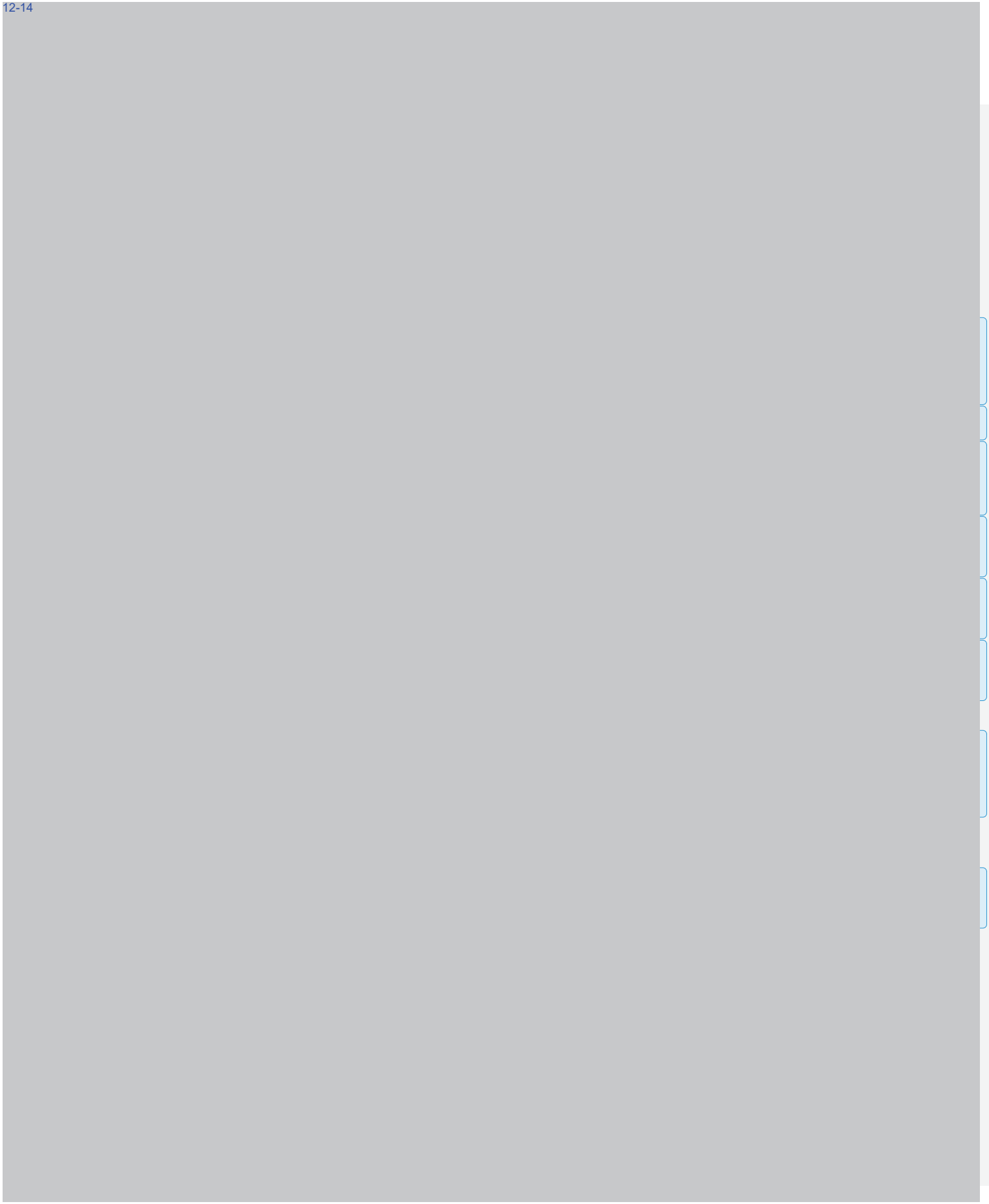
Klik hier als u tekst wilt invoeren.

12-14

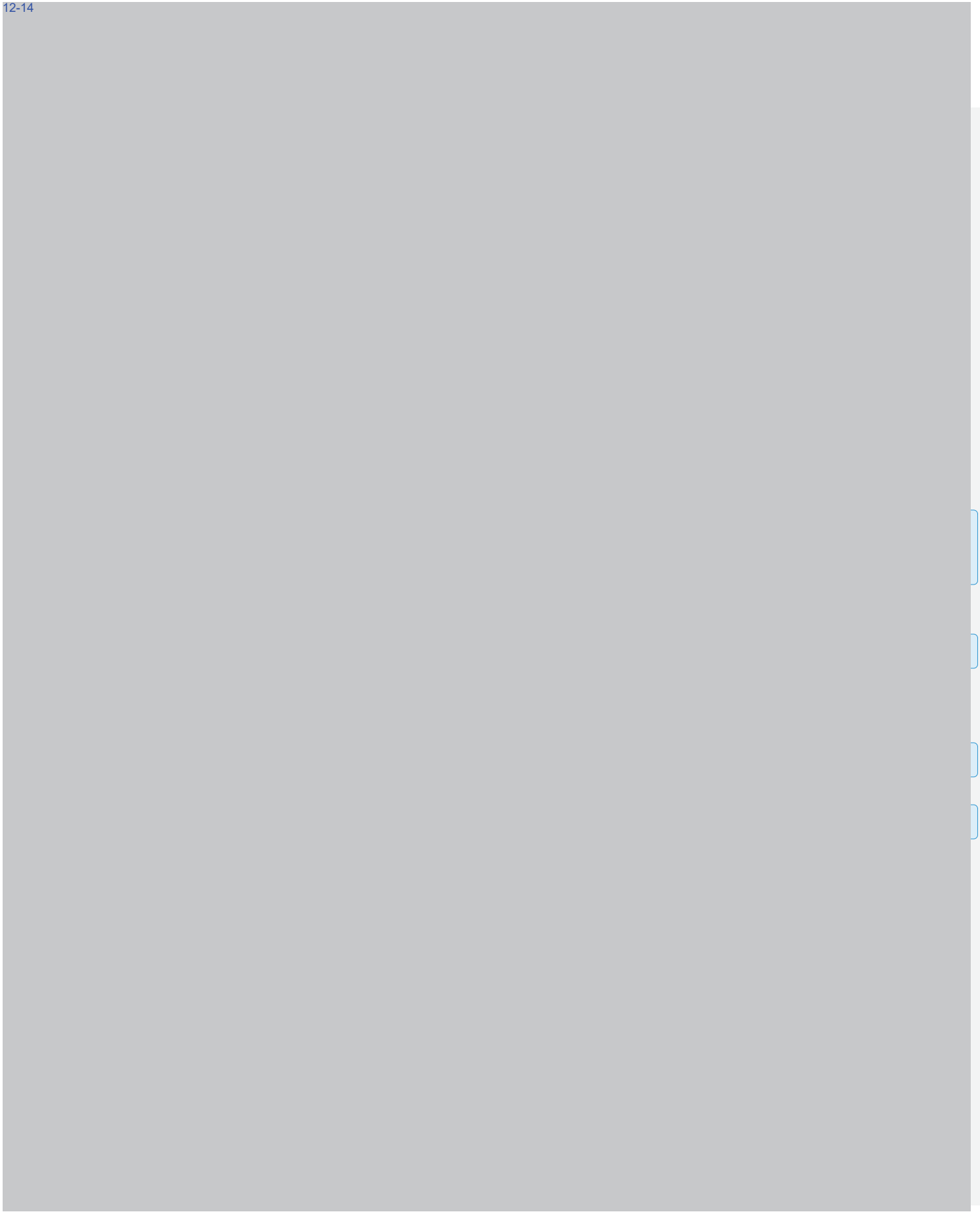


12-14

12-14

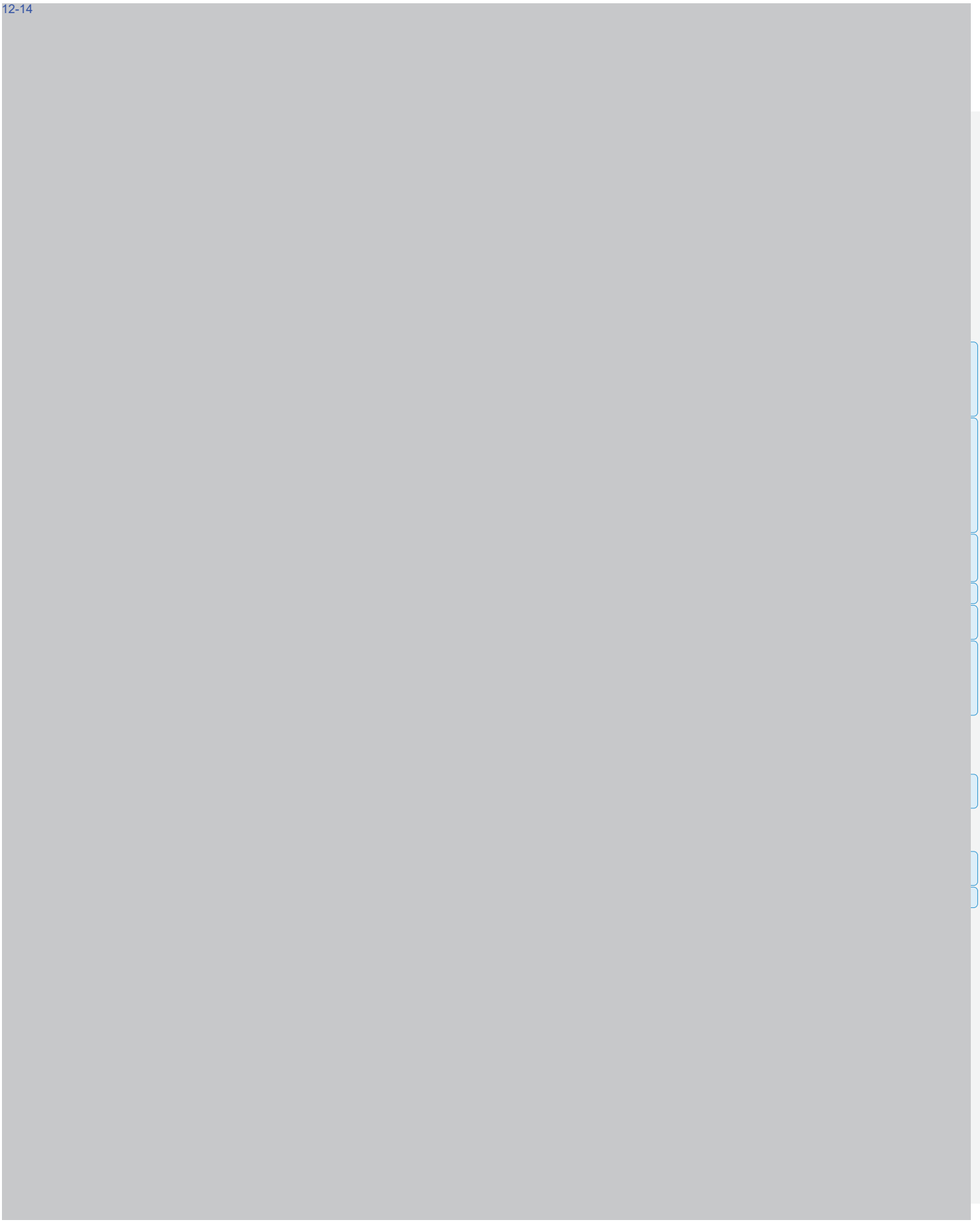


12-14



12-14

12-14

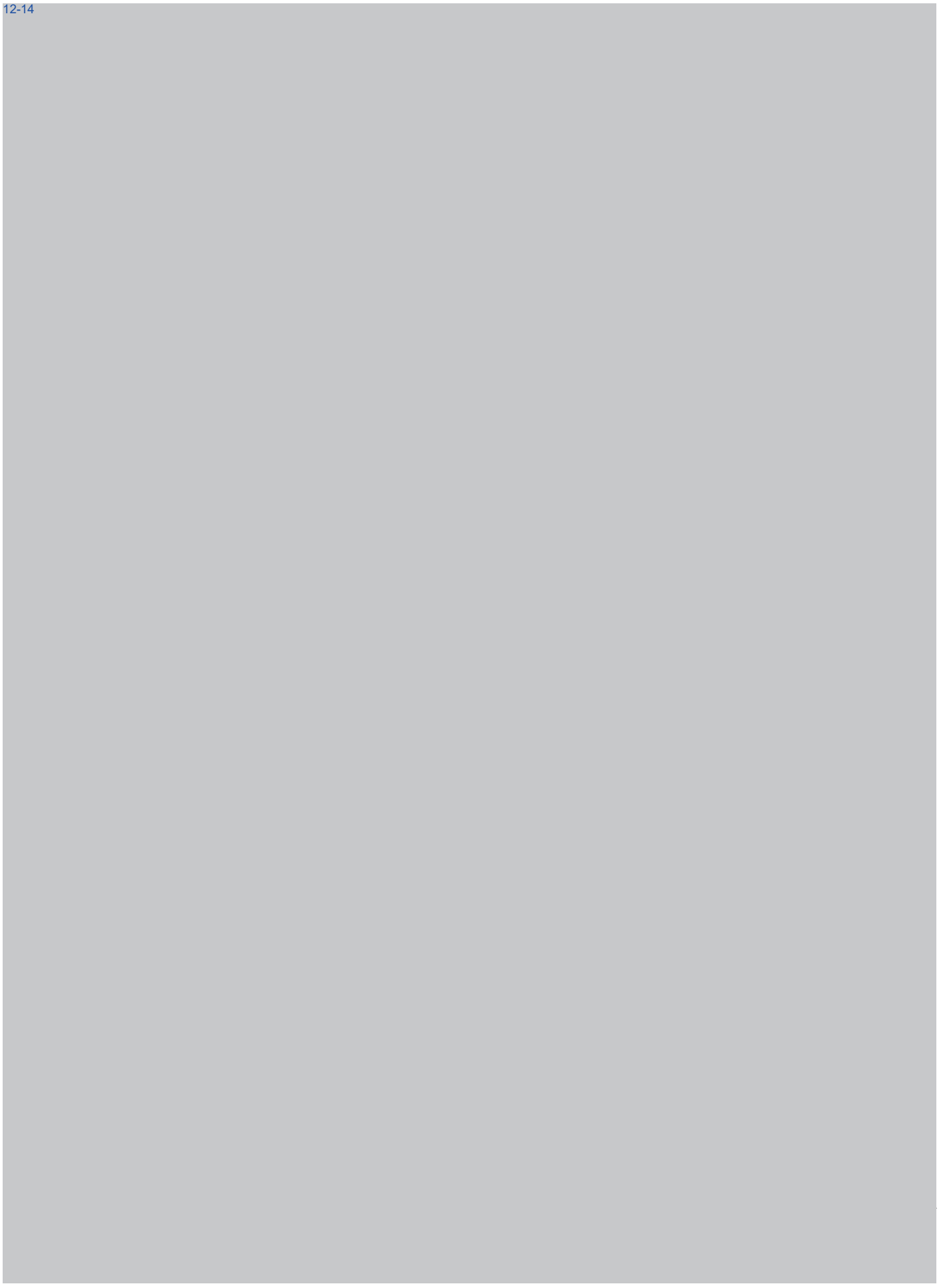


12-14

12-14

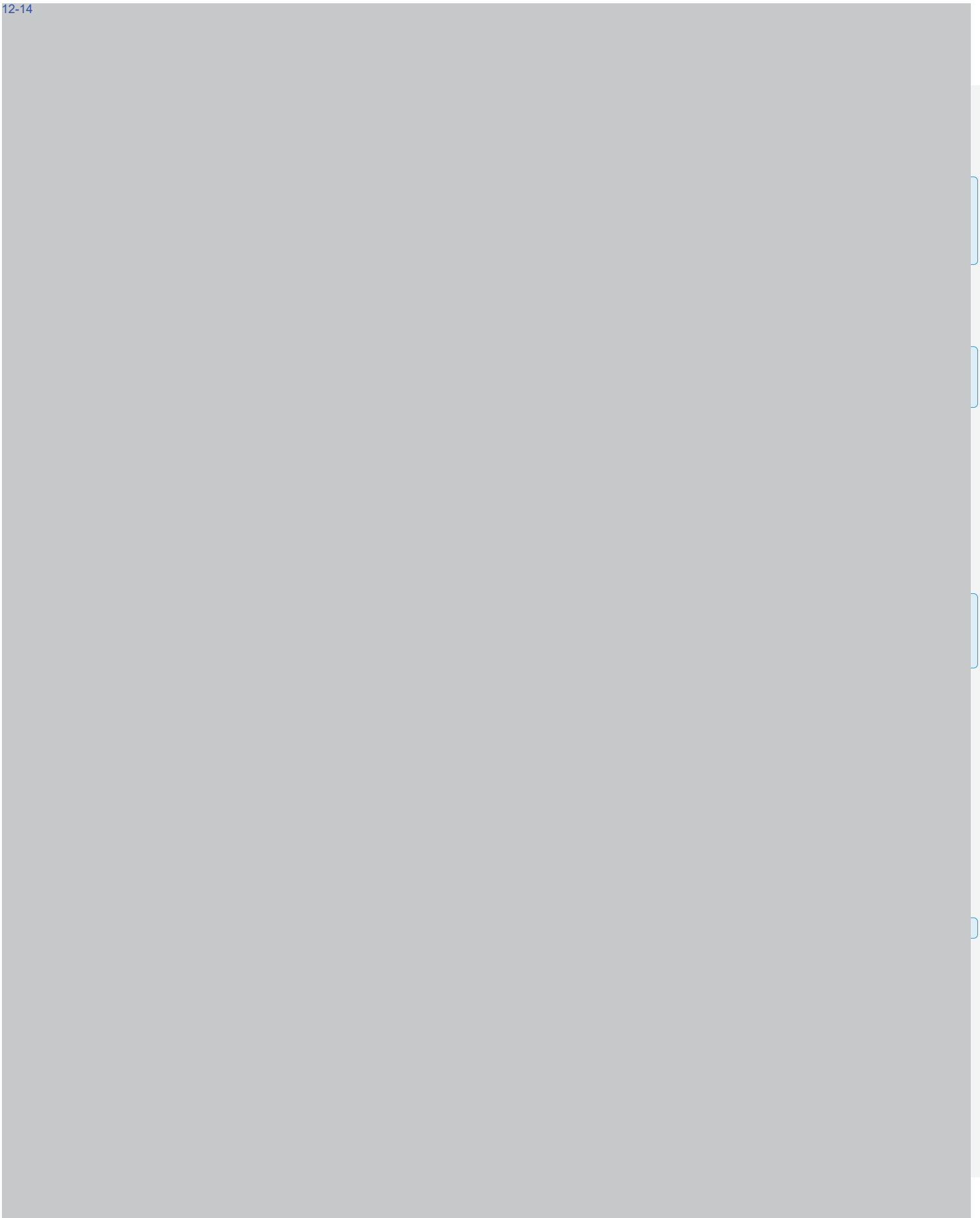
12-14

12-14


12-14

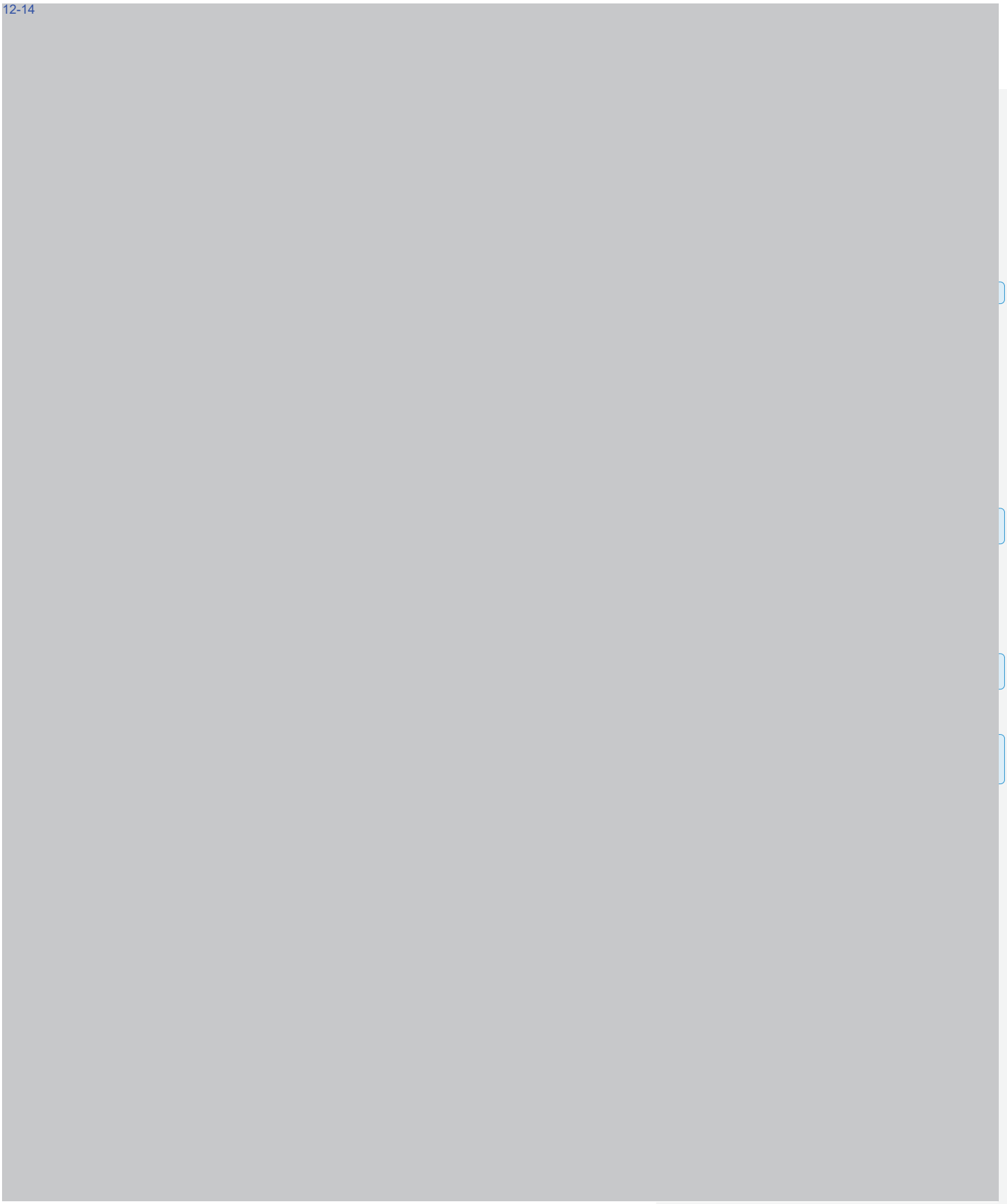
12-14

12-14



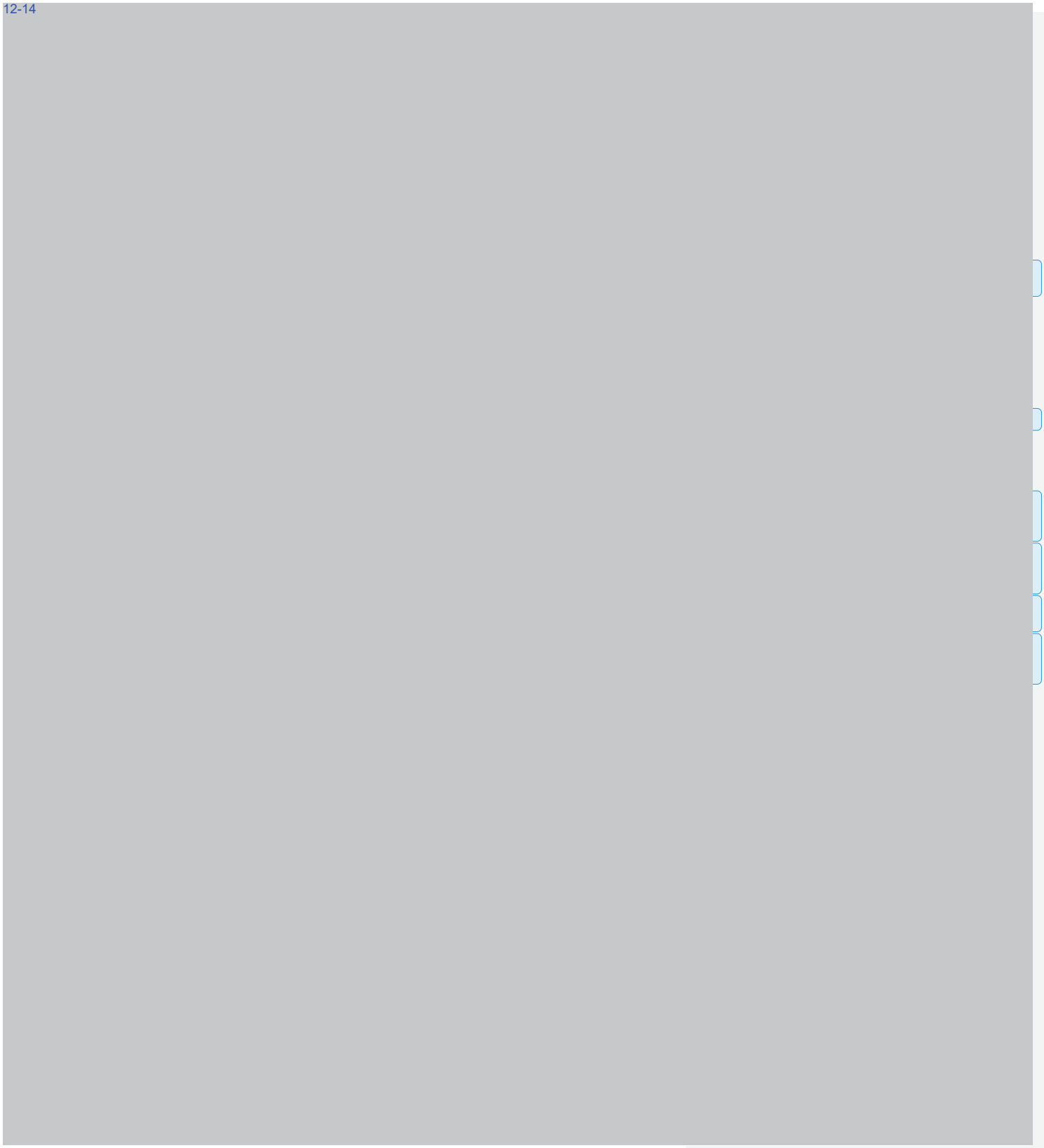
12-14


12-14

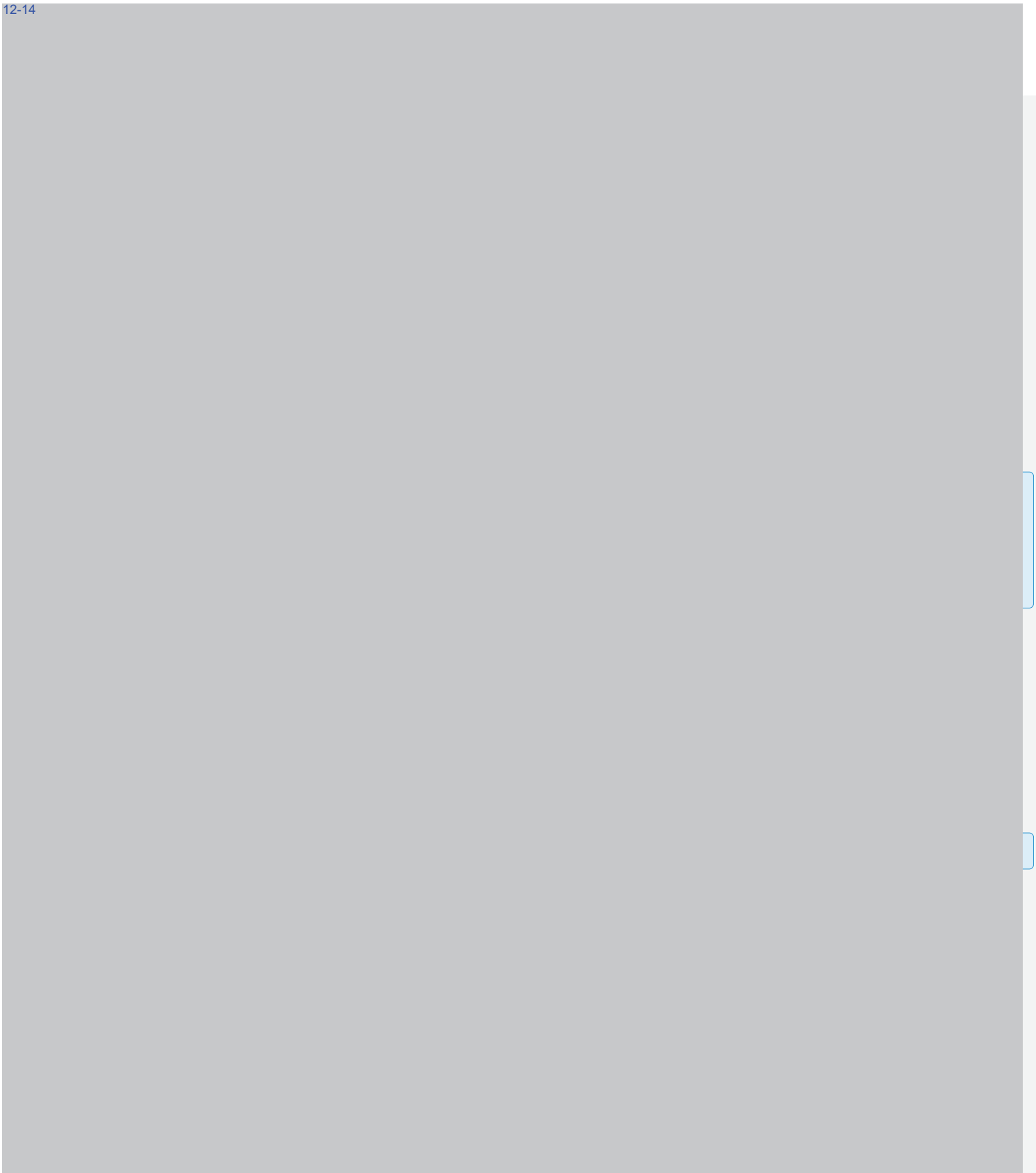

12-14

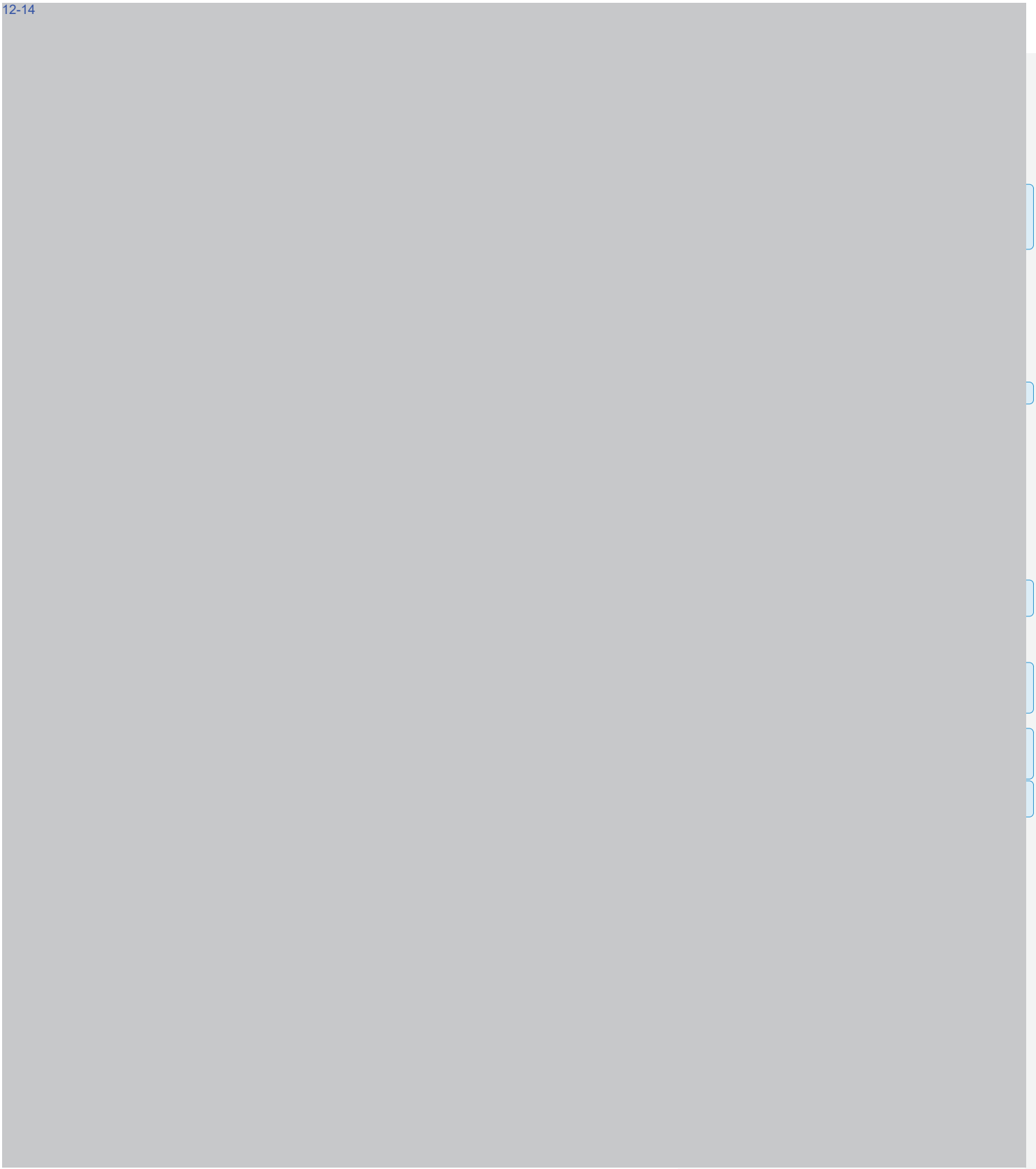
12-14

12-14



12-14

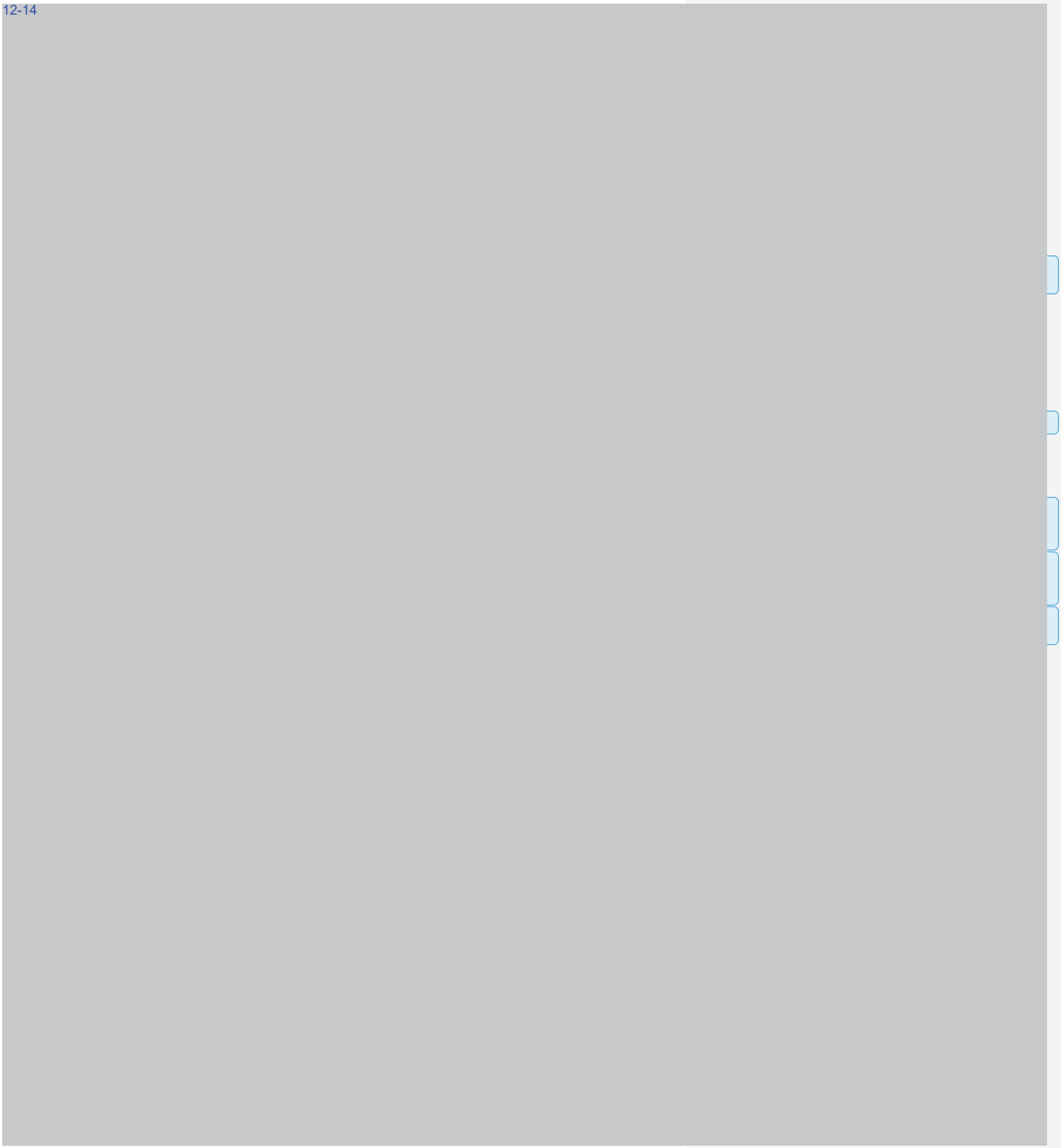



12-14

12-14

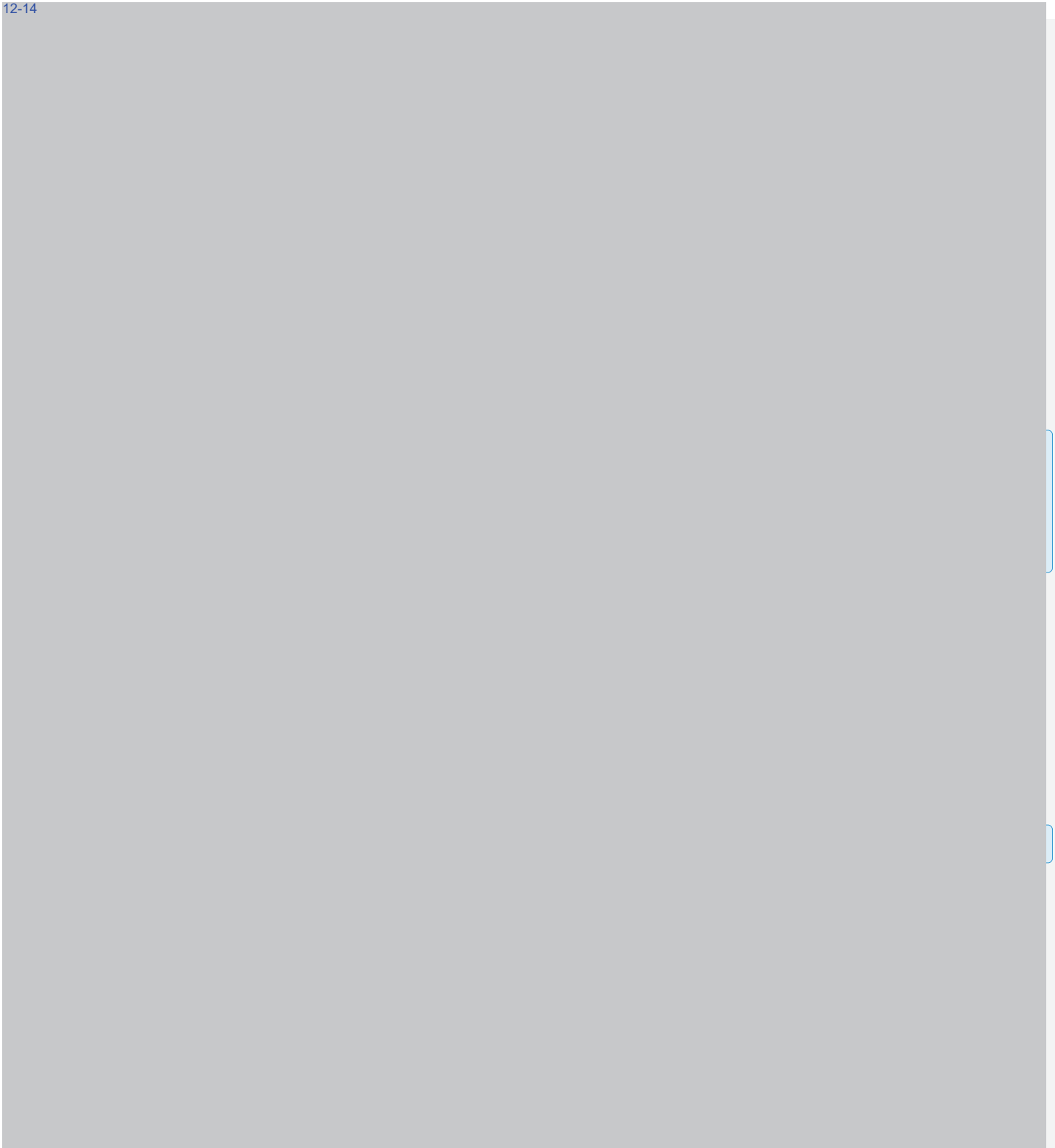
12-14

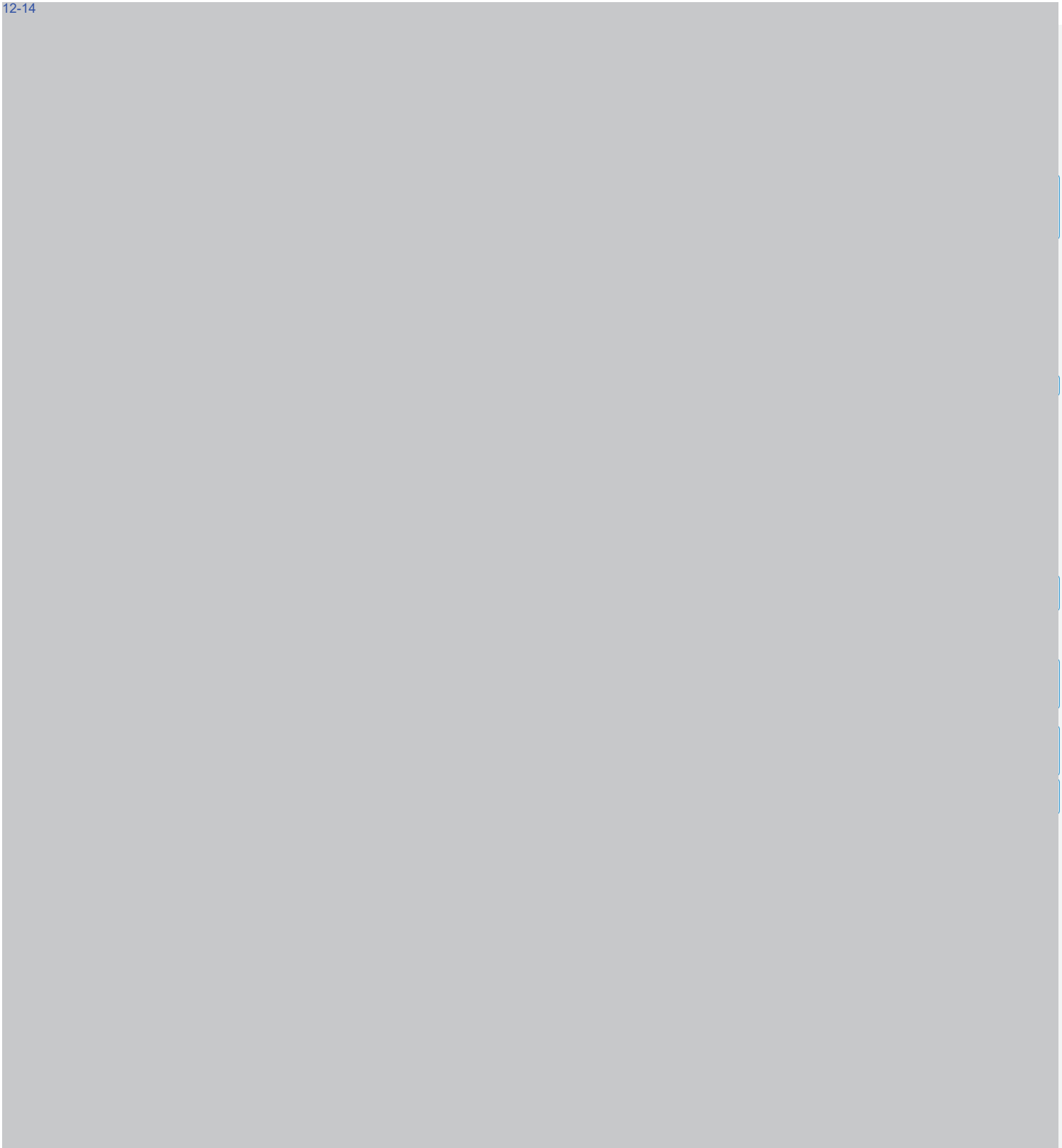
12-14



1

12-14




12-14

12-14

12-14

Van: 10.2.e
Verzonden: woensdag 15 februari 2017 22:01
Aan: Plas, Theo van der (T.G.) 10.2.e s@politie.nl>; 10.2.e @politie.nl>
CC: 10.2.e @vtspn.nl>; 10.2.e @politie.nl>; 10.2.e @politie.nl>
Onderwerp: Hoofdlijnennotitie CCIII tbv BOO

Beste Theo en 10.2.e ,

Bijgaand een nieuwe versie van de hoofdlijnennotitie CCIII ten behoeve van het BOO. Geprobeerd is om concreter te maken wat we vragen en welke rollen/functies we nu en in de komende tijd nodig gaan hebben. Ik hoop dat hiermee aan het verzoek tegemoet is gekomen om het verhaal concreter te maken.

Ik begreep van 10.2.e dat je nog een presentatie wilt over dit onderwerp voor het BOO. Ik zal dit morgenochtend maken op basis van deze versie en mijn uiterste best om dat voor 11 uur bij je te hebben.

Ik hoor graag of je je kunt vinden in deze versie. Mocht je nog wijzigingen willen, dan hoor ik dat natuurlijk ook graag en zal ik dat morgen doen.

Met vriendelijke groet,

10.2.e

Hoofdlijnennotitie voorziening tot binnendringen

Hoofdlijnen voor de inrichting

10.2.e

Concept

Versie 0.1

Versie datum 15 februari 2017

Rubricering Politie INTERN

« waakzaam en dienstbaar »

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	15-02-17	Eerste versie	

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie
0.1	15-02-17	Theo van der Plas, Marjolein Smit 10.2.e , 10.2.e	Portefeuillehouder D&C, leiding DLOS, Leiding Project CCIII

Review commentaar

Versie	Wanneer	Wie	Functie

Inhoudsopgave

Inleiding

Op 21 december 2016 heeft de portefeuillehouder Digitalisering en Cybercrime (D&C) in de Nationale Briefing een presentatie gegeven over het wetsvoorstel CCIII en wat dit betekent voor de Nederlandse Politie. De Korpschef heeft verzocht om een hoofdlijnennotitie op te stellen waarin wordt beschreven hoe de politie over zal gaan tot implementatie van deze wet in de politieorganisatie.

Het KMT wordt gevraagd om:

Kennis te nemen van:

- Deze notitie over het project CCIII en specifiek de implementatie van de bevoegdheid tot 'heimelijk op afstand binnendringen in een geautomatiseerd werk'
- De fasering die in het project 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 7-12 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.

Te besluiten dat:

- Voor het uitvoeren van de experimenten in fase 1 en voor het uitvoeren van de werkzaamheden in fase 2 die noodzakelijk zijn voor het opstellen en uitvoeren van het realisatieplan, door de eenheden 7-12 per eenheid d.m.v. een TTW voor een periode van 2 jaar beschikbaar zal worden gesteld aan de voorziening CCIII.
- Het sectorhoofd van de DLOS van de Landelijke Eenheid de opdracht krijgt van de portefeuillehouder D&C om de voorziening op basis van deze notitie en het realisatieplan in te richten en tot werking te brengen.

1. Fase 0 (opstartfase)

Laboratorium omgeving

In 2014 is een impactanalyse opgesteld waarin een eerste impact op de operatiën en bedrijfsvoering is bepaald. Het project CCIII is daaropvolgend op 1 januari 2015 van start gegaan. Op 14 augustus 2015 is het PID Binnendringen fase 1 opgeleverd en door de portefeuillehouder D&C goedgekeurd, waarmee de start werd gemaakt van de laboratorium omgeving van het project CCIII bij 7-11-12 Vanaf 1 januari 2016 zijn de feitelijke werkzaamheden in de lab omgeving van start gegaan (fase 0).

Verbinding met overige (digitale) ontwikkelingen

De portefeuille D&C investeert in de oprichting van 3 scrumteams, die ingezet gaan worden voor projecten binnen deze portefeuille. Het project CCIII participeert hierin om de implementatie van de nieuwe bevoegdheid vorm te geven. Binnen de lab omgeving van het project wordt ook volgens de scrum-methodiek gewerkt en deze innovatieve aanpak binnen de portefeuille D&C past daar uitstekend bij.

Daarnaast is door het project CCIII aansluiting gevonden bij het Programma Herijking Opsporing. CCIII kan namelijk als katalysator dienen voor de digitale ontwikkeling van de Nationale Politie. De aanpak vanuit CCIII draagt bij aan een innovatieve en vernieuwende aanpak van de digitale ontwikkeling van de opsporing. Ook is de verbinding gezocht binnen de portefeuille Digitalisering en Cybercrime met de projecten Digitaal Opsporen en Cybercrime en met de portefeuilles Zeden en CTER.

Vanuit de KL wordt binnen het project Bijzondere Bedrijfsvoering gewerkt aan de inrichting van een Serviceteam Afgeschermde Operatie & Bedrijfsvoering (STA-OB). Het project sluit hierbij aan om de afgeschermde inkoop van technische middelen te kunnen stroomlijnen

2. Fase 1 (experimenteerfase) naar fase 2 (implementatiefase)

Er in 2016 door 7-12 medewerkers van verschillende onderdelen van 7-12 een infrastructuur gebouwd, waarmee bij inwerkingtreding van de wet de eerste zaken gedraaid kunnen worden. Op basis van experimenten worden de eerste voorbereidingen getroffen voor de uitvoering van de nieuwe bevoegdheid. Hierbij valt te denken aan het bepalen van de juiste architectuur voor een veilige infrastructuur van waaruit de politie kan gaan werken, het experimenteren met demo software op geautomatiseerde werken in een gesloten omgeving of deze software bruikbaar kan zijn, het draaien van oefeningen om te zien of de werkprocessen toepasbaar zijn, het bepalen van de juiste functieprofielen en het evalueren van opsporingsonderzoeken waarin het mogelijk zou zijn geweest om deze bevoegdheid in te zetten. Al deze voorbereidende werkzaamheden leiden er toe dat het bij inwerkingtreding van de wet duidelijk is op welke manier het “echte” werk uitgevoerd wordt.

Er is gekozen voor een (voorlopig) centrale aanpak. Deze keuze is gemaakt vanwege de politiek-bestuurlijke gevoeligheden, de keuze van de wetgever om deze bevoegdheid centraal te willen regelen en vanwege de complexiteit en hoge kosten die de implementatie met zich meebrengt. Het is daarom van groot belang dat er door de Eenheden geparticipeerd wordt in de bouw van deze voorziening voor alle opsporingsinstanties (politie, FIOD en KMAR). Hierdoor

kan er kennis en expertise gedeeld en ontwikkeld worden voor de gehele politieorganisatie. Verdere doorontwikkeling naar de implementatie is nu noodzakelijk en hiervoor is de hulp van alle Eenheden noodzakelijk.

Fase 1

Zoals hierboven is aangegeven is er op dit moment onvoldoende capaciteit om de implementatie van de nieuwe bevoegdheid goed vorm te geven. Aan de Eenheden wordt daarom gevraagd om voor de duur van 2 jaar 7-12 per eenheid ter beschikking te stellen aan de voorziening CCIII om gezamenlijk deze voorziening in te richten. Deze inzet is niet alleen in fase 1, maar ook in de implementatiefase (fase 2) noodzakelijk. In fase 2 zal de voorziening operationeel werkend moeten zijn. Een uitgewerkt realisatieplan zal hiervoor voor 1 juli ter goedkeuring worden aangeboden aan het KMT.

Hierop vooruitlopend is op korte termijn (tot 1 januari 2018) de behoefte aan de volgende rollen/functies met de gedachte dat de voorziening voor binnendringen vanaf 1 januari 2018 uit 7-12 7-12 zal bestaan. Om de processen binnen het lab goed uit te kunnen voeren, moeten er taken worden uitgevoerd die te bundelen zijn in verschillende rollen. Afhankelijk van de grootte van het team en de competenties van de medewerkers zullen medewerkers een of meerdere rollen binnen hun functie uitoefenen. Hieronder is een lijst met rollen opgenomen, met een korte beschrijving van de taken die bij deze rollen horen. Een nadere uitwerking zal in het realisatieplan plaatsvinden.

Er zal gewerkt gaan worden met een vaste kern van 7-12 fte. De DLOS van de Landelijke Eenheid is bereid om 7-12 fte vrij te maken voor de voorziening. Dit betekent dat er vanuit de eenheden, KMAR, FIOD en Dienst ICT gezocht wordt 7-12 fte flexibele formatieruimte per 1 januari 2018. Uitgangspunt om bij de voorziening te werk gesteld te kunnen worden is dat iedereen A-gescreend is.

Huidige bezetting lab CCIII

1. Op dit moment werken er 5 fte vanuit de DLOS in het lab CCIII. Per 1 februari is er vanuit de Eenheid Amsterdam al een medewerker voor 2 jaar te werk gesteld bij het lab CCIII. Daarnaast zullen ook op korte termijn een collega van de KMAR (per 1 maart) en de FIOD (A-screening loopt) op detacheringsbasis bij het lab komen werken.

Behoefte lab CCIII

1. **Coördinator:**
   a. **Taken en verantwoordelijkheden**
      De coördinator is in deze fase verantwoordelijk voor de coördinatie binnen de voorziening. Hij gaat over:
      - de inzet van mensen en middelen binnen het team.
      - de sturing op de kwaliteit van processen, mensen en middelen.
   b. **Functie eis**
      Het functieniveau is OS-D.
   c. **Vraag**
      In verband met de groei van het lab CCIII is de behoefte aanwezig om hier een teamleider verantwoordelijk voor te maken. **Gevraagd wordt om 1 fte te leveren.**
2. 7-12

7-12

3. **Operationeel jurist:**

   a. **Taken en verantwoordelijkheden**

   De operationeel jurist adviseert ten aanzien van de wettelijke mogelijkheden en onmogelijkheden ten aanzien van de operationele inzet. Juridische kennis met betrekking tot het digitale werkveld met name met betrekking tot CCIII is noodzakelijk evenals een zeer grote affiniteit met het digitale werkveld. De operationeel jurist zal in staat moeten zijn om de juridische implicaties van een specifieke technische implementatie te doorzien en aan juristen en niet-juristen te kunnen uitleggen**.** Specifieke verantwoordelijkheden zijn:

   - het geven van juridisch advies voor en tijdens de inzet.
   - bewaken dat bevel binnen de juridische kaders wordt uitgevoerd.

   b. **Functie eisen**

   - heeft een juridische (master) opleiding afgerond
   - heeft een grote affiniteit met het digitale werkveld
   - is executief.
   - het functieniveau is OS D.

   c. **Vraag**

   Het wetsvoorstel CCIII ligt nog bij de Eerste Kamer. De verwachting is dat vanuit de Eerste Kamer nog een groot aantal vragen beantwoord zal moeten worden. Daarnaast wordt er op dit moment door het Ministerie van Veiligheid en Justitie gewerkt aan een besluit onderzoek in een geautomatiseerd werk. Voor beide trajecten is juridische ondersteuning noodzakelijk**. Gevraagd wordt om 1 fte te**

7-12

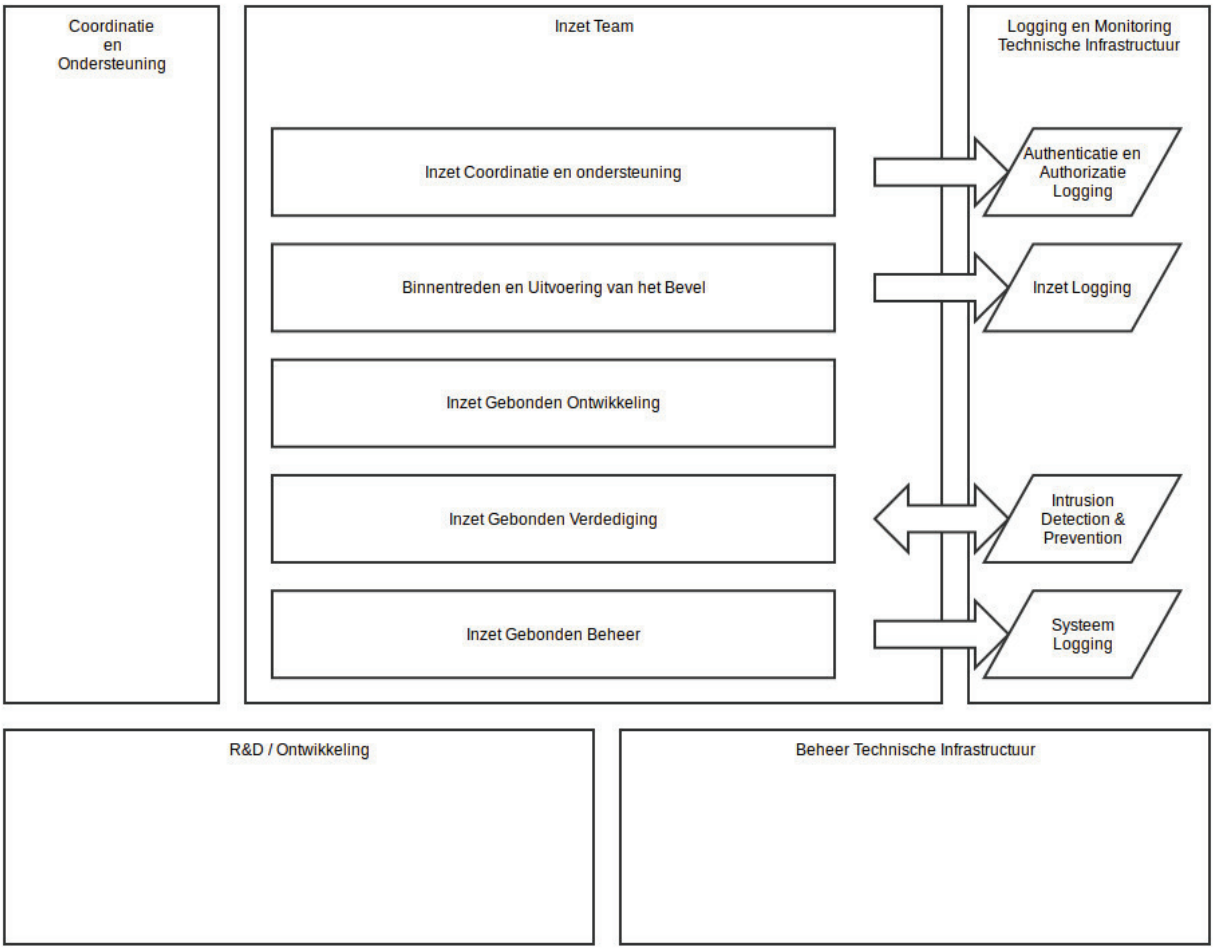
4.

5.

Fase 2

Per 1 januari 2018 zal op basis van de input van het realisatieplan gestart worden met de voorziening tot binnendringen. In dit realisatieplan zullen alle bedrijfsvoeringsaspecten aan de orde worden gesteld om te komen tot een werkende voorziening. Daarop vooruitlopend kan vastgesteld worden dat per 1 januari 2018 de voorziening tot binnendringen uit 7-12 7-12 zal moeten bestaan om de eerste zaken te kunnen draaien. Dit betekend dat er per 1 januari 2018 de behoefte bestaat aan de volgende rollen. Ook hiervoor wordt aan de Eenheden gevraagd om de benodigde capaciteit te leveren.

Het is van belang om op te merken dat sommige rollen zowel in het CCIII inzetteam benodigd zijn als in de periferie rondom het inzetteam. Deze scheiding is noodzakelijk om er zo voor te zorgen dat er ook sprake is van functiescheiding tussen het inzetteam en de overige leden van de voorziening. Op deze wijze wordt voorkomen dat manipulatie van gegevens van binnenuit mogelijk is. Schematisch ziet deze fase er als volgt uit:



CCIII Inzetteam 7-12

Een inzet team is verantwoordelijk voor het uitvoeren van een of meerdere inzetten (tegelijkertijd). Zij zouden als zelfstandig en zelfsturend team moeten functioneren en slechts een heel beperkte afhankelijkheid moeten hebben met de rest van het unit / afdeling. Op basis van ervaringen van o.a. veiligheidspartners is bepaald dat een inzet team uit 7-12 bestaat. Indien er behoefte is aan het opschalen zodat meer zaken tegelijkertijd, dan wel per tijdseenheid uitgevoerd kunnen worden, zullen extra inzet teams toegevoegd moeten worden. Het vergroten van een enkel inzet team is waarschijnlijk contraproductief. Om het inzet team zelfstandig te kunnen laten functioneren, zullen er een redelijk aantal rollen zoals hier gedefinieerd moeten worden ingevuld. Elke medewerker zal binnen het inzet team twee of meerdere rollen moeten kunnen vervullen.

1. **Leider Operaties**
   a. **Taken en verantwoordelijkheden**

      De Leider Operaties is verantwoordelijk voor het uitvoeren van haalbaarheidsonderzoek, de voorbereiding en de uitvoering van de inzet. Hierbij heeft de LO een duidelijke coördinerende verantwoordelijkheid. De LO draait meerdere zaken tegelijkertijd. De eindverantwoordelijkheid van de inzet ligt bij de teamleider.

   b. **Functie eisen**

      De LO is operationeel ingesteld en zal zeer bekend moeten zijn met het werk van de binnentreder en uitvoerder uit eigen ervaring. Het functieniveau is minimaal OS-C.

   c. **Opmerkingen**

      Deze rol kan separaat worden ingevuld, maar kan binnen het CCIII team ook door de Teamleider worden uitgevoerd, onder de voorwaarde dat de teamleider beschikt over de functie eisen; met name

2. 7-12

3.

4. 7-12

5.

6. **Operationeel jurist:**

   a. **Taken en verantwoordelijkheden**

   De operationeel jurist adviseert ten aanzien van de wettelijke mogelijkheden en onmogelijkheden ten aanzien van de operationele inzet. Juridische kennis met betrekking tot het digitale werkveld met name met betrekking tot CCIII is noodzakelijk evenals een zeer grote affiniteit met het digitale werkveld. De operationeel jurist zal in staat moeten zijn om de juridische implicaties van een specifieke technische implementatie te doorzien en aan juristen en niet-juristen te kunnen uitleggen**.**
   Specifieke verantwoordelijkheden zijn:

   - het geven van juridisch advies voor en tijdens de inzet.
   - bewaken dat bevel binnen de juridische kaders wordt uitgevoerd.

   b. **Functie eisen**

   - heeft een juridische (master) opleiding afgerond
   - heeft een grote affiniteit met het digitale werkveld
   - is executief.
   - Het functieniveau is OS D.

7-12

7.

8.

9.

7-12

10.

11.

12.

Schematisch betekent dit het volgende voor de samenstelling van het inzetteam:

Rol	LFNP Functie	Aantal
Teamleider	OS-D	1
Leider Operaties	OS-D	7-12
7-12	OS-C/D	
	OS-C/D/E	
	OS-B/C/D	
	OS-A/B/C	
	OS-C/D	
	OS-B/C/D	
	OS-B/C	
Operationeel Jurist	OS-D	
7-12	OS-A/B	
	OS-B/C/D	

Op basis van een bovenstaande, gecombineerd met een gewichtsverdeling per rol zou er rekening gehouden moeten worden dat voor een Inzetteam de volgende LFNP functies beschikbaar moeten zijn:

LFNP Functie	Aantal
OS-A	7-12
OS-B	
OS-C	
OS-D	
OS-E	

Coördinatie en Ondersteuning CCIII team 7-12

Om het CCIII inzetteam te laten functioneren zijn de volgende ondersteunende rollen/functies nodig binnen de voorziening:

1. **Teamleider:**
    a. **Taken en verantwoordelijkheden**
    De teamleider is het afdelingshoofd van de voorziening. Verantwoordelijk voor de PIOFACH-taken van de voorziening.
    b. **Functie eis**
    Het functieniveau is Teamchef C.
2. 7-12
3.

7-12

4.

5.

Investeren in de Keuringsdienst

Een belangrijk aandachtspunt is de keuring van het technische hulpmiddel. De keuringsdienst van de Landelijke Eenheid wordt hiervoor, naast haar huidige keuringswerkzaamheden, verantwoordelijk. De keuringsdienst is analoog ingesteld en zal op basis van de huidige bezetting niet in staat zijn om tijdig middelen te kunnen keuren die ingezet zullen worden voor de bevoegdheid tot het heimelijk op afstand binnendringen in een geautomatiseerd werk. De keuringsdienst zal moeten worden uitgebreid met digitaal specialisten die in staat zijn om de eisen die het besluit gaat stellen aan de keuring van het technisch hulpmiddel op een snelle en zorgvuldige manier uit te voeren.

Vooruitlopend op fase 2 is het noodzakelijk dat in fase 1 de keuringsdienst wordt uitgebreid met 7-12 om in staat te zijn de digitale middelen voor de voorziening te keuren. Deze vraag staat los van de uitvraag aan de eenheden voor het CCIII team, echter de eenheden worden ook uitgenodigd om hiervoor de expertise te leveren.

1. **Test engineer:**
    a. **Taken en verantwoordelijkheden**
    verantwoordelijk voor het keuren van de technische hulpmiddelen van de voorziening.
    b. **Functie eisen**
        - Moet in staat zijn om testen te automatiseren
        - Moet in staat zijn om regressietesting uit te kunnen voeren.
        - Kennis van de wetgeving rondom het binnendringen is gewenst.
        - Het functieniveau is OS-C/D..
    c. **Vraag**
    Om de keuring van de technische hulpmiddelen uit te kunnen voeren is **uitbreiding van de Keuringsdienst met** 7-12 **noodzakelijk.**

Investeren in security

Op het moment dat er binnengedrongen gaat worden, is het zeer waarschijnlijk dat de politie zelf ook meer aangevallen zal gaan worden. Het is absoluut noodzakelijk dat de security van de digitale infrastructuur van de Nederlandse Politie op een zeer hoog niveau ligt. 7-12 , kan hier aan belangrijke rol in spelen. 7-12

Investeren in opleidingen en huisvesting

Op basis van bovenstaande is duidelijk dat er geïnvesteerd moet worden in mensen. In de praktijk blijkt dit een grote uitdaging te zijn. Daarnaast liggen er ook nog grote uitdagen op de terreinen van opleidingen, huisvesting en middelen. Dit wordt hieronder kort toegelicht

Opleidingen
Hoog gekwalificeerd personeel is nodig om met de meest geavanceerde middelen aan de slag te gaan. Samen met de Directie HRM wordt een strategie bepaald om te komen tot een innovatieve manier van werving. Daarnaast zal er samen met de Politieacademie in 2017 gewerkt worden aan het opstellen van een opleidingsplan, om politiemedewerkers op te leiden en te certificeren om te mogen binnendringen. Tot op heden is de Politieacademie niet in staat geweest om te voldoen aan deze vraag.

Huisvesting
In 2018 zal verder worden gebouwd aan de voorziening tot binnendringen. Na een jaar experimenteren is duidelijk dat de definitieve voorziening uit 7-12 fte zal moeten bestaan om haar werkzaamheden veilig en afgeschermd uit te kunnen voeren. Op dit moment is het lab CCIII in 7-11-12 gehuisvest en deze ruimte is nu al

ontoereikend. Er zal gezamenlijk gezocht moeten worden naar een huisvestingslocatie om de voorziening adequaat te kunnen huisvesten.

Techniek, mensen, huisvesting en middelen vergen grote investeringen, terwijl het structurele budget van de Nationale Politie hierin niet voorziet. Vanuit de portefeuille D&C zijn er gelden beschikbaar gesteld voor de opstartkosten van het laboratorium CCIII, waarmee op het moment van inwerkingtreding van de wet de eerste zaken gedraaid zullen kunnen worden. De structurele kosten zijn meegenomen in de cyber security fiche.

3. Risico's

Een van de belangrijkste risico's is dat de Eerste Kamer niet akkoord gaat met het wetsvoorstel en dat het terug wordt gezonden aan de Tweede Kamer. Dit betekent echter niet dat de ontwikkeling zoals die binnen het lab CCIII is ingezet moet worden stilgezet. Er zal altijd een behoefte bestaan om de middelen die bestemd zijn voor het heimelijk binnendringen in een geautomatiseerd werk ook te gebruiken voor bijvoorbeeld de veiligheid van medewerkers bij acties 7-12 beter te kunnen garanderen. Ook zal de noodzaak blijven bestaan om het laboratorium CCIII als vangnet voor uitzonderlijke gevallen in te zetten.

Overige risico's zijn daarnaast onderschatting van de complexiteit van de materie, onvoldoende draagvlak binnen de politie om deze bevoegdheid op de voorgestelde manier in te regelen, doorlooptijden van de aanvraag van middelen en techniek (inclusief heimelijke inkoop) en de tijdige keuring van de te gebruiken middelen.

Tot slot wordt er vaak gezegd dat de inrichting van deze voorziening een ICT traject is. ICT is een belangrijke component van het binnendringen, echter de menselijke component, zoals altijd bij politiewerk is van veel groter belang. Zonder goed gekwalificeerde (en uitgeruste) mensen is deze bevoegdheid niet uit te voeren.

4. Het wetsvoorstel CCIII

Het wetsvoorstel CCIII is na een lange doorlooptijd op 20 december 2016 door een ruime meerderheid in de Tweede Kamer met twee amendementen goedgekeurd. De lange voorbereidingstijd voordat de wet uiteindelijk is goedgekeurd, gecombineerd met het politieke klimaat, de grote afbreukrisico's als de politie dit onderwerp niet goed ter hand neemt en het vergrootglas waaronder de gehele politie organisatie op dit moment ligt, maakt dat dit onderwerp met de grootste zorgvuldigheid opgepakt moet worden. De politieke discussie spitst zich toe op het heimelijk binnendringen, echter de wet gaat ook over:

- de verbeterde strafbaarstelling van online handelsfraude[1] en heling van gegevens (het wordt makkelijker om aangifte te doen en de bewijslast voor het slachtoffer wordt vereenvoudigd).
- de strafbaarstelling van grooming en corrumperen[2] , waardoor de inzet van bijvoorbeeld een (virtuele) lokpuber mogelijk wordt. Met corrumperen wordt de strafbepaling van 248 Sr uitgebreid door het kind beter te beschermen tegen schadelijke invloeden op de persoonlijke en seksuele ontwikkeling.
- het ontoegankelijk maken van gegevens wordt mogelijk gemaakt langs de digitale weg (naar analogie tegenhouden in de fysieke wereld).

[1] Voor het onderwerp online handelsfraude is een impactanalyse opgesteld en deze is door tussenkomst van de portefeuillehouder D&C op 25 november 2015 aangeboden aan de toenmalig projectleidster LSCeC voor verdere uitwerking.
[2] Met het Landelijk Programma Zeden zijn afspraken gemaakt over de onderwerpen grooming en corrumperen. In 2017 zal er nog een impactanalyse worden opgesteld over de strafbaarstelling van heling van gegevens.

Het wetsvoorstel CCIII gaat over de vergroting van de effectiviteit van het politieoptreden in het gehele opsporingsdomein. Met deze bevoegdheid zullen we als politie onder andere weer in staat zijn om bij de communicatie tussen criminelen te komen. De traditionele interceptietechnieken leveren tegenwoordig steeds minder voldoende inhoudelijke informatie (encryptie) op. Met deze nieuwe bevoegdheid repareren we (gedeeltelijk) de achterstand, die de politie heeft op het terrein van de digitalisering van de maatschappij en de criminaliteit. Deze wet biedt de politie de mogelijkheid om op creatieve wijze de criminaliteit aan te pakken, door juist in de virtuele wereld gebruik te maken van mogelijkheden die in de fysieke wereld niet aanwezig zijn.

Heimelijk op afstand binnendringen

De uitoefening van deze bevoegdheid zal met zware waarborgen omkleed zijn. De belangrijkste hiervan zijn:

- Strafmaat (in principe) > 8 jaar of meer [3]
- Toetsing vooraf door OvJ/RC/CTC
- Keuringseisen software analoog aan de inzet van heimelijke middelen
- Meldingsplicht gebruikte onbekende kwetsbaarheden
- Onafhankelijk toezicht door de Inspectie I&V
- Expliciete functiescheiding technisch team en tactisch team
- Alleen inzet van gekwalificeerde aangewezen ambtenaren

Er zal voldoende transparantie in moeten worden gebouwd om de buitenwereld te overtuigen van de juiste inzet van deze bevoegdheid (voldoende logging en monitoring). Er zal sprake moeten zijn van een functiescheiding tussen techniek en tactiek omwille van de onafhankelijkheid[4]. Dit betekent dat de technische voorziening gescheiden van de tactische opsporing zal worden georganiseerd.

De eerste behandeling in de Eerste Kamer is voorzien op 7 maart 2017. De verwachting is dat het wetsvoorstel uiterlijk 1 januari 2018 in werking zal treden. Daarnaast wordt er op dit moment door de Staatssecretaris van Veiligheid en Justitie, met medewerking van het project CCIII, gewerkt aan het opstellen van een apart besluit “onderzoek in een geautomatiseerd werk”. In dit besluit wordt onder ander nader uitgewerkt aan welke eisen een technisch hulpmiddel moet voldoen, op welke wijze de keuring van dit technisch hulpmiddel moet plaatsvinden, wie toegang heeft tot een

---

[3] Met betrekking tot de strafmaat is het volgende van belang voor wat betreft de onderzoekshandelingen:
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 vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen;
c. de ontoegankelijkmaking van gegevens;
d. de uitvoering van een bevel tot het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie (richtmicrofoon);
e. de uitvoering van een bevel tot stelselmatige observatie.
Voor de bevoegdheden, genoemd in de punten a., d. en e. geldt het vereiste van een feit waarvoor voorlopige hechtenis mogelijk is. Voor de vastlegging van gegevens en de ontoegankelijkmaking van gegevens (punten b en c) geldt het vereiste van een feit waarvoor gevangenisstraf van acht jaar of meer kan worden opgelegd of dat bij AMvB is aangewezen. Deze AMvB is nog in de maak.

[4] De wettelijke regeling moet ook waarborgen bieden tegen willekeurige inmenging door de overheid in het persoonlijke leven van de burger en tegen misbruik van bevoegdheid. In het voorgestelde artikel 126nba Sv zijn deze waarborgen nader uitgewerkt. De bevoegdheid kan slechts worden toegepast als sprake is van een verdenking van ernstige strafbare feiten die een ernstige inbreuk op de rechtsorde opleveren. Daarnaast moet sprake zijn van een dringend onderzoeksbelang. Voorts kan bij de inzet van de bevoegdheid slechts gebruik worden gemaakt van een technisch hulpmiddel dat voldoet aan bepaalde eisen, die zijn neergelegd in het Besluit technische hulpmiddelen strafvordering. Met deze voorwaarden wordt voorzien in adequate en effectieve waarborgen tegen willekeurige inmenging en misbruik alsmede voor het verzekeren van de authenticiteit en integriteit van door middel van het technische hulpmiddel vastgelegde gegevens. Daarbij is voorzien in functiescheiding tussen opsporingsambtenaren die betrokken zijn bij het onderzoek in een geautomatiseerd werk (het technische team) en de opsporingsambtenaren die betrokken zijn bij het operationele opsporingsonderzoek (het tactische team). Ook is voorzien in logging van de gegevens over de handelingen die in het kader van de inzet van het technische hulpmiddel worden verricht. (Memorie van Toelichting, Tweede Kamer, vergaderjaar 2015–2016, 34 372, nr. 3 pagina 54.)

technisch hulpmiddel, wie mag plaatsen en wie mag inzetten. Dit besluit zal door het Ministerie nog formeel ter consulatie aan de Korpsleiding worden voorgelegd.

5. Tot slot:

7-12 **en de Eenheden worden uitdrukkelijk uitgenodigd om naast de reeds benoemde inbreng mee te denken over de werkprocessen, de rol van de TDO's en tactische teams en de operationele behoefte.**

Van: Smit-Arnold Bik, Marjolein (C.P.M.)
Verzonden: donderdag 16 februari 2017 08:26
Aan: 10.2.e Plas, Theo van der (T.G.)
CC: 10.2.e 10.2.e 10.2.e
Onderwerp: RE: Hoofdlijnennotitie CCIII tbv BOO

Beste 10.2.e

Hartelijk dank, ik snap de behoefte maar heb echt geen idee waar wij deze formatie vandaan moeten halen. Theo, kunnen wij hier binnenkort samen even naar kijken? Dit is natuurlijk ook relevant voor de discussie die wij momenteel binnen het EMT voeren.
Zouden jullie mij ajb als 1e aanspreekpunt willen houden voor DLOS? Met 10.2.e heb ik afgesproken dat ik CCIII in portefeuille neem. Mooi onderwerp voor mij om er breed in te komen!

Groeten,

Marjolein

Van: 10.2.e @politie.nl>
Datum: 17 februari 2017 14:44:12 CET
Aan: 10.2.e @politie.nl>, Plas, Theo van der (T.G.)
10.2.e @politie.nl>
CC: 10.2.e @klpd.politie.nl>
Onderwerp: Tijdslijn Besluit Onderzoek in een geautomatiseerd werk

Beste Theo en 10.2.e

Bijgaand de tijdsplanning voor het Besluit onderzoek in een geautomatiseerd werk zoals dat ons door de Directie Wetgeving is voorgehouden

Op dit moment vindt overleg plaats tussen het project CCIII, Wetgeving, DGRR over het besluit. 24 februari is er weer een overleg op het departement. Verwachting is dat kort na dit overleg een laatste versie van het besluit, informeel, aan ons zal worden voorgelegd. Hierna zal de planning er als volgt uitzien, waarin dan ook een formele reactie van de politie (KC) gevraagd zal worden. Met de staf 10.2.e) is afgesproken dat de coördinatie hiervoor bij het project ligt. 10.2.e wordt regelmatig op de hoogte gehouden van de voortgang.

10.2 gaf aan dat op 7 maart de EK voor het eerst een reactie zal geven op het wetsvoorstel CCIII. Dit staat los van de planning van het besluit, dit zal apart worden behandeld. Verwachting is wel dat de vragen van de EK nog het nodige werk voor de politie zullen opleveren.

Dat betekent dat de datum van 11 april nog wel mogelijkheden biedt om CCIII te betrekken bij de discussie over de problematiek die de wetgeving oplevert voor de strafrechtsketen

Start formele consultatieronde (incl. toezending TK/EK): maart/begin april 2017
Ministerraad: juli 2017
Notificatie Europese Commissie (standstill periode): juli – september 2017
Adviesaanvraag Afdeling advisering Raad van State: juli – september 2017
Advies Afdeling Advisering: september 2017
Nader rapport: oktober 2017
Inwerkingtreding (gelijk met Wet CCIII): 1 januari 2018

Hiernaast zal ook nog gewerkt worden aan een AMvB waarin nadere misdrijven zullen worden opgenomen waarop de wet van toepassing zal zijn. De planning hiervan is nog niet bekend.

Mochten er nog vragen zijn, dan hoor ik dat graag.

Met vriendelijke groet,
Mede namens 10.2.
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

Van: Plas, Theo van der (T.G.)10.2.e @politie.nl>
Datum: 17 februari 2017 20:18:07 CET
Aan: 10.2.e @politie.nl>
Onderwerp: Doorst: Tijdslijn Besluit Onderzoek in een geautomatiseerd werk

Ha10.2.e , volgende week bespreken of dit goed in samenhang met jouw activiteiten en verantwoordelijkheden verloopt, groeten, Theo

drs. T.G. (Theo) van der Plas EMPM
Plv. Politiechef/Hoofd Operatiën Landelijke Eenheid
Politie | Landelijke Eenheid
Hoofdstraat 54, 3972 LB Driebergen
Postbus 100, 3970 AC Driebergen
T10.2.e

Van: 1 @politie.nl>
Datum: 17 februari 2017 20:35:16 CET
Aan: Plas, Theo van der (T.G.) 10.2.e @politie.nl>
Onderwerp: Antw: Tijdslijn Besluit Onderzoek in een geautomatiseerd werk

Hallo Theo,

9

9 Even voor het beeld: van alle gestelde vragen bij het TK debat dat ze ook wel zelf zouden regelen heb ik de helft alleen beantwoord....
9

Graag overleg dus.

Groet,

10.2.e

Van: Plas, Theo van der (T.G.)
Verzonden: vrijdag 17 februari 2017 20:44
Aan: 10.2.e
Onderwerp: Antw: Tijdslijn Besluit Onderzoek in een geautomatiseerd werk

...doen we, ook dit gaan we stroomlijnen. Nemen we gelijk mee, net als de rest gaan we dat snel beter in de groef zetten.

Groeten,theo

drs. T.G. (Theo) van der Plas EMPM
Plv. Politiechef/Hoofd Operatiën Landelijke Eenheid
Politie | Landelijke Eenheid
Hoofdstraat 54, 3972 LB Driebergen
Postbus 100, 3970 AC Driebergen
T (0343) 10.2.e

Van: 10.2.e - BD/DGPOL/PBT/PT 10.2.e @minvenj.nl]
Verzonden: maandag 20 maart 2017 12:59
Aan: 10.2.e @politie.nl>
Onderwerp: besluit CC3

Hoi 10.2.e ,
A.s. woensdag praat ik met 10.2.e c.s. bij over het besluit CC3 omdat ik de eerdere bijeenkomsten niet kon bijwonen. In dat kader lijkt het mij goed om even telefonisch bij te praten c.q. af te stemmen. Heb jij daar morgen of woensdagochtend (voor 10.30 uur) tijd voor?
Vriendelijke groet,
10.2.e

Met vriendelijke groet,

10.2.e
(senior) beleidsmedewerker

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
9
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
T 06 10.2.e
10.2.e @minvenj.nll
www.rijksoverheid.nl/venj
.....
Voor een veilige en rechtvaardige samenleving
.....

Van: 9 - BD/DGPOL/PBT/PT 9 @minvenj.nl>
Verzonden: woensdag 22 maart 2017 14:41
Aan: 9); 9
CC: 9 - BD/DGPOL/PMP/HRMO
Onderwerp: RE: besluit CC3

Hoi 9 ,
Inmiddels heb ik samen met 9 (cc) gesproken met 9 en 9 van de directie Wetgeving over de AMvB onderzoek in een geautomatiseerd werk en meer in het bijzonder over de eisen die aan de deskundigheid/opleiding van medewerkers van het technische team moeten worden gesteld. Hebben jullie al ideeen over de (opleidings)eisen die aan deze medewerkers moeten worden gesteld. Moet hiervoor iets aparts geregeld worden of is een verwijzing (ik zeg maar wat) naar een bepaalde categorie van het LFNP voldoende? Gaat het hier om ICT-kennis en toepassing van opsporingsbevoegdheden. Zijn het zij-instromers? Welk niveau?
Een andere vraag is: waar wordt het technische team opgehangen? Als ik het goed heb begrepen, is het de bedoeling dat eerst de LE op deze wijze (a la cc3) aan de slag gaat en wellicht op termijn de eenheden ook. Voor dat laatste zou het besluit overigens wel moeten worden aangepast. Anyway, is ophanging bij LE voldoende of moet de ophanging verder gedefinieerd worden? Zo ja hoe en waarom?

We hebben niet veel tijd om een en ander uit te werken. Ik heb begrepen dat de AMvB volgende maand in consultatie gaat. Dus dan moet dit ook uitgewerkt zijn. Met andere woorden heb je/hebben jullie tijd om op korte termijn om de tafel te gaan?

Groet,
9

Met vriendelijke groet,

9
(senior) beleidsmedewerker

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
9
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
T 06 9
9 @minvenj.nll
www.rijksoverheid.nl/venj
.....
Voor een veilige en rechtvaardige samenleving
.....

Van: 10.2.e
Verzonden: woensdag 22 maart 2017 15:24
Aan: 9 .politie.nl>; 10.2.e @politie.nl>
Onderwerp: Inspectie en AMvB

Hallo collega's,

Ik heb contacten met de inspectie over onderzoek op het gebied van cybercrime. En begrijp daaruit dat jullie al een
aantal maanden met hen praten over het onderzoek CCIII dat zij moeten gaan uitvoeren.
Kunnen jullie me daar svp. over informeren?

En ook over de AMvB die in ontwikkeling is of andere dingen die voor mij van belang zijn om te weten?

Dank vast,
10.2.e

Van: 10.2.e
Verzonden: woensdag 22 maart 2017 16:00
Aan: 10.2.e 10.2.e
Onderwerp: RE: Inspectie en AMvB

10.2.e

Dat is correct, overigens alles in overleg met onze directe opdrachtgever Marjolein en portefeuillehouder Theo.
Jij zou nog steeds een keer langskomen (ook voor een bezoekje lab) en je bent nog steeds even welkom als altijd!
Dan nemen we alles een keer door.

Heb je een aantal data dat je in 3=B e.o. bent? Dan plannen we een afspraak en bezoek, m.vr.gr,

10.2.e
9
Politie | Project CCIII
Lookant 1, 3971 PP Driebergen-Rijsenburg
Postbus 100, 3970 AC Driebergen-Rijsenburg

Van: 1
Verzonden: woensdag 22 maart 2017 18:47
Aan: 1 @klpd.politie.nl>; 10.2.e @politie.nl>
CC: Plas, Theo van der (T.G.) 10.2.e @politie.nl>; Smit-Arnold Bik, Marjolein (C.P.M.) 9 @politie.nl>
Onderwerp: Technische briefing

Hallo collega's,

De EK heeft gisteren besloten een deskundigenbijeenkomst te gaan houden over ANPR en CCIII. Zie hieronder. Er moet nog een datum bepaald worden.
Dit is een soort ronde tafel. We hebben natuurlijk ook al de ronde tafel gehad in de TK, dus er is al wel materiaal beschikbaar.

Laten we elkaar informeren over aanvullende informatie die beschikbaar komt.

1.
33542
Vastleggen en bewaren kentekengegevens door politie
De commissie besluit de nadere procedure aan te houden tot een nader te bepalen datum, om zich te laten informeren door een aantal deskundigen. Zij zal daartoe een deskundigenbijeenkomst organiseren op een nader te bepalen datum, waarbij zowel het onderhavige wetsvoorstel als het wetsvoorstel Computercriminaliteit III (34372) centraal staat. De commissie kiest uit haar midden de volgende leden die de voorbereidingsgroep vormen voor de organisatie van de deskundigenbijeenkomst: Duthler (VVD), Bredenoord (D66), Beuving (PvdA) en Strik (GroenLinks).

Groet,
10.2.e

Van: Smit-Arnold Bik, Marjolein (C.P.M.)
Verzonden: donderdag 23 maart 2017 07:49
Aan: 10.2.e @politie.nl>; 10.2.e @klpd.politie.nl>; 10.2.e @politie.nl>
CC: Plas, Theo van der (T.G.) 10.2.e @politie.nl>
Onderwerp: RE: Technische briefing

Beste allemaal,

Wie bereiden dit voor? Kan ik nog iets doen?

Groeten,

10.2.e

Van: 10.2.e @politie.nl]
Verzonden: donderdag 23 maart 2017 9:58
Aan: 10.2.e - BD/DGPOL/PBT/PT
Onderwerp: RE: besluit CC3

Hoi 10.2.e

Ik was een paar dagen vrij en zie deze mail dus nu pas…Vandaag en morgen ben ik aan het studeren voor een examen volgende week, maar wel redelijkbeschikbaar voor telefonisch overleg, al less ik wel dat je gisteren al met 10.2.e hebt gesproken…

Ik hoor graag of we nog even
moeten bellen!Groet, 10.2.e

Van: 10.2.e
Verzonden: donderdag 23 maart 2017 13:38
Aan: Smit-Arnold Bik, Marjolein (C.P.M.) 9 @politie.nl>; 10.2.e politie.nl>; 10.2.e @politie.nl>
CC: Plas, Theo van der (T.G.) 10.2.e @politie.nl>
Onderwerp: RE: Technische briefing

10.2.e e.a.

Wij hebben dit afgelopen jaar ook uitvoerig en diepgaand voorbereid voor de Tweede Kamer. Dat hebben wij als project gedaan in nauwe samenwerking met jouw voorganger(s) Inge Philips, Dick Pijl, het MvVJ, het Openbaar Ministerie en uiteraard de dir Operatiën, 10.2.e Zodra de planning bekend is, zullen we de voorbereidingen starten. De volgorde der dingen wordt te allen tijde bepaald door de Kamer(s) zelf, uiteraard. Naast de inhoudelijke voorbereiding, zal ook afgesproken dienen te worden wie de officiele woordvoerder namens de politie wordt, ik stel mij voor Theo of jij, onderling af te stemmen. M.vr gr,

10.2.e

9

Politie | Project CCIII
Lookant 1, 3971 PP Driebergen-Rijsenburg
Postbus 100, 3970 AC Driebergen-Rijsenburg

Van: 10.2.e - BD/DGPOL/PBT/PT
Verzonden: donderdag 23 maart 2017 13:46
Aan: 10.2.e
CC: 10.2.e @politie.nl
Onderwerp: RE: besluit CC3

Hoi 10.2.e ,
Dank voor je reactie en succes met je examen! Ik heb naar aanleiding van het gesprek met 10.2.e nog een vraag bij jou neergelegd. Zie bijlage.
Groet,
10.2.e

Met vriendelijke groet,

9
(senior) beleidsmedewerker

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
9
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
T 06 10.2.e
10.2.e @minvenj.nll
www.rijksoverheid.nl/venj
.....

Van: 10.2.e
Verzonden: donderdag 23 maart 2017 14:34
Aan: 10.2.e Smit-Arnold Bik, Marjolein (C.P.M.); 10.2.e
CC: Plas, Theo van der (T.G.); 10.2.e
Onderwerp: RE: Technische briefing

Hallo allemaal,

Ik ga er inderdaad ook vanuit dat we het weer op dezelfde manier kunnen voorbereiden. Dat ging prima. Ik probeer nog wel wat meer informatie te krijgen of dit eenzelfde soort bijeenkomst is als de Ronde Tafel in de TK. Dat is nog niet helemaal duidelijk. En de uitdaging is dat blijkbaar CCIII en ANPR 28 dagen database tegelijk behandeld worden, wat betekent dat we dat in samenhang moeten voorbereiden en ook in de afvaardiging moeten kijken wie dat kunnen doen.
Ik heb al wel aangegeven dat ik dan verwacht dat we meer mensen mogen afvaardigen dan in de vorige Ronde tafel.

Zodra ik meer informatie heb laat ik het weten.

Groet,

10.2.e

Van: 10.2.e BD/DGPOL/PBT/PT10.2.e @minvenj.nl]
Verzonden: zondag 26 maart 2017 14:14
Aan: 10.2.e @politie.nl>
CC: 10.2.e @politie.nl>10.2.e - BD/DGPOL/PMP/HRMC10.2.e @minvenj.nl>
Onderwerp: FW: besluit CC3

Hoi 10.2.e ,
Ik heb nagelaten om jou te wijzen op de urgentie van dit vraagstuk. Bij deze alsnog. Volgende maand gaat de AMvB in consultatie en moet de richting bepaald zijn. Kunnen we morgen, maandag dus, even telefonisch contact hebben?
Ik hoor graag van je.
Vriendelijke groet,
10.2.e

Met vriendelijke groet,

10.2.e
(senior) beleidsmedewerker

.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
9
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
T 06 10.2.e
10.2.e @minvenj.nll
www.rijksoverheid.nl/venj
.....
Voor een veilige en rechtvaardige samenleving
.....

From: 10.2.e @politie.nl>
Subject: **RE: besluit CC3**
To: 10.2.e - BD/DGPOL/PBT/PT" 10.2.e @minvenj.nl>
Date: 27 maart 2017 12:38:22 CEST

Hoi 10.2.e,

Ik zit midden in een studiedag voor een examen morgen. Ik kom hier woensdag pas aan toe. Kan ik je woensdagochtend bellen?

12-14

Ik hoop dat dit al wat helpt, nogmaals woensdag ben ik weer goed bereikbaar om het telefonisch meer toe te lichten.

Met vriendelijke groet,
10.2.e

Van: 10.2.e - BD/DGPOL/PBT/PT
Verzonden: dinsdag 4 april 2017 10:44
Aan: 10.2.e - BD/DWJZ/SSR
CC: 10.2.e - BD/DRC/CV
Onderwerp: AMvB Geautomatiseerd werk CC3

Beste 9
Recent spraken wij over de AMvB GW. Je vroeg ons om input op de vraag of – en zo ja op welk niveau – de opleidingseisen die gesteld worden aan het technische team moeten worden opgenomen in de AMvB. Wij bekijken op dit moment welke systematiek naar aard en inhoud voor de hand zou liggen. In dat kader rijst bij ons de vraag of de leden van het technische team gebruik maken van bijzondere opsporingsbevoegdheden. Zijn de relevante bevoegdheden uit CC3 aan te merken als bijzondere opsporingsbevoegdheden als het technische team geen onderdeel uitmaakt van het onderzoeksteam (functiescheiding)? Verricht het technisch team dan wel opsporingsonderzoek?
Wij vermoeden dat het techn team ook dan bijzondere opsporingsbevoegdheden toepast, maar horen graag hoe jij hier tegenover staat.

En tenslotte, kun je me helpen aan een laatste integrale tekst van de AMvB?

Ik hoor graag van je.
Vriendelijke groet,
10.2.e

Met vriendelijke groet,

10.2.e
(senior) beleidsmedewerker

Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
9
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag

T 06 10.2.e
10.2.e @minvenj.nll
www.rijksoverheid.nl/venj

Voor een veilige en rechtvaardige samenleving

Van: 10.2.e - BD/DWJZ/SSR
Verzonden: dinsdag 4 april 2017 17:31
Aan: 10.2.e - BD/DGPOL/PBT/PT
CC: 10.2.e - BD/DRC/CV
Onderwerp: RE: AMvB Geautomatiseerd werk CC3

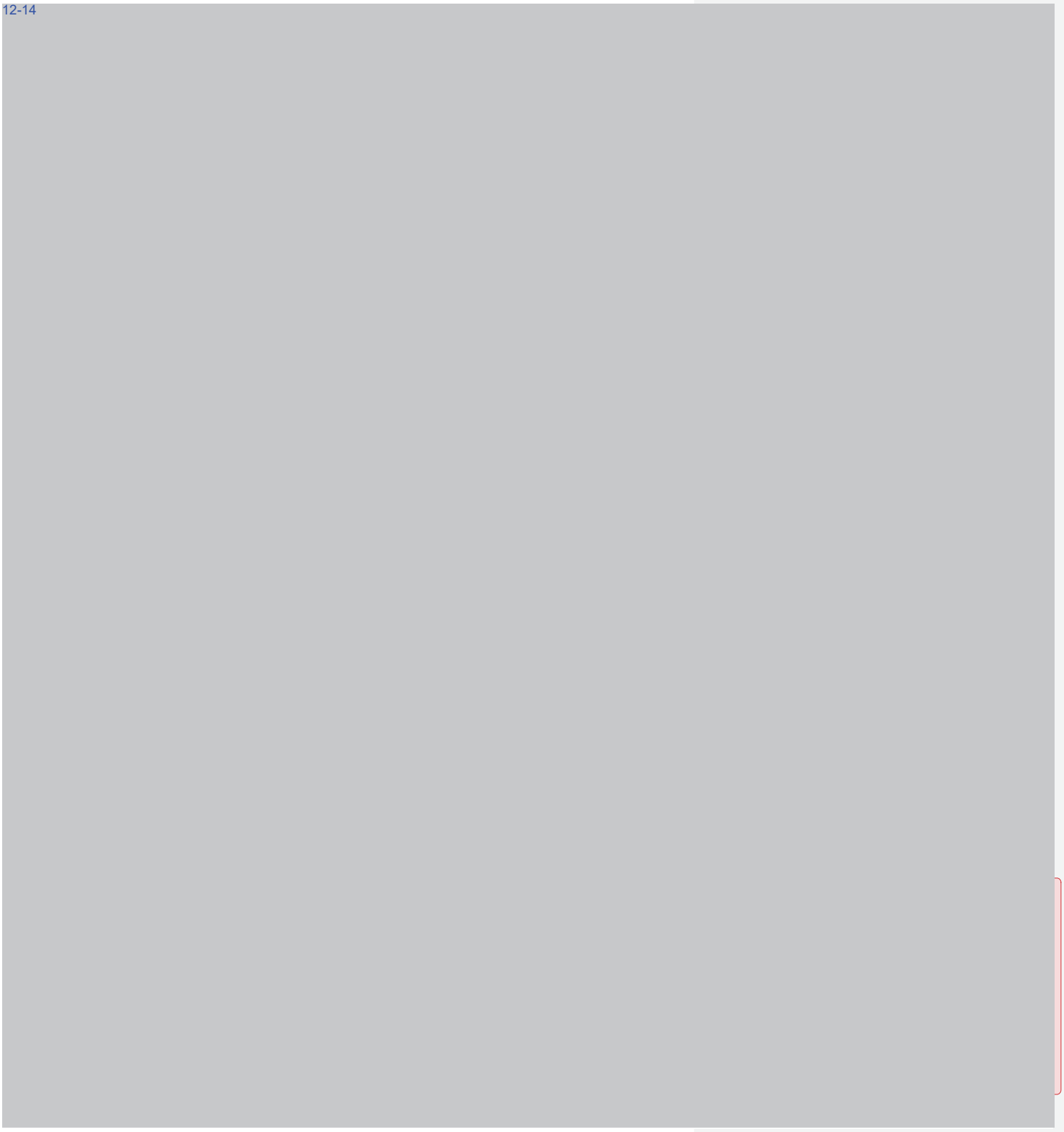
Hoi 10.2.e

De nieuwe bevoegdheden in het wetsvoorstel CCIII (126nba/126uba/126zpa) maken onderdeel uit van Titel IVa van het Wetboek van Strafvordering waarin de bijzondere opsporingsbevoegdheden worden geregeld. De leden van een technisch team worden met de uitvoering hiervan belast en verrichten dus opsporingsonderzoek.

Ik voeg concept-versies van het Besluit onderzoek in een geautomatiseerd werk + nota van toelichting (versie 3 februari) bij. Deze stukken zijn begin februari ook verspreid onder de deelnemers aan het overleg.

Binnenkort hoop ik nieuwe versies op te leveren. Mn de volgorde van de artikelen in het Besluit zal nog wijzigen. En de nota van toelichting wordt aangevuld met een artikelsgewijs deel. Zodra gereed, dan stuur ik deze versies toe.

Groet 10.2.e


12-14

12-14

12-14

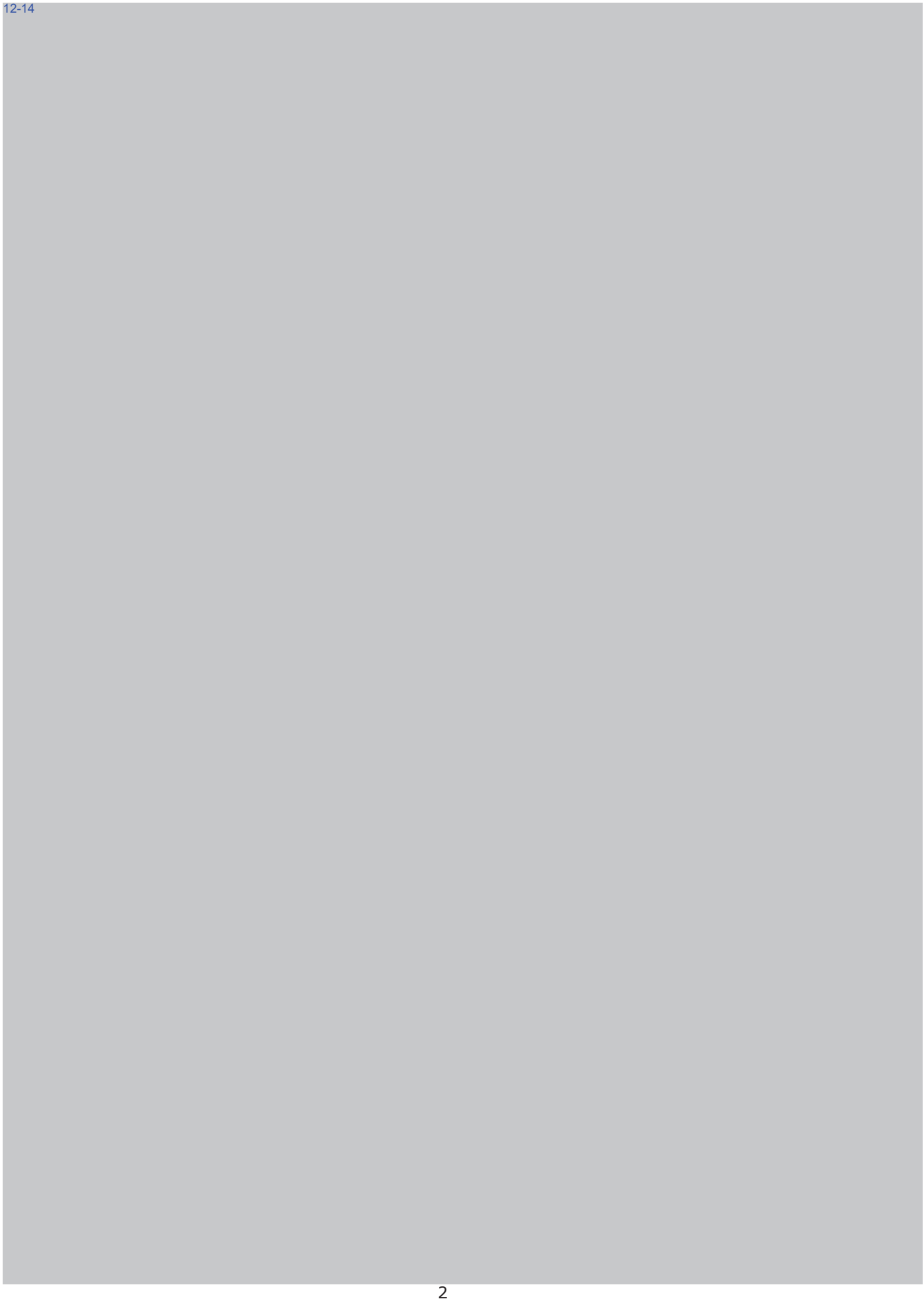
12-14

12-14

Concept-versie voor overleg 3 februari 2017

12-14

12-14



12-14

12-14

12-14

12-14

Van: 10.2.e - BD/DGPOL/PBT/PT 10.2.e @minvenj.nl>
Datum: 4 april 2017 17:42:30 CEST
Aan: 10.2.e @politie.nl>, 9 - BD/DGPOL/PMP/HRMO 9 @minvenj.nl>
CC: 10.2.e @politie.nl>, 9 - BD/DGPOL/PMP/HRMO 9 @minvenj.nl>
Onderwerp: FW: AMvB Geautomatiseerd werk CC3

Beste 10.2.e en 10.2.e

Bij deze de bevestiging van ons overleg over de AMvB CC 3 en de opleidingseisen op 12 april a.s. om 13.00 uur. Locatie: MVenJ, Noordtoren 28e etage. 10.2.e , ik meld je aan.
Bij deze – mede op verzoek van 10.2.e – de laatste versie van de AMvB en van de nota van toelichting.

Graag tot volgende week woensdag!

Groet,

10.2.e

Met vriendelijke groet,

10.2.e
(senior) beleidsmedewerker

Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
9
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag

T 06 10.2.e
10.2.e @minvenj.nll
www.rijksoverheid.nl/venj

Voor een veilige en rechtvaardige samenleving

Van: 10.2.e
Verzonden: dinsdag 4 april 2017 22:06
Aan: 10.2.e @klpd.politie.nl>; 10.2.e @politie.nl>
10.2.e @politie.nl>; 10.2.e @politie.nl>; Plas, Theo van der (T.G.)
10.2.e @politie.nl>
Onderwerp: FW: AMvB Geautomatiseerd werk CC3

Beste 10.2.e, 10.2.e en 10.2.e,

Nog bedankt voor het werkbezoek maandag. Goed om even in alle rust bijgepraat te worden. Een van mijn actiepunten was het regelen van de laatste versie van de AMVB zodat jullie kunnen kijken in hoeverre jullie opmerkingen nu op zijn genomen.

Bij deze de versie die ik vandaag ontving. Willen jullie svp met enige spoed kijken of jullie opmerkingen zijn verwerkt en waar echt nog punten zitten die voor ons echt problematisch zijn?

Dan ga ik kijken of ik daar nog in kan interveniëren.

Is een eerst indicatie van ernstige bezwaren vrijdag mogelijk, zodat ik alvast wat aan de slag kan?
Er wordt aangegeven dat de AMVB deze maand al weggaat, dus de ruimte om nog invloed uit te oefenen is beperkt.

Ik hoor het graag,
Groet,
10.2.e

Van: 10.2.e
Verzonden: woensdag 5 april 2017 08:40
Aan: 10.2.e @politie.nl>; 10.2.e @klpd.politie.nl>; 10.2.e @politie.nl>
CC: 10.2.e @politie.nl>; Plas, Theo van der (T.G.) 10.2.e @politie.nl>
Onderwerp: RE: AMvB Geautomatiseerd werk CC3

Goede morgen 10.2.e

De versies van de AMvB en de NvT die je hebt gekregen zijn van voor het eerste overleg van 3 februari en daarmee identiek aan de versie die we al hadden. Tijdens de drie overleggen die daarna hebben plaatsgevonden zijn door alle partijen *veel* opmerkingen gemaakt, onderwerpen besproken en informatie gegeven. Deze moeten verwerkt worden in de AMvB en de NvT. Ikzelf heb, zoals aangegeven je werkbezoek, mijn bedenkingen of de schrijvers van de AMvB en NvT de materie goed genoeg doorgrond hebben en onze standpunten en argumenten voldoende hebben begrepen.

In deze versies van het AMvB en NvT zijn alle opmerkingen dus nog niet verwerkt en daardoor blijft de beoordeling of ze op 'onze' punten gehoor hebben gegeven nog even uit.

Met vriendelijke groeten,
10.2.e

From 10.2.e @politie.nl>
Subject **RE: AMvB Geautomatiseerd werk CC3**
To 10.2.e @politie.nl>, 10.2.e @klpd.politie.nl>, 10.2.e @politie.nl>
Date 5 april 2017 9:21:08 CEST

Goedemorgen,

Eens met de opmerkingen van 10.2.e . Dit is inderdaad een versie die we een paar maanden geleden gekregen hebben en waar nog geen enkele opmerking van ons in is verwerkt.

Ik hoop dat wij zeer binnenkort alsnog een nieuwe versie krijgen vanuit het ministerie om vooruitlopend op de officiële consultatieronde toch nog informeel een reactie te kunnen geven. 9

Ik zal nog even bij 10.2.e navragen of hij wellicht iets meer info heeft voor ons.

Met vriendelijke groet,
10.2.e

Van: 10.2.e @politie.nl]
Verzonden: donderdag 6 april 2017 10:00
Aan: 10.2.e - BD/DRC/CV
CC: 10.2.e - BD/DGPOL/PBT/PT;10.2.e - BD/DRC/CV
Onderwerp: AMVB CCIII
Urgentie: Hoog

Hallo 10.2.e

Alles goed? Ik begreep van10.2.e en 10.2.e dat er inmiddels al 3 vergaderingen zijn geweest over de AMVB CCIII. Dat was mij niet bekend helaas, maar in begrijp dat er veel inhoudsdeskundigen bij zijn geweest om input te leveren.
Nu blijkt echter dat de laatste versie van de AMVB die ik via 10.2.e ontving dezelfde is als de versie aan het begin van de besprekingen. Ik hoop dat dit een foutje is en dat we de verkeerde versie hebben ontvangen. Zo niet dan vraag ik me af hoe dit kan?

Misschien zou jij wat meer duidelijkheid kunnen scheppen over de stand van zaken?
Wat is nu het vervolg om te komen we tot een werkbare AMVB waarin rekening is gehouden met de uitvoeringseffecten?

Hoor het graag.

Groet,

10.2.e

From 10.2.e - BD/DRC/CV" 10.2.e @minvenj.nl>
Subject **RE: AMVB CCIII**
To 10.2.e @politie.nl>
Date 6 april 2017 13:53:33 CEST

9 - BD/DWJZ/SSR 9 @minvenj.nl 9
9 - BD/DWJZ/JA (9 @minvenj.nl) 9

10.2.e
Policy advisor cyber crime
.....
Ministry of Security and Justice of The Netherlands
Law Enforcement Department
Cybercrime unit
Turfmarkt 147 | 2511 DP | Den Haag | The Netherlands
Postbus 20301 | 2500 EH | Den Haag | The Netherlands
.....
M (+31) 6 10.2.e
10.2.e @minvenj.nl
www.rijksoverheid.nl/venj
.....
Ministerie van Veiligheid en Justitie

Van: 10.2.e **- BD/DGPOL/PMP/HRMO**
Verzonden: woensdag 12 april 2017 16:02
Aan: 10.2.e **- BD/DGPOL/PBT/PT;** 10.2.e **@politie.nl';** 10.2.e **@politie.nl**
CC: 10.2.e **BD/DGPOL/PMP/HRMO**
Onderwerp: POR advies over opleiding CC3

Dag allemaal

Zoals net besproken zou ik een aanzet geven om te komen tot een tekstje waarin we richting POR kenbaar maken dat we een adviesaanvraag willen indienen voor de kwalificaties ten behoeve van een lid van het technisch team in het kader van CC3. Graag jullie aanvullingen (ik denk dan met name aan 10.2.e

Kwalificaties CC3
- graag advies over de kwalificaties die nodig zijn voor een opsporingsambtenaar bij een technisch team op basis van de wet CC3. Het gaat hier om een voorbehouden handeling, modaliteit 2.
- naar het voorbeeld van de internationale opleiding OSCP die ook door de AIVD wordt afgenomen.
- met name de vaardigheden x en y en z zijn hierbij van belang
- willen we ook iets met competenties
- kwalificaties gelden niet alleen voor politie, maar ook voor KMAR, BOD-en en Boa's
- de KMAR en de BOD-en verzorgen hun eigen opleiding
- het gaat om een klein aantal opleidingen voor politie. In eerste instantie 15-20 in 2018, daarna xxxx
- wil de PA zelf de opleiding ontwerpen, of neemt zij onderaannemer

Groeten 10.2.e

Met vriendelijke groet,

10.2.e
Senior beleidsmedewerker
.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
Programma HRM en Onderwijs
Turfmarkt 147 | **2511 DP** | **Den Haag**
Postbus 20301 | **2500 EH** | **Den Haag**
.....
M **06** 10.2.e
10.2.e **@minvenj.nl**
www.rijksoverheid.nl/venj

Van: 10.2.e - BD/DRC/CV 10.2.e @minvenj.nl]
Verzonden: woensdag 12 april 2017 19:16
Aan: 10.2.e politie.nl>
CC: 10.2.e @klpd.politie.nl>;10.2.e BD/DGPOL/PBT/PT 10.2.e @minvenj.nl>
Onderwerp: FW: Verwachting input vragen CCIII

Hallo 10.2.e

In bijgevoegd document heb ik de nnav TK en de handelingen naast het voorlopig verslag van de EK gelegd. In het rood vind je de tekstgedeeltes, als er alleen een cijfer voor staat verwijst dit naar het antwoord op de betreffende vraag in de nnav TK. Uiteraard moeten deze teksten worden herschreven, maar de info lijkt paraat.

In het groen heb ik aangegeven waar mi nog antwoorden moeten komen, of waar we een scherper antwoord nodig hebben. Dit ziet vooral op:

-welke andere mogelijkheden er exact zijn onderzocht anders dan de voorgestelde bevoegdheden (vraag 11).
-zijn er andere terreinen waar opsporingsdiensten onvoldoende resultaat boeken als gevolg van ontbreken voorgestelde hackbevoegdheden (zo mogelijk nadere cijfermatige onderbouwing voor ruime bevoegdheid, vraag 19)
-keuring van de software applicatie zodat zeker is dat deze geen informatie aan derden verschaft (vraag 23)
-2 vragen nav beslissing FBI om kindermisbruikzaak te seponeren om kwetsbaarheid niet vrij te geven (vraag 24, 25)
-de omgang met de markt van hackkennis. Is nu vooral gebaseerd op de handelingen (vraag 26, 27, 28, 29, 30, 33)
-dilemma dat RC A in onderzoek X kan beslissen een kwetsbaarheid te openbaren die geheim mocht blijven volgens RC B in onderzoek Y (vraag 32)
-vraag GL om heel precies in te gaan op gevaar openlaten kwetsbaarheid dat mogelijk tot meer kwaliteit leidt misschien uitgebreider (vraag 35)
-de begroting vragen (vraag 62, 63, 64, 65)
-internationale vragen, nu is geput uit de vragen nav de Internationale cyberstrategie (73, 74, 77)
-of bijvangst van fiscale aard kan worden doorgestuurd naar de belastingdienst (vraag 80)
-procedure wanneer provider/aanbieder en Ovj verschil van inzicht hebben over het ontoegankelijk maken (vraag 81)
-hoe voorkomst de regering de veelvuldig gebruik van de bevoegdheid zoals dat bij andere bijzondere bevoegdheden wel gebeurt (vraag 86, 87)

10.2.e en 10.2.e zijn deze week in het buitenland voor overleg dus ik kan dit pas volgende week met ze bespreken. Maar dit geeft je hopelijk al wel richting naar welke informatie we op zoek zijn.

Met vriendelijke groet,

10.2.e
Beleidsadviseur

2. Effectiviteit van het wetsvoorstel
3. De noodzaak van deze drastische uitbreiding van bevoegdheden is voornoemde leden niet helemaal duidelijk. Kan de regering aangeven **hoe groot het probleem is dat het wetsvoorstel moet oplossen**? Hoeveel zaken kunnen er nu niet opgelost worden, maar zouden met deze wetgeving waarschijnlijk wel worden opgelost? DRC, OM

1. De noodzaak van de nieuwe bevoegdheid ligt in de voortschrijdende techniek en het wijdverbreide gebruik van geautomatiseerde werken voor communicatie en de verwerking en opslag van gegevens. Daardoor wordt het voor de opsporing steeds lastiger om aanknopingspunten te vinden voor de inzet van wettelijke bevoegdheden. De huidige bevoegdheden rond de inbeslagneming van geautomatiseerde werken zijn gekoppeld aan de plaats waar het geautomatiseerde werk zich fysiek bevindt. De ontwikkeling van het internet maakt het echter eenvoudig om vanuit het buitenland met behulp van een geautomatiseerd werk strafbare feiten te plegen jegens personen of objecten die zich in Nederland bevinden. Daarbij kan de locatie van het werk en de betrokkenheid van bepaalde personen eenvoudig worden verhuld door het gebruik van een draadloos netwerk, van de diensten van een buitenlandse aanbieder of van encryptie of andere versleutelings- en anonimiseringstechnieken. Daardoor wordt het voor de opsporing in toenemende mate lastig of zelfs onmogelijk om strafbare gedragingen, die worden gepleegd met behulp van geautomatiseerde werken te koppelen, aan bepaalde personen. Dit belemmert de inzet van traditionele opsporingsbevoegdheden, zoals het aftappen van telecommunicatie, het vorderen van gegevens bij aanbieders en het vragen van rechtshulp aan andere landen. In dergelijke gevallen kan het op afstand binnendringen in het geautomatiseerde werk uitkomst bieden. Deze bevoegdheid wordt niet voorgesteld omdat andere methoden tijdrovender zijn en hacken nu eenmaal makkelijker is maar omdat er misdrijven onopgelost blijven door het ontbreken van een dergelijke bevoegdheid.

Bij de voorbereiding van dit voorstel is uiteraard onderzocht in hoeverre er minder vergaande mogelijkheden beschikbaar zijn waarbij de privacy beter is gewaarborgd. Hiervoor kan worden verwezen naar de memorie van toelichting. Geconcludeerd is dat de bestaande bevoegdheden te kort schieten omdat deze ofwel zijn gekoppeld aan een bepaalde fysieke plaats ofwel niet zijn gericht op de toegang tot elektronische gegevens die zich in een geautomatiseerd werk of op een gegevensdrager elders bevinden. Dit komt hieronder, naar aanleiding van soortgelijke vragen van de leden van andere fracties, nader aan de orde.

3. Proportionaliteit en privacy
7. De leden van de **D66**-fractie merken op dat het wetsvoorstel de zogenaamde 'hackbevoegdheid' introduceert: de bevoegdheid voor de politie om in te kunnen breken in elk digitaal apparaat van willekeurige burgers, inclusief toegang tot alle historische en toekomstige gegevens opgeslagen in randapparatuur en uitgewisseld met alle hiermee verbonden communicatiekanalen. Met de groei van het internet of things zal dit een groeiende lijst (digitale) apparatuur omvatten. Dit zijn niet alleen gegevens die de verdachte betreffen, maar ook gegevens van iedereen die in documenten voorkomt of met wie er digitaal contact is geweest. Daarmee raakt deze bevoegdheid een grote groep onschuldige burgers. **Dit is een dusdanig grove en niet verfijnde maatregel dat er zeer goede argumenten tegenover moeten staan om de inbreuk op de privacy van burgers,** zoals beschermd door artikel 8 van het EVRM**, te rechtvaardigen**. DRC, OM.

2 en 3. De regering is zich bewust van de mogelijke impact van dit wetsvoorstel op de privacy van burgers. De regering is met de CDA-fractie van mening dat de inzet van de bevoegdheid kan leiden tot een kleinere inbreuk op de persoonlijke levenssfeer van

verdachten. De bevoegdheid kan zeer gericht worden ingezet. Een huiszoeking en inbeslagneming kan inderdaad in bepaalde gevallen wellicht achterwege blijven als de nodige gegevens middels het binnendringen in een geautomatiseerd werk kunnen worden vergaard. Dit betreft specifiek de bevoegdheid tot het op afstand binnendringen van een geautomatiseerd werk. In haar advies heeft de Afdeling advisering van de Raad van State erop gewezen dat het heimelijk binnendringen in een geautomatiseerd werk een grote inbreuk op de persoonlijke levenssfeer vormt, die vergelijkbaar is met het betreden van een woning met het oog op het opnemen van vertrouwelijke communicatie (artikel 126l, tweede lid, Sv). Met de Afdeling advisering is de regering van oordeel dat het op afstand, binnendringen en onderzoeken van een geautomatiseerd (net)werk, waarbij zowel historische, actuele als toekomstige gegevens kunnen worden overgenomen, een ingrijpende aantasting van de persoonlijke levenssfeer vormt. Voor een zorgvuldige afweging van de betrokken belangen moeten enkele belangrijke noties worden erkend. De eerste is dat de ontwikkeling van de computercriminaliteit noodzaakt tot aanpassing van de bevoegdheden om die criminaliteit effectief te bestrijden. De huidige opsporingsbevoegdheden zijn niet voldoende om antwoord te kunnen geven op de ontwikkelingen op het gebied van de informatie- en communicatietechnologie. De communicatie tussen mensen en de opslag van gegevens verloopt steeds vaker via het internet. Het internet is grenzeloos. De gegevens zijn niet meer opgeslagen op een computer die zich op een bepaalde plaats bevindt en aldaar in beslag kan worden genomen, maar op een server die zich al dan niet in Nederland bevindt en die met het internet is verbonden. Hierdoor wordt de opsporing met verschillende problemen geconfronteerd. De opslag van gegevens in de cloud heeft tot gevolg dat de gegevens, behalve door tussenkomst van (het geautomatiseerde werk van) de betrokken persoon, uitsluitend via een aanbieder van een communicatiedienst of een communicatienetwerk kunnen worden bereikt. In de praktijk blijkt dit echter weerbarstig omdat de aanbieder in het buitenland is gevestigd is, en soms zelfs onmogelijk wanneer de aanbieder niet te achterhalen is of de gegevens zijn versleuteld. Door het toenemende gebruik van versleuteling van gegevens in informatiesystemen en software worden bestaande opsporingsbevoegdheden, zoals het aftappen van communicatie, zinloos. De enige mogelijkheid om de communicatie in toegankelijke vorm af te tappen is door direct vanaf het ontvangende of verzendende apparaat te tappen, voordat of nadat versleuteling plaatsvindt. In de memorie van toelichting is hierop reeds nader ingegaan. In de tweede plaats wordt voorzien in strikte waarborgen voor een zorgvuldige toepassing van de voorgestelde bevoegdheden. Een belangrijke waarborg vormt een voorafgaande rechterlijke toetsing van de voorgenomen inzet. Verder zijn de voorwaarden voor de uitoefening van de bevoegdheid aangescherpt, overeenkomstig het advies van de Afdeling advisering van de Raad van State. Het destijds voorgestelde artikel 125ja Sv is inmiddels, als artikel 126nba/uba/zpa Sv, verplaatst naar Titel IVA dat betrekking heeft op de bijzondere bevoegdheden tot opsporing. Overeenkomstig het advies van de Afdeling advisering is de toepassing van onderzoekshandelingen waarbij het geautomatiseerde werk op afstand wordt binnengedrongen met het oog op het vastleggen of ontoegankelijk maken van gegevens, uitsluitend toegestaan ingeval van een misdrijf 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. Ten slotte moet voor de beoordeling van de impact van de voorgestelde maatregel ook de huidige situatie in ogenschouw worden genomen. Het Wetboek van Strafvordering bevat thans verschillende regels voor de inbeslagneming van voorwerpen en de vastlegging van (elektronische) gegevens. Zoals eerder opgemerkt, zijn deze bevoegdheden in de digitale wereld minder bruikbaar omdat de fysieke locatie van de gegevens minder goed te achterhalen is. Niettemin moet worden opgemerkt dat in de gevallen waarin bekend is dat de gegevens zich in Nederland bevinden, de computer of server in beslag kan worden genomen waarop die gegevens zijn opgeslagen. De doorzoeking ter vastlegging van

gegevens dan wel de inbeslagneming van een voorwerp als een computer of server, inclusief alle gegevens die op dat geautomatiseerde werk zijn opgeslagen, vormt eveneens een ingrijpende inbreuk op de persoonlijke levenssfeer van de betrokkenen.

127. Aan het advies van de Afdeling advisering op dit punt is deels gevolg gegeven. Met de Afdeling advisering ben ik 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 verdergaande inbreuk op de privacy van de betrokkene oplevert dan wanneer het binnendringen wordt gevolgd door het aftappen van communicatie of de stelselmatige observatie. Beperking van de toepassing van deze onderzoeksbevoegdheden tot zeer ernstige misdrijven, waarop gevangenisstraf van acht jaar of meer is gesteld, zoals de Afdeling advisering voorstelt, is evenwel te beperkend. Dit zou tot gevolg hebben dat de bevoegdheid niet zou kunnen worden ingezet voor een opsporing van een aantal strafbare feiten waarbij het geautomatiseerde werk instrumenteel is maar een lagere wettelijke strafbedreiging kennen. In dergelijke gevallen zijn er echter dikwijls geen andere aanknopingspunten voor de opsporing dan het op afstand heimelijk binnendringen in het geautomatiseerde werk. Ook voor deze gevallen zijn strenge voorwaarden gesteld. Zo is wettelijk vereist dat het gaat om een misdrijf dat bij algemene maatregel van bestuur is aangewezen, dat het misdrijf een ernstige inbreuk op de rechtsorde oplevert en dat er een dringend onderzoeksbelang aanwezig is. Hiermee wordt naar het oordeel van regering voldaan aan de eisen die gesteld worden door artikel 8 van het EVRM. Hierdoor wordt voldoende geborgd dat de inzet van de bevoegdheid op basis van een afweging van belangen en met inachtneming van de proportionaliteit en subsidiariteit plaatsvindt.

Met opmerkingen 9 .1]: meer in lijn te brengen met de proportionaliteits- en subsidiariteitsvereisten in artikel 8 van het EVRM [red]

222. De regering deelt het oordeel van de Autoriteit Persoonsgegevens niet. In het EVRM wordt het recht op eerbiediging van de persoonlijke levenssfeer beschermd (artikel 8 EVRM). Geen inmenging van enig openbaar gezag in de uitoefening van dit recht is toegestaan dan voor zover bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van, onder meer, de nationale veiligheid, de openbare veiligheid of het belang van het voorkomen van wanordelijkheden en strafbare feiten (artikel 8, tweede lid, EVRM). Onder het criterium 'het voorkomen van strafbare feiten' is, zo blijkt uit de rechtspraak van het EHRM, de strafvorderlijke afwikkeling van strafbare feiten, waaronder de opsporing daarvan, begrepen. De eis van de inmenging 'bij wet is voorzien' houdt in dat in het nationale recht is voorzien in een wettelijke regeling die voor de burger voldoende kenbaar en voorzienbaar is. Op basis van de jurisprudentie van het EHRM geldt daarbij dat de betreffende wettelijke regeling voldoende toegankelijk moet zijn en met voldoende precisie geformuleerd, zodanig dat deze een voldoende indicatie bevat van de omstandigheden waarin en de voorwaarden waaronder de overheid tot deze inmenging mag overgaan, en de rechtssubjecten een adequate bescherming tegen willekeurige inmenging biedt. Uit de jurisprudentie van het EHRM vloeit verder voort dat de inmenging door enig openbaar gezag in de privacyrechten moet voldoen aan vereisten inzake noodzakelijkheid en evenredigheid, en derhalve specifieke, expliciete en legitieme doeleinden moet dienen, en moet plaatsvinden op adequate en relevante wijze, en niet buitensporig mag zijn in verhouding van tot het doel van de inmenging. Het 'noodzaakcriterium' wordt in de rechtspraak van het EHRM nader ingevuld aan de hand van de beginselen van proportionaliteit, subsidiariteit en van een 'pressing social need' (er moet een dringende maatschappelijke behoefte bestaan om het legitieme doel te vervullen).

De voorgestelde bevoegdheid tot het op afstand heimelijk binnendringen van een geautomatiseerd werk wordt bij wet vastgelegd. Daarbij worden de omstandigheden waarin, en de voorwaarden waaronder deze bevoegdheid kan worden toegepast, nauwkeurig vastgelegd. De opsporing van strafbare feiten is erkend als een belang dat inmenging van

het openbaar gezag in het recht op bescherming van de persoonlijke levenssfeer kan rechtvaardigen. In dit geval gaat het om de opsporing van ernstige strafbare feiten, waarvoor voorlopige hechtenis mogelijk is. Met de opneming van de voorgestelde bevoegdheid in het Wetboek van Strafvordering wordt voorzien in een wettelijke regeling die voor de burger voldoende toegankelijk is. De voorgestelde regeling beschrijft nauwkeurig in welke omstandigheden, en onder welke voorwaarden de bevoegdheid kan worden toegepast. Vereist zijn een verdenking van een strafbaar feit waarvoor voorlopige hechtenis is toegelaten en dat een ernstige inbreuk op de rechtsorde oplevert, en een dringend onderzoeksbelang. De te verrichten onderzoekshandelingen zijn nauwkeurig omschreven, en sluiten merendeels aan bij bestaande bevoegdheden en maatregelen van het Wetboek van Strafvordering. De officier van justitie moet in het bevel de feiten en omstandigheden vastleggen waaruit blijkt dat de wettelijke voorwaarden voor de toepassing zijn vervuld. Met de wettelijke vereisten, in het bijzonder dat van een voorafgaande rechterlijke toetsing, wordt het risico van een willekeurige toepassing van de bevoegdheid door een overheidsorgaan uitgesloten. Aan het 'noodzakelijkheidscriterium' wordt voldaan doordat de voorgestelde maatregel onvermijdelijk is om het hoofd te kunnen bieden aan de ontwikkeling van de cybercrime gedurende de afgelopen jaren. Dit heeft betrekking op de versleuteling van gegevens en de opslag van gegevens in de cloud, waardoor het in de praktijk onmogelijk wordt een aanbieder te vinden bij wie de gegevens kunnen worden opgevraagd. De inzet van traditionele opsporingsbevoegdheden, als het aftappen van communicatie via de aanbieder en het vorderen van gegevens bij derden, is dan zinloos. De voorgestelde bevoegdheid van het op afstand heimelijk binnendringen van een geautomatiseerd werk voorziet in een dringende behoefte om ernstige vormen van criminaliteit te kunnen bestrijden. Aan het beginsel van evenredigheid is invulling gegeven doordat in het bevel moet worden aangegeven welke categorie van gegevens het betreft. Ook moeten gegevens over de onderzoekshandelingen worden vastgelegd (logging) zodat achteraf controle mogelijk is op de uitvoering van de bevoegdheid. Daarbij wordt, zoals hierboven naar aanleiding van een vraag van de PvdA-fractie aan de orde is gekomen, voorzien in systeemtoezicht op de rechtmatigheid van de uitoefening van de bevoegdheid. Verder is van belang dat de voorgestelde bevoegdheid een aanvulling vormt op de bestaande wettelijke bevoegdheden. De voorgestelde bevoegdheid mag alleen worden toegepast als blijkt dat met de bestaand wettelijke bevoegdheden niet hetzelfde doel kan worden bereikt. Dit komt tevens tot uitdrukking in het vereiste van het dringende onderzoeksbelang. Verder is de bevoegdheid beperkt tot de in de wet vastgelegde onderzoekshandelingen, die merendeels aansluiten bij de bestaande bevoegdheden en maatregelen. Hierbij is tevens van belang dat thans de inbeslagneming van een geautomatiseerd werk mogelijk is, waarbij aanzienlijk lichtere voorwaarden van toepassing zijn en waarbij een aanzienlijke hoeveelheid gegevens die op dat werk zijn opgeslagen in handen komen van de opsporing. Met de voorgestelde bevoegdheid wordt juist voorzien in een bevoegdheid om uitsluitend de gegevens, die nodig zijn voor de opsporing van het betreffende ernstige strafbare feit, vast te leggen ten behoeve van de opsporing. De regering ziet dan ook 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.

246. [...]Het wetsvoorstel computercriminaliteit wijkt op vrijwel al deze punten af van de wettelijke regelingen van de Russische Federatie en Hongarije. Het wetsvoorstel is van toepassing op de opsporing en vervolging van strafbare feiten, en niet op de bescherming van de staatsveiligheid. De gevallen waarin de bevoegdheid kan worden toegepast worden duidelijk in de wet vastgelegd. Dit betreft ernstige misdrijven waarvoor voorlopige hechtenis mogelijk is en die een ernstige inbreuk op de rechtsorde opleveren, waarbij voor bepaalde onderzoekshandelingen de extra drempel geldt dat het een misdrijf betreft waarvoor een gevangenisstraf van acht jaar of meer kan worden opgelegd dan wel een ernstig misdrijf dat

bij algemene maatregel van bestuur is aangewezen. De voorgestelde bevoegdheid kan uitsluitend worden ingezet bij een verdenking dat een persoon betrokken is bij het beramen of plegen van een dergelijk strafbaar feit, waarbij het bevel de nodige gegevens dient te bevatten ter identificatie van de betrokken persoon en het geautomatiseerde werk. Het is dus bepaald niet zo dat de bevoegde autoriteiten volledig naar eigen inzicht kunnen besluiten tot de toepassing van deze bevoegdheid. De duur van de inzet is beperkt tot vier weken, met de mogelijkheid van verlenging. Verder geldt dat altijd een voorafgaande rechterlijke machtiging is vereist, dat de betrokkene wordt geïnformeerd over de toepassing van de bevoegdheid, en dat systeemtoezicht wordt uitgeoefend op de uitvoering van de wettelijke regels in praktijk.

Op grond van het voorgaande moet dan ook geconcludeerd worden dat de wettelijke regelingen voor het aftappen ten behoeve van de staatsveiligheid en de opsporing en vervolging van strafbare feiten in de Russische Federatie en Hongarije, die onderwerp vormde van het arrest van het EHRM, op essentiële punten afwijken van die rond de toepassing van bijzondere opsporingsbevoegdheden in Nederland, zoals de bevoegdheid het op afstand heimelijk binnendringen in een geautomatiseerd werk met het oog op het verrichten van bepaalde onderzoekshandelingen, zodat de arresten in de zaken Zakharov en Szabo geen consequenties hebben voor het onderhavige wetsvoorstel. Er is daarnaast overigens geen reden te veronderstellen dat dit wetsvoorstel niet zou voldoen aan de eisen van die daaraan op grond van het EVRM, specifiek ten aanzien van de 'noodzakelijkheid' en 'voorzienbaarheid', moeten worden gesteld.

248. Met de leden van de PvdD-fractie acht de regering de privacy en de bescherming van de persoonlijke levenssfeer een groot goed. Het recht op privacy is echter geen absoluut recht maar moet worden afgewogen tegen andere belangen, zoals de beveiliging van burgers tegen de misdaad of de bescherming van slachtoffers van strafbare feiten. Het wetsvoorstel biedt de mogelijkheid om op afstand heimelijk een geautomatiseerd werk binnen te dringen. De omschrijving van het begrip geautomatiseerd werk is in internationale verdragen en in de EU-wetgeving vastgelegd, de kern van dit begrip is dat in het apparaat op basis van een programma geautomatiseerd gegevens worden verwerkt. Ook een apparaat als een pacemaker kan in theorie onder de definitie van geautomatiseerd werk vallen. Het is echter niet goed voor te stellen op welke wijze het op afstand binnendringen in een pacemaker kan bijdragen aan de opheldering van misdrijven. 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.

11. Waar zit precies het hiaat in de bestaande wettelijke bevoegdheden op dit terrein? Het antwoord van de regering tijdens eerdere vragenrondes in de Tweede Kamer, is dat de bestaande bevoegdheden tekortschieten, omdat deze ofwel zijn gekoppeld aan een bepaalde fysieke plaats, ofwel niet zijn gericht op de toegang tot elektronische gegevens die zich in een geautomatiseerd werk of op een gegevensdrager elders bevinden.[1] De vraag blijft echter overeind **in hoeverre er minder vergaande mogelijkheden beschikbaar zijn**, waarbij de privacy beter is gewaarborgd ten aanzien van individuele grondrechten. **Welke andere mogelijkheden zijn er exact onderzocht en kan de regering uitleggen waarom deze volgens haar niet voldoen?** DRC, OM.

[1] Zie bijvoorbeeld Kamerstukken II 2016/17, 34 372, nr. 6, p. 1-2.

139. Om binnen te dringen in een geautomatiseerd werk zijn verschillende technieken mogelijk. Er kan bijvoorbeeld worden binnengedrongen door het verkrijgen van inloggegevens door zogenoemde social engineering, door inlichtingenwerk, of door in overleg met beheerders toegang tot een systeem of gegevens te verkrijgen. Deze opties zijn echter niet in elke casus bruikbaar of succesvol. Bijvoorbeeld wanneer het gaat om technisch capabele criminelen die zich bewust zijn van het feit dat de politie naar hen op zoek is, en daarom alles in het werk stellen toegang tot informatie over strafbare feiten voor de politie verborgen te houden.

In aanvulling van het antwoord op vraag 3, waarin wordt ingegaan op de noodzaak voor deze nieuwe bevoegdheden, ga ik in op de beschikbaarheid van minder vergaande mogelijkheden.

23. Er zijn verschillende redenen waarom de voorgestelde nieuwe bevoegdheid niet te gemakkelijk zal worden ingezet zonder dat een zorgvuldige afweging heeft plaatsgevonden, in het kader waarvan ook de mogelijkheid van minder verstrekkende bevoegdheden aan de orde komt. 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, op basis 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, waarop de voorgenomen inzet wordt voorgelegd aan de Centrale Toetsingscommissie (CTC) van het openbaar ministerie. De CTC adviseert het College van procureurs-generaal 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.

13.
Ook de Nederlandse burgerrechtenorganisatie Bits of Freedom vindt het wetsvoorstel te ruim in zijn bevoegdheden.[2] Het inmiddels beruchte voorbeeld is dat de politie je pacemaker

[2] Kamerstukken II 2015/16, 34 372, nr. 3, bijlage Advies Bits of Freedom, p. 3-8.

zelfs mag hacken bij een klein misdrijf. **Waarom is, naast de bestaande mogelijkheden en naast de mogelijkheden in de wetten Computercriminaliteit I en Computercriminaliteit II, nu een extra set vergaande bevoegdheden nodig?** DRC, OM.

Voor de noodzaak van deze nieuwe bevoegdheden en de proportionaliteits- en de subsidiariteitsoverwegingen verwijs ik naar mijn antwoord op vraag 11.

Daarnaast ga ik graag in op het voorbeeld van de pacemaker dat u naar voren brengt. Dit heb ik in de Nota naar aanleiding van het verslag dat ik aan de Tweede Kamer heb gestuurd, als in mijn inbreng in de Tweede Kamer, veelvuldig weerlegt.

57. Hoewel een pacemaker onder de definitie van geautomatiseerd werk valt, zullen hier naar verwachting weinig 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 zwaar wegend belang voordoet dat het door de PvdD gesuggereerde binnentreden van een pacemaker proportioneel zou worden geacht.

248. Het is echter niet goed voor te stellen op welke wijze het op afstand binnendringen in een pacemaker kan bijdragen aan de opheldering van misdrijven. 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.

4. Samenloop bevoegdheden AIVD en MIVD

16. De leden van de **D66**-fractie merken op dat in het wetsvoorstel staat dat de hackbevoegdheid ook ingezet mag worden tegen terrorismedreiging of een internationale cyberdreiging. Echter, het verzamelen van inlichtingen in de strijd tegen het terrorisme is een taak van de Algemene Inlichtingen- en Veiligheidsdienst (hierna: AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (hierna: MIVD). Zij hebben, zoals in een recente brief van Privacy First wordt benadrukt[3], al de bevoegdheid om een geautomatiseerd werk te hacken. **Waarom wil de regering deze bevoegdheid ook uitbreiden naar de politie, als de AIVD en MIVD deze bevoegdheid reeds hebben?** NCTV, DRC

16a. **Kan zij aangeven of dit de afbakening van taken van deze instanties niet juist versnippert en onduidelijker maakt?** NCTV, DRC.

49. De door de leden van de D66-fractie genoemde (nieuwe) bevoegdheden verschillen voor wat betreft het doel waarvoor zij kunnen ingezet. De voorgestelde bevoegdheid tot het op afstand binnendringen van een geautomatiseerd en het verrichten van onderzoekshandelingen en de bevoegdheid tot het vorderen van bewaarde telecomgegevens zijn beide strafvorderlijke bevoegdheden, die kunnen worden ingezet in geval van verdenking van een ernstig strafbaar feit. De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) beschikken al geruime tijd over de bevoegdheid tot het binnendringen in een geautomatiseerd werk (artikel 24 Wiv 2002). Deze bevoegdheid kan uitsluitend worden ingezet voor de uitoefening van de wettelijke taken van de diensten in het belang van de nationale veiligheid. Het doel waarvoor de bevoegdheid kan worden ingezet is dan ook verschillend. Er kan vanuit deze optiek bezien dan ook niet gesproken worden van een overlap tussen beide wetsvoorstellen.

[3] Brief van 7 maart 2017, griffienummer: 160847.

Overigens wordt opgemerkt dat de reikwijdte van de bevoegdheid in de strafvorderlijke sfeer beperkter is dan die in de sfeer van de inlichtingen- en veiligheidsdiensten. Zo wordt in het voorstel voor een nieuwe wet op de inlichtingen- en veiligheidsdiensten onder meer voorzien in de mogelijkheid tot het verkennen van de technische kenmerken van geautomatiseerde werken die op een communicatienetwerk zijn aangesloten en de bevoegdheid om via het geautomatiseerde werk van een derde in het geautomatiseerde werk van het onderzoekssubject binnen te dringen.

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

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 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.

17. De regering geeft aan dat het wetsvoorstel nodig is om terroristische aanslagen te voorkomen. De leden van de fractie van de **SP** vragen haar **of het juist is dat de inlichtingendiensten dit tot taak hebben. Zo ja, waarom wil zij deze bevoegdheid uitbreiden naar de politie?**
NCTV, DRC.

18. De leden van de fractie van de **ChristenUnie** merken op dat de bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk op dit moment al kan worden toegepast door de AIVD en MIVD na de toestemming van de Minister van Binnenlandse zaken en Koninkrijksrelaties en/of de Minister van Defensie. Zij vragen naar **de noodzaak van de nieuwe voorgestelde bevoegdheid en de ratio achter de geringe clausulering voor het gebruik daarvan door de opsporingsdiensten.**
DRC, OM, NP.

Voor de noodzaak van de voorgestelde bevoegdheid verwijs ik naar mijn antwoord op vraag 1. De mening dat de bevoegdheid gering is geclausuleerd deel ik niet. **23.** Er gelden 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, op basis van de proportionaliteit en subsidiariteit, een essentieel bestanddeel. Voor een nadere toelichting op de stricte clausering verwijs ik naar mijn antwoord op vraag 7.

19.
Zij lezen dat de nieuwe bevoegdheid met name noodzakelijk is bij de opsporing van (de voorbereiding) van terroristische misdrijven en de bestrijding van kinderpornografie. **Deze leden vragen of er andere terreinen zijn waar de opsporingsdiensten onvoldoende resultaat boeken als gevolg van het ontbreken van de voorgestelde hackbevoegdheden. Zij vragen om een nadere cijfermatige onderbouwing van de noodzaak om deze bevoegdheid zo ruim uit te breiden.**
DRC, OM.

20. Tevens krijgen zij graag inzicht 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. **Hoe vaak wordt gebruikgemaakt van de bemachtigde gegevens van de veiligheidsdiensten in een strafproces?**
NCTV, .

21. In de Tweede Kamer is uitgebreid debat gevoerd over de in dit wetsvoorstel verleende bevoegdheid aan het Openbaar Ministerie (hierna: OM) 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 (tot in het oneindige) met vier weken worden verlengd.[4] **Het lijkt de CDA-fractieleden verstandig om de maximale termijn alsnog**

[4] Handelingen II 2016/17, 34, item 26, p. 47.

in de wet te noemen, zodat de onbekende kwetsbaarheid kan worden gerepareerd: het is immers niet alleen de opsporingsambtenaar die van die kwetsbaarheid gebruik kan maken, maar criminelen evenzeer. Kan de regering hier nader op in gaan? DWJZ,9 DRC, OM.

223. De regering heeft voor de juridische voorwaarden voor de toepassing van de bevoegdheid aangesloten bij de systematiek rond de toepassing van bijzondere opsporingsbevoegdheden in het Wetboek van Strafvordering.

83. In het bevel dient de officier van justitie het tijdstip waarop, of de periode waarbinnen, aan het bevel uitvoering wordt gegeven te vermelden. Dit is vastgelegd in de voorgestelde artikelen 126nba/uba, tweede lid, onderdeel g., respectievelijk 126zpa, tweede lid, onderdeel e., Sv. Een bevel tot het binnendringen van een geautomatiseerd werk wordt gegeven voor een periode van ten hoogste vier weken. Het bevel kan telkens voor een periode van ten hoogste vier weken worden verlengd. Dit is vastgelegd in het voorgestelde artikelen 126nba, derde lid, respectievelijk 126uba/zpa, derde lid, Sv. Na afloop van het onderzoek wordt de software verwijderd.

223. De regering acht een termijn van vier weken aangewezen, omdat een dergelijke termijn een adequate periodieke toetsing van de rechtmatigheid van de toepassing door de rechter-commissaris verzekert.

22. De politie zal gebruikmaken van niet bekende kwetsbaarheden om in te breken in geautomatiseerde apparatuur, en informatie hierover zelfs inkopen bij organisaties die hier geld aan verdienen. Hiermee houdt de politie het bestaan van dergelijke kwetsbaarheden in stand, waarmee het internet en digitale apparaten onveiliger worden in plaats van veiliger. **Waarom investeert de regering niet in het veiliger maken van de digitale wereld in plaats van financieren en gebruik van niet bekende kwetsbaarheden**, zo vragen de fractieleden van **D66**. DRC.

38 en 39. De regering stimuleert een veilig gebruik van het internet door burgers en bedrijven met verschillende initiatieven. Zo heeft het NCSC bijvoorbeeld een zogenaamd Whitepaper Cloudcomputing gepubliceerd met adviezen hoe organisaties hun wifi kunnen beveiligen (https://www.ncsc.nl/actueel/whitepapers/whitepaper-cloudcomputing.html). Daarnaast wordt informatie en handelingsperspectief geboden aan eindgebruikers via veiliginternetten.nl en de jaarlijkse campagne Alert Online. De regering is van mening dat het in eerste instantie de verantwoordelijkheid van de burgers zelf is en van de bedrijven die internetdiensten leveren om voor adequate beveiliging te zorgen. Daarnaast is het al zo dat bij de installatie van die netwerken, hetzij door de installateurs, hetzij door de gebruikers zelf, instellingen (kunnen) worden ingesteld waardoor de wifi netwerken beveiligd worden.

92. Daarnaast wordt gestimuleerd om te investeren in het veiliger maken van apparaten en een goede cyber hygiëne. Als uitgangspunt verdient het zeker de voorkeur te investeren in de veiligheid van apparaten en de hygiëne op het internet. Dit is een ideaal dat slechts op langere termijn en in samenwerking op supranationaal niveau te realiseren is. In het licht van het open karakter van het internet is hier een lange weg te gaan. Hiervoor zijn inspanningen nodig op mondiaal niveau omdat, vanwege het karakter van de markt, de veiligheid van apparaten en een goede cyberhygiëne niet met enkel nationale inspanningen te bereiken is. Nederland neemt actief deel aan internationale initiatieven die er zijn om het internet veiliger te maken. Dit neemt niet weg dat de botnets thans ook in Nederland een grote bedreiging vormen voor het functioneren van geautomatiseerde werken en daarmee de veiligheid van de digitale wereld aantastten, waardoor de dienstverlening van bedrijven en overheidsinstellingen ernstig kan worden gehinderd en burgers zich in hun veiligheid

aangetast voelen. De voorgestelde bevoegdheid biedt de mogelijkheid om hiertegen op te treden, bijvoorbeeld door de server binnen te dringen van waaruit het botnet wordt aangestuurd (de command and control server) en de gegevens zodanig te bewerken dat de aansturing wordt beëindigd, zodat het aangevallen geautomatiseerde werk weer kan functioneren. Dit is overigens lang niet bij alle botnets mogelijk. Voor het bestrijden van botnets blijven investeringen in de veiligheid van geautomatiseerde werken en samenwerking met andere partijen in binnen- en buitenland van belang.

178. Ik benadruk hier ook graag dat het in het belang is van alle partijen om kwetsbaarheden op internet te verminderen. Tegelijk is het voor een effectieve opsporing en het waarborgen van de nationale veiligheid noodzakelijk toegang te krijgen tot relevante gegevens. Dergelijke gegevens zijn onder meer nodig voor het onderkennen van specifieke dreigingen voor de nationale veiligheid, het bepalen van de strategie in opsporingsonderzoeken, de bewijsvoering en om criminele activiteiten te kunnen stoppen. Deze gegevens zijn veelal, en steeds vaker alleen maar, digitaal en via internet te benaderen.

23. **De bevoegdheden die voorliggen worden gegeven aan de politie.** De kennis van de politie op het gebied van cybercrime is over het algemeen niet erg groot. De aangiftebereidheid is laag en het justitiële apparaat is niet ingericht op de aanpak van cybercrime. Slachtoffers van *sextortion*, sexting of wraakporno voelen zich vaak niet serieus genomen bij de aangifte. Een wet met deze bevoegdheden heeft niet alleen geen enkele zin wanneer de politie slachtoffers naar huis stuurt met de opmerking dat ze niets voor hen kunnen doen, maar draagt ook grote risico's in zich. De kennis die nodig is om de wet uit te voeren, zal niet intern aanwezig zijn. **De SP-fractieleden vragen of het klopt het dat de regering hiervoor externe partijen inhuurt. En zo ja, vindt zij dit dan een wenselijke ontwikkeling?**
NP,DGPOL,DRC.

23. Dit betreft 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.

278. De vraag en noodzaak van de digitaal experts wordt onderkend. De aankomende jaren zal middels door- en zijinstroom van medewerkers in deze vraag worden voorzien.

131. Daarnaast biedt het opleidingsaanbod bij de Politieacademie tal van (verplichte) opleidingen, modules en trainingen aan op het gebied van cybercrime en digitale expertise, zoals Recherchekundige Master Digitaal, digitale opsporing, internet en opsporing, en forensic scripting. De verwachting is dat er voor het verzekeren van voldoende kennis op het gebied van cybercriminaliteit behoefte zal zijn aan specifieke (nieuwe) opleidingen. Gezamenlijk met de Politie Academie zal worden bezien hoe dit in het onderwijsaanbod kan worden opgenomen.

23. Hetzelfde geldt voor het inkopen van hacksoftware. Deze software zal door externe partijen ontwikkeld worden, maar zonder gedegen kennis weet de politie eigenlijk niet wat zij inkoopt. **Hoe voorkomt de regering dat de politie hierbij schadelijke software inkoopt die weliswaar doet wat het zegt, maar tevens informatie over de politie aan derden verschaft?** Graag een reactie.
DWJZ, 9 + NP, DGPOL, DRC.

132. De keuring van de huidige technische hulpmiddelen die gebruikt worden bij de opsporing wordt uitgevoerd door een gespecialiseerde afdeling van de landelijke eenheid van het landelijk politiekorps politie.

104/105. Het onderzoek in een geautomatiseerd werk met behulp van een technisch hulpmiddel, vindt, anders dan het onderzoek met de traditionele technische hulpmiddelen, plaats in een volledig digitale omgeving. Omwille van de overzichtelijkheid zullen de eisen die aan technische hulpmiddelen voor het doen van onderzoek in een geautomatiseerd werk worden gesteld neergelegd worden in een nieuw besluit, dat wordt toegesneden op het doen van onderzoek in een digitale context. De in de memorie van toelichting aangekondigde aanpassing van het Besluit technische hulpmiddelen strafvordering wordt niet langer voorzien.

Het besluit ter uitvoering van het wetsvoorstel wordt gebaseerd op het uitgangspunt dat de gegevens die met een technisch hulpmiddel worden vastgelegd betrouwbaar, voor derden toetsbaar en niet manipuleerbaar dienen te zijn. In het besluit eisen zullen eisen worden gesteld aan de inrichting en werking van het technische hulpmiddel. Een belangrijke inrichtingseis zal zijn dat de instelling van de software kan worden gedifferentieerd naar het gebruik van verschillende functionaliteiten. Verder zal vereist worden dat de inhoud van de geregistreerde gegevens identiek zijn aan de inhoud van de gedetecteerde gegevens. Ook zullen eisen worden gesteld over de automatische opslag van geregistreerde gegevens op – uitsluitend - de beveiligde politieserver. Om de onschendbaarheid van de waarnemingen te kunnen waarborgen en manipulatie door derden te voorkomen, zal als eis gesteld worden dat het transport van de signalen vanuit het geautomatiseerde werk naar de server van de politie plaatsvindt via een versleuteld bestand. Bij de keuring zal getoetst worden of de software aan de eisen voldoet. Alleen wanneer de software is goedgekeurd, mag deze worden ingezet voor het doen van onderzoek in een geautomatiseerd werk. Het besluit zal verder als voorwaarde stellen dat de technische handelingen die worden verricht tijdens het onderzoek doorlopend en automatisch op de politieserver worden vastgelegd (logging), zodat controle op de uitvoering van het bevel van de officier van justitie te allen tijde, zowel tijdens het onderzoek als achteraf, mogelijk is.

24. Een grote zorgt leeft bij de SP-fractieleden over het gebruikmaken van de zogenaamde *Zero Day*-zwaktes. De politie krijgt niet de plicht om deze te melden. **In de Verenigde Staten heeft dit nu geleid tot het seponeren van een zaak van kindermisbruik.[5] Hoe oordeelt de regering over deze situatie?**
DRC, OM, NP.

25. **Is het denkbaar 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? Hoe oordeelt de regering over de morele kant van de zaak?** DRC, OM,

[5] https://arstechnica.com/tech-policy/2016/04/judge-child-porn-search-warrant-issued-in-va-not-valid-for-pc-in-okla/.

NP.

Kwetsbaarheden brief: 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 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 wetsbaarheid 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.

25a. De politie is immers op de hoogte van een zwakte waar vele criminelen gebruik van zullen maken. **Is het niet de taak van de politie om mensen te beschermen tegen criminaliteit? Is het niet melden van kwetsbaarheden in de beveiliging niet een vorm van medewerken aan de criminaliteit?** Graag de mening van de regering. dGPOL, DRC

149. 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.

247. Het wetsvoorstel voorziet in een dringende behoefte van de opsporings- en vervolgingsinstanties om cybercrime beter te kunnen bestrijden en de burgers tegen te kunnen beschermen tegen vormen van criminaliteit die worden gepleegd met behulp van geautomatiseerd werken.

Ik herhaal dat kwetsbaarheden die in het kader van een opsporingsonderzoek aan het licht komen, en waarvan aannemelijk is dat ze nog onbekend zijn, in beginsel direct of zo spoedig mogelijk worden gemeld aan de fabrikant van de desbetreffende hardware of software. Voor de uitzonderlijke gevallen waarin kwetsbaarheden wel worden gebruikt verwijs is naar mijn antwoord op vraag 25.

26. De **PvdA**-fractieleden vragen de regering 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 (ook wel de hackbevoegdheid genoemd) – **impliceert dat de overheid hackkennis op de markt zal gaan verwerven.**
DGPOL, NP, DRC.

Handelingen:

Die handel in kwetsbaarheden is er. Onbekende kwetsbaarheden worden verhandeld. Die handel op zichzelf is niet verboden. Het gebruiken van een kwetsbaarheid voor strafbare feiten

is dat wel. Daar zit de spanning in. Het is een erg dure handel. Anders zou je bijna kunnen zeggen: koop ze allemaal op, niet vanuit de politie, maar bijvoorbeeld vanuit het Nationaal Cyber Security Centrum, en zorg dat ze gedicht worden. Maar zo simpel werkt het niet. Het is niet een markt waarop de politie zich moet bewegen om zero-days te kopen. Het is niet zo dat je zelf gaat bieden op een zero-day, waarbij je een onbekende kwetsbaarheid verwerft. Het is sowieso de vraag of dit nu de standaardmethode is. Mevrouw Van Toorenburg stelde die vraag ook. Dat is niet zo. Je gaat eerst bekijken of er minder ingrijpende bevoegdheden kunnen worden ingezet. Als het gaat om een vordering bij een cloudaanbieder, waarvan je weet dat die gewoon reageert en meewerkt, dan is dat minder ingrijpend dan een van de bevoegdheden uit deze wet. Dan zul je daar gebruik van maken. Als binnendringen wel nodig is, kijkt de politie per geval welke methode nodig is. Daarbij weeg je de inbreuk op de privacy en ook het risico dat het opgemerkt wordt. Onbedoelde neveneffecten probeer je bij de keuze natuurlijk zo klein mogelijk te houden. Vaak levert een vooronderzoek een beeld op van het systeem. Als je dan bijvoorbeeld ziet dat iemand een verouderd besturingssysteem gebruikt waarvan je weet dat dat een bekende kwetsbaarheid is en dat je daarbinnen kunt komen, denk je niet: ik vind het veel leuker om een onbekende kwetsbaarheid te doen of om iets heel moeilijks te hacken. Dat gebeurt in dat geval niet.

Die bedrijven verdienen hun geld met het verkopen van tools om andere systemen in te komen. Dat klopt. Dat zijn soms tools die gebruikmaken van bekende kwetsbaarheden. Het product van dat bedrijf is dus ook eindig, want zodra de kwetsbaarheid ontdekt en verholpen is, is het product niet meer bruikbaar. Misschien is dat dan ook interessant voor ze. Dan moet je immers een nieuw product kopen. Ik weet niet precies waar het businessmodel het meest mee gebaat is, maar dit is inderdaad een lastig punt. Door het niet te kopen, maak je het niet veiliger. Het is niet zo dat daardoor de kwetsbaarheid verholpen wordt. Maar het is inderdaad zo dat je dan een product koopt van een bedrijf dat op zich legitiem opereert en dat wellicht ook andere klanten kan aanspreken. Het ligt eraan waar het gevestigd is en wat dan de dual use policy van dat land is. Daar zijn wellicht ook andere afnemers in geïnteresseerd die minder fris zijn. Dat klopt. Dat is een ongemakkelijk hoekje. Maar het is niet zo dat je een oplossing dichterbij brengt of het probleem verhelpt door het niet te kopen.

Ik wil ten eerste nog iets zeggen over die ongemakkelijke hoekjes. Dan moet de heer Verhoeven ook andere steun aan bestaande praktijken heroverwegen. Wij staan de politie toe om wapens te dragen. De politie is zo ongeveer de enige instantie die dat mag, samen met het leger. Die wapens kopen wij ook van producenten die diezelfde producten ook verkopen aan andere mensen, die er minder prettige plannen mee hebben. Dat is eenzelfde soort ongemakkelijk hoekje. Dat is wat ik daarmee bedoelde.

Ten tweede, het is bij de stelling van de heer Verhoeven de vraag hoe doorslaggevend het feit dat wij ons ook op die markt begeven voor het bestaan van het aanbod is. Ik heb sterk de indruk dat wij door dit te doen, niet het aanbod creëren of versterken. We verzwakken het ook niet. Ik heb de indruk dat wij daar geen cruciale factor in zijn en dat we door het gebruik ervan, omkleed met allerlei waarborgen en puur gericht op mensen die verdacht worden van behoorlijke misdrijven en van specifiek op dit terrein gerichte wetsovertredingen in de cyberhoek, een bijdrage kunnen leveren aan het veiliger houden van de samenleving en aan het kunnen

aanpakken van precies die ongemakkelijke mensen die zich met kwade intenties in datzelfde hoekje begeven.

27. Op grond van het voorliggende wetsvoorstel mogen opsporingsinstanties bij het hacken zelfs gebruikmaken van bij producent en gebruikers van software onbekende zwakheden ('onbekende kwetsbaarheden') in de software. Die software zal echter niet alleen door verdachten worden gebruikt, maar ook door onschuldige burgers. **Loopt de regering zo niet het risico 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?**
DRC .

Handelingen: Ik wil even duidelijk zijn. Mevrouw Van Tongeren zegt dat we ons gaan begeven op de markt voor zero days. Dat doen we dus niet. We gaan niet rechtstreeks zero-days inkopen. Dat heb ik net gezegd. We gaan wel dingen inkopen waarvan we inderdaad niet zeker weten of daar een onbekende kwetsbaarheid in zit. Dat noem ik ongemakkelijk, al ga ik niet zo ver als het oordeel dat mevrouw Van Tongeren er net aan koppelde. Mevrouw Van Tongeren telt alleen de spelers op de markt die tot de overheid en de opsporingsdiensten behoren, maar dat is maar een heel klein deel van die markt.

Het grootste deel van die markt bestaat uit andere spelers. Ik ben er voorstander van dat iedere kwetsbaarheid wordt gemeld. Daarom vind ik het juist goed als je, naast het moeilijk maken van illegale handel, beloningen uitlooft voor responsible disclosure en voor slimme ethische hackers — die mensen zijn veel slimmer dan ik — die een kwetsbaarheid hebben gevonden en die willen verkopen of geven aan het bedrijf. Het liefste heb ik dat een bedrijf standaard zegt: als jij een kwetsbaarheid in ons systeem aan ons meldt, krijg je daar een bonus of een vergoeding voor. Er kan ook een bounty hunt worden uitgeschreven, waarbij je mensen echt laat zoeken. Dat doen we ook allemaal. Het is niet zo dat we bij het aannemen van deze wet al het beleid dat is gericht op cybersecurity — bij deze begroting hebben we daar weer flink in geïnvesteerd — overhoop gooien. Dat beleid blijven we versterken. Het is inderdaad dubbel. We proberen de kwetsbaarheden te dichten. Zolang ze nog niet dicht zijn, kunnen de opsporingsdiensten ze ook gebruiken om de kwaadwillenden die zich in die sferen of in andere sferen van zware misdaden begeven, aan te pakken. Het andere dilemma is dat we betere sloten willen voor iedereen, maar dat we ook de mogelijkheid willen hebben om specifiek gericht op bepaalde personen het slot te kunnen forceren.

De heer Verhoeven vroeg of we kwetsbaarheden aan andere landen gaan verkopen. Dat gaat de politie niet doen. We hebben het er al over gehad dat de inkoop van onbekende kwetsbaarheden niet gaat op de manier die de heer Verhoeven veronderstelde toen hij vroeg of we een hoop geld gaan uitgeven op de zero-daymarkt.

De situatie bestaat onafhankelijk van deze wet. Die situatie vind ik, net als de heer Verhoeven, zorgwekkend en die wil ik samen met hem bestrijden. Dat kan deels via het opsporen van figuren die zich hierin bewegen. Daarvoor heb ik dit soort bevoegdheden nodig. Wat doet de heer Verhoeven echter de hele tijd? Hij doet alsof de situatie die al bestaat, of het wetsvoorstel nu wordt aangenomen of verworpen, pas zal ontstaan of zelfs versterkt zal worden na aanname van het wetsvoorstel. Dat is de link die hij legt. Dat vind ik een afweging. Ik zit er niet blind in, in

de zin van: hoe meer bevoegdheden, hoe beter. Alles overwegende vind ik dat we dit wel moeten doen. De nadelen die de heer Verhoeven terecht noemt, bestaan immers ook zonder deze wet en met deze wet zijn we beter in staat daar iets tegen te doen. Dat is de afweging die ik maak. De heer Verhoeven kan roepen dat dat laatste niet waar is, maar ik kan nu niet achter mensen aan gaan die zich op die markt begeven, die die kwetsbaarheden kopen en verhandelen met kwade intenties en die hacking tools kopen met kwade intenties. Ik kan er niet bij. Een kinderpornonetwerk kan zich in die markt bewegen of dat soort kwetsbaarheden gebruiken, maar dat kan het nu ook en dat zal het met deze wet niet meer of minder doen. Met deze wet kan ik er echter wel voor zorgen dat minder mensen het doen, doordat ik er meer kan opsporen en oppakken en de bewijslast kan verzamelen.

De kans is wel heel groot dat het een bekende kwetsbaarheid is waar deze gebruik van maakt. Dat is het lastige van die markt. Als ik zeg dat je niet bij dat soort bedrijven mag kopen, waarbij je niet weet of onder de motorkap de kwetsbaarheid die wordt gebruikt bekend of onbekend is, sluit ik wel heel veel uit, waarbij ik niet aan onbekende kwetsbaarheden zou raken, die wel erg nuttig zouden kunnen zijn voor de politie om gebruik van te maken.

Stel dat je zegt: die software kopen we ook niet, want hij kan gebruikmaken van onbekende kwetsbaarheden. Dat kan betekenen dat de politie ook niet software kan kopen die geen gebruikmaakt van onbekende kwetsbaarheden. Dat is het probleem met dingen waarvan je niet precies weet hoe ze werken. Met die afweging en om alle redenen die ik zojuist heb genoemd — ik zie niet dat het een verslechtering oplevert van de situatie, omdat die markt er helaas toch al is — vind ik dat je je wel mag begeven op de markt van die producten. Die andere markten betreffen andere producten en andere handelingen. Daar is niets kosmetisch aan. Het is misschien in het belang van de opsporing best interessant om een onbekende kwetsbaarheid te kopen en dan zelf de retool op te bouwen, maar dat doen wij niet. Het zijn echt verschillende producten.

28. Weliswaar gaat het wetsvoorstel uit van de regel dat onbekende kwetsbaarheden door de officier van justitie aan de producent moeten worden gemeld, maar de in artikel 126ffa van de voorgestelde regeling maakt het mogelijk dat die melding op grond van een zwaarwegend opsporingsbelang wordt uitgesteld. Bits of Freedom heeft bij brief van 23 februari 2017[6] de volgende kritische kanttekeningen geformuleerd bij dit artikel:

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.***"[7] DRC, OM.

[6] Griffienummer: 160847.01.

[7] Brief van 23 februari 2017, griffienummer: 160847.01, p. 2.

29. 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."***[8]
DRC.

Zie vraag 27.

30. **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.[9]
DRC.

31. 4. Het gebruik van de betreffende hacksoftware is omstreden, **omdat deze ook zal worden geleverd aan landen die het niet zo nauw nemen met de grondrechten van hun burgers**.[10]
DRC.

Kwetsbaarheden brief: 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 ICTgoederen 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.

32. 5. Het in artikel 126ffa van het wetsvoorstel voorgestelde meldingsregime werkt 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 beveiligingsgat gedicht gaat worden. Dat laatste zou echter**

[8] Brief van 23 februari 2017, griffienummer: 160847.01, p. 2.

[9] Brief van 23 februari 2017, griffienummer: 160847.01, p. 2-3.

[10] Brief van 23 februari 2017, griffienummer: 160847.01, p. 3.

het werk van het eerstgenoemde opsporingsteam verstoren.[11]
DRC, OM

De leden van de PvdA-fractie verzoeken de regering ten gronde te reageren op voornoemde opmerkingen van Bits of Freedom.

33. De PvdA-fractieleden vragen voorts aandacht voor de aanschaf en veiligheid van de malware die Nederlandse opsporingsinstanties gaan gebruiken. Bits of Freedom wijst in bovengenoemde brief op de *Bundestrojaner*-affaire (waarin de malware die de Duitse politie gebruikte, onveilig was en uitlekte) en op de *Verint*-zaak.[12] **De voornoemde leden vragen de regering hoe de opsporingsinstanties aan de benodigde 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 vragen zij de regering hoe van derden gekochte malware wordt gecontroleerd op veiligheid, bijvoorbeeld op de aanwezigheid van zogenaamde *backdoors*.**
DWJZ, Manon/DRC, NP

Voor het antwoord of de software applicatie een backdoor zou bevatten verwijs ik naar het antwoord op vraag 23.

34. Er wordt voorgesteld om gebruik te maken van nog onbekende kwetsbaarheden (onder andere door middel van zogenaamde *Zero Days*) binnen het internet om hacken mogelijk te maken. **Wat zijn de gevolgen hiervan voor de veiligheid van het internet en hoe verhoudt dit wetsvoorstel zich daarmee tot het rapport "De publieke kern van het internet" van de Wetenschappelijke Raad voor het Regeringsbeleid[13] (WRR)?**
DRC.

149. De leden van de SP-fractie hebben gevraagd hoe de conclusie van het in april 2015 verschenen rapport van de WRR («De publieke kern van het internet») dat het functioneren en de integriteit van de publieke kern van het internet veilig gesteld moet worden en beschermd moet worden tegen oneigenlijke interventies door staten en andere partijen, in verhouding staat tot de hackbevoegdheid voor opsporingsdiensten.

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. De AIV spreekt van het internet als een 'mare liberum', waarbinnen de staat zich dient te beperken tot het borgen van de juridische kaders van de rechtstaat en het beschermen van de burgerlijke vrijheden. 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. De 'mare liberum'-vergelijking biedt goede aanknopingspunten, maar gaat niet volledig op omdat veiligheid en het respecteren van mensenrechten voorwaarden zijn voor economische groei en innovatie.

---

[11] Brief van 23 februari 2017, griffienummer: 160847.01, p. 3-4.

[12] Brief van 23 februari 2017, griffienummer: 160847.01, p. 6.

[13] Rapport van de Wetenschappelijke Raad voor het Regeringsbeleid, '*De publieke kern van het internet. naar een buitenlands internetbeleid*', Amsterdam: 2015.

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 het kabinet 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 .

Brief kwetsbaarheden 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 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.

35. De fractieleden van **GroenLinks** vragen de regering 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. Gaat dit wetsvoorstel juist kwetsbaarheden openhouden in plaats van ze te dichten, om zo van deze gaten gebruik te kunnen maken tijdens het hacken?** De voornoemde leden ontvangen graag een toelichting van de regering. DRC.

Brief kwetsbaarheden 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 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.

7. Geautomatiseerd werk
48. Ook geldt de hackbevoegdheid voor 'een geautomatiseerd werk', hetgeen vrijwel alle elektronische apparaten omvat (hetgeen de komende jaren met het internet of things alleen maar in omvang zal toenemen). Kan de regering aan de **D66**-fractieleden **uitleggen waarom niet gekozen is voor een lijst met een limitatieve opsomming van specifieke misdrijven waarvoor de bevoegdheid beperkt moet worden en specifieke apparaten die gehackt mogen worden?**
DRC, OM

74. De brede definitie vormt onderdeel van het Cybercrimeverdrag, dat door de Nederlandse regering is ondertekend. De Nederlandse regering is gehouden dit verdrag te implementeren. De definitie van geautomatiseerd werk, zoals deze in de EU-regelgeving wordt gebruikt, is nog ruimer omdat daarin ook de computergegevens zijn betrokken die met dat apparaat of groep van apparaten worden opgeslagen, verwerkt of verzonden met het oog op de verwerking, het gebruik, de beveiliging en het onderhoud daarvan (Kaderbesluit 2013/40/EU over aanvallen op informatiesystemen). De Nederlandse regering is eveneens gehouden dit kaderbesluit te implementeren. Mede gelet op het advies van de Afdeling advisering van de Raad van State geeft de regering de voorkeur aan de definitie van het Cybercrimeverdrag, waarbij opgemerkt kan worden dat het begrip 'gegevens' reeds in de Nederlandse wetgeving is geïmplementeerd (art. 80 quinquies Sr). Voor het antwoord op de vraag waarom niet is gekozen voor een beperkte lijst van apparaten wordt overigens verwezen naar de beantwoording van een eerdere, soortgelijke vraag van de leden van de SP-fractie.

26. Het begrip geautomatiseerd werk is ingekaderd in het Cybercrimeverdrag van de Raad van Europa. Op grond van artikel 1, onderdeel a, van dit verdrag wordt onder dit begrip verstaan een apparaat of groep van onderling verbonden apparaten, waarvan er een of meer op basis van een programma automatisch computergegevens verwerken. Uit deze begripsomschrijving vloeit voort dat ieder apparaat, dat op basis van een programma automatisch gegevens verwerkt, onder de reikwijdte valt van het begrip geautomatiseerd werk. Nederland is gehouden dit verdrag te implementeren. Vastgesteld kan worden dat deze begripsomschrijving ruim is en, zeker in het licht van de ontwikkeling van 'the internet

Met opmerkingen 9 **:** # CIA 'hack'

of things', veel verschillende apparaten kan omvatten. Ook een groep van onderling verbonden apparaten valt onder de definitie van het begrip geautomatiseerd werk, mits een of meer van die apparaten op basis van een programma gegevens verwerkt. Dit betekent dat de grens niet zozeer ligt in de definitie van het geautomatiseerde werk, als wel in de beperkingen in de toepassing van de bevoegdheid tot het binnendringen van een dergelijk werk. Echter, als verschillende apparaten met elkaar zijn verbonden, bijvoorbeeld in een thuisnetwerk, terwijl meerdere apparaten zelfstandig op basis van een programma gegevens verwerken, dan zal een bevel tot het op afstand binnendringen van een geautomatiseerd werk meerdere geautomatiseerde werken kunnen omvatten. Vereist is dat de geautomatiseerde werken bij de verdachte in gebruik zijn, en dat het binnendringen van die geautomatiseerde werken noodzakelijk is voor de opsporing van ernstige strafbare feiten. De officier van justitie in het bevel moeten opnemen om welke geautomatiseerde werken het precies gaat zodat de rechter-commissaris zich een oordeel kan vormen over de rechtmatigheid van het binnendringen in die werken. Van belang is dat het object van het binnentreden voldoende precies kan worden vastgesteld. Deze omschrijving vormt de basis voor de toets van proportionaliteit en subsidiariteit. De inzet van de bevoegdheid is vervolgens beperkt tot het geautomatiseerde werk zoals in het bevel omschreven. Welke kenmerken de beschrijving van het geautomatiseerde werk vormen kan per voorgestelde inzet verschillen. Zo zal het bijvoorbeeld wanneer de smartphone van de verdachte bekend is, het in de rede liggen dat het zogenaamde MAC-adres van het betreffende geautomatiseerde werk wordt opgenomen. Een MAC-adres is een uniek nummer dat is verbonden aan de betreffende hardware, zodat deze kan worden geïdentificeerd. Wanneer de bevoegdheid bijvoorbeeld wordt ingezet voor het binnendringen in een zwaar beveiligde server waar zich naar verwachting kinderporno bevindt kan niet altijd van te voren duidelijk zijn om welk MAC-adres het gaat, en kan het meer in de rede liggen dat in het bevel het IP-adres wordt opgenomen dat op dat moment de verbinding vormt tussen het betreffende geautomatiseerde werk en het internet. Essentieel is dat de rechter-commissaris zich op basis van de gegeven omschrijving van het geautomatiseerde werk een goed beeld kan vormen van de reikwijdte van het binnendringen en kan beoordelen in hoeverre dit door de omstandigheden wordt gerechtvaardigd. Als tijdens het onderzoek in een geautomatiseerd werk blijkt dat een ander geautomatiseerd werk op afstand moet worden binnengedrongen, dan zijn een aanvullend bevel evenals een aanvullende machtiging van de rechter-commissaris vereist. Het bevel en de machtiging kunnen mondeling worden afgegeven. Aldus zal zich in de praktijk een stapsgewijze aanpak kunnen ontwikkelen, op basis waarvan de betrokkenheid van de rechter-commissaris verzekerd is zodra een geautomatiseerd werk op afstand wordt binnengedrongen met het oog op het verrichten van bepaalde onderzoekshandelingen.

67. Zoals in de memorie van toelichting uiteen gezet is, in lijn met het advies van de Afdeling advisering van de Raad van State, ervoor gekozen om de voorwaarden voor de inzet van de bevoegdheid tot heimelijk binnendringen in een geautomatiseerd werk te differentiëren naar de mate waarin een inbreuk gemaakt wordt op de persoonlijke levenssfeer. Dit heeft tot gevolg dat het binnendringen van een geautomatiseerd werk met het oog op de het vaststellen van bepaalde kenmerken van het geautomatiseerde werk, het opnemen van communicatie of vertrouwelijke communicatie en de stelselmatige observatie

mogelijk is als er sprake is van 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. Het gaat hier om alle misdrijven waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaren of meer is gesteld (onderdeel a) en de specifiek in de in de onderdelen b en c aangewezen misdrijven.

In het geval het geautomatiseerde werk wordt binnengedrongen voor doelen waarbij de mate waarin inbreuk gemaakt wordt op de persoonlijke levenssfeer ingrijpender is, zoals het vastleggen of ontoegankelijk maken van gegevens, geldt een zwaarder verdenkingscriterium. In dergelijke gevallen 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 misdrijven waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld zijn alle zeer ernstige delicten met ingrijpende gevolgen zoals de deelneming aan een terroristische organisatie (artikel 140a Sr), het maken van een beroep of gewoonte van het aanbieden, verspreiden of bezitten van kinderpornografie (artikel 240b, tweede lid, Sr), mensenhandel (artikel 273f, eerste lid, Sr), opzettelijke vrijheidsberoving (artikel 282 Sr), gijzeling (artikel 282a Sr), doodslag (artikel 287 Sr) of moord (artikel 289 Sr).

De bij algemene maatregel van bestuur aan te wijzen misdrijven zullen misdrijven zijn waarop weliswaar geen gevangenisstraf van acht jaar of meer is gesteld maar die worden gepleegd met behulp van een geautomatiseerd werk en waarbij er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders. Dit betreft misdrijven als het gebruik van een botnet (artikel 138ab, derde lid, Sr), het aanbieden, verspreiden of bezitten van kinderpornografie (artikel 240b, de verleiding van een minderjarige tot ontucht (artikel 248a Sr) en ‘grooming’ (artikel 248e Sr). Er is dan vaak geen ander aangrijpingspunt voor de opsporing. Een beperking tot inzet van de bevoegdheid tot heimelijk binnendringen en het verrichten van onderzoekshandelingen tot levensbedreigende en terroristische misdrijven is daarom niet wenselijk. Het voordeel van aanwijzing van de delicten is dat flexibel ingespeeld kan worden op de snelle ontwikkelingen in de computercriminaliteit.

De regering heeft niet gekozen voor een gesloten lijst van delicten omdat de bevoegdheid tot het op afstand binnendringen van een geautomatiseerd werk in een belangrijk deel van de gevallen dient als basis voor de toepassing van bestaande bijzondere opsporingsbevoegdheden, als het aftappen van communicatie en het afluisteren van vertrouwelijke communicatie. De toepassing van deze opsporingsbevoegdheden is thans niet beperkt tot een lijst van delicten, en de opsporing zou naar het oordeel van de regering ernstig worden belemmerd als een dergelijke lijst wel zou gaan gelden voor het aftappen van telecommunicatie of afluisteren van vertrouwelijke communicatie die door middel van een smartphone wordt afgehandeld, als de software voor het afluisteren op de smartphone is geplaatst. De regering geeft er de voorkeur aan het oordeel over de toepassing van de bevoegdheid in concrete gevallen over te laten aan het oordeel van de rechter. Een soortgelijke systematiek geldt niet alleen bij de toepassing van andere bijzondere opsporingsbevoegdheden, maar ook bij andere dwangmaatregelen als de inbeslagneming en de huiszoeking.

9. Begroting
62. Bij het voorgestelde artikel II, onder EE staat vermeld: "Artikel 592, tweede lid, eerste volzin, komt te luiden: De kosten van het nakomen van een vordering tot het verstrekken van gegevens of tot het medewerking verlenen aan het ontsleutelen van gegevens krachtens de artikelen 125k, 126m, 126n, 126na, 126nc tot en met 126ni, 126t, 126u, 126ua, 126uc tot en met 126ui, 126zg, 126zh, 126zi en 126zja tot en met 126zp kunnen de betrokkene uit 's Rijks kas worden vergoed". **Kan de regering aangeven wanneer deze kosten wel en wanneer deze kosten niet worden vergoed? Of zouden deze kosten steeds uit 's Rijks kas behoren te worden vergoed, zo vragen de CDA-fractieleden**.
DWJZ, Luut/DRC.

63. De leden van de fractie van de **ChristenUnie** krijgen graag meer inzicht in hoe verwacht wordt dat de financiële middelen verschuiven binnen het budget van de nationale politie binnen het totaal beschikbare budget. Zij lezen dat de mate van verschuiving afhankelijk is van de verwachtingen van en ervaring met toepassing van het instrument. Dat zal niet alleen gelden voor de feitelijke ontwikkeling en inzet van onderzoek in een geautomatiseerd werk en het gebruik van technische hulpmiddelen ten behoeve van de uitvoering van die bevoegdheid, maar ook voor de inzet van menskracht. **Welke verwachting heeft de regering momenteel, en ten laste van welke andere inzet zal dit wetsvoorstel dan bij de invoering van het wetsvoorstel komen, zo vragen voornoemde leden.**
DGPOL, DRC.

64.
Kan voorzien worden in enkele scenario's en een begroting voor de eerste jaren na inwerkingtreding van het wetsvoorstel? **Is voor de inzet van deze bevoegdheden geen extra capaciteit nodig?**
DGPOL, DRC.

65. Zij krijgen tevens graag inzicht in hoe de **extra voorziene structurele last voor de rechtspraak** van 500.000 euro wordt gedekt in de begroting van het ministerie. Zij missen duidelijkheid over de gevolgen van dit wetsvoorstel voor de begroting van het OM.
DRC
282. De Rechtspraak wordt gefinancierd middels outputfinanciering. In het kader van zijn wettelijke adviestaak heeft de Raad 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 Ministerie.

11. Internationale aspecten
73. Tijdens de plenaire behandeling van het wetsvoorstel in de Tweede Kamer op 13 december 2016 heeft de Staatssecretaris van Veiligheid en Justitie aangegeven dat hij streeft naar **betere paraplu-afspraken met andere staten** in voorkomende gevallen van ernstige strafbare feiten waarbij Nederlandse opsporingsambtenaren onbedoeld toegang krijgen tot geautomatiseerde werken die zich buiten Nederland bevinden. Die afspraken zouden ook voor omgekeerde situaties hebben te gelden wanneer buitenlandse opsporingsambtenaren zich onbedoeld op een Nederlandse server of net bevinden.[14] **Wat is**

[14] Handelingen II 2016/17, 34, item 26, p. 43.

het tijdpad dat de regering zich voorstelt voor het maken van deze paraplu-afspraken, zo vragen de leden van de VVD-fractie. Kan zij binnen een termijn van één jaar de Kamer informeren over de voortgang wat betreft het maken van deze paraplu-afspraken met andere staten en de inhoud van die afspraken?
DRC, OM.

Concept beantwoording ICS: Op 16 september 2016 heeft de Cloud Evidence Group, een subgroep van het comité van verdragspartijen van het Cybercrimeverdrag uit 2001, 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 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 op te stellen.

74. Met betrekking tot opsporing van computercriminaliteit die de landsgrenzen overschrijdt, is in internationaal verband kennelijk vastgesteld dat het **territorialiteitsbeginsel in 'cyberspace'** onder druk staat en dat dit beginsel niet kan worden toegepast als de exacte locatie van gegevens onduidelijk is. **Kan de regering de leden van de VVD-fractie informeren over de stand van zaken en ontwikkelingen om te komen tot internationale regels met het oog op de bestrijding van internationale computercriminaliteit? Is zij van plan om in dezen initiatieven te ontwikkelen, bijvoorbeeld door het organiseren van een internationale conferentie, mede met het oog op de belangrijke positie die Nederland inneemt op het terrein van de handhaving van de internationale rechtsorde?**
DRC, OM.

Concept beantwoording ICS: 51. Vanwege de afwezigheid van grenzen in cyberspace, de mogelijkheden voor anonimiteit en de mogelijkheden om het zeer lastig te maken een geografische plaats van elektronisch bewijs of de oorsprong van een cyberaanval te achterhalen, is het vaak praktisch niet mogelijk de fysieke locatie waar gegevens zijn opgeslagen, worden verwerkt of overgedragen te achterhalen. Door de grenzeloosheid van het internet zijn de mogelijkheden voor criminelen om gegevens en activiteiten snel te verplaatsten en voor de opsporing te verbergen groot, zeker in vergelijking met de op territorialiteit gebaseerde procedures voor internationale opsporing. Vooral in situaties waarin gegevens over strafbare feiten snel worden verplaatst of wanneer het redelijkerwijs niet mogelijk is de fysieke plaats van gegevens te achterhalen, zijn de traditionele mogelijkheden voor internationale opsporing ontoereikend. In juni 2016 heeft de JBZ-raad daarom conclusies 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 EU voor rechtshulp al eerder zijn ontwikkeld en gangbaar zijn;
- het stroomlijnen en versnellen van de bestaande procedures voor wederzijdse rechtshulp (mutual legal assistance, MLA) en wederzijdse erkenning (mutual

recognition) binnen de EU en met derde landen, onder andere door digitalisering van verzoeken en automatische vertaling hiervan, als ook 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 ("enforcement jurisdiction") 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 resultaten van het proces inzake handhavende rechtsmacht te rapporteren aan de JBZ-raad in juni 2017.

77.
Hoe verlopen de **onderhandelingen in EU-verband en in de Raad van Europa** over een helder grensoverschrijdend juridisch kader? De voornoemde leden zijn benieuwd naar de antwoorden van de regering.
DRC, OM.

Zie vraag 73, 74.

12. Overige
78. **Hoe en waar worden gegevens die beschikbaar komen in het kader van het binnendringen in een geautomatiseerd werk op grond van de wet, opgeslagen**, zo vragen de **VVD**-fractieleden.
DRC, NP/DWJZ, Luut.

104/105 Het onderzoek in een geautomatiseerd werk met behulp van een technisch hulpmiddel, vindt, anders dan het onderzoek met de traditionele technische hulpmiddelen, plaats in een volledig digitale omgeving. Omwille van de overzichtelijkheid zullen de eisen die aan technische hulpmiddelen voor het doen van onderzoek in een geautomatiseerd werk worden gesteld neergelegd worden in een nieuw besluit, dat wordt toegesneden op het doen van onderzoek in een digitale context. De in de memorie van toelichting aangekondigde aanpassing van het Besluit technische hulpmiddelen strafvordering wordt niet langer voorzien.

Het besluit ter uitvoering van het wetsvoorstel wordt gebaseerd op het uitgangspunt dat de gegevens die met een technisch hulpmiddel worden vastgelegd betrouwbaar, voor derden toetsbaar en niet manipuleerbaar dienen te zijn. In het besluit eisen zullen eisen worden gesteld aan de inrichting en werking van het technische hulpmiddel. Een belangrijke inrichtingseis zal zijn dat de instelling van de software kan worden gedifferentieerd naar het gebruik van verschillende functionaliteiten. Verder zal vereist worden dat de inhoud van de geregistreerde gegevens identiek zijn aan de inhoud van de gedetecteerde gegevens. Ook zullen eisen worden gesteld over de automatische opslag van geregistreerde gegevens op – uitsluitend - de politieserver. Om de onschendbaarheid van de waarnemingen te kunnen

waarborgen en manipulatie door derden te voorkomen, zal als eis gesteld worden dat het transport van de signalen vanuit het geautomatiseerde werk naar de server van de politie plaatsvindt via een versleuteld bestand. Bij de keuring zal getoetst worden of de software aan de eisen voldoet. Alleen wanneer de software is goedgekeurd, mag deze worden ingezet voor het doen van onderzoek in een geautomatiseerd werk. Het besluit zal verder als voorwaarde stellen dat de technische handelingen die worden verricht tijdens het onderzoek doorlopend en automatisch op de politieserver worden vastgelegd (logging), zodat controle op de uitvoering van het bevel van de officier van justitie te allen tijde, zowel tijdens het onderzoek als achteraf, mogelijk is.

79. Op welke wijze wordt daarbij een **onderscheid gemaakt tussen gegevens die nodig zijn voor de vaststelling van ernstige strafbare feiten** in de zin van artikel 67, eerste lid, van het Wetboek van Strafvordering en zogenoemde bijvangst. **Worden gegevens die als bijvangst gelden, vernietigd**? Zo ja, wanneer en hoe? Zo niet, op welke juridische grondslag wordt bijvangst opgeslagen?
DWJZ, Luut, NP, DRC.

27. Een onderzoek in een geautomatiseerd werk kent een zorgvuldige voorbereiding. In de verkennende fase worden gegevens over strafbare feiten en personen die daarbij betrokken zijn in kaart gebracht. Daarbij wordt ook gekeken of, en zo ja welke, geautomatiseerde werken in gebruik zijn bij een persoon. Deze voorbereidende werkzaamheden verschillen niet wezenlijk van de werkzaamheden die worden verricht bij de voorbereiding van andere (bijzondere) opsporingsbevoegdheden. Als er geen aanknopingspunten voor onderzoek in een geautomatiseerd werk zijn, zal de bevoegdheid niet worden ingezet.

Tijdens de verkennende fase wordt zoveel mogelijk een beeld gevormd van de gegevens die nodig zijn voor het onderzoek naar de specifieke strafbare feiten in relatie tot een verdachte. De verkennende fase vormt de basis voor het bevel van de officier van justitie. De onderzoekshandelingen worden in het bevel vermeld. Voorts vermeldt het bevel het deel van het geautomatiseerde werk en de categorie van gegevens waar het onderzoek betrekking op heeft en bevat het een aanduiding van aard en functionaliteit van de software die gebruikt mag worden bij het onderzoek. Het onderzoek in een geautomatiseerd werk vindt plaats binnen de grenzen van het bevel van de officier van justitie en wordt verricht door het eerdergenoemde technische team. Voor zover het doel van het onderzoek gelegen is in 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 emailverkeer, kan niet worden uitgesloten dat gegevens worden verkregen over andere personen die bij de communicatie zijn betrokken. Dit is thans evenmin anders, als vertrouwelijke communicatie wordt afgeluisterd of communicatie wordt afgetapt (op grond van de artikelen 126l, 126m, 126s, 126t of 126zg Sv) of als gegevens over het emailverkeer van een persoon worden gevorderd bij de aanbieder (artikelen 126nd/ng Sv). Uitsluitend de gegevens die binnen de reikwijdte van het bevel van de officier van justitie vallen worden ter beschikking gesteld van het tactisch onderzoeksteam.

78. Met het vereiste dat het geautomatiseerde werk bij de verdachte in gebruik is wordt voorkomen dat de bevoegdheid wordt ingezet jegens anderen dan de verdachte. Dat gegevens van derden in het kader van de toepassing van bijzondere opsporingsbevoegdheden ter kennis komen van de opsporingsambtenaren is overigens niet

nieuw. Bij de toepassing van een opsporingsbevoegdheid van het aftappen van telecommunicatie komt de communicatie van de personen met wie het gesprek wordt gevoerd uit de aard der zaak ter kennis van de opsporingsambtenaren die zijn belast met het uitluisteren van deze communicatie. Ditzelfde geldt bij het gebruik van de internettap, alsdan komt alle informatie die via een IP-adres wordt gecommuniceerd, ter kennis van de opsporing, ook de gegevens van gebruikers van andere geautomatiseerde werken die gebruik maken van dezelfde router en daarmee van ditzelfde IP-adres. Voor de toepassing van bepaalde bijzondere opsporingsbevoegdheden in het kader waarvan gegevens van derden ter kennis kunnen komen van de politie, gelden specifieke verplichtingen rond het verdere gebruik van de verzamelde gegevens. Dit betreft de observatie met behulp van een technisch hulpmiddel dat signalen registreert, het aftappen van telecommunicatie, het direct afluisteren van vertrouwelijke communicatie en het vorderen van gegevens. De officier van justitie kan bepalen dat de gegevens worden gebruikt voor een ander strafrechtelijk onderzoek, anders worden de gegevens vernietigd zodra twee maanden verstreken zijn nadat de zaak is geëindigd (art. 126cc, tweede lid, en 126dd, eerste lid, Sv). Deze verplichtingen zijn onverkort van toepassing voor de toepassing van het aftappen van telecommunicatie en het opnemen van vertrouwelijke communicatie, nadat op afstand een geautomatiseerd werk is binnengedrongen.

80. **Wordt bijvangst van fiscale aard doorgestuurd naar de Belastingdienst**? Zo nee, waarom niet? Op grond van welke nationale en internationale rechtsregels, uitspraken en arresten, daaronder begrepen van internationale gerechtshoven, dienen fiscale gegevens die kwalificeren als bijvangst, 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?

OM/Financiën, DRC

81. 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, dan wordt er een formele procedure in gang gezet die mogelijk veel tijd in beslag kan nemen, merken de VVD-fractieleden op. **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?**
DRC, OM.

86. De leden van de fractie van de **ChristenUnie** vragen om een **reflectie op het feit dat Nederland bovenmatig vaak gebruikmaakt van telefoon- en gegevenstaps.** Is duidelijk te maken **of en hoe dit uitwerkt op de veiligheid voor Nederlandse burgers vergeleken met andere EU-burgers?**
DRC, OM.

51. In reactie op deze vraag moet voorop worden gesteld dat de toepassing van andere bijzondere opsporingsbevoegdheden niet is beperkt tot een verdachte. Voor de toepassing van bijzondere opsporingsbevoegdheden, zoals de observatie (art. 126g Sv), het stelselmatig inwinnen van informatie (art. 126j Sv) of het aftappen van telecommunicatie (art. 126m Sv), is een verdenking van een misdrijf vereist. Voor het aftappen betreft dit een ernstige misdrijf, waarvoor voorlopige hechtenis mogelijk is. Het is echter niet uitgesloten

dat voormelde bevoegdheden jegens anderen dan de verdachte worden ingezet, wanneer dit van belang is voor de waarheidsvinding. Voor de voorgestelde bevoegdheid van het op afstand binnendringen van een geautomatiseerd werk is echter wel als nadere beperking gesteld dat het geautomatiseerde werk bij de verdachte in gebruik is. Niet is vereist dat de verdachte de enige gebruiker is. Het is derhalve niet bij voorbaat uitgesloten dat het onderzoek in een geautomatiseerd werk, dat bij de verdachte in gebruik is, ook gegevens van anderen in beeld komen.

De voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk kan uitsluitend worden uitgeoefend in geval van verdenking van een ernstig misdrijf dat gezien zijn aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert. De wettelijke voorwaarde van de verdenking van betrokkenheid van een persoon bij een ernstig strafbaar feit staat in de weg aan de inzet van deze bevoegdheid in de vorm van een zogenaamde sleepnetmethode. Daarnaast moet tevoren duidelijk zijn naar welke gegevens wordt gezocht, dit moet in het bevel van de officier van justitie worden opgenomen. Vanwege de functiescheiding wordt het onderzoek in een geautomatiseerd werk uitgevoerd door speciaal daarvoor opgeleide opsporingsambtenaren die niet betrokken zijn bij het betreffende opsporingsonderzoek. Voor het binnendringen en verzamelen van gegevens wordt doorgaans gebruik gemaakt van speciale software die is afgeregeld op de specifieke gegevens waarnaar wordt gezocht. Het is dan niet heel waarschijnlijk dat gegevens van andere gebruikers, als deze geen verband hebben met de gegevens waarnaar wordt gezocht ten behoeve van het opsporingsonderzoek, worden verzameld en vastgelegd. In die gevallen waarin dat wel zo zou zijn ligt het voor de hand dat deze gegevens worden gewist omdat deze niet van belang zijn voor het betreffende opsporingsonderzoek. Het wetsvoorstel bevat dan ook verschillende waarborgen die voorkomen dat deze wet leidt tot een ‘dragnet’, waar ook de omgeving van de verdachte in meegetrokken wordt.

87. **Welke verwachting heeft de regering van het gebruik van de nieuwe voorgestelde bevoegdheid?** De voornoemde leden vragen of van de nieuwe bevoegdheid verwacht wordt dat deze zich ontwikkelt tot een ultimum remedium of juist tot een gangbaar gebruikte opsporingsbevoegdheid.
DRC, OM.

Van: 10.2.e
Verzonden: donderdag 13 april 2017 13:14
Aan: Plas, Theo van der (T.G.)
CC: Smit-Arnold Bik, Marjolein (C.P.M.); 10.2.e ; 10.2.e
Onderwerp: memo besluit onderzoek geautomatiseerd werk
Bijlagen: memo besluit technische hulpmiddelen def.docx; bijlage 1 - BOGW - uitgewerkte observaties en opmerkingen CCIII team - verzend.docx; bijlage 2 - eerste reactie op besluit CC3.pdf; bijlage 3 - tabel voorstel .docx; bijlage 4 - 06-03-2017 CCII overleg.docx

Opvolgingsmarkering: Opvolgen
Markeringsstatus: Gemarkeerd

Beste Theo,

Bijgaand tref je aan een memo (inclusief 4 bijlages) met daarin de belangrijkste punten die door ons (en het OM) zijn ingebracht tijdens de overleggen met het departement om te komen tot een werkbare versie van het besluit onderzoek in een geautomatiseerd werk. Tot op heden is er geen nieuwe versie van het besluit opgesteld door de wetgevingsjuristen van het ministerie, waaruit blijkt dat onze opmerkingen (deels) zijn verwerkt. Het lijkt er op alsof er ook geen nieuwe tussenversie meer zal komen en dat eind deze maand een versie van het besluit voor formele consultatie zal worden rondgestuurd en zal worden gepubliceerd op het internet.

Met deze memo kun jij, eventueel in samenwerking met het OM, op strategisch niveau proberen om onze opmerkingen toch nog te laten verwerken in het besluit. Anders zijn wij als politie straks genoodzaakt om in de formele consultatie veel kanttekeningen te plaatsen bij het besluit en dat willen wij nou juist voorkomen. DGRR (10.2.e en 10.2.e) begrijpt dat dit scenario wellicht niet meer af te wenden is en steunt ons hierin.

Mocht je nog vragen hebben, dan horen wij dat graag.
Met vriendelijke groet,
10.2.e

Interne Memo

Theo van der Plas

Onderwerp
Aandachtspunten Besluit onderzoek geautomatiseerd werk

Organisatieonderdeel
Portefeuille Digitalisering en Cybercrime
Programma CCIII

Behandeld door
10.2.e

Functie
Operationeel Specialist D

Telefoon
06-10.2.e

E-mail
10.2.e @politie.nl

Ons kenmerk
Klik hier als u tekst wilt invoeren.

Uw kenmerk
Klik hier als u tekst wilt invoeren.

In afschrift aan
Marjolein Smit, 10.2.e ,
10.2.e

Datum
11 april 2017

Bijlage(n)
4

Pagina
1

Beste Theo,

Gedurende de afgelopen maanden (vanaf begin februari 2018) is er in verschillende sessies op het Ministerie van VenJ de gelegenheid geboden om te reageren op een 2e concept versie van het besluit onderzoek in een geautomatiseerd werk (versie voor het overleg van 3 februari 2017) en de bijbehorende Nota van Toelichting. In deze 2e versie zijn de opmerkingen zoals die in een eerder stadium door middel van twee brieven (programma CCIII (bijlage 1) en de Keuringsdienst (bijlage 2)) zo goed als niet verwerkt.

12-14

Doel van deze memo is om, voordat het concept besluit in formele consultatie gaat, toch nog een informele reactie aan het Ministerie af te geven, zodat onderstaande punten niet door middel van een formele reactie door de Korpschef hoeven te worden geadresseerd.

Aandachtspunten
De belangrijkste aandachtspunten waar niet voldoende aandacht aan wordt besteed in het concept besluit zijn:

1. 12-14
2.
3.

Onderwerp
Aandachtspunten Besluit onderzoek geautomatiseerd werk

Datum
11 april 2017

Pagina
2 van 6

12-14

Onderwerp
Aandachtspunten Besluit onderzoek geautomatiseerd werk

Datum
11 april 2017

Pagina
3 van 6

12-14

Onderwerp
Aandachtspunten Besluit onderzoek geautomatiseerd werk

Datum
11 april 2017

Pagina
4 van 6

12-14

Onderwerp
Aandachtspunten Besluit onderzoek geautomatiseerd werk

Datum
11 april 2017

Pagina
5 van 6

12-14

Onderwerp
Aandachtspunten Besluit onderzoek geautomatiseerd werk

Datum
11 april 2017

Pagina
6 van 6

12-14

Besluit van * houdende eisen met betrekking tot het doen van onderzoek in een geautomatiseerd werk (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 zevende lid, 126uba, eerste en derde lid, 126zpa, eerste en derde lid, en 126ee van het Wetboek van Strafvordering;
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 als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid, van het Wetboek van Strafvordering;
b. korpschef: korpschef als bedoeld in artikel 27 van de Politiewet 2012;
c. Onze Minister: Minister van Veiligheid en Justitie;
d. server: server van een onderdeel van de Landelijke eenheid, bedoeld in artikel 3 van het Besluit beheer politie: **PM** voorziening Kmar/BOD?;
e. technisch hulpmiddel: technisch hulpmiddel dat gegevens detecteert, registreert en opslaat ter uitvoering van een bevel;
f. technisch team: team van de Landelijke eenheid bedoeld in het Besluit beheer politie2012, (**PM** voorziening Kmar en BOD?) dat is belast met de uitvoering van een bevel.

Artikel 2 Overeenkomstige toepassing werkgever
Hetgeen in de artikelen ** wordt bepaald over de korpschef is van overeenkomstige toepassing op de werkgever van de ambtenaren bedoeld in de artikelen 141, onderdelen c en d, en 142 van het Wetboek van Strafvordering.

Hoofdstuk 2 Eisen aan een technisch hulpmiddel
Artikel 3 Gerichte inzet
***1** Het technische hulpmiddel is zodanig ingericht dat de inzet ervan kan worden beperkt tot de in het bevel vermelde functionaliteit of functionaliteiten.

Artikel 4 Gerichte registratie
Het technische hulpmiddel detecteert en registreert uitsluitend gegevens ten behoeve van de in het bevel vermelde functionaliteit of functionaliteiten.
PM Specificaties per functionaliteit.

Artikel 5 Betrouwbaarheid
Het technische hulpmiddel registreert gegevens op zodanige wijze dat de inhoud van de registreerde gegevens identiek is aan de inhoud van de gedetecteerde gegevens.

Artikel 6 Authenticiteit
Het technische hulpmiddel voorziet de geregistreerde gegevens van een uniek gegeven.

Artikel 7 Datum en tijd
Het technische hulpmiddel registreert de datum en tijd waarop gegevens worden geregistreerd.

12-14

Artikel 8 Beveiliging
Het technische hulpmiddel is beveiligd tegen misbruik door derden.

Artikel 9 Automatische opslag

1. Het technische hulpmiddel slaat automatisch geregistreerde gegevens op de server op.
2. Het technische hulpmiddel slaat geregistreerde gegevens uitsluitend op de server op.
3. Het technische hulpmiddel slaat gegevens op zodanige wijze op dat de inhoud van de op de server opgeslagen gegevens identiek is aan de inhoud van de door het technische hulpmiddel geregistreerde gegevens.

Artikel 10 Beveiliging transport
Het technische hulpmiddel transporteert geregistreerde gegevens naar de opslag op de server via een beveiligd bestand.

Hoofdstuk 3 Voorafgaande keuring van een technisch hulpmiddel

Artikel 11 Voorafgaande keuring

1. Het technische hulpmiddel wordt voorafgaand aan de inzet ervan gekeurd.
2. Uit een keuringsrapport blijkt of het technische hulpmiddel voldoet aan de in de artikelen 3 tot en met 10 gestelde eisen.

Artikel 12 Keuringsdienst

1. Onze Minister kan een onderdeel van een landelijke eenheid als bedoeld in artikel 25, eerste lid, onder b, van de Politiewet 2012, aanwijzen als keuringsdienst.
2. Onze Minister kan één of meer andere organisaties aanwijzen als keuringsdienst.
3. Onze Minister kan regels stellen bij de aanwijzing van een keuringsdienst.

12-14

Artikel 13 Keuringsprotocol

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

12-14

Artikel 14 Keuring

1. De korpschef kan technische hulpmiddelen ter keuring aanbieden aan een keuringsdienst.
2. Een keuringsdienst maakt van de keuring een rapport op, waaruit blijkt in hoeverre het technische hulpmiddel voldoet aan de in de artikelen 3 tot en met 10 gestelde eisen.
3. Het keuringsrapport vermeldt:

a. een referentienummer;

b. een aanduiding van de functionaliteit of functionaliteiten van het technische hulpmiddel;

c. de periode waarvoor de keuring geldt;

d. relevante informatie met betrekking tot de inzet van een functionaliteit of functionaliteiten van het technische hulpmiddel.

12-14

12-14

Artikel 16 Wederzijdse erkenningsclausule

1. Met technische hulpmiddelen in dit besluit worden gelijkgesteld technische hulpmiddelen die rechtmatig zin vervaardigd of in de handel gebracht zijn in een andere lidstaat van de Europese Unie dan wel rechtmatig zijn vervaardigd in een staat, niet zijnde een lid van de Europese Unie, die partij is bij een daartoe strekkend of mede daartoe strekkend verdrag dat Nederland bindt en de 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 lid 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.

12-14

12-14

Hoofdstuk 4 Beheer, verstrekking en plaatsing van een technisch hulpmiddel

Artikel 17 Beheer

De door een keuringsdienst gekeurde technische hulpmiddelen worden beheerd op de politieserver.

12-14

Artikel 18 Toegankelijkheid beheer

De server waarop het beheer plaatsvindt is uitsluitend toegankelijk voor door de korpschef aangewezen en terzake deskundige ambtenaren.

12-14

Artikel 19 Beveiliging beheer

Bij het beheer op de server worden maatregelen genomen om manipulatie te voorkomen en achteraf te kunnen vaststellen of niettemin manipulatie heeft plaatsgevonden.

12-14

Artikel 20 Verstrekking

1. De met het beheer belast ambtenaar verstrekt na ontvangst van een kopie van het bevel het voor de uitvoering daarvan benodigde technische hulpmiddel aan de met de plaatsing belaste opsporingsambtenaar.
2. De met het beheer belaste ambtenaar registreert de verstrekking van het technische hulpmiddel. De registratie bevat ten minste de aanduiding van het technische hulpmiddel, de aanduiding van de in het bevel vermelde functionaliteit of functionaliteiten, het tijdstip van de verstrekking, de verwachte duur van de inzet en de naam van de officier van justitie die het bevel gegeven.
3. Het technische hulpmiddel wordt verstrekt voor de periode die nodig is voor de uitvoering van het bevel.

Zie vorige artikelen

12-14

Artikel 21 Verstrekking voor oefendoeleinden

1. De met het beheer belaste ambtenaar verstrekt na ontvangt van een verzoek door of namens de korpschef technische hulpmiddelen voor oefendoeleinden aan de met de plaatsing belaste opsporingsambtenaar.
2. De met het beheer belaste ambtenaar registreert de verstrekking van het technische hulpmiddel. De registratie bevat ten minste de aanduiding van het technische hulpmiddel, de aanduiding van de in het bevel vermelde functionaliteit of functionaliteiten, het tijdstip van de verstrekking, de verwachte duur van de inzet en de functionaris die het verzoek heeft ingediend.
3. Het technische hulpmiddel wordt verstrekt voor de duur van de oefening.

idem

12-14

12-14

Graag overleg alvorens tekstvoorstel

Artikel 22 Plaatsing
1. De plaatsing van een technisch hulpmiddel geschiedt door een opsporingsambtenaar, die lid is van een technisch team.
2. De opsporingsambtenaar zorgt er bij de plaatsing voor dat de inzet van het technische hulpmiddel beperkt wordt tot de in het bevel vermelde functionaliteit of functionaliteiten.
3. De opsporingsambtenaar maakt proces-verbaal op van de plaatsing, dat wordt toegevoegd aan de zaak.

12-14

Hoofdstuk 5 Inzet van een technisch hulpmiddel

Artikel 23 Inzet

1. De inzet van een technisch hulpmiddel vindt plaats onder verantwoordelijkheid van een opsporingsambtenaar, die lid is van een technisch team.
2. De opsporingsambtenaar maakt proces-verbaal op van de inzet, dat wordt toegevoegd aan de zaak.

12-14

Artikel 24 Opslag
De opslag van door het technische hulpmiddel geregistreerde gegevens vindt plaats op de server.

12-14

Artikel 25 Betrouwbaarheid opslag
De op de server opgeslagen gegevens worden niet bewerkt.

12-14

Geen tekstvoorstel. Te veel varianten mogelijk.
Artikel 26 Authenticiteit opslag
Bij de opslag van gegevens herkent de server het door het technische hulpmiddel geregistreerde unieke gegeven, bedoeld in artikel 6, tweede lid.

12-14

Artikel 27 Datum en tijd opslag De server registreert de datum en tijd van de opslag van gegevens.

12-14

Artikel 28 Toegankelijkheid opslag
De server waarop de opslag van gegevens plaatsvindt is uitsluitend toegankelijk voor door de korpschef aangewezen en terzake deskundige ambtenaren.

12-14

Artikel 29 Beveiliging opslag
Bij de opslag van gegevens op de server worden maatregelen genomen om manipulatie te voorkomen en achteraf te kunnen vaststellen of niettemin manipulatie heeft plaatsgevonden.

12-14

Hoofdstuk 6 Verwijdering van een technisch hulpmiddel

Artikel 30 Verwijdering

1. Het technische hulpmiddel wordt verwijderd zodra het bevel is uitgevoerd of uiterlijk zodra de geldigheidsduur van het bevel is verlopen.
2 De verwijdering van het technische hulpmiddel geschiedt door een opsporingsambtenaar, die lid is van een technisch team.
3. De opsporingsambtenaar maakt proces-verbaal op van de verwijdering, dat wordt toegevoegd aan de zaak.

Artikel 31 Niet of niet volledige verwijdering

1. Indien het technische hulpmiddel niet of niet volledig kan worden verwijderd beëindigt de opsporingsambtenaar het transport van door het technische hulpmiddel geregistreerde gegevens naar de opslag op de server.
2. Indien de niet of niet volledige verwijdering van het technische hulpmiddel risico’s oplevert voor

het functioneren van het onderzochte geautomatiseerde werk 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 wordt toegevoegd aan de zaak.

12-14

Artikel 32 Beëindiging toegang technisch hulpmiddel
PM Na de verwijdering van het technische hulpmiddel of de beëindiging van het transport van door het technische hulpmiddel geregistreerde gegevens heeft de opsporingsambtenaar geen toegang meer tot het technisch hulpmiddel.

12-14

Hoofdstuk 7 Geautomatiseerde vastlegging van de uitvoering van een bevel

Artikel 33 Vastlegging

1. De technische handelingen die worden verricht ter uitvoering van een bevel worden doorlopend en automatisch vastgelegd op de server.
2. De vastlegging vindt plaats onder verantwoordelijkheid van een van een daartoe door de korpschef aangewezen en terzake deskundige ambtenaar.

12-14

Artikel 34 Controlefunctie

1. De vastlegging van de technische handelingen vindt op zodanige wijze plaats dat tijdens de inzet van een technisch hulpmiddel er achteraf gecontroleerd kan worden of bij de opslag van door een technisch hulpmiddel geregistreerde gegevens enige onregelmatigheid heeft plaatsgevonden.
2. Indien bij de vastlegging de technische handelingen op de server een onregelmatigheid wordt geconstateerd maakt de **PM**(opsporings?)ambtenaar daarvan proces-verbaal op, dat wordt toegevoegd aan de zaak.

12-14

12-14

Artikel 35 Betrouwbaarheid vastlegging
De op de server vastgelegde technische handelingen worden niet bewerkt.

12-14

Artikel 37 Beveiliging vastlegging
Bij de vastlegging van gegevens op de politieserver worden maatregelen genomen om manipulatie te voorkomen en achteraf te kunnen vaststellen of niettemin manipulatie heeft plaatsgevonden.

12-14

Hoofdstuk 8 Opsporingsambtenaren
Artikel 38 Aanwijzing opsporingsambtenaren
1. Een opsporingsambtenaar als bedoeld in de artikelen 141, onder b, c en d, en 142 van het Wetboek van Strafvordering kan worden belast met het binnendringen in een geautomatiseerd werk en het, al dan niet met een technisch hulpmiddel, onderzoek doen ter uitvoering van een bevel, indien hij lid is van een technisch team.
2. Een opsporingsambtenaar als bedoeld in het eerste lid kan worden geplaatst bij een technisch team, indien hij heeft voldaan aan de door Onze Minister aangewezen kwalificaties.

12-14

Artikel 39 Opsporingsambtenaren die geen lid zijn van een technisch team

1. Een opsporingsambtenaar als bedoeld in de artikelen 141, onder b, c en d, en artikel 142 van het Wetboek van Strafvordering die geen lid is van een technisch team kan worden belast met het binnendringen in een geautomatiseerd werk en het, al dan niet met een technisch hulpmiddel, onderzoek doen ter uitvoering van een bevel, indien hij beschikt over specifieke kennis en vaardigheden, benodigd voor de uitvoering van het bevel.
2. Het hoofd van het team van de Landelijke eenheid, bedoeld in artikel 3 van het Besluit beheer politie dat is belast met de instandhouding van de technische teams beoordeelt of een opsporingsambtenaar als bedoeld in het eerste lid beschikt over de specifieke kennis en vaardigheden, benodigd voor de uitvoering van het bevel, en adviseert de officier van justitie terzake.
3. Indien de opsporingsambtenaar, bedoeld in het eerste lid, wordt belast met de uitvoering van een bevel wordt hij, gedurende de periode die nodig is voor de uitvoering van het bevel, begeleid door een begeleider van een technisch team.

Hoofdstuk 9 Slotbepalingen

PM Artikel 40 Wijziging Besluit beheer politie

Artikel 41 Inwerkingtreding
Dit besluit treedt in werking op een bij koninklijk besluit te bepalen tijdstip.

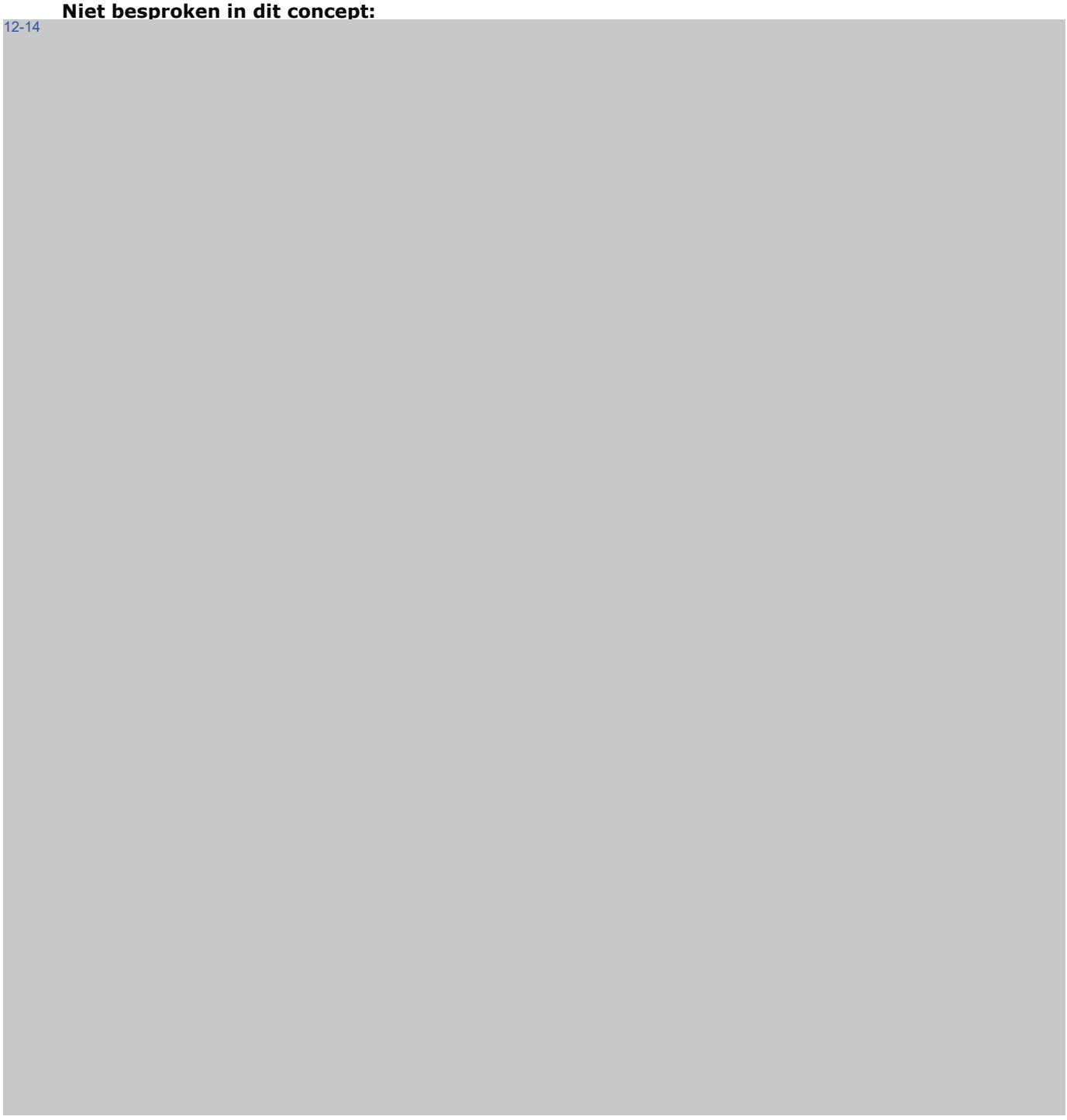
Artikel 42 Citeertitel
Dit besluit wordt aangehaald als: Besluit **onderzoek in** een geautomatiseerd werk.

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,

Niet besproken in dit concept:

12-14



12-14

POLITIE

Organisatieonderdeel Landelijke Eenheid
Dienst Landelijke Operationele Samenwerking
Keuringsdienst

Behandeld door 10.2.e /10.2.e
Functie
Telefoon 0343 10.2.e
E-mail 10.2.e @politie.nl
10.2.e @politie.nl
Datum 3 november 2016
Bijlage(n) 0
Pagina 1 van 4

Aan

mw. mr. 10.2.e
Ministerie van Veiligheid en Justitie
Directie Wetgeving en Juridische Zaken

Onderwerp **Eerste reactie op concept besluit CC3 (oktober 2016) van de Keuringsdienst**

Op verzoek van DWJZ hebben medewerkers van de Keuringsdienst (KD) van de Landelijke Eenheid Nationale Politie het concept Besluit onderzoek in een geautomatiseerd werk (BOGW) van oktober 2016 gelezen en een eerste en voorlopige beoordeling gedaan. Deze beoordeling met advies is, in tegenstelling tot die vanuit de politie-projectgroep CC3, gezien de taakstelling van de KD beperkt gebleven tot hun relevante werkveld en de hanteerbaarheid van de conceptregels tijdens een toekomstige keuring van de softwaretools. Derhalve is geconcentreerd op de artikelen 1 t/m 16. Men heeft getracht zich in te leven in de praktische gevolgen als de conceptregels van kracht zouden worden

Uitdrukkelijk dient bij voorbaat gesteld te worden dat verwacht wordt dat de beoordeling door of namens de CC3-projectgroep natuurlijk veel uitgebreider en dieper zal gaan, immers daar hebben ook alle procedurele beheer-, plaatsing/inzet- en opleidingseisen consequenties.

Onderstaand worden puntsgewijs kort, niet limitatief en in willekeurige volgorde de eerste opgekomen vraagpunten en commentaren van de Keuringsdienst opgesomd.

1. 12-14

2.

12-14

3.

4.

5.

6.

7.

POLITIE

8. 12-14

9.

10.

11.

12.

13.

POLITIE

12-14

Tabel: uitgangspunten bij onderzoek in geautomatiseerd werk

(basis is gesprek op 13 februari bij DLOS, Driebergen van 10.2.e, 10.2.e, 10.2.e, 10.2.e, 10.2.e t, 10.2.e en 10.2.e

Uitgangspunt	eisen	Uitleg en aandacht
1. Onderzoek in GW bestaat uit twee onderdelen: a. binnendringen en b. verrichten van specifieke onderzoekshandelingen	• AmvB stelt eisen aan onderdeel b. (de onderzoekshandelingen) • AmvB stelt geen eisen aan het binnendringen (= geen onderdeel van de delegatiegrondslag + binnendringen niet van invloed op kwaliteit bewijs) • Concept AmvB stelt eisen aan verwijderen • Binnendringen alleen met het oog op verrichten handelingen	• 7-12-14
2. Onderzoekshandelingen in een GW worden in beginsel uitgevoerd met een technisch hulpmiddel (software applicatie). Echter de handelingen kunnen ook handmatig worden uitgevoerd.	• AmvB vereist dat een technisch hulpmiddel (software applicatie) wordt gekeurd voor het wordt ingezet. Verder uitgewerkt in eisen over een protocol voor keuring, een aangewezen keuringsdienst, registratie van een keuring en een (grensoverschrijdende) wederzijdse erkenning van keuringen. • AmvB eist dat inhoud gegevens die worden vastgelegd identiek zijn aan de inhoud van gegevens in GW (betrouwbaarheid) • AmvB eist dat de gegevens worden geregistreerd naar datum en tijd. • AmvB eist dat de gegevens beveiligd zijn tegen manipulatie van buitenaf • AmvB stelt regels aan het transport vanuit de doel GW naar de politie technische infrastructuur en aan de beveiliging daarvan	•

	•	• •
3. Bevel Onderzoek in GW is limitatief	• AmvB eist dat werking van TH wordt beperkt tot de vermelde functionaliteiten • AmvB eist dat de plaatsing van een TH door het technisch team geschiedt	• •
4. Uitgangspunt van functiescheiding	• AmvB neemt als uitgangspunt dat het onderzoek in het GW alleen door leden van technisch team worden uitgevoerd.	•
5. Leden van het technisch team zijn specifiek kenbaar, zijn kundig en hebben voldoende kennis van het onderzoek in het GW; en zij werken volgens procedures	• AmvB definieert technisch team als team van de LE van de NP • AmvB eist dat de plaatsing van een TH door het technisch team geschiedt • AmvB eist dat er centrale registratie is van de toegang tot TH, en dat die toegang beperkt in tijd	• •

7-12-14

7-12-14

	in tijdsvolgordelijk proces.	is (synchroon met bevel). • AmvB eist dat vastlegging van door TH geregistreerde gegevens op een technische infrastructuur van politie plaatsvindt. • AmvB eist verder dat inhoud van technische infrastructuur niet wordt bewerkt, dat wordt vastgesteld dat gegevens van het ingezette Th komen (authenticiteit), dat datum en tijd worden vastgelegd. • AmvB eist dat de technisch infrastructuur alleen door door de KC als leden van technisch team aangewezen personen wordt gebruikt. • AmvB eist dat leden van technisch team als zodanig worden aangewezen door KC. • AmvB eist dat de leden van technisch team die onderzoek in GW doen opsporingsambtenaar zijn en hebben voldaan aan aangewezen kwalificaties • AmvB schept ruimte
6.	Eisen aan onderzoek in GW worden gesteld met het oog op de kwaliteit van het bewijs: de betrouwbaarheid, integriteit moet onomstotelijk zijn en controleerbaar	Zie de hiervoor genoemde eisen, vooral • AmvB eist dat inhoud gegevens die worden vastgelegd identiek zijn aan de inhoud van gegevens in GW (betrouwbaarheid) • AmvB eist dat de gegevens worden geregistreerd naar datum en tijd. • AmvB eist dat de gegevens beveiligd zijn tegen manipulatie van buitenaf • AmvB vereist dat een technisch hulpmiddel (software applicatie) wordt gekeurd voor het wordt ingezet.
7.	Van de handelingen bij het onderzoek aan het GW wordt registratie bijgehouden	• AmvB eist dat inhoud gegevens die worden vastgelegd identiek zijn aan de inhoud van gegevens in GW (betrouwbaarheid)

7-12-14

(logging)	• AmvB eist dat de gegevens worden geregistreerd naar datum en tijd. • AmvB stelt regels aan het transport vanuit de doel GW naar de politie technische infrastructuur en aan de beveiliging daarvan • AmvB eist dat er centrale registratie is van de toegang tot TH, en dat die toegang beperkt in tijd is (synchroon met bevel). • AmvB eist dat vastlegging van door TH geregistreerde gegevens op een technische infrastructuur van politie plaatsvindt. • AmvB eist verder dat inhoud van technische infrastructuur niet wordt bewerkt, dat wordt vastgesteld dat gegevens van het ingezette Th komen (authenticiteit), dat datum en tijd worden vastgelegd. •	
8. Zoveel mogelijk wordt na het onderzoek in het GW het TH verwijderd	• AmvB eist verwijdering van het TH na afronden onderzoek en, of, na afloop looptijd bevel. • AmvB eist verwijdering van het TH door lid technisch team. Er wordt pv opgemaakt. • AmvB eist dat als TH niet volledig kan worden verwijderd dat het transport van gegevens wordt beëindigd. Bij risico's meldt lid technisch team dat aan OvJ en stelt info ter beschikking voor volledige verwijdering.	•

		7-12-14

Tabel: werkproces op hoofdlijnen

processtap	elementen	aandacht
0. Projectvoorstel van tactisch team aan OVJ waarin heimelijk onderzoek GW	• 7-12-14 • •	• 7-12-14
1. Intake door technisch team	• • •	•
2. voorbereiding	• • • •	• • •

3. Uitvoeren onderzoek GW	• 7-12-14	•

		• 7-12-14
4. 7-12	• 7-12 •	•
5. Verwijderen TH	• AmvB eist verwijdering van het TH na afronden onderzoek en, of, na afloop looptijd bevel. • AmvB eist verwijdering van het TH door lid technisch team. Er wordt pv opgemaakt. • AmvB eist dat als TH niet volledig kan worden verwijderd dat het transport van gegevens wordt beëindigd. Bij risico's meldt lid technisch team dat	•

	aan OvJ en stelt info ter beschikking voor volledige verwijdering	• 7-12-14 [redacted] •

Afkortingen:

GW = geautomatiseerd werk

TH = technisch hulpmiddel

Definities / omschrijvingen activiteiten:

Onderzoek in GW = heimelijk binnendringen in een GW ter uitvoering van omschreven onderzoekshandelingen

Heimelijk binnendringen = op afstand toegang verkrijgen tot een GW, eventueel door 7-12-14 .

MO heimelijk binnendringen = verschillende (niet limitatief opgesomde) handelingen . technieken zijn behulpzaam voor binnendringen: 7-12-14

Credentials: authenticatiegegevens voor login (bijvoorbeeld: 7-12-14

Politie technische infrastructuur ; samenstel (van componenten) van geautomatiseerde werken waarop met 7-12-14

Op maandag 6 maart 2017 vond overleg plaats tussen het OM, MVenJ, de keuringsdienst, en politie. Naar aanleiding van dit overleg volgen hieronder enkele voorstellen. Deze voorstellen hebben betrekking op de uitvoering van een bevel zonder technisch hulpmiddel en de logging.

A. Uitvoeren bevel zonder (gekeurd) technisch hulpmiddel

De Memorie van Toelichting spreekt over "handmatig" onderzoek wanneer er geen technisch hulpmiddel wordt gebruikt. Indien het besluit die term overneemt, zal daarvoor een definitie vast moeten komen te staan. Handmatig kan zijn:

- 12-14
-
-

12-14

Voorstel:

Artikel -- onderzoek zonder gekeurd technisch hulpmiddel

12-14

B. Logging

Volgens de Nota van Toelichting vindt logging plaats vanaf het moment dat er onderzoekshandelingen plaatsvinden. Het binnendringen in een geautomatiseerd werk wordt volgens de Nota van Toelichting echter niet gelogd, nu die handelingen geen invloed hebben op de kwaliteit van het bewijs. 12-14

12-14

Artikel 28 Geautomatiseerde vastlegging

1. De gegevens over onderzoekshandelingen die ter uitvoering van een bevel worden verricht en het functioneren van de technische infrastructuur, worden doorlopend en automatisch vastgelegd *en toegevoegd aan de processtukken*.
2. *De gegevens over de overige handelingen die in een geautomatiseerd werk en ter uitvoering van een bevel worden verricht, worden doorlopend en automatisch vastgelegd.*
3. *De vastgelegde gegevens zoals bedoeld in het tweede lid, worden niet toegevoegd aan de processtukken indien de openbaarmaking van die gegevens een zwaarwegend opsporingsbelang schaadt.*

Van: 10.2.e
Verzonden: donderdag 13 april 2017 13:25
Aan: 10.2.e BD/DRC/CV'
CC: 10.2.e 10.2.e - BD/DGPOL/PBT/PT; 10.2.e
Onderwerp: RE: Verwachting input vragen CCIII
Opvolgingsmarkering: Opvolgen
Markeringsstatus: Gemarkeerd

Hallo 10.2.e

Dank je wel.

We gaan er hier intern mee aan de slag en ik kan je hopelijk woensdag/donderdag een eerste concept toesturen van onze antwoorden. Het lijkt zinvol om net als bij de beantwoording van de vragen aan de Tweede Kamer even een moment te plannen om gezamenlijk aan de antwoorden te werken. Wanneer zou dat goed bij jullie uitkomen? Dan probeer ik hier ook tijd vrij te maken.

Groet,

10.2.e

From: 10.2.e BD/DGPOL/PBT/PT
Sent: donderdag 13 april 2017 15:21:54
To: 10.2.e BD/DGPOL/PMP/HRMO; 10.2.e politie.nl'; 10.2.e @politie.nl
Cc: 10.2.e - BD/DGPOL/PMP/HRMO
Subject: RE: POR advies over opleiding CC3

Beste allen,

Gisteren spraken wij over de vraag op welke wijze de verantwoordelijkheid voor de bekwaamheid van de leden van het technisch team geregeld zou moeten worden in de AMvB CC3 en wat er vervolgens nodig is om daar uitvoering aan te geven. Hieronder geef ik kort aan wat de uitkomsten van ons gesprek zijn. Jullie opmerkingen zie ik graag – als het lukt nog deze week - tegemoet.

12-14

Groet,

10.2.e
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
T 0610.2.e
10.2.e **@minvenj.nll**
www.rijksoverheid.nl/venj

Van: 10.2.e BD/DGPOL/PBT/PT"
Verzonden op: woensdag 19 april 2017 09:08
Aan: 10.2.e BD/DGPOL/PMP/HRMO"10.2.e 10.2.e
CC: 10.2.e BD/DGPOL/PMP/HRMO"
Onderwerp: opleiding AmvB CC3 SPOED

Beste allen,

Graag hoor ik vandaag voor 15 uur of jullie kunnen instemmen met onderstaande weergave. Daarna informeer ik DW.

Groet
10.2.e

Van: 10.2.e @politie.nl]
Verzonden: woensdag 19 april 2017 9:48
Aan: 10.2.e BD/DGPOL/PBT/PT;10.2.e BD/DGPOL/PMP/HRMO; 10.2.e
CC: 10.2.e BD/DGPOL/PMP/HRMO
Onderwerp: Re: opleiding AmvB CC3 SPOED

Eens! Ik stuur straks nog iets voor het advies voor de por.

Groet

10.2.e
Verzonden van mijn Samsung

Van: 10.2.e DGPOL/PBT/PT 10.2.e @minvenj.nl]
Verzonden: woensdag 19 april 2017 17:03
Aan: 10.2.e @politie.nl>
Onderwerp: FW: opleiding AmvB CC3 SPOED

Ha 10.2.e

Jij en 10.2.e hebben eea voorbesproken, dus in de weergave hieronder van het gesprek over de opleiding van leden van het technisch team zullen geen verrassingen staan.

Met vriendelijke groet,

10.2.e
(senior) beleidsmedewerker
.....
Ministerie van Veiligheid en Justitie
Directoraat-Generaal Politie
9
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
T 06 10.2.e
10.2.e @minvenj.nll
www.rijksoverheid.nl/venj

Dubbel, zie doc. 618

Van: 10.2.e @politie.nl>
Datum: 19 april 2017 19:21:46 CEST
Aan: Plas, Theo van der (T.G.) 10.2.e @politie.nl>
Onderwerp: GRAAG SNEL REACTIE FW: opleiding AmvB CC3 SPOED

Hi Theo,

Dit is niet met mij afgestemd en ik vraag me af of jij inhoudelijk met alles akkoord bent? Is dit al met jou afgestemd in de gesprekken die jij hebt gevoerd.
Dit is nu dus nu al zo weg naar wetgeving als input voor de AMVB…..
Als er iets niet klopt is een snelle reactie nodig!

Groet,

10.2.e

Van: "Plas, Theo van der (T.G.)"
Verzonden op: woensdag 19 april 2017 19:38
Aan: 10.2.e
Onderwerp: Antw: GRAAG SNEL REACTIE FW: opleiding AmvB CC3 SPOED

Hi 10.2.e niet afgestemd en ik vrees ook niet met Marjolein.
Is de baseline niet dat jij alles ziet wat in het AmvB moet en dat dit met jou wordt besproken ? 9

Zal ik hem bellen morgen dat hij die lijn aanhoudt ? Marjolein nis met vakantie, maar kan het ook via 10.2.e laten lopen.

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
M (06) 10.2.e
E-mail: 10.2.e @politie.nl

Van: 10.2.e
Datum: 19 april 2017 22:15:44 CEST
Aan: Plas, Theo van der (T.G.) 10.2.e @politie.nl>, Plas, Theo van der (T.G.) 10.2.e @politie.nl>
Onderwerp: Antw: GRAAG SNEL REACTIE FW: opleiding AmvB CC3 SPOED

De vraag stellen is het antwoord geven?

De baseline is al sinds start NP dat alles wat met VenJ wordt afgestemd in afstemming met mij/staf moet, zodat ik jou, Jannine, Peije en KL in positie kan houden en kan zorgen dat er is afgestemd voordat dingen weggaan. Niet alleen 9 maar ook 10.2.e weer dat echt hoor.

From: 10.2.e politie.nl>
Sent: woensdag 19 april 2017 22:28:34
To: 10.2.e BD/DGPOL/PBT/PT
Subject: Re: opleiding AmvB CC3 SPOED

Nee 10.2.e Is niet afgestemd. Wil je svp niet meer rechtstreeks communiceren maar via mij?

Van: Plas, Theo van der (T.G.)
Verzonden: woensdag 19 april 2017 22:30
Aan: 10.2.e
Onderwerp: Antw: GRAAG SNEL REACTIE FW: opleiding AmvB CC3 SPOED

Helder,zal ik inzetten,en met Marjolein9 afspreken om toezicht op te houden. Ik begin bij 10.2.e ,

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
M (06)10.2.e
E-mail:10.2.e @politie.nl

Van: 10.2.e - BD/DGPOL/PBT/PT10.2.e @minvenj.nl>
Verzonden: donderdag 20 april 2017 09:12
Aan: 10.2.e
Onderwerp: RE: opleiding AmvB CC3 SPOED

Je kon er vorige week niet bij zijn 10.2.e en je gaf aan dat het gesprek dan maar zonder jou moest plaatsvinden. Je zou het overleg voorbespreken met 10.2.e .i ik heb 10.2.e nog gevraagd of deze lijn is afgestemd intern politie en de goedkeuring heeft van de KL. Dat werd door hem bevestigd. Ik neem jou nu mee in de uitkomsten. Wat gaat er dan mis in jouw optiek?

From: Plas, Theo van der (T.G.) 10.2.e @politie.nl>
Sent: donderdag 20 april 2017 11:40:21
To: 10.2.e - BD/DRC
Subject: Samenwerking Wetgeving CCIII

Beste 10.2.e

Graag zou ik even met je willen overleggen -dat kan telefonisch -over de voortgang van de wetgeving/AmvB rond CC III. Die gaat zo stroef dat er volgens mij iets anders nodig is dan het huidige ambtelijk overleg. Van DGRR is 10.2.e hierbij betrokken, van ons uit 10.2.e

12-14

Ik hoor graag wanneer het je schikt,

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
M (06) 10.2.e
E-mail: 10.2.e @politie.nl

Van: 10.2.e - BD/DRC 10.2.e @minvenj.nl>
Datum: 25 april 2017 09:24:39 CEST
Aan: Plas, Theo van der (T.G.) 10.2.e @politie.nl>
CC: 10.2.e - BD/DWJZ/SSR 10.2.e @minvenj.nl>, 10.2.e BD/DRC/CV 10.2.e @minvenj.nl>, 10.2.e @minvenj.nl>
Onderwerp: RE: Samenwerking Wetgeving CCIII

Theo,

Excuus voor de wat langere dan je van me gewend bent reactietijd. Ik wilde me even laten bijpraten op het dossier. Ik vind het prima om eea met je te bespreken. Dat kan telefonisch. Dat kan ook in persoon. In beide gevallen vind ik het wel dienstig als 'mijn' 10.2.e en 10.2.e van Wetgeving aan het gesprek deelnemen. Het beeld bij ons is 12-14

De amvb is inmiddels ook klaar voor verzending. Zal ik voor volgende week een telefonische afspraak ('op de speaker') laten maken? (Ik ben deze week even in Europa aan de slag.)

Met vriendelijke groet,

10.2.e
Sent with Good (www.good.com)

Van: Plas, Theo van der (T.G.)
Verzonden: dinsdag 25 april 2017 13:12
Aan: 10.2.e
Onderwerp: Doorst: Samenwerking Wetgeving CCIII

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
M (06)10.2.e
E-mail:10.2.e @politie.nl

Van: 10.2.e
Verzonden: dinsdag 25 april 2017 15:15
Aan: 10.2.e
CC: Plas, Theo van der (T.G.); 10.2.e
Onderwerp: BOO Hoofdlijnennotitie

Hoi 10.2.e

Vanochtend met Theo en Marjolein afgesproken dat we de hoofdlijnennotitie CCIII willen gaan agenderen ter besluitvorming in het volgende BOO. Theo dacht dat dit op 12 mei is?

Kun jij helpen met het agenderen? En als ik met niet vergis moet er ook een oplegger bij. Heb jij een format voor mij zodat ik met de oplegger kan beginnen? Ik kan zelf ook even met de secretaris van het BOO contact opnemen, maar ben even haar gegevens kwijt.

De laatste versie van de notitie komt ook jouw kant op zodra ik de reactie van 10.2.e en 10.2.e heb verwerkt (mochten zijn nog opmerkingen hebben).

Groet en dank!
10.2.e

Van: 10.2.e
Verzonden op: dinsdag 2 mei 2017 11:57
Aan: "Secretaris.BOO"
CC: "Plas, Theo van der (T.G.)" 10.2.e 10.2.e 10.2.e)" ," 10.2.e 10.2.e
Onderwerp: Hoofdlijnennotitie CCIII tbv BOO 12 mei

Beste 10.2.e

Bijgaand tref je aan de laatste versie van de hoofdlijnennotitie CCIII (incl. oplegnotitie) ter bespreking in het BOO op 12 mei. Deze versie is voorbesproken met 10.2.e en 10.2.e

Theo en ik schuiven graag aan om eventuele vragen en opmerkingen te kunnen beantwoorden.

Kun je nog laten weten wanneer wij verwacht worden?

Met vriendelijke groet,

10.2.e
10.2.e
9
Politie | Project CCIII
Hoofdstraat 54, 3972 LB Driebergen-Rijsenburg
Postbus 100, 3970 AC Driebergen-Rijsenburg

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 , 06-10.2.e

☑ **Opinievormend** ☑ **Ter implementatie** ☐ **Ter kennisname**

Gevraagd

Het BOO wordt gevraagd:
Kennis te nemen van:
- Deze 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 7-12 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.

Een keuze te maken tussen onderstaande scenario’s:
1. De Landelijke Eenheid wer7-12 2 voor de centrale voorziening. Vanuit de eenheden wordt daarnaast formatieruimte ter grootte v7-12 2 afgeroomd ten behoeve van de Landelijk Eenheid. Hiermee wordt, gezamenlijk met de partners, een voorziening 7-12 7-12 gecreëerd. Hierdoor komt de opgedane kennis en ervaring uiteindelijk niet terug naar de Eenheden, maar blijft centraal beschikbaar voor de politie.
2. De Landelijke Eenheid wer7-12 2 voor de centrale voorziening. Vanuit de Eenheden wordt daarnaast in tota7-12 2 door een gekwalificeerde medewerker tewerkgesteld bij de voorziening. Hiermee wordt, gezamenlijk met de partners, een voorziening 7-12 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.

Op basis van bovenstaande keuze te besluiten 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 te starten, waarbij medewerkers van de eenheden mee kunnen solliciteren.

Voortraject		
Gremium	Datum	uitkomst/bijzonderheden bespreking (uit verslagen overnemen)
☐ KLO		
☐ MT Staf KL		
☑ Overleg Operatiën	17-02-17	Aan de hand van de presentatie van de Theo van der Plas is besloten om de hoofdlijnennotitie verder uit werken met 10.2.e 10.2.e en 10.2.e voordat deze ter besluitvorming in zal worden gebracht.
☐ Bedrijfsvoeringsoverleg		
☑ Nationale Briefing Veiligheid	21-12-16	Opdracht aan PC LE om een hoofdlijnennotitie CCIII op te stellen waarin wordt beschreven hoe de politie over zal gaan tot implementatie van de wet CCIII en deze januari/februari in het KMT te brengen.
☐ Projectmanagers		
☐ Extern <invullen wie>		
☑ Met: Hoofd DLOS	25-04-17	Akkoord met hoofdlijnennotitie

Samenvatting notitie/voorstel

Doel, aanleiding en context
Op 21 december 2016 heeft de portefeuillehouder Digitalisering en Cybercrime (D&C) in de Nationale Briefing een presentatie gegeven over het wetsvoorstel CCIII en wat dit betekent voor de Nederlandse Politie. De Korpschef heeft verzocht om een hoofdlijnennotitie op te stellen waarin wordt beschreven hoe de politie over zal gaan tot implementatie van deze wet in de politieorganisatie. Met deze notitie wordt hieraan invulling gegeven. De wet CCIII is op 20 december 2016 door de Tweede Kamer aangenomen en zal naar verwachting na goedkeuring door de Eerste Kamer per 1 januari 2018 in werking treden. Op 20 juni 2017 is een hoorzitting met deskundigen gepland in de Eerste Kamer (gezamenlijk met het wetsvoorstel ANPR 28 dagen opslag) om over dit onderwerp met de Eerste Kamer in discussie te gaan. Daarop vooruitlopend zal door de Staatssecretaris halverwege mei 2017 het antwoord op het voorlopig verslag van de Eerste Kamer naar de Eerste Kamer worden gestuurd.

Beoogd resultaat
Kennis te nemen van de voorgestelde ontwikkelrichting voor de implementatie van de nieuwe bevoegdheden uit de wet CCIII en akkoord te gaan met de start van de centrale werving, waarbij Eenheden (incl. DLOS) gevraagd wordt om vacatureruimte ter beschikking te stellen voor 2 jaar en/of mogelijk gekwalificeerde mensen ter beschikking te stellen ten behoeve van de experimenteerfase (fase 1) en implementatiefase (fase 2). Na akkoord van het BOO deze notitie door te geleiden naar het KMTO (evt. nog door tussenkomst van het BBVO).

Samenvatting inhoud
In deze notitie wordt op hoofdlijnen aangegeven welke stappen er door het project CCIII zijn ondernomen om te komen tot een werkende voorziening voor alle opsporingsinstanties (incl. FIOD en KMAR) voor het heimelijk op afstand kunnen binnendringen in een geautomatiseerd werk. Deze ontwikkeling is ingedeeld in een aantal fases. De huidige fases (0 en 1) hebben betrekking op het creëren van een lab omgeving bij 7-12 om te kunnen experimenteren met de nieuwe bevoegdheid en de eerste voorbereidingen te treffen voor fase 2, waarin de implementatie- en realisatiefase van start gaat.

Aangegeven wordt dat het noodzakelijk is om te investeren in techniek, huisvesting, middelen, mensen, security, formatie en de Keuringsdienst. Het inrichten van een dergelijke voorziening is erg complex en gaat potentieel hoge kosten met zich mee brengen. Het is van groot belang om dit gezamenlijk als politie op te pakken om zodoende goed voorbereid te zijn op het moment van inwerkingtreding van de wet.

Tot slot wordt kort stilgestaan bij wat het wetsvoorstel inhoudt (met name de nieuwe bevoegdheid tot binnendringen) en welke eisen en waarborgen worden gesteld aan de invoering hiervan.

Argumenten en kanttekeningen

Risico's voor de implementatie zijn de volgende:
- Eerste Kamer gaat niet akkoord gaat met het wetsvoorstel.
- Onderschatting van complexiteit van de materie
- Doorlooptijden van de aanvraag van middelen en techniek (inclusief heimelijke inkoop
- Tijdige keuring van de te gebruiken middelen
- Onvoldoende gekwalificeerd (en uitgerust) personeel
- Implementatie zien als een ICT-project

Het externe risico van het niet akkoord gaan door de Eerste Kamer betekent niet dat de ontwikkeling zoals die binnen het lab CCIII is ingezet moet worden stilgezet. 12-14

Consequenties (afgestemd met relevante betrokkenen)

☑ Personeel/ HRM	Werving in- en extern van medewerkers voor voorziening tot binnendringen. Nog niet afgestemd met HRM
☑ Financieel:	Inrichting van deze voorziening is duur. Verder uitwerken ism directie FM wat precieze consequenties gaan zijn.
☑ Informatievoorziening:	Aanschaf van middelen dient nog verder afgestemd te worden met IV. Overleg hierover vindt reeds plaats.
☑ Facility Management:	Specifieke hoogbeveiligde huisvestigin is noodzakelijk. Overleg vindt plaats met FM over mogelijkheden.
☐ Communicatie:	
☐ Juridisch:	
☐ Politiek-bestuurlijk:	
☑ Operatie:	Afgestemd met Hoofden Operatien
☐ Realisatie NP:	< samenhang c.q. invloed op realisatie NP >
☐ Personele reorganisatie:	< samenhang c.q. invloed op personele reorganisatie >
☐ Administratieve lasten:	< invloed op administratieve lasten >
☐ met…..	

Vervolgtraject

Overleg		Overleg	
☐ KMTO	x ter besluitvorming/instemming ☐ ter opinievorming ☐ ter kennisgeving	☐ COR (WOR)	☐ ter informatie ☐ voor instemming ☐ voor advies
☐ MT Staf KL	☐ ter bespreking/opinievorming ☐ ter integrale toetsing/impactanalyse ☐ ter implementatie ☐ ter kennisgeving	☐ Vakbonden	☐ formeel, via CGOP ☐ informeel via overleg KL-vakbonden
☐ KLO	☐ ter besluitvorming/instemming ☐ ter opinievorming ☐ ter kennisgeving	☐ Programma-raad	☐ ter bespreking/opinievorming ☐ ter kennisgeving
☐ Overleg met DG Pol	☐ ter besluitvorming ☐ ter bespreking/opinievorming ☐ ter kennisgeving	☐ Directie	☐ ter bespreking/opinievorming ☐ ter implementatie ☐ ter kennisgeving
☐ Projectmana-gersoverleg	☐ ter bespreking/opinievorming ☐ ter implementatie ☐ ter kennisgeving	☐ met….	☑ ter bespreking/opinievorming ☐ ter kennisgeving ☐ ....

Communicatie

Verantwoordelijke:	
☐ Strategische boodschap:	

Uitvoering / implementatie / monitoring

x Verantwoordelijk:	Pfh Digitalisering en Cybercrime J. van den Berg
☐ Voortgangsrapportage:	1 juli wordt een realisatieplan aan het KMT aangeboden ter besluitvorming

Documenten

Titel (hoofd)document en bijlagen

< opsomming documenten die worden voorgelegd, incl. bijlagen >

- Hoofdlijnennotitie CCIII BOO

Hoofdlijnennotitie voorziening tot binnendringen

Hoofdlijnen voor de inrichting

10.2.e

Concept

Versie 0.5

Versie datum 28 april 2017

Rubricering Politie Vertrouwelijk

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Gemarkeerde wijzigingen
0.1	15-02-17	Eerste versie	
0.2	06-03-17	Opmerkingen verwerkt 10.2.e , 10.2.e en Theo van der Plas	
0.3	13-03-17	Opmerkingen verwerkt Theo van der Plas, 10.2.e , Marjolein Smit	
0.4	20-04-17	Opmerkingen verwerkt Theo van der Plas, 10.2.e , 10.2.e en Marjolein Smit	
0.5	28-04-17	Opmerkingen verwerkt 10.2.e en 10.2.e en kleine redactionele wijzigingen	

Distributie

Versie	Verzend datum	Naam	Afdeling / Functie
0.1	15-02-17	Theo van der Plas, Marjolein Smit, 10.2.e 10.2.e	Portefeuillehouder D&C, leiding DLOS, Leiding Programma CCIII
0.2	06-03-17	Theo van der Plas, 10.2.e , 10.2.e Marjolein Smit, 10.2.e	Portefeuillehouder D&C, BOO-leden, leiding DLOS, leiding programma CCIII
0.3	13-03-17	Theo van der Plas, 10.2.e , 10.2.e , Marjolein Smit, 10.2.e	Portefeuillehouder D&C, BOO-leden, leiding DLOS, leiding programma CCIII
0.4	20-04-17	Theo van der Plas, Willem Woelders, 10.2.e , 10.2.e , Marjolein Smit,10.2.e	Programmadirecteur D&C, Portefeuillehouder D&C, BOO-leden, leiding DLOS, leiding programma CCIII
0.5	28-04-17	Theo van der Plas, Willem Woelders, 10.2.e , 10.2.e Marjolein Smit, 10.2.e , 10.2.e	Programmadirecteur D&C, Portefeuillehouder D&C, BOO-leden, leiding DLOS, leiding programma CCIII, Directie Operatien
0.5	02-05-17	Leden van het BOO	BOO

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

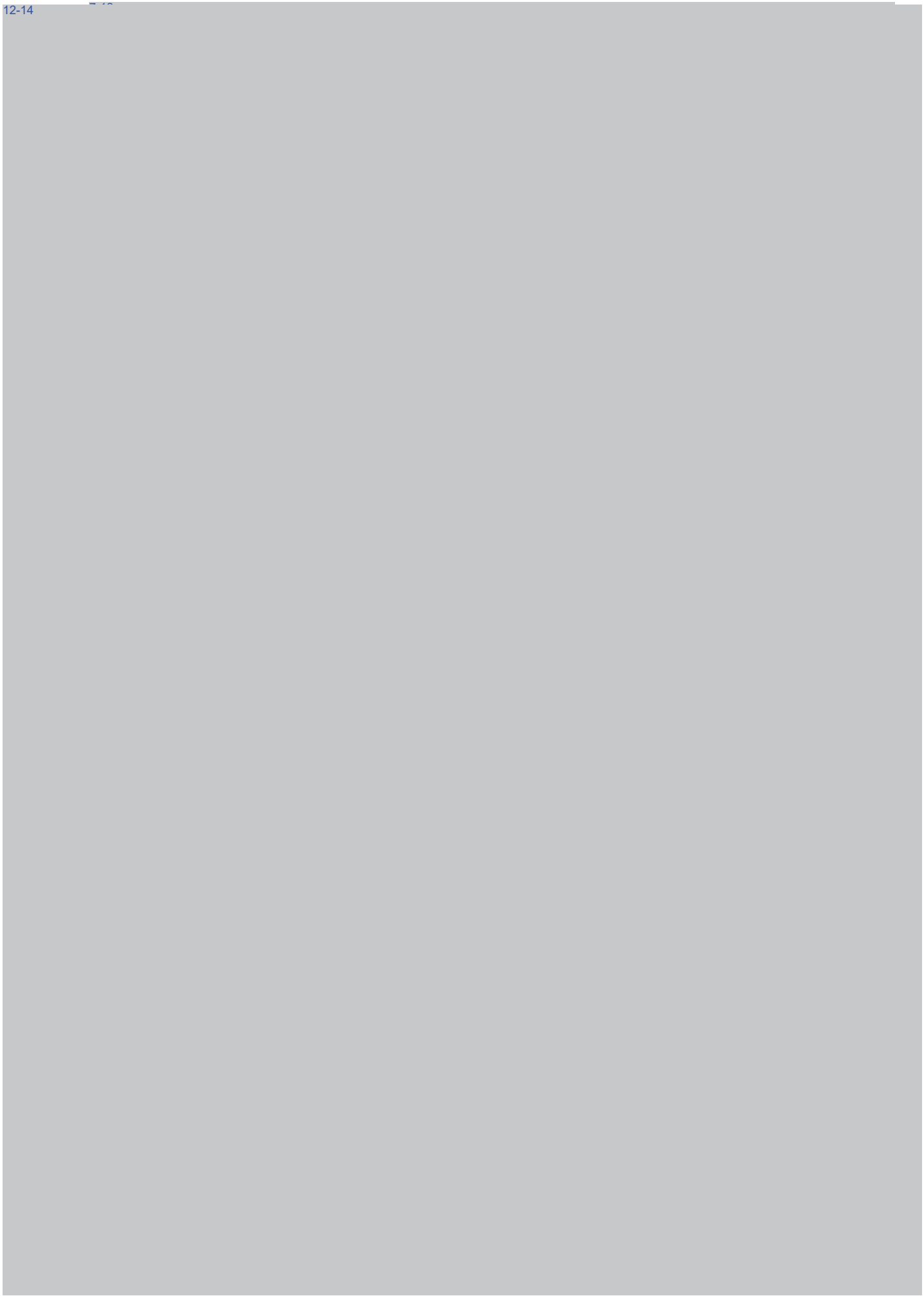
12-14

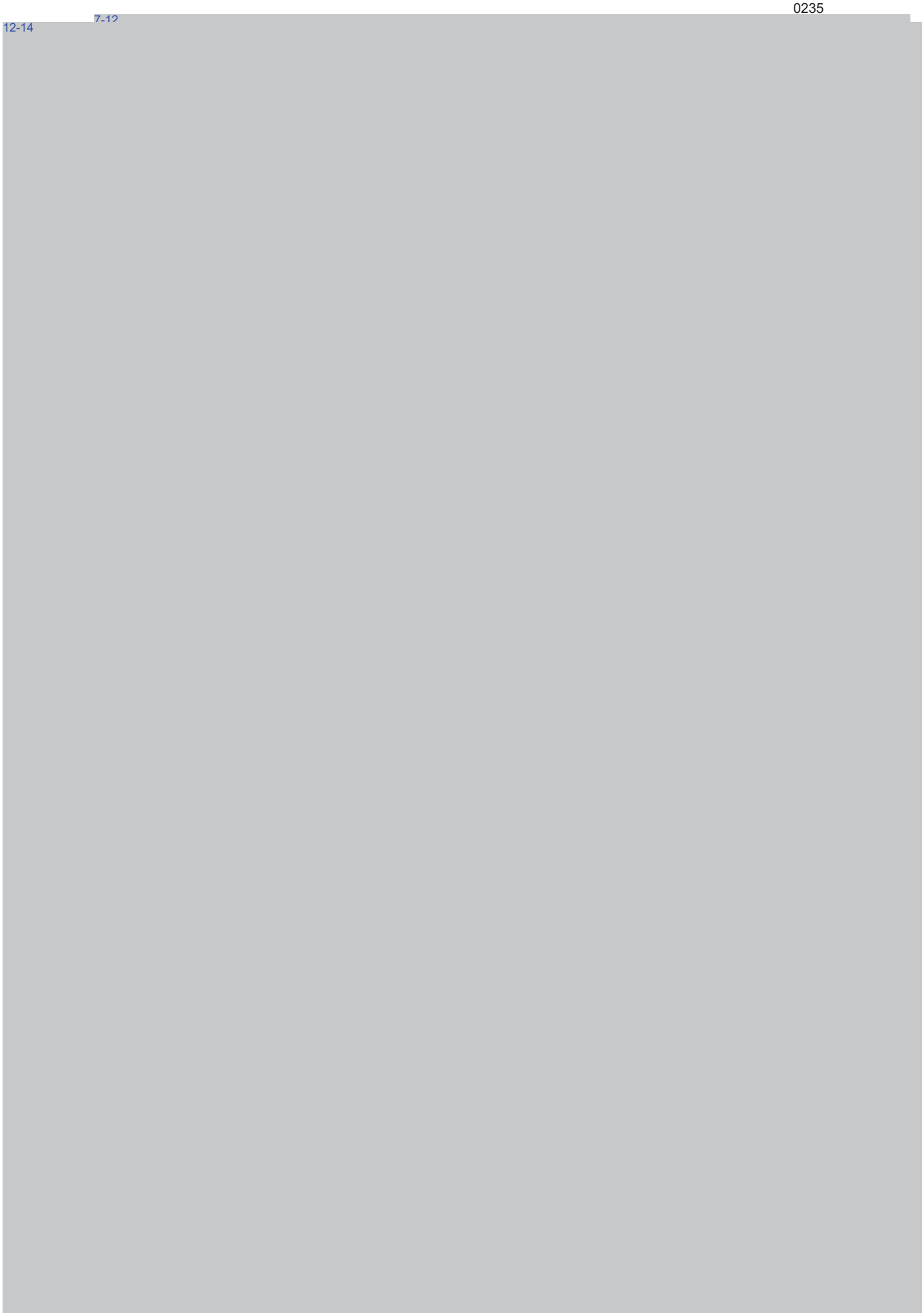
12-14

12-14

12-14

12-14

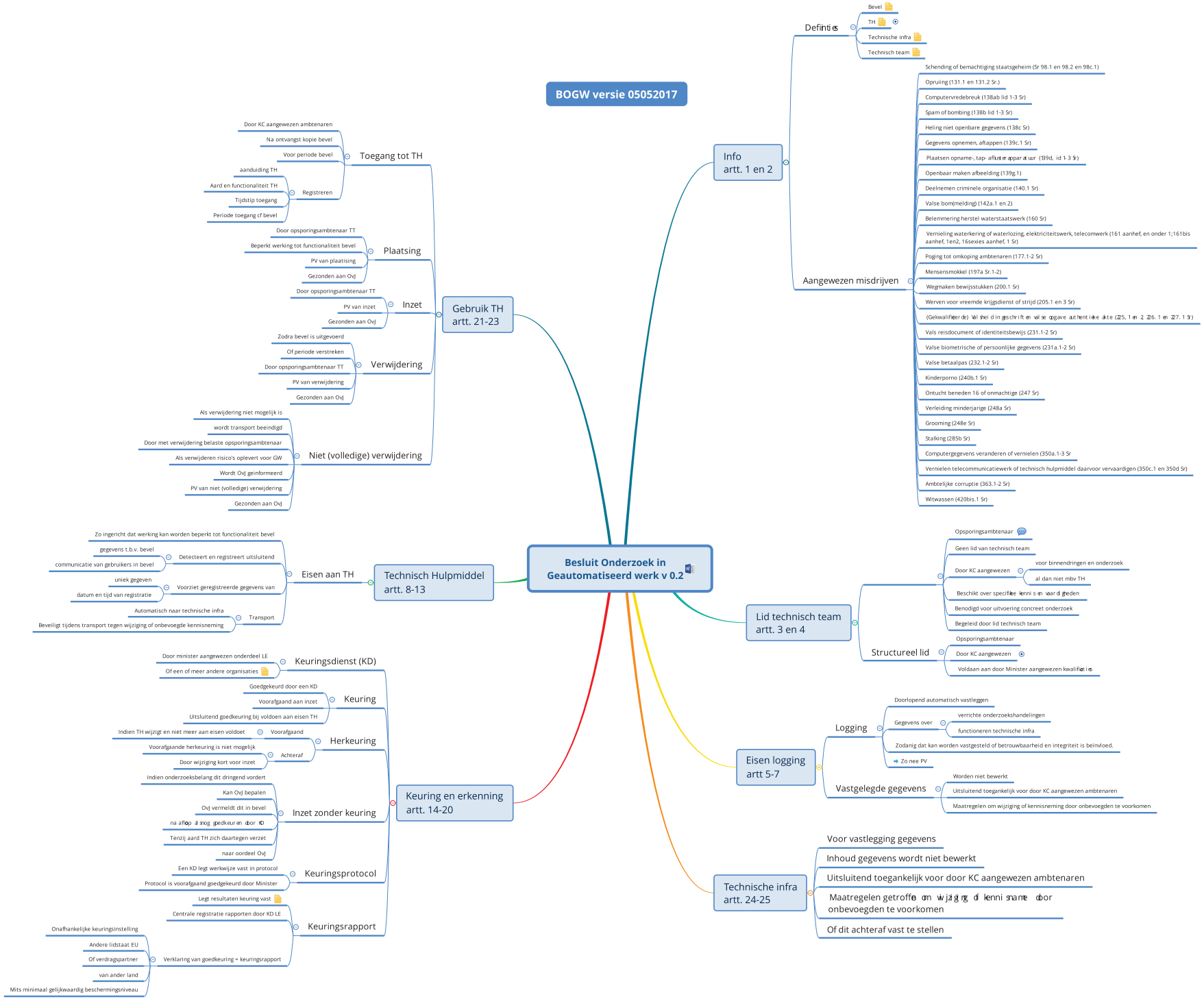



7-12
12-14

12-14

12-14

12-14


BOGW versie 05052017
Besluit Onderzoek in Geautomatiseerd werk v 0.2
Info artt. 1 en 2
Definities
Bevel
TH
Technische infra
Technisch team
Aangewezen misdrijven
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)
Gegevens opnemen, aftappen (139c.1 Sr)
Plaatsen opname-, tap- aflusteraparatuur (139d, id 1-3 Sr)
Openbaar maken afbeelding (139g.1)
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 geschriften 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)
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)
Gebruik TH artt. 21-23
Toegang tot TH
Door KC aangewezen ambtenaren
Na ontvangst kopie bevel
Voor periode bevel
Registreren
aanduiding TH
Aard en functionaliteit TH
Tijdstip toegang
Periode toegang cf bevel
Plaatsing
Door opsporingsambtenaar TT
Beperkt werking tot functionaliteit bevel
PV van plaatsing
Gezonden aan Ovj
Inzet
Door opsporingsambtenaar TT
PV van inzet
Gezonden aan Ovj
Verwijdering
Zodra bevel is uitgevoerd
Of periode verstreken
Door opsporingsambtenaar TT
PV van verwijdering
Gezonden aan Ovj
Niet (volledige) verwijdering
Als verwijdering niet mogelijk is
wordt transport beeindigd
Door met verwijdering belaste opsporingsambtenaar
Als verwijderen risico's oplevert voor GW
Wordt Ovj geinformeerd
PV van niet (volledige) verwijdering
Gezonden aan Ovj
Technisch Hulpmiddel artt. 8-13
Eisen aan TH
Detecteert en registreert uitsluitend
gegevens t.b.v. bevel
communicatie van gebruikers in bevel
Voorziet geregistreerde gegevens van
uniek gegeven
datum en tijd van registratie
Transport
Automatisch naar technische infra
Beveiligt tijdens transport tegen wijziging of onbevoegde kennisneming
Zo ingericht dat werking kan worden beperkt tot functionaliteit bevel
Keuring en erkenning artt. 14-20
Keuringsdienst (KD)
Door minister aangewezen onderdeel LE
Of een of meer andere organisaties
Keuring
Goedgekeurd door een KD
Voorafgaand aan inzet
Uitsluitend goedkeuring bij voldoen aan eisen TH
Herkeuring
Vooraf gaand
Indien TH wijzigt en niet meer aan eisen voldoet
Achteraf
Door wijziging kort voor inzet
Voorafgaande herkeuring is niet mogelijk
Inzet zonder keuring
Indien onderzoeksbelang dit dringend vordert
Kan Ovj bepalen
Ovj vermeldt dit in bevel
na afloop alsnog goedkeuren door KD
Tenzij aard TH zich daartegen verzet
naar oordeel Ovj
Keuringsprotocol
Een KD legt werkwijze vast in protocol
Protocol is voorafgaand goedgekeurd door Minister
Keuringsrapport
Legt resultaten keuring vast
Centrale registratie rapporten door KD LE
Verklaring van goedkeuring = keuringsrapport
Onafhankelijke keuringsinstelling
Andere lidstaat EU
Of verdragspartner
van ander land
Mits minimaal gelijkwaardig beschermingsniveau
Lid technisch team artt. 3 en 4
Opsporingsambtenaar
Geen lid van technisch team
Door KC aangewezen
voor binnendringen en onderzoek
al dan niet mbv TH
Beschikt over specifieke kennis en vaardigheden
Benodigd voor uitvoering concreet onderzoek
Begeleid door lid technisch team
Structureel lid
Opsporingsambtenaar
Door KC aangewezen
Voldaan aan door Minister aangewezen kwalificaties
Eisen logging artt 5-7
Logging
Doorlopend automatisch vastleggen
Gegevens over
verrichte onderzoekshandelingen
functioneren technische infra
Zodanig dat kan worden vastgesteld of betrouwbaarheid en integriteit is beïnvloed.
Zo nee PV
Vastgelegde gegevens
Worden niet bewerkt
Uitsluitend toegankelijk voor door KC aangewezen ambtenaren
Maatregelen om wijziging of kennisneming door onbevoegden te voorkomen
Technische infra artt. 24-25
Voor vastlegging gegevens
Inhoud gegevens wordt niet bewerkt
Uitsluitend toegankelijk voor door KC aangewezen ambtenaren
Maatregelen getroffen om wijziging of kennisname door onbevoegden te voorkomen
Of dit achteraf vast te stellen

Memorie van antwoord inzake het voorstel tot 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)

Conceptversie 05-05-2017

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 het wetsvoorstel computercriminaliteit III (34 372). 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. In recente rapporten onderschrijven de notie van politie en justitie dat de dreiging groeit en er behoefte is aan meer bevoegdheden voor de opsporing om deze 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, de commissie Verhagen, het Cybersecuritybeeld Nederland dat jaarlijks wordt gepubliceerd , de veiligheidsmonitor , en [het Nationaal dreigingsbeeld? **P.M.**]. Voor de dreiging op Europees niveau kan worden gewezen op The Internet Organised Crime Threat Assessment (IOCTA) , alsook het Serious and Organised Crime Threat Assessment (SOCTA) . In veel rapporten zijn overeenkomsten te herkennen, onder andere wordt gesteld dat de dreiging groeit en er behoefte is aan meer bevoegdheden voor de opsporing om deze dreiging te adresseren. Het kabinet 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 hiervoor een voorwaarde. Dit wetsvoorstel is van essentieel belang voor de handhaving van de rechtsstaat in cyberspace. 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 een wetsvoorstel. Zij hebben gevraagd of de regering kan toelichten waarom zij beide terreinen in een wetsvoorstel heeft willen vatten.

De regering deelt de opvatting van de leden van de fractie van de SP, dat in dit wetsvoorstel twee totaal verschillende problemen zijn vervat, bepaald niet. De gedachte dat computercriminaliteit uitsluitend betrekking heeft op het handelen in de digitale dimensie, en daarmee ook vanuit juridisch perspectief strikt kan worden gescheiden van het handelen in de fysieke wereld, is achterhaald. Beide dimensies lopen in elkaar over en werken op elkaar in. 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 ICT meer mogelijkheden om het handelen af te schermen van de buitenwacht, zoals het gebruik van encryptie. Tenslotte zijn de strafbaarstellingen niet meer voldoende toegesneden op de technologische ontwikkeling, daarvoor kan worden gewezen op een delict als het overnemen en helen van vertrouwelijke gegevens. Deze verschillende aspecten hebben een gezamenlijk kenmerk, namelijk dat deze onderdeel vormen van de computercriminaliteit. Beide dimensies lopen in elkaar over en werken op elkaar in. 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 echter 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 slachtoffers te zoeken, 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 en niet op een strategische keuze. De bevoegdheden van de politie en justitie hebben geen gelijke tred gehouden met de ontwikkeling van de computercriminaliteit en daarom dienen deze bevoegdheden te worden aangepast. De suggestie van de fractie van de SP, dat een aantal dringende maatschappelijke problemen zijn meegenomen zodat discutabele onderdelen eerder geaccepteerd worden, is dan ook niet terecht. De regering acht alle onderdelen van het wetsvoorstel voor essentieel belang voor de bestrijding van computercriminaliteit, anders waren deze onderdelen ook niet in het wetsvoorstel opgenomen, en hoopt daarbij ook de SP-fractie aan haar zijde te vinden.

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 de 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, 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. In de Grondwet en diverse mensenrechtenverdragen wordt het huisrecht beschermd. De woning is bij uitstek een plaats waar dit recht bescherming geniet.

De noodzaak van deze drastische 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 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. 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. Bovengenoemde technologische vooruitgang belemmert de inzet van traditionele opsporingsbevoegdheden, zoals het aftappen van telecommunicatie, 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 fracties van GroenLinks, nader ingegaan op de noodzaak en de bruikbaarheid van bestaande bevoegdheden in.

Naast de toelichting op de urgentie in de memorie van toelichting (§ 2.1), de nota naar aanleiding van het verslag (blz. 1/2 en § 2.1, i.h.b. blz. 18/19) en tijdens de mondelinge behandeling in de Tweede Kamer verwijs ik voor een schets van de omvang van computercriminaliteit tevens naar de rapporten waarin in de inleiding naar is verwezen. 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, nr. 6, blz. 15/16).

3. Proportionaliteit en privacy

De leden van de VVD-fractie 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 te aanzien van het recht op bescherming van de persoonlijke levenssfeer.

In paragraaf 2.9 van de memorie van toelichting is uitgebreid ingegaan op de bescherming van grondrechten en het recht op eerbiediging van de persoonlijke levenssfeer. In dit verband is artikel 8 van het Europees Verdrag tot bescherming van Rechten van de Mens en de fundamentele vrijheden (EVRM) van bijzonder belang. In paragraaf 2.9 van de nota naar aanleiding van het verslag is nader ingegaan op de recente jurisprudentie van het EHRM rond het heimelijk vergaren van persoonsgegevens ten behoeve van de opsporing en vervolging van strafbare feiten. Dit 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 Szabo en Vissy tegen Hongarije (zaak 37138/14). Voorop gesteld 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 in een formele 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 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. 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. 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 onderzoek. 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. 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. Er is voorzien in de nodige waarborgen voor een zorgvuldige uitvoering. 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 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 ze gebruiken, kan de waarde van onafhankelijk toezicht volgens het EHRM niet overschat worden (Szabo en Vissy tegen Hongarije, § 79). 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 gebruik voor het heimelijk binnentreden. Alle onderzoekshandelingen zullen kunnen worden verantwoord op basis van logging, zodat 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 de Besluit onderzoek in een geautomatiseerd werk. Op de uitvoering van het onderzoek in een geautomatiseerd werk door de opsporingsambtenaren wordt, aanvullend op de rechterlijke controle, systeemtoezicht uitgeoefend door de Inspectie Veiligheid en Justitie. Dit komt verderop, in paragraaf 8, nader aan de orde. Tenslotte is voorzien in een verplichting tot notificatie van de betrokkene, hiervoor is aangesloten bij de bestaande regeling voor de notificatie van bijzondere opsporingsbevoegdheden (art. 126bb Sv). Het EHRM acht het van groot belang dat de betrokkene achteraf op de hoogte kan komen van de geheime surveillance en genoegdoening 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 VVD-fractie 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 bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten. Deze doelen betreffen de uitoefening van reeds bestaande bevoegdheden. Het heimelijk binnendringen in 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 II 2016/17, 34 588) 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 (onderzoek in een geautomatiseerd werk). Het wetsvoorstel inlichtingen- en veiligheidsdiensten 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 staatsveiligheid beter kunnen uitvoeren. Dit betreft algemene bevoegdheden inzake de verzameling van gegevens, zoals het stelselmatig verzamelen van gegevens over personen uit open bronnen en de raadpleging van informanten, 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 en de onderzoeksopdrachtgerichte interceptie van communicatie.

Voor 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 de 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 taken van de betreffende overheidsorganen, de toepasselijkheid van de Europese 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 EU-verdrag. 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 (art. 8 Wiv 20xx). De Europese Unie is niet bevoegd op het gebied van de nationale veiligheid. In het wetsvoorstel inlichtingen- en veiligheidsdiensten 20xx is een specifieke paragraaf opgenomen over de verstrekking van persoonsgegevens (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 anderzijds. 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 verrichten van het zogenoemde systeemtoezicht. 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 als een rechter zich niet heeft uitgelaten over een gedraging die een strafvorderlijk aspect kent (art. 9:22 en 9:23 Awb). Tenslotte kan het parlement een rol vervullen. De inzet van de bevoegdheden van de inlichtingen- en veiligheidsdiensten vindt plaats onder verantwoordelijkheid van Onze Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie. De rechtmatigheid van de uitvoering van een bevoegdheid waarvoor Onze Minister toestemming heeft verleend wordt vooraf getoetst door een onafhankelijke commissie, de Toetsingscommissie inzet bevoegdheden (TIB). De CTIVD is belast met het toezicht op de rechtmatigheid van de uitoefening van de bevoegdheden door de inlichtingen- en veiligheidsdiensten. Het parlement kan openbare of besloten controle uitvoeren, onder meer in de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD) van de Tweede Kamer.

Hieronder wordt, naar aanleiding van vragen van de leden van de fracties van D66, de SP en de ChristenUnie, nader ingegaan op het toezicht op de toepassing van de bevoegdheid van het onderzoek in een geautomatiseerd werk, mede in verhouding tot het toezicht op de inzet van bevoegdheden door de Inlichtingen- en veiligheidsdiensten.

De leden van de CDA-fractie 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 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 Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (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 van communicatie of de stelselmatige observatie. Naar aanleiding van het advies van de Afdeling advisering is 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. Er zijn bepaalde ernstige strafbare feiten waarop een vrijheidsstraf van minder dan 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 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 doorzoeken van de gegevens in het geautomatiseerde werk, teneinde deze vast te leggen of ontoegankelijk te maken, is essentieel voor het opsporen van dergelijke delicten. Dit betreft misdrijven als het gebruik van een botnet (artikel 138ab, derde lid, Sr), het aanbieden, verspreiden of bezitten van kinderpornografie (artikel 240b Sr), de verleiding van een minderjarige tot ontucht (artikel 248a Sr) de «grooming» (artikel 248e Sr) of andere ernstige delicten waarbij het gebruik van een geautomatiseerd werk instrumenteel is en de

inzet van deze bevoegdheid op basis van een afweging van belangen en met inachtneming van de proportionaliteit en subsidiariteit aangewezen is.

De leden van de D66-fractie hebben opgemerkt dat de voorgestelde 'hackbevoegdheid' de bevoegdheid voor de politie introduceert om in te kunnen breken in elk digitaal apparaat van willekeurige burgers, inclusief toegang tot alle historische en toekomstige gegevens opgeslagen in randapparatuur en uitgewisseld met alle hiermee verbonden communicatiekanalen. Met de groei van het internet of things zal dit een groeiende lijst (digitale) apparatuur omvatten. Daarmee raakt deze bevoegdheid een grote groep onschuldige burgers. De leden van deze fractie hebben opgemerkt dat dit een dusdanig grove en niet verfijnde maatregel is dat er zeer goede argumenten tegenover moeten staan om de inbreuk op de privacy van burgers, zoals beschermd door artikel 8 van het EVRM, te rechtvaardigen.

Er is geen sprake van een grove en niet-verfijnde maatregel en het wordt niet mogelijk gemaakt geautomatiseerde werken van willekeurige burgers binnen te dringen. 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 nauwkeurig maatwerk, toegesneden op een specifieke situatie. 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 de waarborgen die aan de inzet en uitvoer van de bevoegdheden van dit wetsvoorstel verwijs ik naar de eerdere beantwoording van een vraag van de leden van de fractie van de VVD over de vereisten die voortvloeien uit het Europees Verdrag voor de Rechten van de Mens. 12-14

Met opmerkingen [9]: 12-14

Het wetsvoorstel is een reactie op de snelle ontwikkelingen van de technologie en het internet. Helaas heeft de criminaliteit die ontwikkeling beter kunnen bijhouden dan de wetgever. Een belangrijk onderdeel van het wetsvoorstel betreft de bevoegdheid om op afstand, dus via het internet, binnen te dringen in een geautomatiseerd werk om vervolgens specifieke onderzoekshandelingen in het geautomatiseerd werk te verrichten. De politie heeft vanwege verschillende redenen dringend behoefte aan deze bevoegdheid. Digitale gegevens worden steeds

vaker versleuteld. Kwaadwillenden kunnen ervoor kiezen om gegevens te versleutelen door het gebruik van speciale software. Maar versleuteling vindt ook plaats zonder dat de gebruiker daar invloed op heeft, doordat een fabrikant versleuteling als standaard inbouwt in de hard- en software die aan de gebruiker wordt aangeboden. Het ontsleutelen van gegevens wordt steeds lastiger, niet alleen doordat de software steeds geavanceerder wordt maar ook doordat een aanbieder meestal zelf niet in staat is om de encryptie ongedaan te maken. Daardoor is de communicatie van de criminaliteit voor de overheid niet meer toegankelijk, en komt de functie van de staat als hoeder van de veiligheid van burgers in het gedrang. Dit probleem speelt niet alleen bij het aftappen van telecommunicatie. Dit is ook aan de orde bij het opnemen van emailverkeer tussen computers, met behulp van een zogenaamde IP-tap. Daarnaast maakt anoniem gebruik van internet het moeilijk de herkomst van communicatie en de locatie van gegevens te bepalen. Bijvoorbeeld door vanaf een nepadres te communiceren ('IP-spoofing'), door versleutelde toegang in de computer aan te zetten (VPN) of door gebruik te maken van anonimeringssoftware zoals TOR.

De snelle ontwikkelingen rond de informatie- en communicatietechnologie zorgen er voor dat de politie nadat zij door aangifte melding of uit andere wetenschap op de hoogte is van computercriminaliteit geen onderzoek kan opstarten en, of voortzetten om verdachten van deze strafbare feiten op te sporen. Zonder opsporing, geen vervolging en rechterlijke afdoening. Dit holt de rechtshandhaving in cyberspace uit. Zo wordt het internet een mogelijke vrijplaats voor allerlei vormen van ernstige criminaliteit waartegen burgers en bedrijven zich overigens ook anderszins onvoldoende kunnen verweren, noch kan er aan slachtoffers recht worden gedaan.

Bij het voorstellen van deze nieuwe bevoegdheid wordt uiteraard rekening gehouden met de privacy van burgers. Het recht op privacy is een heel belangrijk recht, maar het is geen absoluut recht. In bepaalde gevallen moet het mogelijk zijn dat de overheid kennis neemt van de communicatie van burgers in het belang van algemeen aanvaarde belangen, zoals de opsporing van strafbare feiten. Een goed voorbeeld is het aftappen van telecommunicatie. Als we zouden uitgaan van een absoluut recht op privacy dan zou dat ook niet mogelijk zijn. In dit wetsvoorstel worden uiteraard de waarborgen van de rechtstaat 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 en 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 onderzoeksbevoegdheden. Dit betreft deels bestaande bevoegdheden, zoals het aftappen van telecommunicatie en het direct afluisteren. 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 (ex ante) door een rechter commissaris als (achteraf) ex post door de zittingsrechter, zodat een adequate rechterlijke controle verzekerd is. Tenslotte geldt een verplichting tot notificatie van de betrokkene, is voorzien in systeemtoezicht 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.

De leden van de fractie van D66 hebben opgemerkt dat een beperking van het recht op privacy gelegitimeerd kan zijn indien deze proportioneel en noodzakelijk is. Deze leden 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. Deze leden hebben 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.

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-fractie hebben opgemerkt dat het binnendringen van een geautomatiseerd werk altijd tot gevolg heeft dat er veel 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 is wat overtrokken om te stellen dat het binnendringen van een geautomatiseerd werk altijd tot gevolg heeft dat er veel meer data worden verzameld dan doelmatig gezien nodig is. Daarnaast zullen onschuldige burgers via het netwerk niet in de gaten zullen worden gehouden. De term ‘in de gaten houden’ suggereert een structureel gerichte inzet, dat is bij onschuldige burgers niet van toepassing, al kan de verzameling van hun gegevens wel een ongewenste consequentie zijn van de inzet. De regels rond de inzet van de bevoegdheid zijn er juist op gericht op 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 van telecommunicatie 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 betreffende aansluiting gebruiken.

Op grond van de jurisprudentie van het EHRM inzake artikel 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 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 een vergaande inbreuk op individuele grondrechten.

Dit is inderdaad het geval. 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 waarop 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 heimelijk op afstand 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 de 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 10 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 op afstand binnendringen met het oog op het verrichten van onderzoekshandelingen in een geautomatiseerd werk is mogelijk als er sprake is van 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 bijzondere opsporingsbevoegdheden met een heimelijk karakter als de infiltratie (artikelen 126h, 126p en 126ze Sv), het direct afluisteren (artikelen 126l, 126s, en 126zf) of het vorderen van bijzondere persoonsgegevens, zoals gegevens over iemand godsdienst of levensovertuiging, ras of politieke gezindheid (artikelen 126nf, 126uf en 126zn, tweede lid, Sv).

Overigens, als het geautomatiseerde werk wordt binnengedrongen met het oog op het veiligstellen of ontoegankelijk maken van gegevens geldt 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. Ondanks het antwoord van de regering tijdens eerdere vragenrondes in de Tweede Kamer blijft de vraag overeind in hoeverre er minder vergaande mogelijkheden beschikbaar zijn, waarbij de privacy beter is gewaarborgd ten aanzien van individuele grondrechten. De leden van deze fractie hebben 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. Hiervoor kan worden verwezen naar de memorie van toelichting (§ 2.1), de nota naar aanleiding van het verslag (blz. 1/2 en § 2.1, i.h.b. blz. 18/19), de mondelinge behandeling in de Tweede Kamer en de rapporten waarin in de inleiding naar is verwezen.

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 op Nederlands grondgebied 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 de vordering moet worden verstuurd. Als de locatie van het betreffende geautomatiseerde werk of de gegevens niet bekend is dan kan evenmin een doorzoeking ter vastlegging van gegevens (artikel 125i Sv) of een netwerkzoeking (artikel 125j, eerste lid, 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 dan kan de versleuteling van de gegevens de opsporing voor grote problemen plaatsen, sommige vormen van versleuteling zijn vrijwel niet te kraken. 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 was het bewijsmateriaal verloren. Overigens brengt de inzet van deze 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 mogelijk andere bevoegdheden uitkomst kunnen bieden. Dat lijkt op het eerste gezicht soms wel het geval, maar dan zijn er bij nadere beschouwing 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 van 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 zelf heeft geadviseerd om het wetsvoorstel niet op deze wijze in te dienen omdat het wetsvoorstel een grondwettelijke toetsing niet zou doorstaan en hebben gevraagd wat de verwachting van de regering is ten aanzien van een dergelijke grondwettelijke toetsing van het wetsvoorstel.

Hierboven is, naar aanleiding van vragen van de fracties van de fractie van de VVD, reeds ingegaan op de vraag in hoeverre het wetsvoorstel voldoet aan de vereisten die voortvloeien uit het Europees Verdrag voor de Rechten van de Mens (EVRM), in het bijzonder te aanzien van het recht op bescherming van de persoonlijke levenssfeer. Hiervoor kan tevens worden verwezen naar paragraaf 2.9. van de nota naar aanleiding van het verslag (Kamerstukken II 2016/17, 34 372, nr. 6). Anders dan het College bescherming 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.

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 inmiddels beruchte 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 een extra set vergaande bevoegdheden nodig is.

Het is niet juist dat de politie een pacemaker kan hacken bij een klein misdrijf. Er gelden strikte regels 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 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. 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 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 en 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 met zich 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. Uiteraard wordt, indien mogelijk, gekozen voor de inzet van minder vérgaande 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.

Voor de noodzaak van deze nieuwe bevoegdheden en de proportionaliteits- en de subsidiariteitsoverwegingen verwijs ik naar de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van GroenLinks.

De leden van de fractie van GroenLinks hebben gevraagd wat precies de reikwijdte is van deze wet, en of 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 schenden.

Het wetsvoorstel betreft een uitbreiding van de bijzondere opsporingsbevoegdheden met een bevoegdheid tot het op afstand heimelijk binnendringen van een geautomatiseerd werk. Voor de criteria en waarborgen van de voorgestelde bevoegdheid is nauw aangesloten bij het wettelijk 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 de 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 een 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 ruim 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 van een soortgelijke vraag van de leden van de fractie van de VVD.

4. Samenloop bevoegdheden AIVD en MIVD

16. De leden van de D66-fractie hebben opgemerkt dat in het wetsvoorstel staat dat de hackbevoegdheid ook ingezet mag worden tegen terrorismedreiging of een internationale cyberdreiging. Echter, het verzamelen van inlichtingen in de strijd tegen het terrorisme is een taak van de Algemene Inlichtingen- en Veiligheidsdienst (hierna: AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (hierna: MIVD). 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. De belangrijkste functie van het strafrecht bij terroristische misdrijven ligt echter in het voorkomen van terroristische aanslagen. Zodra een terroristische aanslag gepleegd is, is het te laat. 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), is gekomen tot een verruiming van de toepassingsmogelijkheden van bijzondere opsporingsbevoegdheden ten behoeve van een adequate bestrijding van terroristische misdrijven. De bijzondere opsporingsbevoegdheden, als de stelselmatige observatie, de pseudokoop en –dienstverlening, de infiltratie en het aftappen van telecommunicatie, kunnen worden toegepast in geval van aanwijzingen van een terroristisch misdrijf. 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. In de eerste plaats omdat een dergelijke versnippering niet zozeer samenhangt met de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk als wel met de aanpassing van de strafbaarstellingen en de strafvorderlijke bevoegdheden ten behoeve van de bestrijding van terrorisme. De mogelijke versnippering vloeit dus niet voort uit het voorliggende wetsvoorstel. In de tweede plaats zijn de taken en bevoegdheden van de inlichtingen- en veiligheidsdiensten enerzijds en het openbaar ministerie en de politie anderzijds fundamenteel verschillend. 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 (art. 38, eerste lid, Wiv 2002). Andersom zijn de leden van het openbaar ministerie gehouden, door tussenkomst van het College van procureurs-generaal dan wel, aan een dienst mededeling te doen van de te hunner kennis gekomen gegevens die zij voor die dienst van belang achten (art. 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 niet beoogd de bevoegdheid om terroristische aanslagen te voorkomen uit te breiden naar de politie. De bevoegdheid voor het openbaar ministerie en de opsporingsambtenaren om dergelijke aanslagen te voorkomen vormt namelijk reeds onderdeel van het Wetboek van Strafvordering. Wel voorziet dit wetsvoorstel in uitbreiding van de strafvorderlijke

bevoegdheden bij de bestrijding van terrorisme. Hiervoor kan worden verwezen 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 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 naar de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van D66. De mening dat de bevoegdheid gering is geclausuleerd deel ik bepaald niet, 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 gelezen dat de nieuwe bevoegdheid met name noodzakelijk is bij de opsporing van (de voorbereiding) van terroristische misdrijven en de bestrijding van kinderpornografie, en gevraagd of er andere terreinen zijn 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 in vele vormen van criminaliteit wel 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. In deze vorm van criminaliteit komen de encryptieproblemen, afschermingsproblemen, alsmede het internationale karakter van de pleegplaatsen en aanwezigheid van bewijsmateriaal in alle dringendheid naar voren, zoals door vele cybersecurity specialisten wordt onderschreven. Voorts zal de bevoegdheid van belang zijn bij de bestrijding van de gevestigde georganiseerde criminaliteit. Zoals uit recente onderzoeken is gebleken, is de invoering van ‘pretty good privacy’ (PGP) en andere afschermingmethodieken, waarbij het niet meer mogelijk is voor de politie om de inhoud van de communicatie te onderscheppen, gemeengoed geworden. Organisaties worden op alle manieren gefaciliteerd in het zo anoniem mogelijk communiceren, ook over het plegen van huurmoord, drugstransporten, grootschalige corruptie en wapenhandel. Juist in deze zaken zit de uitdaging 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 wordt 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, en kan ik derhalve uitsluitend via de daartoe geëigende kanalen aan de Tweede Kamer verstrekken. 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 mededeling is schriftelijk, in een vorm van een ambtsbericht. In spoedeisende gevallen kan de mededeling mondeling geschieden. De procedure is vastgelegd in artikel 38 Wiv 2002. Ook dergelijke cijfers kunnen uitsluitend via de daartoe geëigende kanalen aan de Tweede Kamer worden verstrekt.

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 (tot in het oneindige) 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.

Indien de politie of het openbaar ministerie kennis verwerft van onbekende kwetsbaarheden in hardware 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 hardware of software. In uitzonderlijke gevallen kunnen er redenen kunnen 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, 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 onderkenning van het opsporingsonderzoek door de verdachte. 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 hardware 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 financieren en gebruik van niet bekende kwetsbaarheden.

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 enkele onbekende kwetsbaarheden worden gebruikt, bekende kwetsbaarheden kunnen nog steeds bruikbaar zijn.

Het kabinet heeft 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. 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 leden van de SP-fractie hebben geconstateerd dat de hacksoftware door externe partijen ontwikkeld zal worden en dat de politie zonder gedegen kennis eigenlijk niet 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 12-14 [redacted] 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 wordt gebruik gemaakt van een goedgekeurd technisch hulpmiddel mag er vanuit worden gegaan dat aan de wettelijke eisen is voldaan.

Met opmerkingen 12-14 [redacted]

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 systeemtoezicht 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, en 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 College van PG’s,

worden besloten om de rechter-commissaris toestemming te vragen om de melding uit te stellen. De kans dat politie en justitie een onbekende kwetsbaarheid ontdekken die niet eerder reeds is ontdekt en besproken, is naar verwachting erg klein

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.

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 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 medewerken aan de criminaliteit is, en hebben hierover de mening van de regering gevraagd.

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 dit wetsvoorstel een belangrijke bijdrage hieraan. Daarnaast is de inzet en het gebruik van onbekende kwetsbaarheden met diverse waarborgen omkleed, zoals genoemd in de eerdere beantwoording van een vraag van de leden van de fractie van D66 over onbekende kwetsbaarheden, en bestaat de verplichting tot melden daarvan, zoals hierboven aangegeven in antwoord op een vraag van de leden van de fractie van de SP.

De PvdA-fractieleden 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 (ook wel de hackbevoegdheid genoemd) – 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 binnendringen in geautomatiseerd werk. Wel is het mogelijk dat 12-14

Met opmerkingen 12-14

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, het technische team. Om hun kennis actueel te houden zullen zij ~~wel continue~~ cursussen en opleidingen volgen die wereldwijd hoog staan aangeschreven als het gaat om deze materie.

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 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 binnendringen in 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 van de voorgestelde regeling maakt het mogelijk 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 voorstelde bevoegdheid tot binnendringen in geautomatiseerd werk. Wel is het mogelijk dat

12-14

Met opmerkingen 9 4]: 12-14

12-14
.

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 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 binnendringen in 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. Het is lastig 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. De regering hecht aan beperking van de uitvoer van ICT goederen en -software naar regimes met een slechte staat van dienst op het gebied van mensenrechten. 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.

5. Het in artikel 126ffa van het wetsvoorstel voorgestelde meldingsregime werkt 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 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. De opdracht om de kwetsbaarheid te gaan melden komt terecht bij hetzelfde team 12-14 . Bij dat team is het overzicht over het gebruik en melden van onbekende kwetsbaarbeden. Ook bij het Landelijk Parket zal een speciale officier van justitie worden aangesteld om de coördinatie hierop te houden.

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 kunnen worden betrokken of binnen de politieorganisatie zelf kunnen worden ontwikkeld, mits aan de wettelijke vereisten voor keuring wordt voldaan. Voor de selectie van bedrijven geldt de bestaande regelgeving voor inkoop. 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. Doorgaans zal de broncode van de software niet aan de politie bekend worden gemaakt. Leveranciers van dergelijke software geven hun broncode gewoonlijk niet prijs.

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. De AIV spreekt van het internet als een ‘mare

liberum', waarbinnen de staat zich dient te beperken tot het borgen van de juridische kaders van de rechtstaat en het beschermen van de burgerlijke vrijheden. 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. De 'mare liberum'-vergelijking biedt goede aanknopingspunten, maar gaat niet volledig op omdat veiligheid en het respecteren van mensenrechten 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 het kabinet 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 van de inzet 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.

De fractieleden 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 levert dit wetsvoorstel hieraan een belangrijke bijdrage. Het gebruik van onbekende kwetsbaarheden kan hier een onderdeel van zijn. De inzet en het gebruik van onbekende kwetsbaarheden is met diverse waarborgen omkleed, deze zijn aan de orde gekomen in de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van het CDA. Tevens bestaat

de verplichting tot melden, dit is aan de orde gekomen in de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van de SP.

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. De Afdeling advisering heeft gelet hierop 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 (Kamerstukken II 2008/09, 31 808 (R1872), nr. 3; artikelsgewijze toelichting bij artikel 24) is, met verwijzing naar artikel 45 Sr opgemerkt dat poging tot het plegen van misdrijven in Nederland strafbaar is. 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 CDA-fractie 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 materieelrechtelijk niet strafbaar om contact te leggen met iemand die in werkelijkheid geen minderjarige is. Het wetsvoorstel wijzigt deze artikelen waardoor het contact leggen 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 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 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 en 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 opsporingsbeambten 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 preventieve 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 professionele 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 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 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 onvermijdbaar is. Naar aanleiding van het Sweetieproject van Terres des Hommes, waarin gebruik werd gemaakt van bewegende animaties, heeft het openbaar ministerie enkele tientallen zaken in onderzoek gehad. In geen van de zaken is vervolging ingesteld, 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 van een minderjarige tot ontucht strafbaar als de dader een minderjarige of iemand die zich als zodanig voordoet benadert voor seksuele doeleinden. In de eerste plaats 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 zouden 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 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 van telecommunicatie of het opnemen van vertrouwelijke communicatie - gelijk aan die voor de voorgestelde bevoegdheid van het op afstand heimelijk binnendringen van een geautomatiseerd werk. Dit houdt verband met het doel van het binnendringen met het oog op het verrichten van die onderzoekshandelingen in dergelijke gevallen - het aftappen van telecommunicatie of het opnemen van vertrouwelijke communicatie - niet afwijkt van de bestaande bevoegdheid van het aftappen van telecommunicatie of het gebruik van een richtmicrofoon. De bevoegdheid van het op afstand heimelijk binnendringen van de smartphone met het oog op het aftappen van telecommunicatie 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 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 (tele)communicatie.

De regering is ook overigens geen voorstander van een lijst van specifieke misdrijven waarvoor de bevoegdheid beperkt moet worden of specifieke apparaten die gehackt mogen worden omdat dit de

opsporing van ernstige strafbare feiten ernstig kan 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 uitzonderingen van geautomatiseerde werken omdat niet valt te voorzien welke ontwikkelingen diverse apparaten en de werkwijzen van criminelen doormaken. 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 vérgaande bevoegdheden, zoals een vordering 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 inbreken 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.

In het advies over het voorliggende wetsvoorstel heeft de Afdeling advisering gewezen op de ontwikkelingen op het gebied van de communicatietechnologie, die voor binnenlandse en buitenlandse inlichtingen- en opsporingsdiensten grote mogelijkheden bieden om strafbare feiten op te sporen en in het kader daarvan (gedragingen van) burgers die niet of nog niet als verdachte kunnen worden aangemerkt te controleren. Naar het oordeel van de Afdeling advisering kan niet om de vraag worden heengegaan naar de wenselijkheid van aanvullend toezicht op de toepassing van opsporingsbevoegdheden door politie en justitie in zaken waarbij van deze technologie gebruik is gemaakt en die niet hebben geleid tot een procedure voor de strafrechter. De Afdeling is van oordeel dat systeemtoezicht wenselijk is waarbij structureel wordt toegezien op de rechtmatige uitoefening van opsporingsbevoegdheden, waarbij door middel van informatie- en communicatietechnologie naar gegevens wordt gezocht en/of deze worden verkregen. Het toezicht zal zich in het bijzonder kunnen richten op de noodzakelijkheid, proportionaliteit en subsidiariteit van de toepassing van de betreffende bevoegdheden, waarbij op systeemniveau aanbevelingen voor verbetering kunnen worden gedaan. Wat betreft de taken en bevoegdheden van de toezichthouder zou gekeken kunnen worden naar de regeling ten aanzien van de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD). Met betrekking tot de positionering kan eraan worden gedacht de toezichthoudende instantie onder te brengen bij het openbaar ministerie, waar de Centrale Toetsingscommissie al een rol in dezen vervult, maar daarbij externe elementen aan te brengen door middel van bijvoorbeeld een externe onafhankelijke voorzitter en (deels) bemensing met externe terzake deskundigen. Voor zaken die niet zijn voorgelegd aan de rechter zou een dergelijke instantie klachten in individuele zaken kunnen onderzoeken.

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 kunnen 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 (art. 10 GW), afhankelijk van een voorafgaande rechterlijke instemming. De officier van justitie is gehouden aan de betrokkene schriftelijk mededeling van de uitoefening van een bijzondere opsporingsbevoegdheid, zodra het belang van het onderzoek dat toelaat (art. 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 rechterlijke macht toeziet, is de Nationale ombudsman bevoegd de klacht in behandeling te nemen (art. 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.

Op dit moment voorziet de regeling rond de inzet van bijzondere opsporingsbevoegdheden in het Wetboek van Strafvordering in uitgebreide waarborgen voor een rechtmatige en zorgvuldige inzet van die bevoegdheden. De kern daarvan wordt gevormd door het onafhankelijk toezicht door een rechter (ex post). 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 (ex ante). Voor de voorgestelde bevoegdheid van het op afstand heimelijk binnendringen van een geautomatiseerd werk zal aanvullend komen te gelden dat de Centrale Toetsingscommissie (CTC) 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. Voor 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.12-14

12-14

De oordeelsvorming door de officier of de rechter-commissaris, zoals deze tot uitdrukking komt in het bevel respectievelijk de machtiging, valt buiten dit kader. Als de inspecteurs bij de uitoefening van het toezicht in aanraking zouden komen met mogelijke schendingen van wettelijke voorschriften door of in opdracht van de officier van justitie, dan kan het hoofd van de Inspectie VenJ de procureur-generaal bij de Hoge Raad daarover informeren.

Met opmerkingen [9]: 12-14 ?

Gelet op de bestaande structuren en voorzieningen is een meer aanvullend toezicht overbodig. Als, naast de instanties, nog eens een afzonderlijk orgaan wordt ingericht voor het uitoefenen van meer aanvullend toezicht op de voorgestelde bevoegdheid tot het binnendringen van een geautomatiseerd werk, dan zullen de verschillende instanties elkaar eenvoudig voor de voeten gaan lopen bij het toezicht op de uitvoering van bijzondere opsporingsbevoegdheden door politie en justitie. Voor wat betreft het onderzoeken van klachten door een dergelijk orgaan moet worden opgemerkt dat de Nationale ombudsman daartoe thans bevoegd is. Het valt niet goed in te zien op welke wijze de een nieuw toezichthoudend orgaan op dit punt van toegevoegde waarde kan 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 systeemtoezicht door de Inspectie VenJ. Op basis van de 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. Er bestaat geen aanleiding om te komen tot meer toezicht, bijvoorbeeld door de oprichting van een nieuwe toezichthoudend orgaan dat eveneens wordt belast met het toezicht op de toepassing van bepaalde opsporingsbevoegdheden op het gebied van de communicatietechnologie. Gelet op de bestaande structuren en voorzieningen is een dergelijk meer aanvullend toezicht overbodig. Voor wat betreft de behandeling van klachten van burgers leidt de oprichting van een nieuw toezichthoudend orgaan tot spanning met de positie van de Nationale ombudsman.

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 de eerdere beantwoording van soortgelijke vragen 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 (art. 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 is (art. 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 (art. 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 van communicatie en het opnemen van vertrouwelijke communicatie (art. 126l/s/zf en 126m/t/zg Sv), die vanwege het belang van de waarheidsvinding ook gericht 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. Bij de toepassing van een opsporingsbevoegdheid van het aftappen van telecommunicatie komt de communicatie van de personen met wie het gesprek wordt gevoerd uit de aard der zaak ter kennis van de opsporingsambtenaren die zijn belast met het uitluisteren van deze communicatie.

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 aan de orde gesteld hoe de rechter zou moeten oordelen als de indringing heeft plaatsgevonden op het terrein van een ander land, en de regering gevraagd om een reactie hierop.

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 exclusief 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. Inmiddels is in verschillende strafzaken het verweer gevoerd dat het optreden van Nederlandse opsporingsambtenaren op het grondgebied van een andere staat, zonder voorafgaande instemming van die staat, als onbevoegd moet worden aangemerkt en de informatie onrechtmatig verkregen is.

Inmiddels 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 BL5629 en HR 17 april 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.

De leden van de fractie van GroenLinks meenden dat onafhankelijk toezicht van fundamenteel belang is voor de Nederlandse rechtstaat en hebben gevraagd of de regering toezeggingen kan doen over of, 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 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 de vraag waarom niet is gekozen voor een vorm van onafhankelijk toezicht door een orgaan buiten het Ministerie van Veiligheid en Justitie. De inzet van deze bevoegdheid stelt hoge eisen aan de deskundigheid van de betrokkene 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 vrijwel permanent 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 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 artikelen126m, 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 gemaakt moeten worden.

De leden van de fractie van de ChristenUnie zouden graag meer inzicht krijgen in hoe verwacht wordt dat 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, dat zal niet alleen gelden voor het gebruik van technische hulpmiddelen ten behoeve van de uitvoering van die bevoegdheid maar ook voor de inzet van menskracht. Deze leden hebben gevraagd welke verwachting de regering momenteel heeft, en ten laste van welke andere inzet zal dit wetsvoorstel dan bij de invoering van het wetsvoorstel komen, zo vragen voornoemde leden.

P.M. Zie het antwoord op vraag 64.

64. De leden van de fractie van de ChristenUnie hebben gevraagd of voorzien kan worden in enkele scenario’s en een begroting voor de eerste jaren na inwerkingtreding van het wetsvoorstel. De leden van deze fractie hebben tevens gevraagd of voor de inzet van deze bevoegdheden geen extra capaciteit nodig is.

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.

De leden van de fractie van de ChristenUnie zouden krijgen graag inzicht verkrijgen in hoe de extra voorziene structurele last voor de rechtspraak van 500.000 euro 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 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 VVD-fractie 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, zo ja, wat deze criteria zijn en wanneer de tekst naar verwachting beschikbaar komt.

Het wetsvoorstel bevat een facultatieve grondslag om bij algemene maatregel van bestuur nadere regels te stellen over de toepassing van de bevoegdheid tot het 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 in op het territorium 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.

De leden van de CDA-fractie hebben opgemerkt op dat het op afstand binnendringen in een geautomatiseerd werk alleen mag als er een vermoeden (verdenking, aanwijzing) bestaat van een misdrijf waarop een gevangenisstraf van vier jaar of meer gesteld is, maar ook van 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.

De voorwaarden waaronder een geautomatiseerd werk mag worden binnengedrongen en met het oog op bepaalde onderzoeksdoelen onderzoek mag worden verricht differentiëren naar de mate waarin een inbreuk wordt gemaakt op de persoonlijke levenssfeer en of het onderzoeksdoel op een andere, minder ingrijpende, manier kan worden bereikt. 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. Voorts dient het misdrijf gezien zijn aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde op te leveren. 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. Gelet op de mate van inbreuk die hiermee wordt gemaakt op de persoonlijke levenssfeer mag de bevoegdheid met het oog op deze doelen 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). 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 is er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders. Met uitzondering van de computerdelicten in enge zijn de aangewezen misdrijven grotendeels 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, omdat 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 brief van *, waarin beide Kamers zijn geïnformeerd over de consultatieversie van het Besluit onderzoek in een geautomatiseerd werk.

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.

Beperking van de toepassing van deze onderzoeksbevoegdheden tot de wet aangewezen misdrijven, waarop gevangenisstraf van acht jaar of meer is gesteld zou tot gevolg hebben dat de bevoegdheid niet zou kunnen worden ingezet voor een opsporing van een aantal strafbare feiten die een lagere wettelijke strafbedreiging kennen en waarbij het geautomatiseerde werk zodanig instrumenteel is dat als gevolg hiervan er vaak geen andere aangrijpingspunten zijn voor de opsporing. Door de aanwijzing bij algemene maatregel van bestuur van de misdrijven met een lager strafmaximum waarvoor de bevoegdheid mag worden ingezet kan flexibel ingespeeld worden op ontwikkelingen in de computercriminaliteit. De strafvorderlijke waarborgen voor de inzet van de bevoegdheid voor misdrijven die bij algemene maatregel van bestuur zijn aangewezen zijn identiek aan de waarborgen die gelden bij de inzet voor de opsporing van misdrijven die bij wet zijn aangewezen. Zo is wettelijk vereist dat het misdrijf een ernstige inbreuk op de rechtsorde oplevert en dat er een dringend onderzoeksbelang aanwezig is.

De leden van de fractie van de PvdA hebben opgemerkt dat het wetsvoorstel op verschillende plaatsen delegatiebepalingen bevat, en 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 onderzoekbevoegdheid. 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 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). 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 is het besluit gebaseerd op het uitgangspunt dat de gegevens die met een technisch hulpmiddel worden vastgelegd betrouwbaar, integer en herleidbaar dienen te zijn.

De leden van de PvdA-fractie 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, gemeld dat geen formele voorhangprocedure plaatsvindt maar dat wel op andere wijze in de betrokkenheid van het parlement wordt voorzien. Bij brief van * zijn beide Kamers geïnformeerd over de consultatieversie van het Besluit onderzoek in een geautomatiseerd werk. Het besluit is op * ter internetconsultatie aangeboden via 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 onbedoeld 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 is gemeld (paragraaf 3), bestaat er vanwege het open internationale karakter van het internet behoefte aan internationale afspraken inzake het vergaren van bewijs (E-evidence). 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-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 EU voor rechtshulp al eerder zijn ontwikkeld en gangbaar zijn;

- het stroomlijnen en versnellen van de bestaande procedures voor wederzijdse rechtshulp (mutual legal assistance, MLA) en wederzijdse erkenning (mutual recognition) binnen de EU en met derde landen, onder andere door digitalisering van verzoeken en automatische vertaling hiervan, als ook 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 (“enforcement jurisdiction”) 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 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 Cybercrime verdrag uit 2001. Dit is het tot nog nu meest verspreide verdrag met geharmoniseerde strafbaarstellingen, extra strafprocessuele bevoegdheden (zoals bevriezing van gegevens) en vangnetbepalingen voor internationale samenwerking. Op dit moment hebben 52 landen dit verdrag geratificeerd (Raad van Europa landen behalve Rusland en landen zoals VS, Canada, Australië, Japan, Sri Lanka, Paraquay, Dominicaanse republiek, 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.

Uw Kamer zal op de geëigende momenten worden geïnformeerd over de voortgang van genoemde internationale onderhandelingen.

De leden van de fractie van GroenLinks hebben gevraagd hoe het wetvoorstel 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 gebruikgemaakt 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 zogenaamde Cybercrimeverdrag (Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Trb. 2002, 18 en Trb. 2004, 290). Met de wet Computercriminaliteit II is dit verdrag in de Nederlandse wetgeving geïmplementeerd (Kamerstukken II 2004/05, 26 671, nr. 7). Naar aanleiding 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 een andere staat 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. Indien echter 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, deze leden waren benieuwd naar de antwoorden van de regering.

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 opsporingsambtenaren van een technisch team, vanwege hun specialistische kennis en vaardigheden op het terrein van ICT. Binnen de Landelijke eenheid van de Nationale Politie worden één of meer technische teams ingericht. De tijdens het onderzoek in een geautomatiseerd werk met een technisch hulpmiddel geregistreerde gegevens worden automatisch vastgelegd op de een technische voorziening bij het betreffende technisch 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 kennisneming hiervan door onbevoegden. De resultaten van het onderzoek worden door het technische team ter beschikking gesteld aan het tactische team. Op basis van het bevel worden de vastgelegde gegevens 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 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 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. 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, 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 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 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 (art. 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 (art. 14 Wpg).

De leden van de fractie van de VVD hebben gevraagd of bijvangst van fiscale aard wordt doorgestuurd naar de Belastingdienst, en zo nee, waarom niet. 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 justitie en strafvorderlijke gegevens biedt een wettelijke grondslag voor de verstrekking van strafvorderlijke gegevens aan personen of instanties voor buiten de strafrechtspleging gelegen doeleinden (art. 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 op grond van de wet aan andere personen of instanties worden verstrekt. 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). Het beleid terzake is uitgewerkt in de Aanwijzing verstrekking van strafvorderlijke gegevens voor buiten de strafrechtspleging gelegen doeleinden (Aanwijzing wet justitiële en strafvorderlijke gegevens; 2013A014). 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, de officier van justitie behoeft daarvoor niet te wachten op een definitieve beslissing van de rechter naar aanleiding van de ingestelde strafvervolging, 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. Het zou dan enkele maanden of langer duren voordat er een definitieve uitspraak van de rechter is, die de grondslag kan vormen voor het ontoegankelijk maken van de gegevens. 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, en 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. De voorgestelde bevoegdheid namelijk heimelijk wordt toegepast, zonder dat de betrokkene daar weet van heeft, en vertoont inhoudelijk overeenkomsten met de bijzondere opsporingsbevoegdheden van Titel IVA van het Eerste Boek van het Wetboek van Strafvordering. Daarom is gekozen voor plaatsing in die titel. In titel IVa is als criterium voor de toepassing van de diverse bevoegdheden opgenomen de verdenking van een misdrijf. Met de Wet Bijzondere opsporingsbevoegdheden is destijds een afzonderlijk wettelijk regime opgenomen 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).

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 V van het Eerste Boek is voor de opsporingsbevoegdheden als verdenkingscriterium opgenomen: een redelijk vermoeden op grond van feiten of omstandigheden dat in georganiseerd verband misdrijven als omschreven in artikel 67, eerste lid, 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 opnemen van telecommunicatie 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.

Voorgesteld wordt 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 de 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 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 leden van de SP-fractie 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, en 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 geintroduceerd om bij verdenking van een strafbaar feit waarvoor voorlopige hechtenis is toegestaan een tussenpersoon te bevelen terstond alle maatregelen nemen die redelijkerwijs gevergd kunnen worden om gegevens on toegankelijk 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 en 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 SP-fractie 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 en verzoeken om een toelichting van de regering.

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 natuurlijk de situatie onverlet dat, bijvoorbeeld als 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 wordt dit als mirror omschreven). Voor zo een

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 gebruikmaakt 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 nieuwe voorgestelde bevoegdheid, of deze zich ontwikkelt 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, 20011/12, 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. Overigens is in Duitsland eenzelfde ontwikkeling kenbaar. 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 vast 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 exponentiele 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, melding gemaakt wordt 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, waardoor het aantal taps aanzien lijk 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, op basis 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 bevriezings-bevel, 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, waarop de voorgenomen inzet wordt voorgelegd aan de Centrale Toetsingscommissie (CTC) van het openbaar ministerie. De CTC adviseert het College van procureurs-generaal 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 het door deze constructie materieelrechtelijk gezien niet strafbaar is om iemand die zich als minderjarige voordoet te verleiden tot ontucht. Hierdoor is de preventieve 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 meer 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. Een verdachte kan in

voorkomende gevallen het beroep doen op de aanwezigheid van de schulduitsluitingsgrond “afwezigheid van alle schuld”. Het is dan aan de rechter om hierover een oordeel te vellen.

De leden 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 van het Wetboek van Strafrecht. De leden van deze fractie hebben tevens gevraagd of ‘ontucht plegen’ in dit artikel door het voorgestelde artikel 248a 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: 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. Naar verwachting zal een wetsvoorstel tot modernisering van de zedenwetgeving tijdens de zomer van dit jaar gereed zijn voor consultatie.

De Staatssecretaris van Veiligheid en Justitie,

++

Memorie van antwoord inzake het voorstel tot 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)

Conceptversie 05-05-2017

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 het wetsvoorstel computercriminaliteit III (34 372). 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. In recente rapporten onderschrijven de notie van politie en justitie dat de dreiging groeit en er behoefte is aan meer bevoegdheden voor de opsporing om deze 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, de commissie Verhagen, het Cybersecuritybeeld Nederland dat jaarlijks wordt gepubliceerd , de veiligheidsmonitor , en [het Nationaal dreigingsbeeld? **P.M.**]. Voor de dreiging op Europees niveau kan worden gewezen op The Internet Organised Crime Threat Assessment (IOCTA) , alsook het Serious and Organised Crime Threat Assessment (SOCTA) . In veel rapporten zijn overeenkomsten te herkennen, onder andere wordt gesteld dat de dreiging groeit en er behoefte is aan meer bevoegdheden voor de opsporing om deze dreiging te adresseren. Het kabinet 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 hiervoor een voorwaarde. Dit wetsvoorstel is van essentieel belang voor de handhaving van de rechtsstaat in cyberspace. 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 een wetsvoorstel. Zij hebben gevraagd of de regering kan toelichten waarom zij beide terreinen in een wetsvoorstel heeft willen vatten.

De regering deelt de opvatting van de leden van de fractie van de SP, dat in dit wetsvoorstel twee totaal verschillende problemen zijn vervat, bepaald niet. De gedachte dat computercriminaliteit uitsluitend betrekking heeft op het handelen in de digitale dimensie, en daarmee ook vanuit juridisch perspectief strikt kan worden gescheiden van het handelen in de fysieke wereld, is achterhaald. Beide dimensies lopen in elkaar over en werken op elkaar in. 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 ICT meer mogelijkheden om het handelen af te schermen van de buitenwacht, zoals het gebruik van encryptie. Tenslotte zijn de strafbaarstellingen niet meer voldoende toegesneden op de technologische ontwikkeling, daarvoor kan worden gewezen op een delict als het overnemen en helen van vertrouwelijke gegevens. Deze verschillende aspecten hebben een gezamenlijk kenmerk, namelijk dat deze onderdeel vormen van de computercriminaliteit. Beide dimensies lopen in elkaar over en werken op elkaar in. 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 echter 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 slachtoffers te zoeken, 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 en niet op een strategische keuze. De bevoegdheden van de politie en justitie hebben geen gelijke tred gehouden met de ontwikkeling van de computercriminaliteit en daarom dienen deze bevoegdheden te worden aangepast. De suggestie van de fractie van de SP, dat een aantal dringende maatschappelijke problemen zijn meegenomen zodat discutabele onderdelen eerder geaccepteerd worden, is dan ook niet terecht. De regering acht alle onderdelen van het wetsvoorstel voor essentieel belang voor de bestrijding van computercriminaliteit, anders waren deze onderdelen ook niet in het wetsvoorstel opgenomen, en hoopt daarbij ook de SP-fractie aan haar zijde te vinden.

Met opmerkingen 9]: 12-14

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 de 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, 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. In de Grondwet en diverse mensenrechtenverdragen wordt het huisrecht beschermd. De woning is bij uitstek een plaats waar dit recht bescherming geniet.

De noodzaak van deze drastische 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 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. 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. Bovengenoemde technologische vooruitgang belemmert de inzet van traditionele opsporingsbevoegdheden, zoals het aftappen van telecommunicatie, 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 fracties van GroenLinks, nader ingegaan op de noodzaak en de bruikbaarheid van bestaande bevoegdheden in.

Naast de toelichting op de urgentie in de memorie van toelichting (/ 2.1), de nota naar aanleiding van het verslag (blz. 182 en / 2.1, i.h.b. blz. 1981K) en tijdens de mondelinge behandeling in de Tweede xamer verwijs ik voor een schets van de omvang van computercriminaliteit tevens naar de rapporten waarin in de inleiding naar is verwezen. 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 (xamerstukken II 2016817, nr. 6, blz. 15816).

Met opmerkingen 9]: 12-14

3. Proportionaliteit en privacy

De leden van de VVD-fractie 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 te aanzien van het recht op bescherming van de persoonlijke levenssfeer.

In paragraaf 2.K van de memorie van toelichting is uitgebreid ingegaan op de bescherming van grondrechten en het recht op eerbiediging van de persoonlijke levenssfeer. In dit verband is artikel 9 van het Europees Verdrag tot bescherming van Rechten van de Mens en de fundamentele vrijheden (EVRM) van bijzonder belang. In paragraaf 2.K van de nota naar aanleiding van het verslag is nader ingegaan op de recente jurisprudentie van het EHRM rond het heimelijk vergaren van persoonsgegevens ten behoeve van de opsporing en vervolging van strafbare feiten. Dit betreft de arresten in de zaken van Digital Rights Ireland en Seitlinger (zaken C-2K3812 en C-2K4812), Ma: imilian Schrems8Data protection Commission (zaak C-362815), Zakharov tegen Rusland (zaak 47143806, ECLI§CE§ECHR§2015§1204JUD004714306) en Szabo en Vissy tegen Hongarije (zaak 37139814). Voorop gesteld 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 9, 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 in een formele 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 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. 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. 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 onderzoek. 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. 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. Er is voorzien in de nodige waarborgen voor een zorgvuldige uitvoering. 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 e: ecutive 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 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 ze gebruiken, kan de waarde van onafhankelijk toezicht volgens het EHRM niet overschat worden (Szabo en Vissy tegen Hongarije, / 7K). 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 gebruik voor het heimelijk binnentreden. Alle onderzoekshandelingen zullen kunnen worden verantwoord op basis van logging, zodat 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 de Besluit onderzoek in een geautomatiseerd werk. Op de uitvoering van het onderzoek in een geautomatiseerd werk door de opsporingsambtenaren wordt, aanvullend op de rechterlijke controle, systeemtoezicht uitgeoefend door de Inspectie Veiligheid en Justitie. Dit komt verderop, in paragraaf 9, nader aan de orde. Tenslotte is voorzien in een verplichting tot notificatie van de betrokkene, hiervoor is aangesloten bij de bestaande regeling voor de notificatie van bijzondere opsporingsbevoegdheden (art. 126bb Sv). Het EHRM acht het van groot belang dat de betrokkene achteraf op de hoogte kan komen van de geheime surveillance en genoegdoening zoeken voor een eventuele inbreuk op zijn privacy (Zakharov tegen Rusland, / 234; Szabó en Vissy tegen Hongarije, / 96). 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 VVD-fractie 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 bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten. Deze doelen betreffen de uitoefening van reeds bestaande bevoegdheden. Het heimelijk binnendringen in 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 20: : (xamerstukken II 2016817, 34 599) 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 20: : 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 (onderzoek in een geautomatiseerd werk). Het wetsvoorstel inlichtingen- en veiligheidsdiensten 20: : 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 staatsveiligheid beter kunnen uitvoeren. Dit betreft algemene bevoegdheden inzake de verzameling van gegevens, zoals het stelselmatig verzamelen van gegevens over personen uit open bronnen en de raadpleging van informanten, 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 en de onderzoeksopdrachtgerichte interceptie van communicatie.

Voor 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 de 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 taken van de betreffende overheidsorganen, de toepasselijkheid van de Europese 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 EU-verdrag. 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 690820 16). 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 67K820 16). De wettelijke taken van de inlichtingen- en veiligheidsdiensten hebben betrekking op de bescherming van de nationale veiligheid (art. 9 Wiv 20: :). De Europese Unie is niet bevoegd op het gebied van de nationale veiligheid. In het wetsvoorstel inlichtingen- en veiligheidsdiensten 20: : is een specifieke paragraaf opgenomen over de verstrekking van persoonsgegevens (par. 3.4. Wiv 20: :) en een afzonderlijk hoofdstuk over de kennisneming van door of ten behoeve van de diensten verwerkte gegevens (hoofdstuk 5 Wiv 20: :).

Vanwege het onderscheid in de wettelijke taken zijn de rechtshandhavingsdiensten staatsrechtelijk op een andere wijze ingebed dan de inlichtingen- en veiligheidsdiensten anderzijds. 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 verrichten van het zogenoemde systeemtoezicht. 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 als een rechter zich niet heeft uitgelaten over een gedraging die een strafvorderlijk aspect kent (art. K§2 2 en K§2 3 Awb). Tenslotte kan het parlement een rol vervullen. De inzet van de bevoegdheden van de inlichtingen- en veiligheidsdiensten vindt plaats onder verantwoordelijkheid van Onze Ministers van Binnenlandse Zaken en xoninkrijksrelaties en van Defensie. De rechtmatigheid van de uitvoering van een bevoegdheid waarvoor Onze Minister toestemming heeft verleend wordt vooraf getoetst door een onafhankelijke commissie, de Toetsingscommissie inzet bevoegdheden (TIB). De CTIVD is belast met het toezicht op de rechtmatigheid van de uitoefening van de bevoegdheden door de inlichtingen- en veiligheidsdiensten. Het parlement kan openbare of besloten controle uitvoeren, onder meer in de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD) van de Tweede xamer.

Met opmerkingen 9]: 12-14

Hieronder wordt, naar aanleiding van vragen van de leden van de fracties van D66, de SP en de ChristenUnie, nader ingegaan op het toezicht op de toepassing van de bevoegdheid van het onderzoek in een geautomatiseerd werk, mede in verhouding tot het toezicht op de inzet van bevoegdheden door de Inlichtingen- en veiligheidsdiensten.

De leden van de CDA-fractie 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 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 Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (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 van communicatie of de stelselmatige observatie. Naar aanleiding van het advies van de Afdeling advisering is 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. Er zijn bepaalde ernstige strafbare feiten waarop een vrijheidsstraf van minder dan 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 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 doorzoeken van de gegevens in het geautomatiseerde werk, teneinde deze vast te leggen of ontoegankelijk te maken, is essentieel voor het opsporen van dergelijke delicten. Dit betreft misdrijven als het gebruik van een botnet (artikel 139ab, derde lid, Sr), het aanbieden, verspreiden of bezitten van kinderpornografie (artikel 240b Sr), de verleiding van een minderjarige tot ontucht (artikel 249a Sr) de «grooming» (artikel 249e Sr) of andere ernstige delicten waarbij het gebruik van een geautomatiseerd werk instrumenteel is en de

inzet van deze bevoegdheid op basis van een afweging van belangen en met inachtneming van de proportionaliteit en subsidiariteit aangewezen is.

De leden van de D66-fractie hebben opgemerkt dat de voorgestelde 'hackbevoegdheid' de bevoegdheid voor de politie introduceert om in te kunnen breken in elk digitaal apparaat van willekeurige burgers, inclusief toegang tot alle historische en toekomstige gegevens opgeslagen in randapparatuur en uitgewisseld met alle hiermee verbonden communicatiekanalen. Met de groei van het internet of things zal dit een groeiende lijst (digitale) apparatuur omvatten. Daarmee raakt deze bevoegdheid een grote groep onschuldige burgers. De leden van deze fractie hebben opgemerkt dat dit een dusdanig grove en niet verfijnde maatregel is dat er zeer goede argumenten tegenover moeten staan om de inbreuk op de privacy van burgers, zoals beschermd door artikel 9 van het EVRM, te rechtvaardigen.

Er is geen sprake van een grove en niet-verfijnde maatregel en het wordt niet mogelijk gemaakt geautomatiseerde werken van willekeurige burgers binnen te dringen. 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 nauwkeurig maatwerk, toegesneden op een specifieke situatie. 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 de waarborgen die aan de inzet en uitvoer van de bevoegdheden van dit wetsvoorstel verwijs ik naar de eerdere beantwoording van een vraag van de leden van de fractie van de VVD over de vereisten die voortvloeien uit het Europees Verdrag voor de Rechten van de Mens. Aanvullend kan worden opgemerkt dat de voorgenomen de inzet nauwgezet wordt voorbereid.12-14

Met opmerkingen 9]: 12-14

Met opmerkingen 9]: 12-14

Het wetsvoorstel is een reactie op de snelle ontwikkelingen van de technologie en het internet. Helaas heeft de criminaliteit die ontwikkeling beter kunnen bijhouden dan de wetgever. Een belangrijk onderdeel van het wetsvoorstel betreft de bevoegdheid om op afstand, dus via het internet, binnen te dringen in een geautomatiseerd werk om vervolgens specifieke onderzoekshandelingen in het geautomatiseerd werk te verrichten. De politie heeft vanwege

verschillende redenen dringend behoefte aan deze bevoegdheid. Digitale gegevens worden steeds vaker versleuteld. xwaadwillenden kunnen ervoor kiezen om gegevens te versleutelen door het gebruik van speciale software. Maar versleuteling vindt ook plaats zonder dat de gebruiker daar invloed op heeft, doordat een fabrikant versleuteling als standaard inbouwt in de hard- en software die aan de gebruiker wordt aangeboden. Het ontsleutelen van gegevens wordt steeds lastiger, niet alleen doordat de software steeds geavanceerder wordt maar ook doordat een aanbieder meestal zelf niet in staat is om de encryptie ongedaan te maken. Daardoor is de communicatie van de criminaliteit voor de overheid niet meer toegankelijk, en komt de functie van de staat als hoeder van de veiligheid van burgers in het gedrang. Dit probleem speelt niet alleen bij het aftappen van telecommunicatie. Dit is ook aan de orde bij het opnemen van emailverkeer tussen computers, met behulp van een zogenaamde IP-tap. Daarnaast maakt anoniem gebruik van internet het moeilijk de herkomst van communicatie en de locatie van gegevens te bepalen. Bijvoorbeeld door vanaf een nepadres te communiceren ('IP-spoofing'), door versleutelde toegang in de computer aan te zetten (VPN) of door gebruik te maken van anonimeringssoftware zoals TOR.

Met opmerkingen 9]: 12-14

De snelle ontwikkelingen rond de informatie- en communicatietechnologie zorgen er voor dat de politie nadat zij door aangifte melding of uit andere wetenschap op de hoogte is van computercriminaliteit geen onderzoek kan opstarten en, of voortzetten om verdachten van deze strafbare feiten op te sporen. Zonder opsporing, geen vervolging en rechterlijke afdoening. Dit holt de rechtshandhaving in cyberspace uit. Zo wordt het internet een mogelijke vrijplaats voor allerlei vormen van ernstige criminaliteit waartegen burgers en bedrijven zich overigens ook anderszins onvoldoende kunnen verweren, noch kan er aan slachtoffers recht worden gedaan.

Bij het voorstellen van deze nieuwe bevoegdheid wordt uiteraard rekening gehouden met de privacy van burgers. Het recht op privacy is een heel belangrijk recht, maar het is geen absoluut recht. In bepaalde gevallen moet het mogelijk zijn dat de overheid kennis neemt van de communicatie van burgers in het belang van algemeen aanvaarde belangen, zoals de opsporing van strafbare feiten. Een goed voorbeeld is het aftappen van telecommunicatie. Als we zouden uitgaan van een absoluut recht op privacy dan zou dat ook niet mogelijk zijn. In dit wetsvoorstel worden uiteraard de waarborgen van de rechtstaat 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 en 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 onderzoeksbevoegdheden. Dit betreft deels bestaande bevoegdheden, zoals het aftappen van telecommunicatie en het direct afluisteren. 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 (e: ante) door een rechter commissaris als (achteraf) e: post door de zittingsrechter, zodat een adequate rechterlijke controle verzekerd is. Tenslotte geldt een verplichting tot notificatie van de betrokkene, is voorzien in systeemtoezicht door de Inspectie Veiligheid en Justitie en zal periodiek aan de xamer 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.

Met opmerkingen 9]: Evt verwijzen naar uiteenzetting hiervoor nav vragen SP

Met opmerkingen 9]: Hoe gaan we dit doen? Gebeurt dit eventueel al niet via de Inspectie?

De leden van de fractie van D66 hebben opgemerkt dat een beperking van het recht op privacy gelegitimeerd kan zijn indien deze proportioneel en noodzakelijk is. Deze leden 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. Deze leden hebben 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 9 van het EVRM.

Voor het antwoord op de vraag hoe de inzet van deze bevoegdheid zich verhoudt met het recht op privacy, zoals beschermd door artikel 9 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-fractie hebben opgemerkt dat het binnendringen van een geautomatiseerd werk altijd tot gevolg heeft dat er veel 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 9 van het EVRM hebben deze leden gevraagd om een reactie hierop.

Het is wat overtrokken om te stellen dat het binnendringen van een geautomatiseerd werk altijd tot gevolg heeft dat er veel meer data worden verzameld dan doelmatig gezien nodig is. Daarnaast zullen onschuldige burgers via het netwerk niet in de gaten zullen worden gehouden. De term ‘in de gaten houden’ suggereert een structureel gerichte inzet, dat is bij onschuldige burgers niet van toepassing, al kan de verzameling van hun gegevens wel een ongewenste consequentie zijn van de inzet. De regels rond de inzet van de bevoegdheid zijn er juist op gericht op 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 van telecommunicatie 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 betreffende aansluiting gebruiken.

Op grond van de jurisprudentie van het EHRM inzake artikel 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 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 een vergaande inbreuk op individuele grondrechten.

Dit is inderdaad het geval. 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 waarop 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 heimelijk op afstand 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 de 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 9 EVRM. Te dien aanzien kan een vergelijking worden gemaakt met het huisrecht, dat bescherming geniet op grond van artikel 10 van de Grondwet en artikel 9 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 op afstand binnendringen met het oog op het verrichten van onderzoekshandelingen in een geautomatiseerd werk is mogelijk als er sprake is van 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 bijzondere opsporingsbevoegdheden met een heimelijk karakter als de infiltratie (artikelen 126h, 126p en 126ze Sv), het direct afluisteren (artikelen 126l, 126s, en 126zf) of het vorderen van bijzondere persoonsgegevens, zoals gegevens over iemand godsdienst of levensovertuiging, ras of politieke gezindheid (artikelen 126nf, 126uf en 126zn, tweede lid, Sv).

Overigens, als het geautomatiseerde werk wordt binnengedrongen met het oog op het veiligstellen of ontoegankelijk maken van gegevens geldt 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. Ondanks het antwoord van de regering tijdens eerdere vragenrondes in de Tweede xamer blijft de vraag overeind in hoeverre er minder vergaande mogelijkheden beschikbaar zijn, waarbij de privacy beter is gewaarborgd ten aanzien van individuele grondrechten. De leden van deze fractie hebben gevraagd welke andere mogelijkheden er e: act 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. Hiervoor kan worden verwezen naar de memorie van toelichting (/ 2.1), de nota naar aanleiding van het verslag (blz. 182 en / 2.1, i.h.b. blz. 1981K), de mondelinge behandeling in de Tweede xamer en de rapporten waarin in de inleiding naar is verwezen.

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 op Nederlands grondgebied 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. 126nd8ud 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 de vordering moet worden verstuurd. Als de locatie van het betreffende geautomatiseerde werk of de gegevens niet bekend is dan kan evenmin een doorzoeking ter vastlegging van gegevens (artikel 125i Sv) of een netwerkzoeking (artikel 125j, eerste lid, Sv) worden uitgevoerd. Ditzelfde geldt voor de andere bevoegdheden tot inbeslagneming van een geautomatiseerd werk of een gegevensdrager (artikelen. K5, eerste lid, K5, eerste lid, K6c, eerste lid, K7 eerste lid, K9, eerste lid, en KK, eerste lid, Sv). Maar ook als de locatie wel bekend dan kan de versleuteling van de gegevens de opsporing voor grote problemen plaatsen, sommige vormen van versleuteling zijn vrijwel niet te kraken. 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 was het bewijsmateriaal verloren. Overigens brengt de inzet van deze 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 (xamerstukken II, 1KK98KK, 26 671, nr. 3, blz. 1K).

Onderzocht is of mogelijk andere bevoegdheden uitkomst kunnen bieden. Dat lijkt op het eerste gezicht soms wel het geval, maar dan zijn er bij nadere beschouwing 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 van 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 zelf heeft geadviseerd om het wetsvoorstel niet op deze wijze in te dienen omdat het wetsvoorstel een grondwettelijke toetsing niet zou doorstaan en hebben gevraagd wat de verwachting van de regering is ten aanzien van een dergelijke grondwettelijke toetsing van het wetsvoorstel.

Hierboven is, naar aanleiding van vragen van de fracties van de fractie van de VVD, reeds ingegaan op de vraag in hoeverre het wetsvoorstel voldoet aan de vereisten die voortvloeien uit het Europees Verdrag voor de Rechten van de Mens (EVRM), in het bijzonder te aanzien van het recht op bescherming van de persoonlijke levenssfeer. Hiervoor kan tevens worden verwezen naar paragraaf 2.K. van de nota naar aanleiding van het verslag (xamerstukken II 2016817, 34 372, nr. 6). Anders dan het College bescherming 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 9 EVRM.

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 inmiddels beruchte 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 een e: tra set vergaande bevoegdheden nodig is.

Het is niet juist dat de politie een pacemaker kan hacken bij een klein misdrijf. Er gelden strikte regels 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 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. 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 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 en 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 met zich 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. Uiteraard wordt, indien mogelijk, gekozen voor de inzet van minder vérgaande 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.

Voor de noodzaak van deze nieuwe bevoegdheden en de proportionaliteits- en de subsidiariteitsoverwegingen verwijs ik naar de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van GroenLinks.

De leden van de fractie van GroenLinks hebben gevraagd wat precies de reikwijdte is van deze wet, en of 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 schenden.

Het wetsvoorstel betreft een uitbreiding van de bijzondere opsporingsbevoegdheden met een bevoegdheid tot het op afstand heimelijk binnendringen van een geautomatiseerd werk. Voor de criteria en waarborgen van de voorgestelde bevoegdheid is nauw aangesloten bij het wettelijk 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 de 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 een voorafgaande rechterlijke toestemming.

Met opmerkingen 9 12-14

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 ruim 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 van een soortgelijke vraag van de leden van de fractie van de VVD.

4. Samenloop bevoegdheden AIVD en MIVD

16. De leden van de D66-fractie hebben opgemerkt dat in het wetsvoorstel staat dat de hackbevoegdheid ook ingezet mag worden tegen terrorismedreiging of een internationale cyberdreiging. Echter, het verzamelen van inlichtingen in de strijd tegen het terrorisme is een taak van de Algemene Inlichtingen- en Veiligheidsdienst (hierna§AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (hierna§MIVD). 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 conte: t 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, 2K0), 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. De belangrijkste functie van het strafrecht bij terroristische misdrijven ligt echter in het voorkomen van terroristische aanslagen. Zodra een terroristische aanslag gepleegd is, is het te laat. 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, 590), is gekomen tot een verruiming van de toepassingsmogelijkheden van bijzondere opsporingsbevoegdheden ten behoeve van een adequate bestrijding van terroristische misdrijven. De bijzondere opsporingsbevoegdheden, als de stelselmatige observatie, de pseudokoop en –dienstverlening, de infiltratie en het aftappen van telecommunicatie, kunnen worden toegepast in geval van aanwijzingen van een terroristisch misdrijf. 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. In de eerste plaats omdat een dergelijke versnippering niet zozeer samenhangt met de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk als wel met de aanpassing van de strafbaarstellingen en de strafvorderlijke bevoegdheden ten behoeve van de bestrijding van terrorisme. De mogelijke versnippering vloeit dus niet voort uit het voorliggende wetsvoorstel. In de tweede plaats zijn de taken en bevoegdheden van de inlichtingen- en veiligheidsdiensten enerzijds en het openbaar ministerie en de politie anderzijds fundamenteel verschillend. 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 (art. 39, eerste lid, Wiv 2002). Andersom zijn de leden van het openbaar ministerie gehouden, door tussenkomst van het College van procureurs-generaal dan wel, aan een dienst mededeling te doen van de te hunner kennis gekomen gegevens die zij voor die dienst van belang achten (art. 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 niet beoogd de bevoegdheid om terroristische aanslagen te voorkomen uit te breiden naar de politie. De bevoegdheid voor het openbaar ministerie en de opsporingsambtenaren om dergelijke aanslagen te voorkomen vormt namelijk reeds onderdeel van het Wetboek van Strafvordering. Wel voorziet dit wetsvoorstel in uitbreiding van de strafvorderlijke

bevoegdheden bij de bestrijding van terrorisme. Hiervoor kan worden verwezen 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 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 naar de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van D66. De mening dat de bevoegdheid gering is geclausuleerd deel ik bepaald niet, 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 gelezen dat de nieuwe bevoegdheid met name noodzakelijk is bij de opsporing van (de voorbereiding) van terroristische misdrijven en de bestrijding van kinderpornografie, en gevraagd of er andere terreinen zijn 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 in vele vormen van criminaliteit wel 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. In deze vorm van criminaliteit komen de encryptieproblemen, afschermingsproblemen, alsmede het internationale karakter van de pleegplaatsen en aanwezigheid van bewijsmateriaal in alle dringendheid naar voren, zoals door vele cybersecurity specialisten wordt onderschreven. Voorts zal de bevoegdheid van belang zijn bij de bestrijding van de gevestigde georganiseerde criminaliteit. Zoals uit recente onderzoeken is gebleken, is de invoering van ‘pretty good privacy’ (PGP) en andere afschermingmethodieken, waarbij het niet meer mogelijk is voor de politie om de inhoud van de communicatie te onderscheppen, gemeengoed geworden. Organisaties worden op alle manieren gefaciliteerd in het zo anoniem mogelijk communiceren, ook over het plegen van huurmoord, drugstransporten, grootschalige corruptie en wapenhandel. Juist in deze zaken zit de uitdaging 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 wordt 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, en kan ik derhalve uitsluitend via de daartoe geëigende kanalen aan de Tweede xamer verstrekken. 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 mededeling is schriftelijk, in een vorm van een ambtsbericht. In spoedeisende gevallen kan de mededeling mondeling geschieden. De procedure is vastgelegd in artikel 39 Wiv 2002. Ook dergelijke cijfers kunnen uitsluitend via de daartoe geëigende kanalen aan de Tweede xamer worden verstrekt.

5. Kwetsbaarheden

De leden van de fractie van het CDA hebben erop gewezen dat in de Tweede xamer 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 (tot in het oneindige) met vier weken worden verlengd. Het lijkt de leden van deze fractie verstandig om de ma: imale 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.

Indien de politie of het openbaar ministerie kennis verwerft van onbekende kwetsbaarheden in hardware 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 hardware of software. In uitzonderlijke gevallen kunnen er redenen kunnen 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, 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 onderkenning van het opsporingsonderzoek door de verdachte. Ook kan de onbekende kwetsbaarheid een systeem of computerprogramma betreffen dat door criminelen is vervaardigd en8of 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 hardware 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 financieren en gebruik van niet bekende kwetsbaarheden.

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 enkele onbekende kwetsbaarheden worden gebruikt, bekende kwetsbaarheden kunnen nog steeds bruikbaar zijn.

Met opmerkingen 9]: 12-14

Het kabinet heeft 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. 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 leden van de SP-fractie hebben geconstateerd dat de hacksoftware door e: terne partijen ontwikkeld zal worden en dat de politie zonder gedegen kennis eigenlijk niet 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.

7-12

Met opmerkingen 9 § 12-14

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 systeemtoezicht 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, en 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 Recourt8Tellegen (xamerstukken II 2016817, 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 College van PG’s,

worden besloten om de rechter-commissaris toestemming te vragen om de melding uit te stellen. De kans dat politie en justitie een onbekende kwetsbaarheid ontdekken die niet eerder reeds is ontdekt en besproken, is naar verwachting erg klein

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.

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 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 medewerken aan de criminaliteit is, en hebben hierover de mening van de regering gevraagd.

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 dit wetsvoorstel een belangrijke bijdrage hieraan. Daarnaast is de inzet en het gebruik van onbekende kwetsbaarheden met diverse waarborgen omkleed, zoals genoemd in de eerdere beantwoording van een vraag van de leden van de fractie van D66 over onbekende kwetsbaarheden, en bestaat de verplichting tot melden daarvan, zoals hierboven aangegeven in antwoord op een vraag van de leden van de fractie van de SP.

De PvdA-fractieleden 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 (ook wel de hackbevoegdheid genoemd) – impliceert dat de overheid hackkennis op de markt zal gaan verwerven.

Met opmerkingen 9]: 12-14

De politie zal geen informatie over onbekende kwetsbaarheden inkopen ten behoeve van de inzet van de voorstelde bevoegdheid tot binnendringen in geautomatiseerd werk. Wel is het mogelijk dat de politie software aanschaft waarmee in bepaalde gevallen het binnendringen in geautomatiseerd werk wordt uitgevoerd, waarbij de broncode van de software niet aan de politie bekend wordt gemaakt. Leveranciers van dergelijke software geven hun broncode doorgaans niet prijs. In dat geval is niet met zekerheid vast te stellen of de software van bekende of onbekende kwetsbaarheden gebruik maakt.

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 e: pertise beschikken en die deel uitmaken van een speciaal team, het technische team. Om hun kennis actueel te houden zullen zij ~~wel continue~~ cursussen en opleidingen volgen die wereldwijd hoog staan aangeschreven als het gaat om deze materie.

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 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 binnendringen in 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 van de voorgestelde regeling maakt het mogelijk 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 voorstelde bevoegdheid tot binnendringen in geautomatiseerd werk. Wel is het mogelijk dat de politie software aanschaft waarmee in bepaalde gevallen het binnendringen in geautomatiseerd werk wordt uitgevoerd, waarbij de broncode van de software niet aan de politie bekend wordt gemaakt. Leveranciers van dergelijke software geven hun broncode doorgaans niet prijs. In dat geval is niet met zekerheid vast te stellen of de software van bekende of onbekende kwetsbaarheden gebruik maakt. Indien de politie of het OM kennis verwerft van onbekende kwetsbaarheden in hardware 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

Met opmerkingen 9]: Zelfde antwoord als hierboven bij vraag van de SP.

hardware 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 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 binnendringen in 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. Het is lastig deze markt aan controle te onderwerpen. Wel is de verkoop van zogenaamde intrusion software, die gebruik maakt van kwetsbaarheden, in bepaalde omstandigheden onderhevig aan e: portcontrole. De regering hecht aan beperking van de uitvoer van ICT goederen en -software naar regimes met een slechte staat van dienst op het gebied van mensenrechten. 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.

5. Het in artikel 126ffa van het wetsvoorstel voorgestelde meldingsregime werkt 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 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. De opdracht om de kwetsbaarheid te gaan melden komt terecht bij hetzelfde team 12-14). Bij dat team is het overzicht over het gebruik en melden van onbekende kwetsbaarbeden. Ook bij het Landelijk Parket zal een speciale officier van justitie worden aangesteld om de coördinatie hierop te houden.

Met opmerkingen 9 **:** 12-14 .

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 worden betrokken of binnen de politieorganisatie zelf kunnen worden ontwikkeld, mits aan de wettelijke vereisten voor keuring wordt voldaan. Voor de selectie van bedrijven geldt de bestaande regelgeving voor inkoop. 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. Doorgaans zal de broncode van de software niet aan de politie bekend worden gemaakt. Leveranciers van dergelijke software geven hun broncode gewoonlijk niet prijs.

Met opmerkingen [12-14]**:** Zin loopt niet

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. De AIV spreekt van het internet als een ‘mare

liberum', waarbinnen de staat zich dient te beperken tot het borgen van de juridische kaders van de rechtstaat en het beschermen van de burgerlijke vrijheden. 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. De 'mare liberum'-vergelijking biedt goede aanknopingspunten, maar gaat niet volledig op omdat veiligheid en het respecteren van mensenrechten 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 het kabinet 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 van de inzet 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. xwetsbaarheden 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.

De fractieleden 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 levert dit wetsvoorstel hieraan een belangrijke bijdrage. Het gebruik van onbekende kwetsbaarheden kan hier een onderdeel van zijn. De inzet en het gebruik van onbekende kwetsbaarheden is met diverse waarborgen omkleed, deze zijn aan de orde gekomen in de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van het CDA. Tevens bestaat

de verplichting tot melden, dit is aan de orde gekomen in de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van de SP.

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 (xamerstukken II 2015816, 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. De Afdeling advisering heeft gelet hierop geadviseerd om de bewuste passage te schrappen.

In het nader rapport (xamerstukken II 2015816, 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. 2009, 59) (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 (xamerstukken II 200980K, 31 909 (R1972), nr. 3; artikelsgewijze toelichting bij artikel 24) is, met verwijzing naar artikel 45 Sr opgemerkt dat poging tot het plegen van misdrijven in Nederland strafbaar is. In reactie op het advies van de Afdeling advisering is de memorie van toelichting aangevuld met een passage over het ratificatietraject (xamerstukken II 2015816, 34 372, nr. 3, blz. K1).

De leden van de CDA-fractie 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 249a Sr (verleiding van een minderjarige) en 249e Sr (grooming), is het materieelrechtelijk niet strafbaar om contact te leggen met iemand die in werkelijkheid geen minderjarige is. Het wetsvoorstel wijzigt deze artikelen waardoor het contact leggen 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 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 Ars Aequi van mr. dr. x. 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 en 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 1K7K, NJ 1K9K, 356; zie Hoge Raad 29 oktober 2009, NJ 200K, 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 249a Sr ruimte biedt voor anderen dan opsporingsbeambten 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 249a 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 preventieve 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 professionele opsporingsorganisaties, die beschikken over de benodigde bevoegdheden en e: pertise. 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 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 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 onvermijdbaar is. Naar aanleiding van het Sweetieproject van Terres des Hommes, waarin gebruik werd gemaakt van bewegende animaties, heeft het openbaar ministerie enkele tientallen zaken in onderzoek gehad. In geen van de zaken is vervolging ingesteld, omdat telkens sprake was van ongeoorloofde uitlokking (zie ook§Aanhangsel Handelingen, 2016817, nr. K49).

De leden van de fractie van de ChristenUnie hebben gevraagd om uitleg bij de voorgestelde redactie van artikel 249a Sr.

Door de voorgestelde wijziging van artikel 249a Sr wordt verleiding van een minderjarige tot ontucht strafbaar als de dader een minderjarige of iemand die zich als zodanig voordoet benadert voor seksuele doeleinden. In de eerste plaats 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 xinderen 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 zouden 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 e: pliciet 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 van communicatie (artikelen 126m8t 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 van telecommunicatie of het opnemen van vertrouwelijke communicatie - gelijk aan die voor de voorgestelde bevoegdheid van het op afstand heimelijk binnendringen van een geautomatiseerd werk. Dit houdt verband met het doel van het binnendringen met het oog op het verrichten van die onderzoekshandelingen in dergelijke gevallen - het aftappen van telecommunicatie of het opnemen van vertrouwelijke communicatie - niet afwijkt van de bestaande bevoegdheid van het aftappen van telecommunicatie of het gebruik van een richtmicrofoon. De bevoegdheid van het op afstand heimelijk binnendringen van de smartphone met het oog op het aftappen van telecommunicatie 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 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 (tele)communicatie.

De regering is ook overigens geen voorstander van een lijst van specifieke misdrijven waarvoor de bevoegdheid beperkt moet worden of specifieke apparaten die gehackt mogen worden omdat dit de

opsporing van ernstige strafbare feiten ernstig kan 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 uitzonderingen van geautomatiseerde werken omdat niet valt te voorzien welke ontwikkelingen diverse apparaten en de werkwijzen van criminelen doormaken. 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 vérgaande bevoegdheden, zoals een vordering 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 90se: ies 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 inbreken 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.

In het advies over het voorliggende wetsvoorstel heeft de Afdeling advisering gewezen op de ontwikkelingen op het gebied van de communicatietechnologie, die voor binnenlandse en buitenlandse inlichtingen- en opsporingsdiensten grote mogelijkheden bieden om strafbare feiten op te sporen en in het kader daarvan (gedragingen van) burgers die niet of nog niet als verdachte kunnen worden aangemerkt te controleren. Naar het oordeel van de Afdeling advisering kan niet om de vraag worden heengegaan naar de wenselijkheid van aanvullend toezicht op de toepassing van opsporingsbevoegdheden door politie en justitie in zaken waarbij van deze technologie gebruik is gemaakt en die niet hebben geleid tot een procedure voor de strafrechter. De Afdeling is van oordeel dat systeemtoezicht wenselijk is waarbij structureel wordt toegezien op de rechtmatige uitoefening van opsporingsbevoegdheden, waarbij door middel van informatie- en communicatietechnologie naar gegevens wordt gezocht en8of deze worden verkregen. Het toezicht zal zich in het bijzonder kunnen richten op de noodzakelijkheid, proportionaliteit en subsidiariteit van de toepassing van de betreffende bevoegdheden, waarbij op systeemniveau aanbevelingen voor verbetering kunnen worden gedaan. Wat betreft de taken en bevoegdheden van de toezichthouder zou gekeken kunnen worden naar de regeling ten aanzien van de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD). Met betrekking tot de positionering kan eraan worden gedacht de toezichthoudende instantie onder te brengen bij het openbaar ministerie, waar de Centrale Toetsingscommissie al een rol in dezen vervult, maar daarbij e: terne elementen aan te brengen door middel van bijvoorbeeld een e: terne onafhankelijke voorzitter en (deels) bemensing met e: terne terzake deskundigen. Voor zaken die niet zijn voorgelegd aan de rechter zou een dergelijke instantie klachten in individuele zaken kunnen onderzoeken.

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 e: tra 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 kunnen 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 (art. 10 GW), afhankelijk van een voorafgaande rechterlijke instemming. De officier van justitie is gehouden aan de betrokkene schriftelijk mededeling van de uitoefening van een bijzondere opsporingsbevoegdheid, zodra het belang van het onderzoek dat toelaat (art. 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 rechterlijke macht toeziet, is de Nationale ombudsman bevoegd de klacht in behandeling te nemen (art. K§22 en K§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.

Op dit moment voorziet de regeling rond de inzet van bijzondere opsporingsbevoegdheden in het Wetboek van Strafvordering in uitgebreide waarborgen voor een rechtmatige en zorgvuldige inzet van die bevoegdheden. De kern daarvan wordt gevormd door het onafhankelijk toezicht door een rechter (e: post). 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 (e: ante). Voor de voorgestelde bevoegdheid van het op afstand heimelijk binnendringen van een geautomatiseerd werk zal aanvullend komen te gelden dat de Centrale Toetsingscommissie (CTC) 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. Voor 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. Dit is systeemtoezicht. Het systeemtoezicht 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 e: pertise 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. Het kader voor het toezicht wordt gevormd door de grenzen van het bevel en de machtiging voor het onderzoek in een geautomatiseerd werk. De oordeelsvorming door de officier of de rechter-commissaris, zoals deze tot uitdrukking komt in het bevel respectievelijk de machtiging, valt buiten dit kader. Als de inspecteurs bij de uitoefening van het toezicht in aanraking zouden komen met mogelijke schendingen van wettelijke voorschriften door of in opdracht van de officier van justitie, dan kan het hoofd van de Inspectie VenJ de procureur-generaal bij de Hoge Raad daarover informeren.

Gelet op de bestaande structuren en voorzieningen is een meer aanvullend toezicht overbodig. Als, naast de instanties, nog eens een afzonderlijk orgaan wordt ingericht voor het uitoefenen van meer aanvullend toezicht op de voorgestelde bevoegdheid tot het binnendringen van een geautomatiseerd werk, dan zullen de verschillende instanties elkaar eenvoudig voor de voeten gaan lopen bij het toezicht op de uitvoering van bijzondere opsporingsbevoegdheden door politie en justitie. Voor wat betreft het onderzoeken van klachten door een dergelijk orgaan moet worden opgemerkt dat de Nationale ombudsman daartoe thans bevoegd is. Het valt niet goed in te zien op welke wijze de een nieuw toezichthoudend orgaan op dit punt van toegevoegde waarde kan 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 systeemtoezicht door de Inspectie VenJ. Op basis van de 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. Er bestaat geen aanleiding om te komen tot meer toezicht, bijvoorbeeld door de oprichting van een nieuwe toezichthoudend orgaan dat eveneens wordt belast met het toezicht op de toepassing van bepaalde opsporingsbevoegdheden op het gebied van de communicatietechnologie. Gelet op de bestaande structuren en voorzieningen is een dergelijk meer aanvullend toezicht overbodig. Voor wat betreft de behandeling van klachten van burgers leidt de oprichting van een nieuw toezichthoudend orgaan tot spanning met de positie van de Nationale ombudsman.

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 de eerdere beantwoording van soortgelijke vragen 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 (art. 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 is (art. 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 (art. 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 van communicatie en het opnemen van vertrouwelijke communicatie (art. 126l&s&f en 126m&t&zg Sv), die vanwege het belang van de waarheidsvinding ook gericht 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. Bij de toepassing van een opsporingsbevoegdheid van het aftappen van telecommunicatie komt de communicatie van de personen met wie het gesprek wordt gevoerd uit de aard der zaak ter kennis van de opsporingsambtenaren die zijn belast met het uitluisteren van deze communicatie.

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 aan de orde gesteld hoe de rechter zou moeten oordelen als de indringing heeft plaatsgevonden op het terrein van een ander land, en de regering gevraagd om een reactie hierop.

De Nederlandse wet staat niet in de weg aan optreden buiten het Nederlandse grondgebied. Artikel 53Ka 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 e: clusief 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. Inmiddels is in verschillende strafzaken het verweer gevoerd dat het optreden van Nederlandse opsporingsambtenaren op het grondgebied van een andere staat, zonder voorafgaande instemming van die staat, als onbevoegd moet worden aangemerkt en de informatie onrechtmatig verkregen is.

Inmiddels 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 BL562K en HR 17 april 2012 BVK070). 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.

De leden van de fractie van GroenLinks meenden dat onafhankelijk toezicht van fundamenteel belang is voor de Nederlandse rechtstaat en hebben gevraagd of de regering toezeggingen kan doen over of, 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 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 de vraag waarom niet is gekozen voor een vorm van onafhankelijk toezicht door een orgaan buiten het Ministerie van Veiligheid en Justitie. De inzet van deze bevoegdheid stelt hoge eisen aan de deskundigheid van de betrokkene 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. 12 -1 4

Met opmerkingen 9]: 12-14

Met opmerkingen 9]: 12-14

Verder zal de xamer in de gelegenheid worden gesteld zich een oordeel te vormen over de inzet van deze bevoegdheid doordat, conform de werkwijze bij het aftappen van communicatie, jaarlijks aan de xamer zal worden gerapporteerd over de inzet van de bevoegdheid (xamerstukken II 2007809, 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. (xamerstukken II 2015816, 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 5K2 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 artikelen126m, 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. xosten die aan de nakoming van de vordering kunnen worden toegerekend in de vorm van e: tra personeelskosten en e: tra 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 gemaakt moeten worden.

De leden van de fractie van de ChristenUnie zouden graag meer inzicht krijgen in hoe verwacht wordt dat 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, dat zal niet alleen gelden voor het gebruik van technische hulpmiddelen ten behoeve van de uitvoering van die bevoegdheid maar ook voor de inzet van menskracht. Deze leden hebben gevraagd welke verwachting de regering momenteel heeft, en ten laste van welke andere inzet zal dit wetsvoorstel dan bij de invoering van het wetsvoorstel komen, zo vragen voornoemde leden.

P.M. Zie het antwoord op vraag 64.

64. De leden van de fractie van de ChristenUnie hebben gevraagd of voorzien kan worden in enkele scenario’s en een begroting voor de eerste jaren na inwerkingtreding van het wetsvoorstel. De leden van deze fractie hebben tevens gevraagd of voor de inzet van deze bevoegdheden geen e: tra capaciteit nodig is.

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 €13,9 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

Met opmerkingen [9]: 12-14

de begroting van de politie is bij najaarsnota structureel een bedrag toegevoegd voor de aanpak van cybercrime. 12-14

Met opmerkingen 9 : 12-14

Met opmerkingen 9]: 12-14

De leden van de fractie van de ChristenUnie zouden krijgen graag inzicht verkrijgen in hoe de e: tra voorziene structurele last voor de rechtspraak van 500.000 euro 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 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 VVD-fractie 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, zo ja, wat deze criteria zijn en wanneer de tekst naar verwachting beschikbaar komt.

Het wetsvoorstel bevat een facultatieve grondslag om bij algemene maatregel van bestuur nadere regels te stellen over de toepassing van de bevoegdheid tot het 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 126uba8126zpa, 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 in op het territorium 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.

De leden van de CDA-fractie hebben opgemerkt op dat het op afstand binnendringen in een geautomatiseerd werk alleen mag als er een vermoeden (verdenking, aanwijzing) bestaat van een misdrijf waarop een gevangenisstraf van vier jaar of meer gesteld is, maar ook van 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.

De voorwaarden waaronder een geautomatiseerd werk mag worden binnengedrongen en met het oog op bepaalde onderzoeksdoelen onderzoek mag worden verricht differentiëren naar de mate waarin een inbreuk wordt gemaakt op de persoonlijke levenssfeer en of het onderzoeksdoel op een andere, minder ingrijpende, manier kan worden bereikt. 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. Voorts dient het misdrijf gezien zijn aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde op te leveren. 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. Gelet op de mate van inbreuk die hiermee wordt gemaakt op de persoonlijke levenssfeer mag de bevoegdheid met het oog op deze doelen 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 126nba8126uba8126zpa, 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 alleen kunnen 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 is er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders. Met uitzondering van de computerdelicten in enge zijn de aangewezen misdrijven grotendeels misdrijven met een strafma: imum 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 fle: ibel worden ingespeeld. Indien zich in de toekomst nieuwe vormen van computercriminaliteit en8of 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, omdat reeds op andere wijze in de betrokkenheid van het parlement wordt voorzien. Bij de plenaire behandeling van het wetsvoorstel in de Tweede xamer is toegezegd dat de algemene maatregel van bestuur voorafgaand aan de inwerkingtreding van het wetsvoorstel naar de xamer wordt gestuurd. Deze toezegging is gestand gedaan bij brief van …, waarin beide xamers zijn geïnformeerd over de consultatieversie van het Besluit onderzoek in een geautomatiseerd werk.

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.

Beperking van de toepassing van deze onderzoeksbevoegdheden tot de wet aangewezen misdrijven, waarop gevangenisstraf van acht jaar of meer is gesteld zou tot gevolg hebben dat de bevoegdheid niet zou kunnen worden ingezet voor een opsporing van een aantal strafbare feiten die een lagere wettelijke strafbedreiging kennen en waarbij het geautomatiseerde werk zodanig instrumenteel is dat als gevolg hiervan er vaak geen andere aangrijpingspunten zijn voor de opsporing. Door de aanwijzing bij algemene maatregel van bestuur van de misdrijven met een lager strafma: imum waarvoor de bevoegdheid mag worden ingezet kan fle: ibel ingespeeld worden op ontwikkelingen in de computercriminaliteit. De strafvorderlijke waarborgen voor de inzet van de bevoegdheid voor misdrijven die bij algemene maatregel van bestuur zijn aangewezen zijn identiek aan de waarborgen die gelden bij de inzet voor de opsporing van misdrijven die bij wet zijn aangewezen. Zo is wettelijk vereist dat het misdrijf een ernstige inbreuk op de rechtsorde oplevert en dat er een dringend onderzoeksbelang aanwezig is.

De leden van de fractie van de PvdA hebben opgemerkt dat het wetsvoorstel op verschillende plaatsen delegatiebepalingen bevat, en 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 onderzoekbevoegdheid. 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 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 126nba8126uba8126zpa, 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 is het besluit gebaseerd op het uitgangspunt dat de gegevens die met een technisch hulpmiddel worden vastgelegd betrouwbaar, integer en herleidbaar dienen te zijn.

De leden van de PvdA-fractie 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, gemeld dat geen formele voorhangprocedure plaatsvindt maar dat wel op andere wijze in de betrokkenheid van het parlement wordt voorzien. Bij brief van …zijn beide xamers geïnformeerd over de consultatieversie van het Besluit onderzoek in een geautomatiseerd werk. Het besluit is op …ter internetconsultatie aangeboden via 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 onbedoeld 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 xamer 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 is gemeld (paragraaf 3), bestaat er vanwege het open internationale karakter van het internet behoefte aan internationale afspraken inzake het vergaren van bewijs (E-evidence). 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-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 EU voor rechtshulp al eerder zijn ontwikkeld en gangbaar zijn;

- het stroomlijnen en versnellen van de bestaande procedures voor wederzijdse rechtshulp (mutual legal assistance, MLA) en wederzijdse erkenning (mutual recognition) binnen de EU en met derde landen, onder andere door digitalisering van verzoeken en automatische vertaling hiervan, als ook 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 (“enforcement jurisdiction”) 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 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 Cybercrime verdrag uit 2001. Dit is het tot nog nu meest verspreide verdrag met geharmoniseerde strafbaarstellingen, e: tra strafprocessuele bevoegdheden (zoals bevriezing van gegevens) en vangnetbepalingen voor internationale samenwerking. Op dit moment hebben 52 landen dit verdrag geratificeerd (Raad van Europa landen behalve Rusland en landen zoals VS, Canada, Australië, Japan, Sri Lanka, Paraquay, Dominicaanse republiek, 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.

Uw xamer zal op de geëigende momenten worden geïnformeerd over de voortgang van genoemde internationale onderhandelingen.

De leden van de fractie van GroenLinks hebben gevraagd hoe het wetvoorstel 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 gebruikgemaakt 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 zogenaamde Cybercrimeverdrag (Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Trb. 2002, 19 en Trb. 2004, 2K0). Met de wet Computercriminaliteit II is dit verdrag in de Nederlandse wetgeving geïmplementeerd (xamerstukken II 2004805, 26 671, nr. 7). Naar aanleiding 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 een andere staat 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 (xamerstukken II 2016817, 34 372, nr. 3, par. 2.9.3. en nr. 6, blz. K48K5). Diverse landen, waaronder Nederland zelf, hebben ten behoeve van de snelle afhandeling van rechtshulp in cybercrimezaken een 2487 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. Indien echter 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, deze leden waren benieuwd naar de antwoorden van de regering.

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 opsporingsambtenaren van een technisch team, vanwege hun specialistische kennis en vaardigheden op het terrein van ICT. Binnen de Landelijke eenheid van de Nationale Politie worden één of meer technische teams ingericht. De tijdens het onderzoek in een geautomatiseerd werk met een technisch hulpmiddel geregistreerde gegevens worden automatisch vastgelegd op de een technische voorziening bij het betreffende technisch team. 12-14 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. Op basis van het bevel worden de vastgelegde gegevens 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.

Met opmerkingen 9]: Daartoe aangewezen

Met opmerkingen 9]: 12-14

Met opmerkingen 9]: Nog iets melden over bewaren en vernietigen gegevens? Dit zegt ook iets over de zorgvuldigheid.

De leden van de fractie van de VVD hebben gevraagd op welke 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 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. 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, 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 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 moeten worden verwijderd zodra deze niet langer noodzakelijk zijn voor het doel van het onderzoek, of gedurende een periode van ma: imaal een half jaar bewaard teneinde te bezien of zij aanleiding geven tot een nieuw onderzoek. Na afloop van deze termijn worden de gegevens verwijderd (art. K, 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 (art. 14 Wpg).

De leden van de fractie van de VVD hebben gevraagd of bijvangst van fiscale aard wordt doorgestuurd naar de Belastingdienst, en zo nee, waarom niet. 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 justitie en strafvorderlijke gegevens biedt een wettelijke grondslag voor de verstrekking van strafvorderlijke gegevens aan personen of instanties voor buiten de strafrechtspleging gelegen doeleinden (art. 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 op grond van de wet aan andere personen of instanties worden verstrekt. 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). Het beleid terzake is uitgewerkt in de Aanwijzing verstrekking van strafvorderlijke gegevens voor buiten de strafrechtspleging gelegen doeleinden (Aanwijzing wet justitiële en strafvorderlijke gegevens; 2013A014). 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 provider8aanbieder 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, de officier van justitie behoeft daarvoor niet te wachten op een definitieve beslissing van de rechter naar aanleiding van de ingestelde strafvervolging, 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. Het zou dan enkele maanden of langer duren voordat er een definitieve uitspraak van de rechter is, die de grondslag kan vormen voor het ontoegankelijk maken van de gegevens. 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, en 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. De voorgestelde bevoegdheid namelijk heimelijk wordt toegepast, zonder dat de betrokkene daar weet van heeft, en vertoont inhoudelijk overeenkomsten met de bijzondere opsporingsbevoegdheden van Titel IVA van het Eerste Boek van het Wetboek van Strafvordering. Daarom is gekozen voor plaatsing in die titel. In titel IVa is als criterium voor de toepassing van de diverse bevoegdheden opgenomen de verdenking van een misdrijf. Met de Wet Bijzondere opsporingsbevoegdheden is destijds een afzonderlijk wettelijk regime opgenomen voor het onderzoek naar georganiseerde criminaliteit (xamerstukken II 1KK68K7, 25 403, nr. 2). Later is,

met Titel VB, een afzonderlijk regime ingevoegd voor de opsporing van terroristische misdrijven (xamerstukken II 2004805, 30 164, nr. 2).

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 V van het Eerste Boek is voor de opsporingsbevoegdheden als verdenkingscriterium opgenomen§een redelijk vermoeden op grond van feiten of omstandigheden dat in georganiseerd verband misdrijven als omschreven in artikel 67, eerste lid, 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 opnemen van telecommunicatie 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 K 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.

Voorgesteld wordt 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 de 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 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 leden van de SP-fractie wilden graag weten wat artikel 125p Sv e: tra 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, en 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 geintroduceerd om bij verdenking van een strafbaar feit waarvoor voorlopige hechtenis is toegestaan een tussenpersoon te bevelen terstond alle maatregelen nemen die redelijkerwijs gevergd kunnen worden om gegevens on toegankelijk 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 en 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 SP-fractie 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 en verzoeken om een toelichting van de regering.

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 natuurlijk de situatie onverlet dat, bijvoorbeeld als 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 wordt dit als mirror omschreven). Voor zo een

toegankelijkheid kan de provider niet verantwoordelijk worden gehouden, tenzij de provider hiervan e: pliciet 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 gebruikmaakt 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 nieuwe voorgestelde bevoegdheid, of deze zich ontwikkelt 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 xamer is aangeboden (xamerstukken II, 20011812, 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. Overigens is in Duitsland eenzelfde ontwikkeling kenbaar. 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 1KK9 is toe te schrijven aan de opkomst van de mobiele telefonie. Daar het aantal taps op vast lijnen ongeveer gelijk is gebleven, kan hieruit worden opgemaakt dat het aantal telefoontaps het stijgende aantal mobiele telefoons op de voet is gevolgd (blz. 91). Ook in Duitsland is een dergelijke ontwikkeling kenbaar, in het rapport wordt melding gemaakt van een e: ponentiele stijging van het aantal tapbevelen in dat land van 6.3K1 tot 3K.200 in de periode van 1KK9 tot en met 2007. Dit betreft een toename van ruim 600 % (blz. 242). In de tweede plaats worden door de verdachten8gebruikers 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, melding gemaakt wordt gemaakt van een zaak waarbij bij iemand thuis 150 verschillende telefoons en 390 SIM-kaarten zijn gevonden; op grond van de huidige regeling zijn dan in ieder geval 390 verschillende tapbevelen en machtigingen vereist (blz. 12K). 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. 25K). 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, waardoor het aantal taps aanzien lijk 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, op basis 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 bevriezings-bevel, 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 e: pertise 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, waarop de voorgenomen inzet wordt voorgelegd aan de Centrale Toetsingscommissie (CTC) van het openbaar ministerie. De CTC adviseert het College van procureurs-generaal 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 249a Sr en 249e 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 249e 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 249a 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 249a Sr wordt gekozen voor een objectivering van de leeftijdsaanduiding.

Het huidige artikel 249a 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 het door deze constructie materieelrechtelijk gezien niet strafbaar is om iemand die zich als minderjarige voordoet te verleiden tot ontucht. Hierdoor is de preventieve 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 meer 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. Een verdachte kan in

voorkomende gevallen het beroep doen op de aanwezigheid van de schulduitsluitingsgrond “afwezigheid van alle schuld”. Het is dan aan de rechter om hierover een oordeel te vellen.

De leden van de ChristenUnie hebben ook gevraagd of de nieuwe invulling van artikel 249a Sr gevolgen heeft voor de interpretatie van de daaropvolgende artikelen en in het bijzonder artikel 249b van het Wetboek van Strafrecht. De leden van deze fractie hebben tevens gevraagd of ‘ontucht plegen’ in dit artikel door het voorgestelde artikel 249a in het vervolg ook met een webcam of ander technisch hulpmiddel kan plaatsvinden.

In zowel het huidige artikel 249a Sr als het voorgestelde artikel 249a 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 249a 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§ ECLI§NL§RBAMS§2017§1627).

Het plegen van ontucht met iemand is in artikel 249a 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 249b 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. Naar verwachting zal een wetsvoorstel tot modernisering van de zedenwetgeving tijdens de zomer van dit jaar gereed zijn voor consultatie.

De Staatssecretaris van Veiligheid en Justitie,

++

Zie definitieve versie doc 640

Zie definitieve versie doc 640

Zie definitieve versie doc 640

Zie definitieve versie doc 640

Is gelijk aan doc 640

Position Paper politie

Wetsvoorstel CCIII: aanpassing instrumentarium in een snel veranderende wereld.

Onze samenleving verandert onder invloed van digitalisering steeds sneller en ingrijpender. Vrijwel alle vormen van traditionele criminaliteit hebben inmiddels een digitale component. Daarnaast neemt cybercriminaliteit sterk toe. Het is van groot belang om zicht te kunnen krijgen op digitale activiteiten van criminelen. In de praktijk blijkt echter dat criminelen steeds vaker gebruik maken van encryptie en anonimiseringstechnieken, waardoor hun activiteiten voor de politie buiten beeld blijven. Opsporing en rechtshandhaving komen daardoor steeds meer onder druk te staan. De recente zaak waarbij criminelen via versleutelde PGP telefoons communiceerden, toont aan dat politie en OM door het gebruik van encryptie essentiële informatie missen in grote onderzoeken naar vaak ernstige feiten.

De aanpak van cybercrime is al geruime tijd onderdeel van de landelijke prioriteiten en is als prioriteit opgenomen in de Gemeenschappelijke Veiligheidsagenda 2015-2018. Om ernstige criminaliteit met een digitale component en cybercrime effectief aan te kunnen pakken, is het voor de politie van cruciaal belang om bevoegdheden te hebben die aansluiten bij de technologische ontwikkelingen. Het wetsvoorstel Computercriminaliteit III is een nieuw en noodzakelijk wapen in de strijd tegen ernstige delicten.

Dit wetsvoorstel past binnen de bredere ontwikkelingen op het terrein van digitalisering van de maatschappij. Aan de ene kant vormt deze digitalisering een bedreiging, omdat criminelen de digitale mogelijkheden gebruiken om nieuwe of gedigitaliseerde vormen van traditionele criminaliteit te plegen. Aan de andere kant biedt de digitalisering de politie potentieel ook mogelijkheden hiertegen op te treden. Dan moeten de bevoegdheden van de politie echter wel in de pas blijven lopen met de ontwikkelingen in de maatschappij. De huidige wet Computercriminaliteit II is al 10 jaar oud en een actualisatie is noodzakelijk om de slagkracht en de effectiviteit van de politie op peil te houden. Met dit wetsvoorstel wordt de achterstand die is ontstaan weer deels ingelopen.

De politie onderstreept het belang om de inzet van deze bevoegdheid met de allerhoogste waarborgen te omgeven. Het wetsvoorstel beoogt inzet van deze bevoegdheid in zeer specifieke omstandigheden. Zo moet sprake zijn van bestrijding van ernstige strafbare feiten. Daarnaast is de inzet omgeven met de hoogst mogelijke toetsing binnen strafvordering (toetsing door de RC op vordering van de officier en goedkeuring door de Centrale Toetsingscommissie) en moet de inzet voldoen aan de eisen van proportionaliteit en subsidiariteit. De eventuele vrees dat de politie op grote schaal computers kan gaan binnendringen is dus ongegrond.

Naast deze juridische waarborgen zal toezicht worden uitgeoefend op toepassing van de nieuwe bevoegdheden door de inspectie Veiligheid en Justitie. De politie houdt bij de inrichting van de organisatie rekening met transparantie ten behoeve van de toekomstige inspecties en de juridische onderbouwing, door logging van uitgevoerde handelingen.
Verder is het binnendringen alleen toegestaan in een geautomatiseerd werk dat in gebruik is bij een verdachte. Om de privacy nog extra te waarborgen zorgt functiescheiding tussen het technisch team dat de bevoegdheid uitvoert en het team dat om de inzet vraagt ervoor dat alleen informatie vallend binnen het bevel van de officier beschikbaar komt voor het opsporingsteam.

Naast de bevoegdheid tot het op afstand kunnen binnendringen, bevat het wetsvoorstel ook wijzigingen op het terrein van online handelsfraude, heling van gegevens, ontoegankelijk maken, het corrumperen en grooming. Deze voorgestelde wijzigingen zijn voor de politie evenzeer belangrijk. Zij 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 worden vergemakkelijkt.

De politie bereidt zich op landelijk niveau voor op een zorgvuldige invoering van deze wetswijziging, waarbij de focus ligt op de bevoegdheid tot binnendringen in een geautomatiseerd werk. Hiertoe is een programmaorganisatie ingericht en wordt gespecificeerde capaciteit vrijgemaakt binnen de organisatie, die wordt aangevuld met expertise die via zij-instroom wordt verkregen. De technische infrastructuur wordt momenteel voorbereid.

De inzet van de bevoegdheid tot binnendringen zal gefaseerd worden opgebouwd, zodat kennis en ervaring van alle partners in de keten zorgvuldig kunnen meegroeien. De nieuwe wetgeving geeft de politie de mogelijkheden die ze de afgelopen jaren heeft gemist in de bestrijding van ernstige criminaliteit. Dit wetsvoorstel zorgt ervoor dat de politie ook in de gedigitaliseerde wereld recht kan doen aan haar motto “waakzaam en dienstbaar” voor een veilige samenleving.

Kernbepalingen Wet CCIII versie 0.5 d.d. 20170508

- Binnendringen GW algemeen (126nba Sv)
  - Info
    - Doel
    - Definities
      - Geautomatiseerd Werk (GW 80 Sexies)
      - Technisch Hulpmiddel (TH)
    - Nadere regels
      - Bij of krachtens AMvB, over:
      - Autorisatie en deskundigheid opsporingsambtenaren
      - Samenwerking met andere opsporingsambtenaren
      - Geautomatiseerde vastlegging gegevens bevel
      - Binnendringen als niet bekend is waar gegevens zijn opgeslagen
  - Onderzoek in GW (art 126nba Sv)
    - Wanneer?
      - Misdrijf VH toegelaten (67.1 Sv)
      - EN ernstige inbreuk rechtsorde
      - EN het onderzoek dit dringend vordert
      - Inzet voldoet aan beginselen proportionaliteit & subsidiariteit
    - Wie?
      - Kan de Ovj bevelen
      - Na schriftelijke machtiging RC
      - Dat een aangewezen opsporingsambtenaar
      - Binnendringt in een GW
      - Bij verdachte ingebruik
      - En al dan niet met behulp van een TH
      - Onderzoek doet
    - Voorwaarden?
      - RC
        - Voorafgaande schriftelijke machtiging
        - Door RC
        - Op vordering OvJ
        - Aanbieder wordt in gelegenheid gesteld
        - Te worden gehoord
      - Centrale Toetsings Commissie (CTC)
        - Ovj legt voorgenomen inzet voor aan CTC
        - CTC adviseert college PG's
        - Voorafgaande toestemming college PG's = nodig
          - Wet- en regelgeving
          - Jurisprudentie
          - Proportionaliteit en subsidiariteit
          - Afbreukrisico's
          - afweging effectiviteit en afbreukrisico tegen belang concreet geval
        - College brengt periodiek verslag uit aan minister
    - Doel?
      - Vaststelling bepaalde kenmerken GW of gebruiker
      - Stelselmatige observatie [bestaand]
      - Opnemen (vertrouwelijke) communicatie [bestaand]
      - Vastlegging opgeslagen gegevens
      - Ontoegankelijkmaking gegevens
  - Nieuwe strafbare feiten
    - Overnemen van gegevens (138c Sr)
    - Afbeelding maken in woning (139f Sr)
    - Heling gegevens (139g Sr)
    - Verleiding minderjarige (248a Sr)
    - Grooming (248e Sr)
    - Valse internetwinkel (326d Sr)
  - Toezicht 126nba.7 Sv)
    - Op uitvoering bevel
    - Door ambtenaren 141d en personen 142.1b Sv
    - Wordt uitgeoefend door Inspectie Veiligheid en Justitie
  - Bevel ontoegankelijk maken gegevens (125p Sv)
    - Bevel
      - Misdrijf waarvoor VH is toegelaten
      - Door OVJ
      - Aan aanbieder telecomdienst
      - Tot ontoegankelijk maken gegevens
    - Voorwaarden
      - Voorafgaande schriftelijke machtiging
      - Door RC
      - Op vordering OvJ
      - Aanbieder wordt in gelegenheid gesteld
      - Te worden gehoord
  - Verwijderen TH (126nba.6 Sv)
    - Nadat onderzoek is beeindigd
    - Verwijdering onmogelijk
      - Niet (volledig)
      - EN risico's voor functioneren GW
      - Stelt OvJ beheerder in kennis
      - EN verstrekt informatie over volledige verwijdering
      - Bewaarplicht van toepassing (16cc.1 Sv)
  - Vastleggen en ontoegankelijk maken gegevens GW art 126 nba.1cde
    - Bevel
      - Eisen
        - Misdrijf
        - Naam verdachte
        - Aanduiding GW
        - Gegevens niet in NL opgeslagen
        - Feiten en omstandigheden
        - Aanduiding en functionaliteit TH
        - Doel en te verrichten handelingen
        - Het deel van het GW
        - Voornemen plaatsen op persoon
      - Tijdstip/periode
        - Maximaal vier weken
        - Verlenging telkens voor max vier weken
      - Wijziging
        - Door de Ovj
        - Na machtiging RC
        - Schriftelijk met redenen omkleed
          - Bij dringende noodzaak mondeling
          - Binnen 3 dagen alsnog op schrift
      - *Zelfde eisen*
    - Bevel
    - Wanneer?
      - Misdrijven met gevangenisstraf van 8 jaren of meer
      - Bij AMvB aangewezen misdrijven
    - Doel?
      - Vastleggen van gegevens (126cc.5)
      - Ontoegankelijk maken gegevens (126cc.5)

Van: 10.2.e
Verzonden: dinsdag 9 mei 2017 14:32
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: Hoofdlijnennotitie CCIII BOO 12 mei 2017.pptx

Beste Theo,

Bijgaand een opzet voor een korte presentatie tijdens het BOO over de notitie. Ik hoor graag of je dit in gedachten had?

Groet,

10.2.e

Hoofdlijnennotitie CCIII

BOO 12 mei 2017

« waakzaam en dienstbaar »

Update politiek/wetgeving

- Voorlopig verslag EK ontvangen op 3 april
- Beantwoording door MVenJ uiterlijk 15 mei
- Deskundigenbijeenkomst in EK op 20 juni
- Besluit Onderzoek in Geautomatiseerd werk in formele consultatie rond 15 mei

Update notitie

- Besproken met [redacted], [redacted] en Theo
- Gaat met name over de HRM-component
- Keuze uit 2 scenario's voor BOO
- Na akkoord BOO → BBVO → KMTO
- Besluitvorming KMTO in juni?

Uitgangspunten notitie

- Deze 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.
- 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.

Scenario’s

1. De Landelijke Eenheid wer[7-12] fte voor de centrale voorziening. Vanuit de eenheden wordt daarnaast formatieruimte ter grootte v[7-12] fte afgeroomd ten behoeve van de Landelijk Eenheid. Hiermee wordt, gezamenlijk met de partners, een voorziening va[7-12 7-12] gecreëerd. Hierdoor komt de opgedane kennis en ervaring uiteindelijk niet terug naar de Eenheden, maar blijft centraal beschikbaar voor de politie.
2. De Landelijke Eenheid wer[7-12] fte voor de centrale voorziening. Vanuit de Eenheden wordt daarnaast in tota[7-12] fte door een gekwalificeerde medewerker tewerkgesteld bij de voorziening. Hiermee wordt, gezamenlijk met de partners, een voorziening va[7-12 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

Besluiten

1. 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.
2. Er gestart wordt met de centrale werving. Eenheden (incl. DLOS) te vragen vacatureruimte ter beschikking te stellen.
3. Daartoe een landelijke wervingscampagne te starten, waarbij medewerkers van de eenheden mee kunnen solliciteren.

Vragen

Ruimte voor discussie

Van: 10.2.e
Verzonden: dinsdag 9 mei 2017 16:33
Aan: 10.2.e
CC: 10.2.e
Onderwerp: FW: Stukken onderzoekslijn Technologie en Informatiegebruik
Bijlagen: Onderzoeksvoorstel Impact technologie en informatiegebruik opsporing_compact.docx; Oplegnota bij onderzoeksvoorstellen Technologie opsporing.docx; 150807 LR 15-049 Strategische onderzoeksagenda - B5 selfcover.pdf

Opvolgingsmarkering: Opvolgen
Markeringsstatus: Gemarkeerd

Hoi 10.2.e

Hier zijn de stukken die gaan over het onderzoek waarin wij als CCIII worden meegenomen als onderzoeksproject.

Gr.
10.2.e

Titel: Oplegnotitie politie, technologie en effectief informatiegebruik

Kern onderzoeksprogramma:

Eén van de thema's van de strategische onderzoeksagenda van de Nationale Politie (SOANP) is de lijn 'politie, technologie en effectief informatiegebruik'. De Politieacademie werkt deze onderzoekslijn de komende vier jaar verder uit. Gebruikmakend van de inzichten die er inmiddels zijn opgedaan op dit thema wordt gestart met de invulling van de genoemde onderzoekslijn. Tevens zal er verbinding worden gezocht bij de ontwikkelingen die momenteel volop gaande zijn vanuit de recent gepubliceerde contourennota voor de opsporing, waar het gebruik van technologie expliciet wordt genoemd.

De maatschappij verandert snel waarbij de impact van technologische en sociale ontwikkelingen verstrekkend is op de gehele samenleving, waaronder de overheid en bedrijfsleven (Rijksbrede trendverkening, 2013). Ontwikkelingen op het gebied van nieuwe en laagdrempelig beschikbare technologie beïnvloeden sterk de veiligheid in ons land en daarbuiten (Teeuw & Vedder, 2008). Technologische en sociale innovaties zorgen er niet alleen voor dat de criminaliteit zich ontwikkelt; ook de wijze waarop de politie haar taken en functies kan uitvoeren is hierdoor voortdurend onderhevig aan verandering en versnelling (Schönfeld, 2015).

Het hier voorgestelde onderzoeksprogramma heeft als doel:

1) kennis op leveren over technologische ontwikkelingen in het veiligheidsdomein die relevant zijn voor effectief informatiegebruik in de opsporing
2) inzichtelijk maken op welke wijze technologische ontwikkelingen die gericht zijn op informatiegebruik bijdragen aan de kwaliteit van de opsporing
3) indiceren / monitoren van nieuwe technologische toepassingen van informatiegebruik binnen specifieke onderdelen van de opsporing

Centrale vraag:
Op welke wijze dragen technologische ontwikkelingen die gericht zijn op informatiegebruik bij aan de kwaliteit van de opsporing?

Deze centrale onderzoeksvraag wordt in deze fase van het onderzoeksprogramma (voorlopig) uitgewerkt in twee deelonderzoeken. Gestart wordt met het zicht krijgen op lopende initiatieven om vervolgens een goede en verantwoorde keuze te maken voor de vervolgonderzoeken die binnen deze lijn worden uitgewerkt. Als het gaat om politietaken waarvoor geldt dat nieuwe technieken nieuwe mogelijkheden bieden (zoals bij forensisch technisch onderzoek het geval is) of waarvoor geldt dat er zich knelpunten voordoen waarvoor bestaande of toekomstige technieken mogelijkheden kunnen bieden (zoals het geval is bij uitvoeren en registreren van verhoor) zou dergelijk onderzoek versneld kunnen worden uitgevoerd vanwege de urgentie van het probleem of de winsten die van nieuwe technieken worden verwacht.

Bijgevoegd de volgende twee uitgewerkte onderzoeksvoorstellen:

1) De impact van technologische ontwikkelingen op de opsporing
2) Technologiegebruik bij het verhoor en het verwerken van verbale data

De impact van technologische ontwikkelingen op de opsporing

Kern onderzoek:

De huidige tijd wordt ook wel "the age of big data" genoemd. Het staat in het teken van groeiende technologische mogelijkheden en de daaruit voortkomende toename in hoeveelheid beschikbare informatie doordat iedereen en alles met elkaar verbonden is[1, 2]. Het is ook de tijd waarin technologie en het gebruik ervan zich sneller ontwikkelen dan beleid en wetgeving[3]. Ook technologie die de effectiviteit van politieoptreden beoogt te vergroten neemt de afgelopen jaren een hoge vlucht[4, 5, 6]. Recentelijk zijn verscheidene technologieverkenningen en innovatieagenda's gepubliceerd in Nederland die gericht zijn op belangrijke ontwikkelrichtingen binnen het veiligheidsdomein[7, 8, 9, 10]. Voor de politie zijn hierin relevante trends en ontwikkelingen te identificeren waarbij technologische en sociale innovaties het politiewerk ingrijpend kunnen of zullen veranderen. Voorbeelden hiervan zijn ontwikkelingen voor het vergaren van informatie (zoals GPS en ANPR), nieuwe mogelijkheden voor het doorzoeken van big data, ontwikkeling van het "internet of things" en het gebruik van social media.[3, 5]

De exponentiele groei van deze technologieën zorgt voor een haast ongebreidelde vastlegging en beschikbaarheid van informatie over mensen en hun gedragingen[11]. Voor de politie betekent dit het verleggen van haar traditionele focus 'informatie vergaren' naar de wijze waarop de organisatie deze informatie kan benutten[3]. Hier sluiten de operationele doelen van de Nationale Politie zoals een betere informatievoorziening en ICT en beter informatiegestuurd werken bij aan. Er is echter weinig empirisch wetenschappelijk onderzoek gedaan naar de toepassing van technologische ontwikkelingen binnen politieorganisaties en de impact ervan op zowel de organisatie als op criminaliteit[12, 13, 14]

Het is op dit moment dus niet duidelijk wat de impact is van technologische ontwikkelingen op het politieoptreden. Onderzoek hiernaar is op dit moment vooral voor de opsporing van groot belang. De recherche verzamelt dagelijks grote hoeveelheden informatie uit diverse bronnen. Dit varieert van getuigenverklaringen en vingersporen tot financiële gegevens en data afkomstig uit telecommunicatie, internet en servers van betrokken partijen. Om effectiever en efficiënter strafbare feiten op te sporen is verbeterde analyse en distributie van deze informatie noodzakelijk. Deze kwaliteiten van de Nederlandse opsporing worden immers door diverse partijen bekritiseert.[15, 16, 17]

Het probleem is echter dat onduidelijk is welke rol technologieën hierbij spelen. Het is onbekend welke technologieën op het gebied van informatiegebruik momenteel worden verkend of ingezet door de Nederlandse recherche en wat de invloed daarvan is op de effectiviteit en efficiëntie van opsporing en preventie van strafbare feiten. Bovendien is niet inzichtelijk welke methoden de politie gebruikt om deze technologieën werkend te krijgen in de rechercheprakijk.

Dit onderzoek heeft daarom als hoofddoel de impact van deze technologische ontwikkelingen en daaraan gekoppeld informatiegebruik op het opsporingsproces binnen de Nationale Politie in kaart te brengen. Een tweede doel van dit onderzoek is om inzichtelijk te krijgen op welke wijze technologieën binnen de recherche tot feitelijke toepassing komen om zodoende de implementatie van technologieën in het proces opsporing te kunnen bevorderen. Studies naar implementatievraagstukken richtten zich tot op heden voornamelijk op het veld van de gezondheidszorg[18]. Het ontbreekt daardoor aan zicht op aspecten die doorwerking van technologieën voor de politiepraktijk bevorderen. [3, 19, 20, 21, 22, 23]

Onderzoeksdesign:

De centrale onderzoeksvraag is: *Op welke wijze dragen technologische ontwikkelingen die gericht zijn op informatiegebruik bij aan een verbetering van de kwaliteit van de opsporing?*

Hierbij wordt antwoord gezocht op de volgende deelvragen:

1. In welke technologische ontwikkelingen binnen de opsporing die gericht zijn op informatiegebruik wordt momenteel door de Nationale Politie geïnvesteerd?
2. Hoe en met welk doel worden deze technologische ontwikkelingen verkend of ingezet? (o.a. uitvoering, functionaliteiten)
3. Wat zijn de (beoogde) effecten van deze technologische ontwikkelingen op de Nederlandse opsporing?
4. Welke sociale en organisatorische factoren zijn van belang voor het werkend krijgen en benutten van deze technologische ontwikkelingen in de Nederlandse opsporingspraktijk?

5 Welke aanbevelingen kunnen worden gedaan om de bijdrage van technologische ontwikkelingen aan het verbeteren van de kwaliteit van de opsporing te optimaliseren?

Binnen dit onderzoek wordt met technologische ontwikkelingen het volgende bedoeld:
het ontwikkelen en gebruik van geavanceerde elektronische apparaten en computers ten behoeve van (innovatieve) methodes, technieken en processen binnen de opsporing.

Het beantwoorden van onderzoeksvraag 1 is voorwaardelijk voor het beantwoorden van de andere onderzoeksvragen. Daarom wordt eerst ingezet op het creëren van een overzicht van technologische ontwikkelingen en de relevante actoren binnen de opsporing. Hiermee wordt vervolgens door nog nader op te stellen criteria een selectie gemaakt van relevante technologische ontwikkelingen voor de vier overige onderzoeksvragen. Hiervan worden vooralsnog maximaal 10 projecten/ontwikkelingen als casestudy geëvalueerd.

Contactpersoon:
10.2.e 10.2.e @politieacademie.nl, 06-10.2.e
10.2.e , 10.2.e t@hva.nl, 06-10.2.e

Opdrachtgever:
10.2.e

Referenties

1. McKinsey Global Institute, 2011. Big data: The next frontier for innovation, competition, and productivity. Ontleend aan: http://www.mckinsey.com/insights/business_technology/
2. Rijksbrede trendverkenning, strategieberaad rijksbreed, 2013. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Directie DCB/BO/Kennis & Strategie, Den Haag.
3. President's Task Force on 21st Century Policing. 2015. Final Report of the President's Task Force on 21st Century Policing. Washington, DC: Office of Community Oriented Policing Services.
4. Strategische onderzoeksagenda Nationale Politie, 2014.
5. Police Executive Research Forum. 2014. Future Trends in Policing. Washington, D.C.: Office of Community Oriented Policing Services.
6. Schönfeld J.J., 2015. Innovation, Collaboration and leadership. The key to an innovative ecosystem. Apeldoorn: Politieacademie.
7. Teeuw & Vedder (red.), 2008. Security applications for converging technologies. Impact on the constitutional state and legal order. Den Haag: Boom Juridische Uitgevers, WODC-reeks Onderzoek en Beleid, nummer 269.
8. TNO, 2014. Technologieradar Veiligheid. Relevante technologische ontwikkelingen als input voor (kennis- en) innovatieagenda's, 2014. Uitgevoerd door TNO in opdracht van NCTV en NP.
9. Innovatieagenda Veiligheid en Justitie (2014). Ministerie van Veiligheid en Justitie, Den Haag.
10. The Hague Security Delta, 2014. Nationale Innovatieagenda Veiligheid. Den Haag.
11. Est, R. van, m.m.v. V. Rerimassie, I. van Keulen en G. Dorren, 2014. Intieme technologie: de slag om ons lichaam en gedrag. Den Haag: Rathenau Instituut
12. Byrne, J., Marx, G. (2011). 'Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact.' Journal of Police Studies 20(3): 17–40.
13. Terpstra, J., Ponsaers, P., de Poot, C., Bockstaele, M., Gunther Moor, L., 2013. Vernieuwing in de opsporing. Cahiers Politiestudies jaargang 2013-3, nr. 28, 7-20
14. Koper, C.S., Lum, C., Woods, D.J., Hibdon, J., 2015. Realizing the potential of technology in policing. A multisite study of the social, organizational and behavioral aspects of implementing pilicing technologies.

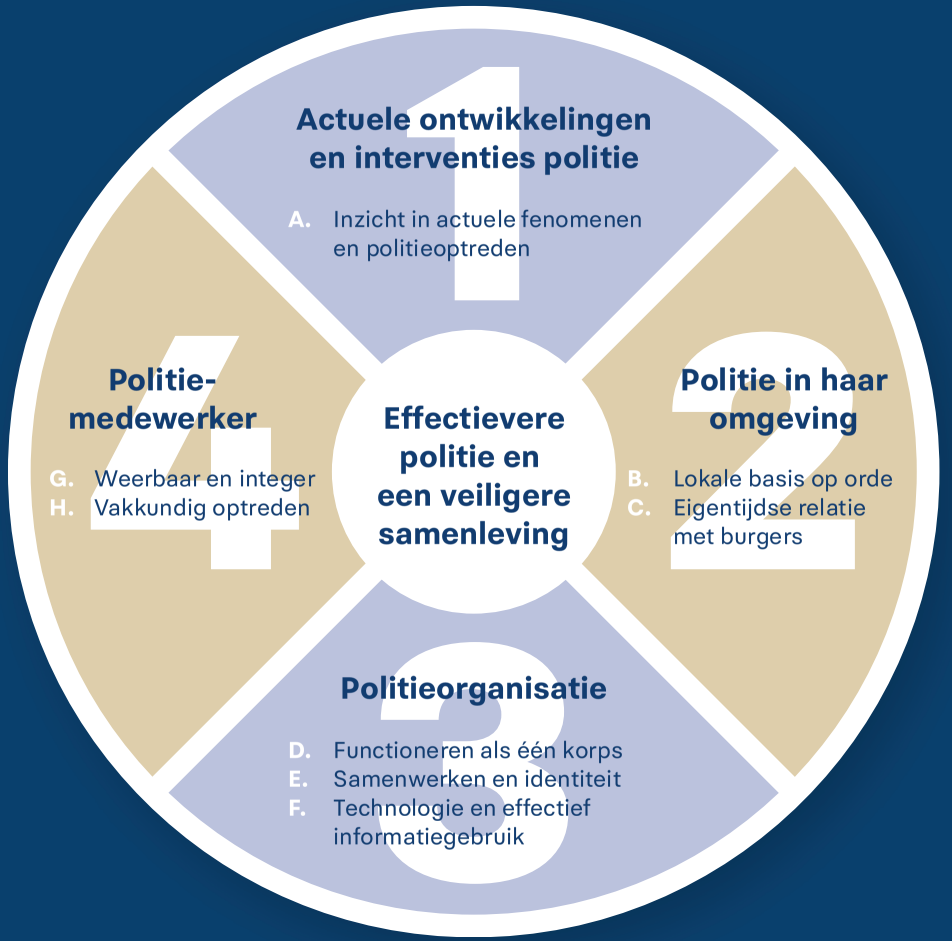
15. Kop, N, & Van der Wal, R. (2011). Recherchetoestanden. Een onderzoek naar de manier waarop in de dagelijkse rechercheprakijk met obstakels wordt omgegaan. Politieacademie, Lectoraat Criminaliteitsbeheersing & Recherchekunde.
16. Liedenbaum, C.M.B., Poot, C.J. de, Straalen, E.K. van, R.F. Kouwenberg, 2015. Focus in de opsporing. Een onderzoek naar de implementatie en uitvoering van de maatregelen uit het programma Versterking Opsporing en Vervolging en het Programma Permanent Professioneel tegen de achtergrond van het voorkomen van tunnelvisie. WODC, Den Haag.
17. Herijkingsnota: Herijking realisatie Nationale Politie (2015). Ministerie van Veiligheid en Justitie, Den Haag.
18. Eccles, M. P., & Mittman, B. S. (2006). Welcome to implementation science. Implement Sci, 1(1), 1-3.
19. Chan, J. (2001). 'Technological Game: How Information Technology is Transforming Police Practice.' Criminal Justice: The International Journal of Policy and Practice 1: 139–159.
20. Chan, J. (2003). 'Police and New Technologies.' In Newburn, T. (ed.), Handbook of Policing. Portland: Willan Publishing, pp. 655–679.
21. Custers, B., 2012. Technology in policing: Experiences, obstacles and police needs. Computer Law and Security Review 28, 62-68
22. Darroch, S., & Mazerolle, L. (2012). Intelligence-led policing: a comparative analysis of organizational factors influencing innovation uptake. Police quarterly, 1098611112467411.
23. Dean, G., Gottschalk, P., 2007. Technologies for Police Knowledge management. In: G. Dean & P. Gottschalk: Knowledge Management in Policing and Law Enforcement. Foundations, Structures, Applications. Oxford University Press. pp. 103- 126.

Voor een effectievere politie en een veiligere samenleving

Strategische onderzoeksagenda voor de Politie 2015-2019

2015-2019

De thema’s



1

Inleiding

Op 1 januari 2013 zijn de vijfentwintig regionale politiekorpsen en het korps Landelijke Politiediensten op basis van de Politiewet 2012 opgegaan in het korps Nationale Politie. Doeleinden van het nieuwe korps zijn het leveren van beter politiewerk, het functioneren als eenheid en het vergroten van de legitimiteit van en het vertrouwen in de politie. In zijn visie op de te leveren politiezorg spreekt het korps nadrukkelijk de wens uit een politie te zijn “die vertrouwt op haar professionals, leert en innoveert” en die daarom behoefte heeft aan “geïnterpreteerde, betekenisvolle en gestructureerde informatie op basis van wetenschappelijk of technologisch onderzoek.”[1]

1 Minister van Veiligheid en Justitie, Realisatieplan Nationale Politie. Den Haag, december 2012, p. 18.
Minister van Veiligheid en Justitie, Inrichtingsplan Nationale Politie. Den Haag, december 2012 , p. 118.

Instrument om samenhang, focus en doorwerking onderzoek te vergroten

In lijn met dit streven wil de regering de Politieacademie sterker binden aan de Nationale Politie. Eén van de kerntaken van de Politieacademie is het verrichten van onafhankelijk, toegepast sociaal-wetenschappelijk onderzoek ten behoeve van de politiepraktijk, het politieonderwijs, de aansturing van de politie en de beleidsvorming ten behoeve van de politie. Een hoogwaardige onderzoekspraktijk is eveneens een vereiste voor het onderhoud van politieopleidingen. Binnen de academie voorzien bovenal de lectoraten in deze kennis-, onderzoeks- en ontwikkelfunctie. Soortgelijk onderzoek, maar op afstand van de politiepraktijk, wordt buiten de academie verricht door onderzoekers aan universiteiten, hogescholen en commerciële onderzoeks-bureaus. De afgelopen jaren heeft Politie en Wetenschap op het terrein van het politieonderzoek een belangrijke, stimulerende rol gespeeld. Bij evaluaties van deze onderzoekspraktijk en bij visitaties van de lectoraten is vastgesteld dat veel kwalitatief hoogwaardig onderzoek wordt verricht maar dat de doorwerking van de vergaarde kennis naar onderwijs, beleid en beroepspraktijk kan worden verbeterd.[2]

De Strategische Onderzoeksagenda voor de Politie is een door de minister van Veiligheid en Justitie aangewezen instrument om meer samenhang en meer focus in het onderzoek aan te brengen en om de doorwerking naar onderwijs, beleid en beroepspraktijk te verbeteren. De agenda bevat de belangrijkste thema's die de komende jaren in het politieonderzoek bijzondere aandacht verdienen en stelt zo de kaders voor het toepassingsgericht sociaal-wetenschappelijk onderzoek dat door de Politieacademie wordt uitgevoerd en voor het wetenschappelijk onderzoek dat wordt uitbesteed.[3] De agenda wordt eenmaal in de vier jaar opgesteld door de Politieacademie ten behoeve van de Nationale Politie en wordt vastgesteld door de minister, na advies van de Politie Onderwijsraad te hebben ingewonnen.
De agenda 2015-2019 is de eerste Strategische Onderzoeksagenda voor de Politie die in de nieuwe organisatorische context is opgesteld. Deze dient als groeidocument te worden beschouwd. In 2015 zal worden bezien of de agenda aanpassing behoeft.

2 C.D. van der Vijver, De professionaliteit van de politie. Apeldoorn, P & W, 2012; P. van Reenen, Tot op heden is dergelijk onderzoek niet verricht. Apeldoorn, P & W, 2012. C. Fijnaut, H. de Jong, L. Kuijs, Rapport Visitatie lectoraten. Apeldoorn 2009.

3 Kamerstukken II, 2012/13, 29 628, nr. 409, blz. 14.

a. Het doel

Een goede, innovatieve politie heeft hoogwaardige kennisontwikkeling en kennisoverdracht nodig. De Nationale Politie krijgt daarom, zo stelde de minister van Veiligheid en Justitie, de beschikking over een onafhankelijke, kritische maar ook efficiënte en complementaire kennis- en onderzoeksfunctie, die ook van strategische betekenis voor het beleid en de politie kan zijn.[4]
Deels betreft dit toegepast sociaal-wetenschappelijk onderzoek verricht door de lectoraten van de Politieacademie, deels wetenschappelijk onderzoek dat wordt uitbesteed aan externe onderzoeksinstituten. De Strategische Onderzoekagenda voor de Politie beoogt focus en richting aan al dit onderzoek te geven.
Al eerder is met dit oogmerk de balans van het politieonderzoek opgemaakt, soms door de centrale overheid en de politieleiding die onderzoek financieren, soms door academische onderzoekers die zich bekommeren om cumulatie van kennis en inzichten. Ruim tien jaar geleden werd gesignaleerd dat die onderzoekpraktijk werd gedomineerd door kortstondige onderzoeken, gericht op momentopnamen en veelal ingegeven door onverwacht opgedoken beleidsproblemen.[5] Sindsdien heeft Politie en Wetenschap een stimulerende en coördinerende invloed op het politieonderzoek uitgeoefend, onder meer door enkele langlopende onderzoekslijnen te ontwikkelen. In 2011 bracht de Politieacademie de Strategische Onderzoeksagenda Politie uit, opgezet in nauw overleg met diverse stakeholders en onderbouwd door meta-analyses. Deze agenda formuleerde vier aandachtsvelden: de maatschappelijke positie, de professionalisering, het gezag en de prestaties van de politie.
De nieuwe Strategische Onderzoeksagenda voor de Politie is een volgende stap in deze ontwikkeling, ingegeven door de vorming van de Nationale Politie en de eerder genoemde evaluaties van de onderzoekspraktijk. Doel van de agenda is ook in de nieuwe situatie de productie te bevorderen van nieuwe kennis die van nut is voor de politiepraktijk, het politieonderwijs en de beleidsvorming. Daarbij wordt acht geslagen op het brede domein van de politiezorg, met bijzondere aandacht voor nieuwe en verwachte ontwikkelingen, en wordt een beroep gedaan op een breed palet van wetenschappelijke disciplines, niet alleen de traditioneel belangrijke politiesociologie, rechtswetenschap en criminologie, maar ook bijvoorbeeld psychologie, (bedrijfs-)economie, geschiedschrijving en technische wetenschappen. De agenda heeft tegenover de onderzoekspraktijk een sturende en faciliterende rol. Onderzoeksresultaten laten zich niet afdwingen, alleen de vrijheid van onderzoekers biedt perspectief op betrouwbare onderzoeksresultaten, maar sturing kan ook stimulerend werken: het kan vakinhoudelijke discussie stimuleren en zo tot verdieping van kennis leiden. Tegenover de politiepraktijk, het politieonderwijs en de beleidsvorming heeft de agenda een verbindende rol. Zij incorporeert in de praktijk gesignaleerd kennisgebrek, draagt bij die praktijk kennis aan die ontleend is aan evaluaties van bestaande praktijken en attendeert op nieuwe fenomenen en effectievere werkwijzen en bevordert dat de politiepraktijk zich die kennis eigen maakt en er haar voordeel mee doet. Voor de agenda zijn daarom het Strategisch Beleidsplan Operatiën van het korps Nationale Politie en de toekomstige innovatieagenda van het korps richtinggevende documenten. Voorts wordt de agenda afgestemd met het onderzoeksprogramma van het WODC van het ministerie van Veiligheid en Justitie, dat van het NSCR en dat van de Inspectie Veiligheid en Justitie.[6]

4 Kamerstukken II, 2012/13, 29 628, nr. 398, blz. 2.

5 G.J.N. Bruinsma, H.G. van der Bunt, I. Haen Marshall, Met het oog op de toekomst. Verkenning naar de kennisvragen over misdaad en misdaadbestrijding in 2010. Den Haag: Adviesraad voor het Wetenschaps- en Technologiebeleid, 2001. G. Meershoek (red.), Politiestudies: terugblik en vooruitzicht. SMVP/Dordrecht, 2009.

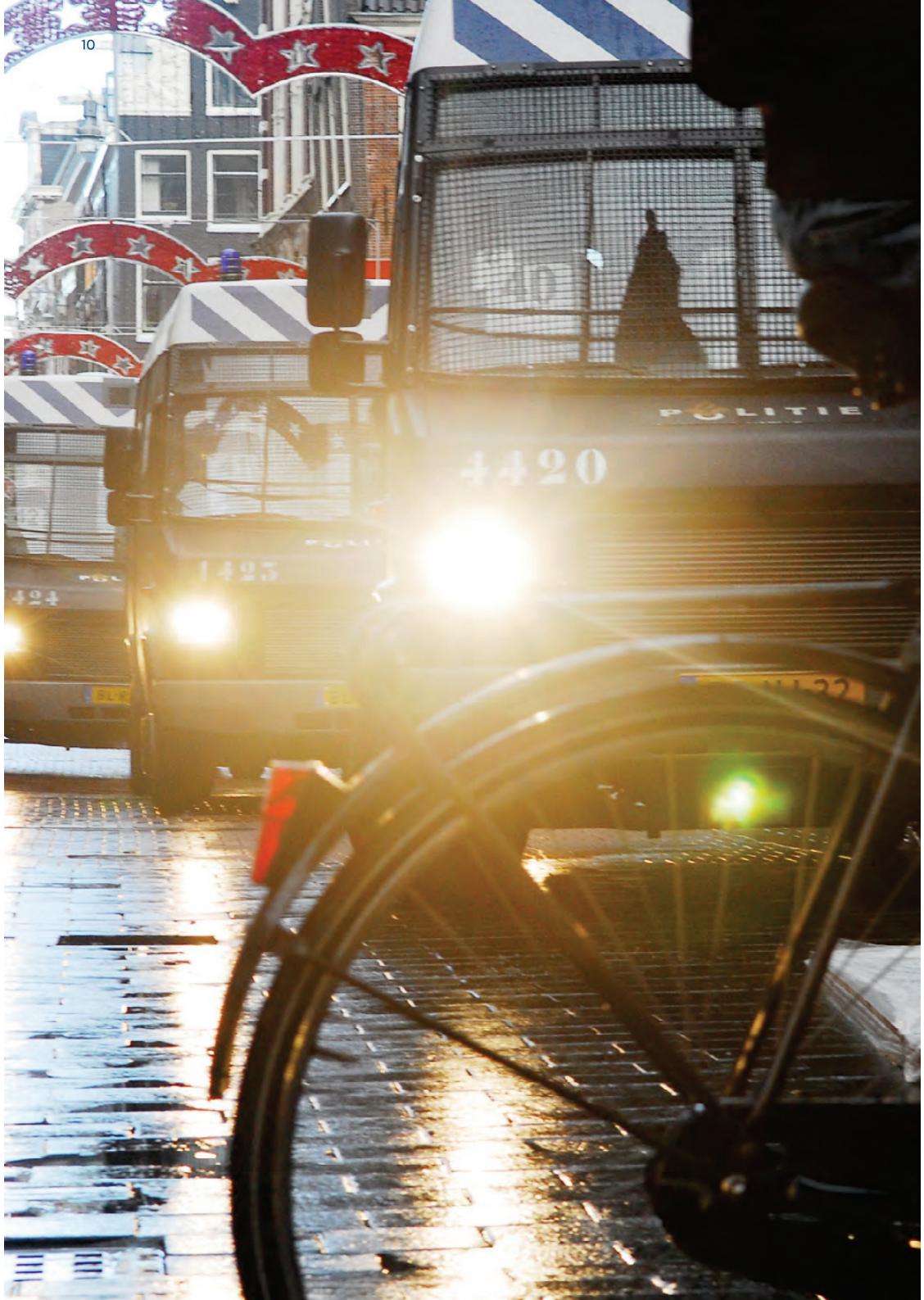
6 Bij het opstellen van deze agenda kon nog slechts van een aanzet tot genoemd plan kennis worden genomen. Afstemming met de twee vermelde onderzoeksprogramma's behelsde vooralsnog alleen het voorkomen van dubbelingen. Zie voorts: www.wodc.nl/onderzoek/onderzoeksprogramma/#paragraph1 en www.nscr.nl/index.php/nl/home

b. De opbouw

De Strategische Onderzoeksagenda voor de Politie is in principe vanaf 2015 voor vier jaar van kracht. Wel zal in 2015 worden bezien of de agenda aanpassing behoeft. Mede omdat de agenda een nieuw instrument is dat nog in ontwikkeling is. De agenda geldt zowel voor onderzoek uitgevoerd door de Politieacademie als voor onderzoek dat middels de Commissie Kennis en Onderzoek van de Politie Onderwijsraad wordt uitbesteed aan onderzoeksbureaus en universiteiten. Zo wordt gericht kennis opgebouwd voor de politiepraktijk en het politieonderwijs, de uitvoering gecoördineerd en daarmee de belasting voor het korps klein gehouden. De cyclus van de agenda is afgestemd op de beleids- en beheercyclus, de begroting voor de periode 2015-2019 en de landelijke prioriteiten van de Nationale Politie.
De Onderzoeksagenda berust op een inventarisatie van de behoefte aan onderzoek bij de Nationale Politie en andere stakeholders maar is geen willekeurige verlanglijst. De verzamelde wensen zijn geanalyseerd, getoetst aan hun betekenis voor het vergroten van de effectiviteit van de politie en de veiligheid in de samenleving en in een onderling verband samengebracht. De uitgangspunten van dat verband worden in de volgende twee hoofdstukken toegelicht: eerst de context waarbinnen het beoogde onderzoek fungeert, vervolgens de centrale vraagstukken waarvoor de politie zich geplaatst ziet en die de onderzoeksthema's verbinden. De Onderzoeksagenda omvat één operationeel thema waarbinnen ruimte is om jaarlijks wisselende accenten te zetten en zeven, vaste, strategische thema's.
Het operationele thema is specifiek opgenomen om recht te doen aan de vele verzoeken uit de politiepraktijk en om actuele ontwikkelingen te volgen en te bezien op hun consequenties voor de politie. Het omvat brandende kwesties in de politiepraktijk die dringend moeten worden doorgrond en de landelijke en regionale/lokale prioriteiten.
Hiertoe behoren fenomenen en politietactieken zoals (de aanpak van) ondermijning, cybercrime en criminele jeugdgroepen. Het bijpassende onderzoek beoogt op korte termijn inzicht te geven in lopende ontwikkelingen en bij te dragen aan beter politie-optreden en betere resultaten. Dergelijk onderzoek zal daarom een relatief korte doorlooptijd hebben. Binnen de jaarlijkse onderzoeksprogrammering van de Politieacademie zal aanzienlijke ruimte worden gecreëerd zodat jaarlijks diverse van zulke onderzoeken kunnen worden uitgevoerd.
De zeven strategische thema's omvatten fenomenen en maatschappelijke en organisatorische ontwikkelingen die een fundamenteler karakter hebben, de politie meer duurzaam raken of naar hun aard grondiger onderzoek vergen. Tot deze categorie behoren bijvoorbeeld onderwerpen die relevant zijn voor de strategische beleidsvorming, de organisatieontwikkeling, de kennisopbouw in het politieonderwijs en het lerend vermogen. Deze thema's liggen voor vier jaar vast maar behoeven niet allemaal jaarlijks in concreet onderzoek te resulteren.

c. De totstandkoming

Omdat de onderzoeksagenda zich richt op de behoefte aan kennis en inzicht bij de Nationale Politie en in het bijzonder tot doel heeft om samenhang en focus aan te brengen in het genereren van onderzoek en onderzoeksresulaten te laten doorwerken in de politiepraktijk, het politieonderwijs en het beleid, is allereerst geïnventariseerd welke behoeften aan kennis daar bestaan. In de Nationale Politie is een enquête uitgezet en zijn met sleutelfiguren interviews gehouden om de behoefte aan onderzoek te peilen. Op deze wijze zijn ruim honderdvijftig suggesties verzameld. Vervolgens zijn in het politieonderwijs vraaggesprekken gevoerd met de managementteams van de politiescholen om na te gaan welke concrete behoeften aan kennis in het onderwijs bestaan. Deze gesprekken leverden ruim veertig suggesties op. Voorts zijn universitaire wetenschappers en onderzoekers van particuliere onderzoeksbureaus tijdens een expertmeeting geconsulteerd om te achterhalen welke lacunes in wetenschappelijke kennis over de politie zij signaleren en welke kwesties zij van groot belang voor de politie achten. Dit leverde vijf thema's op en een groot aantal losse suggesties. Tenslotte hebben de lectoren van de Politieacademie zelfstandig een inventarisatie gemaakt van onderzoeksthema's die zij van belang voor de politie achten, nu en in de toekomst.
Dit leverde enkele tientallen suggesties op, ondergebracht in zeven thema's.
Al deze wensen en suggesties zijn geordend. Van een deel van de opgeworpen vragen vergde de beantwoording geen onderzoek (feitelijk betrof het wensen en verlangens) en deze hebben op andere wijze een vervolg gekregen. Vervolgens is van de resterende vragen nagegaan in hoeverre mag worden verwacht dat onderzoek een onmisbare bijdrage gaat leveren aan de aanpak of oplossing van het achterliggende probleem. Zo is vastgesteld of het voorzien in deze kennisbehoefte werkelijk voor de politiepraktijk of politieonderwijs en voor de veiligheid in de samenleving van belang is. Dat bleek lang niet altijd het geval. De resterende onderwerpen zijn gewaardeerd aan de hand van de prioriteitstelling van de Nationale Politie en een inschatting van de ontwikkelingen die op de politie af komen. Het resultaat is vervolgens voorgelegd aan en besproken met de staf van de korpsleiding van de Nationale Politie, vertegenwoordigers van het Openbaar Ministerie, burgemeesters en vakbonden en met enkele wetenschappers. Hun suggesties maakten het mogelijk het ontwerp verder te verdiepen.



2

De context

De Onderzoeksagena gaat sturing geven aan het wetenschappelijk onderzoek voor de politie. Die sturing vergt niet alleen kennis van de nu in de politiepraktijk levende behoefte aan onderzoek, maar ook een visie op de ontwikkeling van het veld waarin kennis over en voor de politie wordt voortgebracht en uitgedragen. Dat veld omvat vier domeinen: de samenleving, de politie, het politieonderwijs en de onderzoekspraktijk.

a. Relevante ontwikkelingen in de samenleving

De politie is een in de frontlinie van de samenleving fungerende uitvoeringsorganisatie, gericht op het verzekeren van een veilige omgeving. Problemen in de samenleving hebben directe impact op haar takenpakket. Sommige opgaven van de politie zijn vrijwel onveranderlijk. Daarnaast wordt de politie als frontlijnorganisatie ook als eerste en het heftigst met nieuwe problemen geconfronteerd. Het tijdig onderkennen van nieuwe maatschappelijke fenomenen is voor haar dan ook van wezenlijk belang. Drie nieuwe ontwikkelingen lijken de politie in het bijzonder te raken.

Allereerst de globalisering: het openbreken van nationale gemeenschappen voor het internationale verkeer van goederen en personen. Als handelsland ondergaat Nederland in sterke mate deze transformatie. Veel Nederlandse burgers functioneren dagelijks in internationale communities. Burgeroorlogen en rampen elders in de wereld brengen internationale migratiestromen op gang, een crisis in de financiële wereld heeft mondiale impact, maar ook direct gevolgen in wijken en buurten in Nederland. Naar verwachting zal een volledig economisch herstel van de crisis nog geruime tijd uitblijven en de werkloosheid voorlopig groot blijven. Dit kan een deel van de bevolking langdurig in de marge van de samenleving dringen en de sociale spanningen snel doen oplopen. Burgers uit andere EU-landen zoeken hier werk, huisvesting en soms ook vertier. Sommigen veroorzaken overlast, anderen plegen criminaliteit. Ook lokale criminaliteit heeft tegenwoordig al snel een internationale dimensie. Criminelen zijn bijzonder mobiel en maken slim gebruik van grenzen. De Europese Unie heeft in de afgelopen decennia een raamwerk opgericht om de politiële en justitiële samenwerking te vergemakkelijken. Dat biedt de Nederlandse politie kansen om haar werk beter te doen, maar legt haar ook verplichtingen op tegenover haar partners elders in Europa.
Ten tweede ondergaan de relaties tussen burgers, organisaties en instituties als gevolg van digitalisering ingrijpende veranderingen. Door nieuwe communicatietechnologieën reageren burgers en organisaties steeds sneller op gebeurtenissen. Burgers wisselen onderling snel informatie uit: filmen bijvoorbeeld met hun smartphone voorvallen waarbij de politie betrokken is en zetten het resultaat in een oogwenk op internet. Politieoptreden kan zo razendsnel onder een vergrootglas komen te liggen. Incidenten worden door de massamedia scherp uitgelicht. In de afgelopen twintig jaar is de overheid zelf ook op allerlei niveaus haar optreden gaan digitaliseren, teneinde de dienstverlening te optimaliseren en de efficiency te verhogen. Veelal in reactie op technologische innovaties, vaak op basis van incidenten. Niet alleen binnen de overheid zelf, niet alleen tussen beleidsterreinen maar ook dwars door de grenzen die de publieke en private sector scheiden, vindt voortdurend informatie-uitwisseling plaats. Gedacht kan worden aan de OV-chipkaart en het Elektronisch Patiëntendossier. De sturing door de overheid wordt zo permanent doorkruist door afstemmingsprocessen, gaande gehouden door informatiestromen die zich een weg banen door instituties, organisaties en verbanden. De WRR signaleerde drie jaar geleden reeds het ontstaan “van een geheel andere werkelijkheid dan de werkelijkheid die momenteel op de politiek-bestuurlijke radar staat.”[7]
Als gevolg van de globalisering en digitalisering raken burgers, organisaties en instituties steeds sterker met elkaar verweven in netwerkachtige samenwerkingsverbanden. Burgers organiseren zich makkelijker, ze tonen zich hierdoor minder van de overheid afhankelijk dan vroeger het geval was. Organisaties en instituties gaan steeds meer met hen en onderling de samenwerking aan. Door de toegenomen transparantie wordt de politie steeds meer onderwerp van het openbaar debat. Ook de politiek is zich sterker met de politie gaan bemoeien. Gezag is geen rustig bezit meer; interventies dienen steeds meer op bewezen professionele handelingen te berusten.

7 WRR, I-government. Den Haag 2011.

b. Relevante ontwikkelingen in de politie

De afgelopen decennia heeft de Nederlandse politie, mede door de ontwikkelingen in de netwerksamenleving, een ingrijpende verandering ondergaan: van monopolist in de wetshandhaving en criminaliteitsbestrijding werd zij een partner in de integrale veiligheidsaanpak. Ook andere handhavende en opsporende organisaties zoals particuliere toezichthouders, bestuurlijke hand- havers, private rechercheburea’s en forensisch onderzoekers zijn spelers op dit terrein geworden. In het kader van onder meer de criminaliteitspreventie is de politie intensiever gaan samenwerken met andere instanties en organisaties. De Veiligheidshuizen en RIEC’s zijn hiervan sprekende voorbeelden. Die samenwerking betreft niet alleen de afstemming van optreden, maar ook de uitwisseling van informatie en het gezamenlijk optrekken bij de aanpak van concrete problemen. Het veiligheidsdomein is in beweging geraakt, met als consequentie dat de politie haar rol moet definiëren en herdefiniëren in aansluiting op die van haar partners.

Na de vorming van de regionale politiekorpsen in het laatste decennium van de vorige eeuw ontstond in de politieleiding, mede op aandrang van de politiek, een sterke drang om de bedrijfsvoering te verbeteren en zo de efficiëntie van de organisatie te bevorderen. Nieuwe managementtechnieken, veelal gerekend tot het New Public Management, maakten opgang. Er werden prestatie-indicatoren geformuleerd die de output van het politiewerk werden geacht te meten.
In 2003 sloten de beide politieministers met de regiokorpsen prestatieconvenanten. De sturing op cijfers die opkwam, riep binnen en buiten de organisatie kritiek op en na jaren zijn de meest uitgesproken vormen verlaten. Andere aspecten van de bedrijfsvoering van de politie zoals de ICT en de registratiesystemen, trokken vervolgens kritische aandacht.

Sedert de eeuwwisseling is de druk op de politie om snel, optimaal geïnformeerd te zijn groter geworden. Burgers, organisaties en bedrijven kunnen dankzij de nieuwe communicatietechnologie steeds sneller op gebeurtenissen reageren. Ook sommige criminaliteit krijgt zo vleugels.
In de politie maakte het begrip Intelligence Led Policing opgang. Locatietechnologie (GPS, Sensing en ANPR) stelt de politie in staat om op afstand personen te volgen of hun identiteit vast te stellen. De introductie van camera’s, sensoren en drones en de mogelijkheid om big data te doorzoeken, veranderen het politiewerk. Tegelijk ondergaat de politie zelf onder invloed van deze technologieën ook een radicale verandering. De beschikbaarheid van eindeloze hoeveelheden informatie verlegt het accent in het politiewerk van het vergaren van informatie naar het beschikbaar stellen van de juiste informatie op de juiste plek op het juiste moment. De politie ervaart de noodzaak een data-
driven organisatie te worden, dat wil zeggen flexibeler en professioneler. De oprichting van Real Time Intelligence Centers is een stap in die ontwikkeling.

Ondertussen is de op 1 januari 2013 ingezette vorming van de Nationale Politie zich nog volop aan het voltrekken. De inrichting van de organisatie en de herpositionering in de veiligheidsnetwerken en in de samenleving zullen ook de komende jaren nog het nodige vergen. Te verwachten is dat - zeker als het stof rond de reorganisatie bij de politie enigszins is neergedaald - de eisen die burgers en politici aan politiewerk stellen verder zullen toenemen. De noodzaak tot samenwerking met andere politiële diensten (Koninklijke Marechaussee, BOD’s, AIVD, bestuurlijke handhavers), met partners in de strafrechtelijke keten en met andere organisaties zal onverminderd groot blijven. De vraag naar internationale samenwerking, in het bijzonder die binnen Europees verband, zal zelfs toenemen. Werving van aspiranten met een betere vooropleiding kan op deze ontwikkelingen slechts ten dele het gepaste antwoord zijn. Van de politie wordt ook een aanmerkelijke verbetering van het optreden en de dienstverlening gevergd.

c. Relevante ontwikkelingen in het politieonderwijs

De volwaardige beroepsopleidingen, waar de Nederlandse politie in de afgelopen vijftig jaar de beschikking over kreeg, zijn onderhevig aan een duurzaam spanningsveld dat in die decennia talloze veranderingen en verbeteringen opriep, zonder ooit te kunnen worden opgeheven. Naast de instructie, training en inwijding door ervaren collega's, die op de politiescholen en het Rijksinstituut voor Opleiding van Hogere Politieambtenaren centraal hadden gestaan, kwam namelijk aandacht voor maatschappelijke oriëntatie, innovatie en reflectie, zaken die het Politiestudiecentrum had geïntroduceerd en die in de Politieacademie door veelal academici tot wasdom werden gebracht. In de vernieuwde opleidingen groeide naast de traditionele, instrumentele taakopvatting waarin efficiëntie en doeltreffendheid centraal staan, een professionele beroepsopvatting, gericht op effectiviteit en werkzaamheid. Moderne politiemensen in opleiding moet dan ook verschillende soorten kennis worden bijgebracht: zowel de beproefde technieken zoals de meest vakbekwame collega's die in de praktijk met succes toepassen, als de inventiviteit om eigen optreden kritisch te evalueren en adequaat op de nieuwe veiligheidsbehoeften van een snel veranderende samenleving te reageren.

De huidige positionering van het politieonderwijs is het resultaat van de grote ingreep kort na de eeuwwisseling. Gekozen werd toen voor een stelsel van volwaardige beroepsopleidingen, naar analogie van dat van andere frontlijnorganisaties, maar binnen het bestaande politiebestel, gezien de bijzondere aard van het politieambt (de bevoegdheden tot opsporing en gebruik van geweld). Accreditatie van het onderwijs door een reguliere, externe organisatie zou zorgen voor een maatschappelijk erkende kwalificatiestructuur en daarmee een beter personeelsbeleid van de politie mogelijk maken. Integratie van het politieonderzoek dat vooral buiten de Politieacademie, aan enkele universiteiten, tot wasdom was gekomen, moest zorgen voor beter onderwijs en meer vakmanschap in de politiepraktijk. Naar analogie van andere hogescholen riep de Politieacademie daartoe lectoraten in het leven die op de praktijk toegesneden onderzoek, vaak in nauwe samenspraak met de praktijk, zijn gaan verrichten en in het politieonderwijs zijn gaan participeren. De huidige herinrichting van de Politieacademie beoogt de band met de beroepspraktijk en de verbinding tussen onderwijs, onderzoek en kennis te versterken.

d. Het terrein van de politieonderzoekers

Onderzoek naar het eigen functioneren en de uitkomsten van het eigen optreden zijn de afgelopen decennia een vast en onmisbaar bestanddeel geworden van een professionele politie. In reactie op de confrontaties met de opstandige jeugd in de jaren zestig en zeventig is ook in Nederland een traditie van onderzoek naar en voor de politie ontstaan die het politieoptreden en de politie-organisatie kritisch tegen het licht houdt. Soms het doorlichten van de politiële bedrijfsvoering, soms de effectiviteit van de aanpak van specifieke criminaliteit. De rellen van de jaren tachtig introduceerden het onderzoek naar grootschalig optreden bij ernstige ordeverstoringen, de IRT-affaire het onderzoek naar de opsporing en de georganiseerde misdaad, de publiciteit rond het oorlogsverleden van de politie het onderzoek naar de politiegeschiedenis. In de loop der tijd ontstonden aan enkele universiteiten groepen politieonderzoekers en vormden zich enkele gespecialiseerde, particuliere onderzoeksbureaus. Vanaf 2001 heeft Politie en Wetenschap door middel van een jaarlijkse call het politieonderzoek bevorderd en er sturing aan gegeven. Enkele jaren later stelde de Politieacademie de eerste lectoraten in. Deze gingen toegepast onderzoek verrichten en zorgden door middel van kenniskringen, participatie in het onderwijs en praktijkonderzoek voor de overdracht van kennis en inzichten aan de politie. De kracht van deze onderzoeken is dat ze direct gerelateerd zijn aan de beroepspraktijk en het onderwijs van de politie en handreikingen geven om het onderwijs en die praktijk te verbeteren en het optreden effectiever te maken. De bevindingen hebben bijvoorbeeld hun weerslag gehad op het programma tot versterking van de weerbaarheid van de politie, de organisatie van grootschalig politieoptreden bij evenementen, de aanpak van HIC zaken, de inrichting van de basisteams, de inzet van heterdaadkracht en het terugdringen van het aantal plankzaken.

3

Drie centrale vraagstukken voor de politie

Na de beoordeling en selectie van de wensen en suggesties voor onderzoek en na de schets van de context van de onderzoekspraktijk is nog een derde stap nodig om tot een samenhangende onderzoeksagenda te komen: een globale diagnose van de belangrijkste reeds te signaleren en te voorziene opgaven in de veiligheidszorg. Puttend uit het erfgoed van eerder en nog lopend onderzoek helpt zo'n diagnose hoofdzaken van bijzaken te onderscheiden en kwesties op de korte termijn van lange termijn vraagstukken. Het kader van een onderzoeksagenda laat echter niet toe om daarbij te zeer in detail te treden: de agenda zou dan gemakkelijk voorwerp van politieke of wetenschappelijke discussie worden. Daarom wordt hier volstaan met een schets van drie centrale thema's die oriëntatie kunnen bieden bij de strategische onderzoeksprogrammering.

Visies op de toekomst van de politie en haar opgaven zijn schaars. De nieuwe Nationale Politie wordt – begrijpelijk – nog sterk in beslag genomen door de opgave de eigen organisatie op orde te krijgen. Daarbij komt dat het politieke en maatschappelijke klimaat haar – evenals andere instituties – dwingt zich te richten op de korte termijn. Welke situatie men hoopt te bereiken, is een vraag die zich niet makkelijk laat stellen en die onder druk der omstandigheden zelden wordt gesteld. De politie moet meer presteren, zo luidt eenvoudig het parool. Politieoptreden dient steviger, robuuster te zijn dan we het in de tijd van ´de politie is je beste vriend´ gewend waren. Het gaat om het 'aanpakken', het leveren van 'betekenisvolle interventies', het vergroten van 'de slagkracht', het betrokken zijn 'in de operatie.'

Toch heeft de politie als maatschappelijke organisatie met als centrale opgave de (rechts)orde te handhaven behoefte aan een inschatting van de verstoringen van die orde op langere termijn teneinde zich bijtijds op het pareren van die bedreigingen in te kunnen stellen.
In het buitenland zijn dergelijke visies wel voorhanden. In België heeft een stuurgroep onder voorzitterschap van Willy Bruggeman onlangs na vier jaar studie het rapport 'Een visie voor de politie in 2025' gepubliceerd.[8] Zij heeft verschillende scenario's van de maatschappelijke ontwikkeling ontworpen, diverse modellen van de politieorganisatie tegen het licht van de verwachte opgaven en maatschappelijke problemen gehouden en uiteindelijk de conclusie getrokken dat een netwerkende organisatie het beste op de toekomst zal zijn voorbereid. In Engeland heeft een onafhankelijke onderzoekscommissie, onder voorzitterschap van de voormalige korpschef van Londen - Lord Stevens - en gesteund door een keur van wetenschappers, een vergelijkbare exercitie ondernomen. In het rapport Policing for a better Britain bepleit zij een politie die sociale cohesie nastreeft, op nieuwe manieren publiekelijk verantwoording aflegt en onder meer regelmatig de vakbekwaamheid van het personeel toetst.[9] Beide documenten zijn moedige pogingen om de toekomst van de politiezorg te verkennen maar de ontwikkelde visies zijn sterk gekleurd door de eigen inrichting van het politiebestel en de problemen waarmee de politie in die landen te kampen heeft en daarom niet zonder meer toepasbaar op de Nederlandse situatie.
In het moderne onderzoek naar en voor de politie zoals dat de afgelopen vijftig jaar - ook in Nederland - tot bloei is gekomen, worden in de regel drie deelterreinen onderscheiden: (1) de uitvoering met de daaraan verbonden kwesties van effectiviteit, bevoegdheden en integriteit, (2) de inrichting en het functioneren van de politieorganisatie en tenslotte (3) het bestel, het politiemanagement en de positie/rol/functie van de politie in de samenleving. De hiervoor geschetste context van het politieonderzoek wijst er op dat deze drie terreinen van onderzoek nog steeds relevant zijn. Voor elk van deze drie velden laat zich met het oog op de nabije toekomst een centraal vraagstuk formuleren.

(1) Wat zijn de bronnen van effectief politieoptreden?

De Nederlandse politieleiding - zowel het bevoegd gezag als de politiechefs - hecht veel waarde aan de legitimiteit van de politie. Het belang van legitimiteit wordt zelden betwist want een legitieme politie ontmoet minder weerstand als zij corrigerend optreedt en haar interventies hebben een duurzamer resultaat. Onlangs heeft een vooraanstaande politieonderzoeker echter de fundamentele vraag gesteld of de Nederlandse politie wel reden heeft zich zorgen te maken over haar legitimiteit.[10] In de meeste enquêtes eindigt de politie namelijk steevast als een van de meest gewaardeerde instanties, veelal direct na de rechterlijke macht. Affaires doen aan die waardering zelden afbreuk.
Achter het verschil van mening over de factoren die legitimiteit van de politie versterken, gaat een meningsverschil schuil met ingrijpende implicaties. Sommigen menen dat burgers beter gevolg zullen geven aan aanwijzingen van de politie en de politie meer zouden gaan waarderen als deze meer zou gaan presteren of betere resultaten zou boeken; anderen als de politie zich onbuigzamer en minder soepel zou opstellen; weer anderen als de politie bij haar optreden blijk geeft goed geïnformeerd te zijn over de onveiligheid die burgers zorgen baart; nog weer anderen als de politie zich beter aan de rechtstatelijke regels zou houden. Onderzoek naar de effectiviteit van specifiek politieoptreden dat de fundamentele aspecten niet uit de weg gaat maar ook overtuigend empirisch is gefundeerd, zou van richtinggevende betekenis kunnen zijn voor de politiepraktijk, het beleid en de samenleving.

8 D. van Ryckegem (eindred.) *Een politie in verbinding. Een visie voor de politie in 2025.* Z.p.z.j.

9 http://independentpolicecommission.org.uk/uploads/37d80308-be23-9684-054d-e4958bb9d518.pdf. Voor de wetenschappelijke studies die het rapport onderbouwden, zie: J. Brown (ed.), The future of policing. London, Routledge, 2013.

10 P. van Reenen. 'De legitimiteit van de politie is haar zorg niet. Twee stellingen beargumenteerd', in Cahiers Politiestudies 2014, nr. 31. p. 107-120.

(2) Hoe en hoezeer dient de politie de eigen organisatie en taakuitvoering aan te passen om mee te komen in de informatierevolutie?

Ontegenzeggelijk heeft de digitale informatie-uitwisseling in de samenleving en binnen organisaties de afgelopen decennia voor radicale veranderingen gezorgd. De politie participeert in deze veranderingen, zoals zij in het verleden participeerde in de opkomst van de moderne administratie en die van de telegraaf en telefoon, dat wil zeggen met enige vertraging en af en toe een misslag. De snelheid en de overvloed van het informatieaanbod dwingt tot herinrichting van de politieorganisatie, tot aanpassing van werkzaamheden en tot herverdeling van verantwoordelijkheden. Lag traditioneel het accent op het vergaren van informatie, later steeds meer op het tijdig invoeren en uitwisselen van informatie, binnenkort op het snel analyseren en beoordelen van informatie. De vorming van Real Time Intelligence Centers zijn een stap in deze richting. De ontwikkeling houdt niet voor de deur van de wijkagent halt. Deze participeert in toenemende mate zowel in de digitale wereld met zijn informatieovervloed als in de fysieke wereld die om traditionele interventies vraagt.

Ondertussen blijft de kern van het politiewerk onveranderd: het preventief en repressief optreden tegen misdragingen van burgers. De opgave voor de politie is de organisatie zo in te richten dat het uitvoerend personeel wordt ondersteund bij de uitvoering van haar taak in de veranderende samenleving. Allerlei administratieve handelingen die politiepersoneel nu nog aan het bureau binden, zouden wel eens kunnen verdwijnen. Het nog steeds gangbare onderscheid tussen strategisch, tactisch en operationeel leiderschap zou daarbij wel eens kunnen vervagen. Van personeel zouden eens andere vaardigheden en een andere opleiding kunnen worden gevraagd. Een dergelijk ingrijpend transformatieproces vergt begeleiding van onderzoek naar concrete ontwikkelingen waarbij knelpunten worden gesignaleerd, oplossingen verkend en nieuwe vormen van interventie worden geëvalueerd.

(3) Wat is de identiteit van de politie in een fragmenterende en globaliserende samenleving?

De opname van een belangrijk deel van de politie in Nederland in één nationale organisatie en bijkomende zaken als de introductie van een nieuw uniform gaan gepaard met een herdefiniëring van haar positie in de samenleving. Wat gaan burgers van die politie verwachten? Zien politiemensen zich als deel van een nationale organisatie? De identiteit van de politie was echter al eerder een nijpend vraagstuk geworden door de opkomst van de private veiligheidszorg en de bestuurlijke handhavers en door de expansie van de Koninklijke Marechaussee. Welke maatschappelijke functie is er voor een relatief goed opgeleide civiele politie die enerzijds tamelijk duur is en anderzijds niet in het hoogste geweldsspectrum kan acteren?

En als veiligheidszorg een kwestie van samenwerking is, hoe laat de rol van de politie zich dan tegenover haar partners definiëren? Het is bovendien heel wel mogelijk dat de globalisering van de samenleving de politie dwingt zich transnationaal te organiseren. Als de politieeenheid Rotterdam wordt geconfronteerd met overlast door Roemenen of Polen, heeft zij meer belang bij een steunpunt in de landen waar deze vandaan komen dan aan de band met de eenheid Noord of Amsterdam. Tegelijkertijd heeft zij bij dergelijk ‘grenzeloos’ optreden, wellicht meer nog dan voorheen, behoefte te weten voor welke waarden zij staat: wat goed, effectief en wettelijke toelaatbaar politieoptreden is.

4

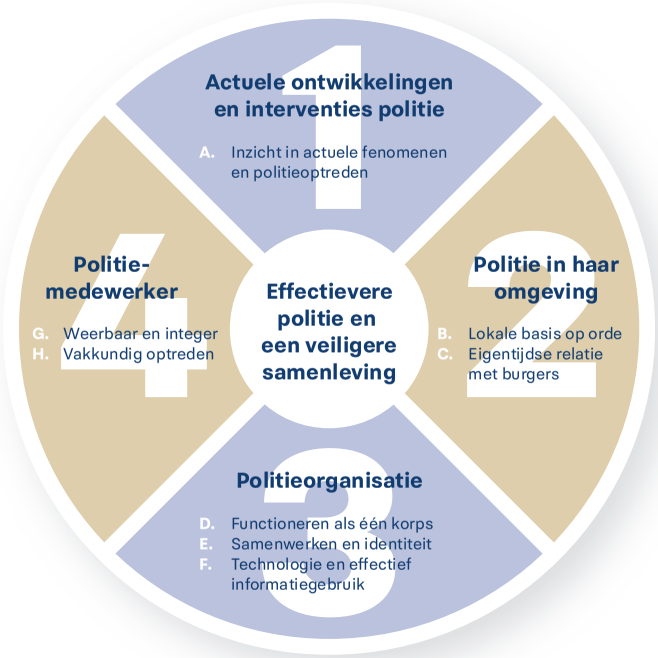
De thema’s

De consultatie van sleutelfiguren in de Nationale Politie, van managers in het politieonderwijs, van de lectoren en van academische en private politieonderzoekers leverde een groot aantal wensen en suggesties voor relevant onderzoek op. Deze onderwerpen zijn, zoals hiervoor is uiteengezet, geordend, beoordeeld en gewaardeerd. Doorslaggevend bij die waardering was dat van beantwoording van de onderzoeksvraag een bijdrage aan een effectievere politie en een veiligere samenleving kan worden verwacht. De onderwerpen zijn samengevoegd tot acht thema’s, ondergebracht in vier categorieën.







Hieronder worden de acht thema's toegelicht.

Voor elk thema geldt dat veelal zowel verkennend en analyserend als evaluerend en toetsend onderzoek wenselijk is, dat - vooruitblikkend - wordt onderzocht welke nieuwe kwesties op de politie afkomen en wat de bronnen van criminaliteit en overlast zijn. Maar ook dat - terugblikkend - wordt vastgesteld hoe effectief het politieoptreden is geweest, welke oorzaken voor criminaliteit en overlast kunnen worden vastgesteld, welke factoren het succes in de aanpak verklaren en welke lessen de politie uit de afloop zou behoren te trekken. Daarbij wordt voortgebouwd op de in de voorafgaande jaren opgebouwde kennis en inzichten. Het ´toepassingsgericht wetenschappelijk onderzoek ten behoeve van de politiepraktijk´ dat de Politieacademie en anderen verrichten, heeft nadrukkelijk ook betrekking op de gereedschapskist van politiemensen. Vragen over de methoden en technieken die de politie hanteert, zullen onderdeel van de onderzoeken zijn.

In de toelichting op elk thema wordt eerst op basis van de door de stakeholders aangedragen wensen en suggesties aangegeven welk vraagstuk het betreft. Vervolgens wordt kort vermeld welke opgave de Nationale Politie zich op dat terrein heeft gesteld. Daarna wordt in globale termen uiteengezet welke lacunes zich in de kennis op dat terrein voordoen. Duidelijk moet zijn dat de verwachte opbrengst van het onderzoek een daadwerkelijke bijdrage levert aan beter politieoptreden. Op basis van deze drie aspecten worden vervolgens enkele oriëntatievragen voor het onderzoek geformuleerd. Hiermee wordt niet beoogd het toekomstig onderzoek ´in beton te gieten´ maar enig inzicht te bieden in de richting die toekomstig onderzoek kan opgaan. Tenslotte wordt in algemene termen aangegeven welke producten het onderzoek naar dit thema zou moeten opleveren.

Actuele ontwikkelingen en interventies politie

A. Inzicht in actuele fenomenen en politieoptreden

Gesignaleerd probleem: Bij velen in het korps Nationale Politie bestaat een dringende behoefte aan onderzoek dat op korte termijn inzicht biedt in (georganiseerde) criminaliteit, in de effectiviteit van politieoptreden daartegen en in nieuwe methodes van criminaliteitsbestrijding, al dan niet samen met partners en burgers. Hoewel Nederland veiliger wordt, heerst de overtuiging dat de eisen die burgers en politici op dit vlak aan de politie stellen onverminderd groot zijn, in het bijzonder in het geval van delicten die zijn gedefinieerd als High Impact Crime (HIC): woninginbraak, straatroof, geweld, overvallen en cybercrime. Ook de ondermijnende werking van georganiseerde misdaad wordt hoog opgenomen. Intimidatie van ambtenaren en corruptie kunnen het openbaar bestuur ontwrichten. Speciale aandacht werd gevraagd voor het kindersekstoerisme en de productie van kinderporno.

Daarnaast is er ook een sterke behoefte om knelpunten in het uitvoerend politieoptreden nader te onderzoeken. Hoe kan de politie met haar beperkte middelen meer bijdragen aan de veiligheid van de samenleving, hoe kan het ‘rendement’ van haar inspanningen worden vergroot? Is de bestaande organisatie van de intake en afhandeling wel efficiënt in het licht van het hele opsporingsproces? Hoe kan de politie haar reactie op niet spoedeisende meldingen verbeteren? Hoe kan de politie samen met haar partners het best woninginbraak terugdringen? Het gaat daarbij zowel om effectieve strategieën voor de organisatie als werkbare tools voor de medewerker. De geschetste problemen beslaan het hele werkveld van de politie en vormen het hart van de Strategische Onderzoeksagenda.

Effectieve strategieën voor de organisatie én werkbare tools voor de medewerker

Taakstelling Nationale Politie: In haar realisatieplan heeft de Nationale Politie zich tot doel gesteld beter in te spelen op lokale veiligheidsproblemen en de slagkracht in de opsporing te vergroten, in het bijzonder bij gevallen van HIC en ondermijning. Voor de komende vier jaar heeft de Nationale Politie als landelijke prioriteiten gesteld ondermijning (waaronder mensenhandel), cybercrime, kinderporno, fraude en high impact crime (waaronder criminele jeugdgroepen en mobiele bendes). Daar komen de op lokaal en eenheidsniveau gestelde prioriteiten bij.

Kennis en leemte in kennis: Onderzoek naar straatroof is al enigszins gedateerd. Er is recent onderzoek naar overvallen, straatroof en geweld, maar veel minder naar de aanpak door de politie. Er is onderzoek naar (de politiële aanpak van) cybercrime maar gezien het groeiend gewicht van dit probleem blijft de behoefte daaraan groot. De aanpak van ondermijning en de bijdrage die de politie aan de RIEC’s levert, verdienen nader onderzoek. Er is recent onderzoek naar internationaal opererende buitenlandse dadergroepen die zich schuldig maken aan onder meer overvallen en woninginbraak, maar niet naar de aanpak door de politie waaronder de samenwerking met buitenlandse zusterdiensten. Onderzoek naar kindersekstoerisme ontbreekt.

Vragen ter oriëntatie:

- Welke fenomenen zoals het jihadisme komen ineens zo op dat ze een andere inzet en prioritering van de politie vragen?
- Hoe kunnen HIC zaken effectiever en efficiënter worden aangepakt? Wat is bijvoorbeeld de meest effectieve aanpak van straatroof?
- Raakt cybercrime verweven met gewone criminaliteit en wat vergt dat van de reactie van de politie?
- Hoe kan de politie effectiever optreden tegen ondermijning?
- Wat is het effect van de directe aanpak van niet spoedeisende meldingen?

Beoogd resultaat: Rond enkele thema’s is duidelijk behoefte aan verkennende studies die nieuwe (criminele) fenomenen blootleggen op een voor de politie herkenbare wijze en evaluatiestudies die knelpunten in de huidige aanpak van criminaliteit signaleren, daarvoor verklaringen bieden en concrete handreikingen geven om verbeteringen door te voeren.
Daarnaast moet vooral bij dit thema worden gezocht naar andere effectieve (bijvoorbeeld audiovisuele) vormen om nieuwe inzichten vlot aan de politiepraktijk over te dragen.

Politie in haar omgeving

B. Lokale basis op orde

Gesignaleerd probleem: De politie is een uitvoeringsorganisatie en haar lokale verankering in wijk of buurt is daarom van wezenlijk belang. Onderkent de politie de werkelijke veiligheidsproblemen in een wijk en speelt zij daar gepast op in? Heeft zij aansluiting bij de nieuwe, digitale vormen van communicatie door burgers? Onderkent zij nieuwe, digitale vormen van overlast en criminaliteit? Hoe wordt uitvoering gegeven aan de lokale integrale veiligheidsplannen? De start van de robuuste basisteams verdient alle aandacht. Hoe pakt de nieuwe inrichting uit? Hoe wordt uitvoering gegeven aan de lokale integrale veiligheidsplannen?

Van belang daarbij zijn thema´s als generale taakstelling versus specialisme, het loslaten van processcheiding als inrichtingsprincipe, het ontschotten van opsporing en blauw, de positie van de wijkagent en de nagestreefde uniformering en standaardisering van werkprocessen. Speciale aandacht verdient voorts het optreden van de politie in ´lastige´ buurten. Hoe treedt zij daadkrachtig op zonder de relatie met wijkbewoners te verliezen? Lokaal komt ook de veranderende positie van de politie in het veiligheidsdomein tot uiting: hoe wordt samengewerkt met bestuurlijke handhavers, actieve burgers en particuliere veiligheidszorg.

Hoe kan de politie beter inspelen op lokale veiligheidsproblemen?

Taakstelling Nationale Politie: De Nationale Politie heeft zich ten doel gesteld om beter in te spelen op lokale veiligheidsproblemen, in het bijzonder door lokale gezagsdragers meer invloed te schenken en burgerparticipatie te vergroten. Een bijzondere doelstelling is de ontwikkeling van een nieuwe visie op de aanpak van overlast en criminaliteit door jongeren.

Kennis en leemte in kennis: Er is vrij veel bekend over de lokale inbedding van de politie tot kort voor de start van het korps Nationale Politie, zoals de door de gemeenten ervaren afstand tot de politie en de rol van wijkagenten in buurten. Sinds de start worden zaken als de lokale inbedding van de politie, de schaalvergroting en de sterkte van de basisteams kritisch gevolgd, maar nog niet systematisch onderzocht. Er is onderzoek naar de inrichting van de politie, de plaats van de recherche in basisteams, de operationele sturing en de factoren die specialisatie bevorderen. Naar burgerparticipatie op lokaal niveau is nog weinig onderzoek gedaan. Er is onderzoek naar criminele of overlastgevende jeugdgroepen, maar gezien het belang van het thema is meer evaluatieonderzoek naar de lokale aanpak van dit probleem gewenst.

Vragen ter oriëntatie:

- Is er nieuwe onveiligheid te onderkennen op lokaal niveau die specifieke aandacht van de politie verdient? Hoe kan de nieuwe politie deze goed aanpakken?
- In hoeverre is de vraag van buiten leidend bij de inrichting van de basisteams?
- Welke impact heeft de landelijke beleidssturing en het landelijk beheer op de lokale politieprioriteiten? Krijgen het lokale gezag en de basisteamchef genoeg speelruimte?
- Behouden het bevoegd gezag en de lokale politieleiding de regie over de aanpak van de lokale veiligheidsproblemen?

Beoogd resultaat: Observatiestudies en enquêtes die het politiemanagement en landelijke en lokale bestuurders zicht bieden op de lokale verankering van de politie en suggesties aanreiken hoe die zo nodig kan worden versterkt. Surveys onder de bevolking naar de herkenbaarheid en waardering voor de basispolitieteams.

C. Een eigentijdse relatie met burgers

Gesignaleerd probleem: Aan burgers wordt een steeds actievere rol in de rechtshandhaving toegekend. Steun en medewerking van burgers wordt steeds belangrijker voor de politie. Sinds enkele jaren wordt die hulp dan ook op diverse manieren ingeroepen, met initiatieven als Meld Misdaad Anoniem, Amber-alert en Burgernet. Burgers zoeken ook direct contact met mobiel bereikbare en twitterende (wijk)agenten. Slachtoffers van delicten worden zorgvuldig opgevangen maar wensen steeds vaker ook te worden gehoord. Keerzijde van deze ontwikkeling is dat de moderne (sociale) media in een oogwenk politieoptreden scherp kunnen uitlichten en goed optreden in een kwaad daglicht kunnen stellen. Ontevreden burgers kunnen zelf voor politie gaan spelen en eigenrichting plegen. Alleen al de suggestie van etnisch profileren kan het imago van de politie aantasten en de relatie met bevolkingsgroepen ernstig verstoren.

Steun en medewerking van burgers wordt steeds belangrijker

Taakstelling Nationale Politie: Meer burgerparticipatie en dienstverlening staan hoog in het vaandel. Veel belang wordt gehecht aan de zorg voor slachtoffers, het betrekken van burgers bij de aanpak van veiligheidsproblemen in hun omgeving, de vergroting van het gemak om aangifte te doen en het informeren van burgers over de behandeling van hun aangifte.

Kennis en leemte in kennis: Over het effect van burgerparticipatie op de objectieve en subjectieve veiligheid en op het vertrouwen in de politie is weinig bekend. Burgers lijken gretig mobiel contact te zoeken met de politie maar hoeveel dit bijdraagt aan de effectiviteit van politieoptreden is niet bekend. Anonieme meldpunten lijken veel ruis te veroorzaken en maar weinig nuttige opsporingsinformatie op te leveren. Er is enig onderzoek naar ongelijke behandeling van minderheden door de politie. Niet bekend is hoe marginale groepen in de samenleving tegen de politie aankijken en welke impact slachtofferschap heeft op de aangiftebereidheid van burgers.

Vragen ter oriëntatie:

- Vergroten de nieuwe vormen van burgerparticipatie de veiligheid? Hoe kan politie dat effect versterken?
- Welke factoren in de politiële dienstverlening bevorderen de tevredenheid van burgers, het vertrouwen in de politie en de aangiftebereidheid?
- Welk beeld van de politie hebben marginale groepen in stedelijke samenlevingen? En wat betekent dit voor het optreden van de politie?

Beoogd resultaat: Er is behoefte aan verkennende studies naar hoe de politie nieuwe vormen van burgerparticipatie in haar aanpak over onveiligheid een plaats kan geven en aan een evaluatiestudie naar de werking van het dienstverleningsconcept. Wenselijk zijn ook verkenningen van het beeld van de politie bij slachtoffers van delicten en bij marginale groepen in de samenleving.

Politieorganisatie

In toenemende mate wordt een beroep op de flexibiliteit van de organisatie gedaan

D. Functioneren als één korps

Gesignaleerd probleem: De leiding van het korps Nationale Politie staat voor de opgave vijfentwintig regionale organisaties en een landelijke organisatie om te smeden tot een geheel, onder meer door te komen tot uniformering van werkprocessen. Tegelijk wordt gestreefd naar meer ruimte voor de professionaliteit van het uitvoerend personeel en komt het zwaartepunt in de organisatie te liggen bij de robuuste basisteams.

Duidelijk is ook dat in toenemende mate een beroep op de flexibiliteit van de organisatie wordt gedaan, zoals snel op- en afschalen, vlot schakelen tussen handhaving en hulpverlening en samenwerken met diverse partners. De ingrijpende veranderingen in de technische toerusting, het functioneren en de organisatorische positie die de meldkamers momenteel ondergaan, dienen hierop te worden afgestemd.

Taakstelling Nationale Politie: Eén van de drie strategische doelen die met de vorming van de Nationale Politie worden nagestreefd, is het functioneren als één korps. Daarbij wil men komen tot zowel een betere interne samenwerking, een zorgvuldige tewerkstelling van het personeel en meer flexibiliteit in het optreden als tot het bieden van betrouwbaarheid in de samenwerking met partners in de veiligheidszorg. Al deze verbeteringen moeten ook leiden tot besparingen, één van de tactische doeleinden.

Kennis en leemtes in kennis: Het WODC laat onderzoek verrichten naar de omvorming tot een nationale politie. De minister heeft opdracht gegeven tot de instelling van een cultuurmonitor die licht gaat werpen op de heersende opvattingen en het saamhorigheidsgevoel in de nieuwe organisatie. Er is slechts incidenteel onderzoek naar het optreden van de politie onder de nieuwe omstandigheden. Wel is er buitenlands onderzoek naar buitenlandse korpsen die een vergelijkbare transformatie ondergaan.

Vragen ter oriëntatie:

- Hoe wordt in de praktijk een balans gevonden tussen sturing en professionele ruimte? In welke mate is protocollering een effectief middel?
- Welke plaats krijgt de politieman/vrouw in de nieuwe organisatie? Ontstaat een nieuwe, gedeelde beroepsopvatting en hoe valt dit proces te ondersteunen?
- Hoe vinden de nieuwe meldkamers aansluiting bij de nieuwe organisatie en nieuwe technische mogelijkheden?
- Hoe kunnen interne afdelingen politiemensen in de frontlijn beter ondersteunen? Welke verbeteringen zijn er mogelijk in de planning?

Beoogd resultaat: Onderzoek zou burgers en politici een beeld moeten geven van het maatschappelijk functioneren van het nieuwe korps en het politiemanagement zicht moeten geven op opdoemende knelpunten bij de omvorming en handvatten moeten bieden om deze weg te nemen.

E. Samenwerken en identiteit

Gesignaleerd probleem: De politie is nauw verbonden met tal van instanties en organisaties, lokaal, nationaal en transnationaal, soms geïnstitutionaliseerd, soms informeel. Haar rol in de samenwerking verandert. Was zij vroeger als regisseur eerstverantwoordelijke voor de veiligheid, nu is zij soms niet meer dan eerste onder gelijken. De netwerksamenleving vergt van de politie steeds meer samenwerking. Te denken valt aan die met gemeenten en andere partners bij de integrale aanpak van onveiligheid en overlast, aan het speelveldmodel in de opsporing en aan de samenwerking in de strafrechtsketen.
Sinds het Verdrag van Amsterdam (1999) heeft de Europese Unie de mogelijkheden om snel, effectief internationaal samen te werken flink verruimd. Politie en Justitie hebben daar op gereageerd en formele en informele transnationale banden aangeknoopt. Met het Verdrag van Lissabon (2009) is een nieuwe, forse stap gezet. De nieuwe Nationale Politie moet in de komende jaren een nieuwe positie vinden in al deze veiligheidsnetwerken. Daarbij is het voor haar van belang in de samenwerking haar eigen identiteit en taakstelling te bewaren en van de verbindingen met succes gebruik te maken.

De rol van de politie in samenwerking met partners verandert

Taakstelling Nationale Politie: Versterking van de samenwerking is een thema dat direct verbonden is met de regie van het lokale bevoegde gezag en zo verweven is met tal van strategische en tactische doeleinden van de Nationale Politie. Daarbij gaat het om versterking van de strafrechtsketen, de probleemgerichte aanpak van criminaliteit en overlast en een betere verankering in samenwerkingsverbanden door een betrouwbare partner te zijn.

Kennis en leemte in kennis: Naar samenwerking en de resultaten daarvan op lokaal niveau is reeds vaak onderzoek gedaan, maar kennis over de effectiviteit van (nieuwe) vormen van samenwerking, ontbreekt grotendeels. Naar internationale politiesamenwerking is slechts incidenteel onderzoek gedaan, en dan voornamelijk op euregionaal niveau. Er is onderzoek naar de betekenis van (het vertellen van) verhalen voor de oriëntatie van politiemensen op het eigen vak.

Vragen ter oriëntatie:

- Hoe kan de regie van het lokale bevoegde gezag over de politiezorg verder worden versterkt?
- Hoe houdt de politie een scherp profiel in de diverse vormen van samenwerking? En welke inzet mag van de politie hierbij worden verwacht?
- Welke ervaringen zijn doorslaggevend voor de beroepsmatige identiteit van politiemensen?
- Welke nieuwe mogelijkheden tot transnationale samenwerking zijn werkbaar en effectief? Waar liggen de knelpunten (werkwijzen, opleidingen, infrastructuur, kennisuitwisseling)?

Beoogd resultaat: Evaluatiestudies die een overzicht bieden van de stand van zaken en handreikingen bieden voor de keuze van optimale samenwerkingsvormen, ook aan burgers en partners van de politie in de veiligheidszorg. Historisch onderzoek naar de aanloop tot de Nationale Politie, met aandacht voor de veranderingen in de regionale korpsculturen. Een studie naar vormen van internationale politiesamenwerking, belicht vanuit de werkvloer en op basis van ontwikkelingen in de (internationale) samenleving.

Een goede informatievoorziening wordt van betekenis voor besluitvormingsprocessen op alle niveaus in de organisatie

F. Technologie en effectief informatiegebruik

Gesignaleerd probleem: De laatste jaren neemt de technologie die de effectiviteit van politieoptreden vergroot, zoals GPS, ANPR, sensoren en drones, een hoge vlucht. Ook de mogelijkheid om big data te doorzoeken opent nieuwe mogelijkheden voor de politie. Tegelijk dwingt de beschikbaarheid van eindeloze hoeveelheden informatie in de samenleving en bij instituties en organisaties de politie tot het verleggen van het accent van het vergaren van informatie – haar traditionele focus – naar het beschikbaar stellen van de juiste informatie op de juiste plek op het juiste moment. De organisatie moet flexibeler worden, medewerkers moeten meer verantwoordelijkheid krijgen en dan ook meer professionaliteit tonen. Hoewel informatie altijd al belangrijk voor de politie was, wordt nu van haar gevergd een data-driven organisatie te worden. Een goede informatievoorziening wordt van betekenis voor besluitvormingsprocessen op alle niveaus in de organisatie. En niet alleen bij technisch sterk gespecialiseerd politiewerk als het forensisch onderzoek, maar ook bij het alledaagse politiewerk op straat.

Taakstelling Nationale Politie: De Nationale Politie heeft als operationele doelen een betere Informatievoorziening en ICT en beter informatiegestuurd werken. Beide doelstellingen moeten eerst en vooral in de basisteams worden verwezenlijkt. Voorts wil het korps meer interventiekracht op de fysieke en virtuele infrastructuur verkrijgen. De informatievergaring moet onder meer verbeterd worden door de installering van nieuwe tech- nieken zoals sensing; de verbeterde analyse en distributie van informatie moeten leiden tot een slagvaardiger optreden tegen ondermijning.

Kennis en leemte in kennis: De technieken van informatie-uitwisseling ontwikkelen zich razendsnel: analyse van big data, mobile devices, gamification en social media. In vergelijking met de samenleving staat de politie nog steeds op achterstand, zowel bij de inlijving van deze technologie in de werkprocessen als bij de kennisontwikkeling. Die kennis betreft de mogelijkheden van de technieken voor de eigen organisatie, de consequenties voor het eigen functioneren maar ook de mogelijkheden die de nieuwe technologieën aan criminelen bieden en de nieuwe risico's die zulke criminele praktijken met zich meebrengen.

Vragen ter oriëntatie:

- Wat betekent de digitalisering en de dynamiek daarvan voor de taakontwikkeling bij de politie en voor de vertaling daarvan naar het onderwijs?
- Hoe loopt besluitvorming binnen de politie-operatie, welke informatie helpt politiemensen daarbij werkelijk en hoe kan in die informatie zo efficiënt mogelijk worden voorzien?
- Hoe kan informatievoorziening en ICT de integrale, probleemgerichte aanpak van criminaliteit en overlast verder versterken?
- Wat betekent het voor het uitvoerende politiepersoneel om in een data-driven omgeving het reguliere corrigerende werk te doen?
- Hoe wordt in zo'n werkomgeving de dienstbaarheid aan het publiek vormgegeven?

Beoogd resultaat: De technologie die het politiële informatiegebruik kan verbeteren, wordt door de markt ontwikkeld. Duidelijk is dat verbetering niet een eenvoudig implementatievraagstuk is en kostbaar is. Het voornaamste knelpunt is het gebruik van informatie. Onderzoek kan de implementatie begeleiden, opdat deze tot werkelijke verbeteringen in de uitvoering leidt, maar ook zicht bieden op de consequenties voor burgers, de samenleving in zijn geheel en de politie zelf.

Politiemedewerker

Van politiepersoneel wordt ook weldoordachte weerbaarheid en onkreukbaarheid verwacht

G. Weerbaar en integer

Gesignaleerd probleem: Politiemensen worden geconfronteerd met assertieve, door moderne communicatiemiddelen verbonden burgers en snelle, onberekenbare massamedia. Van de politie wordt meer dan enige jaren geleden corrigerend optreden gevraagd – het hart van het politiewerk – en dat roept (ook) meer dan in het verleden onvoorspelbare reacties op. Er lijkt een verschuiving gaande van ´een beroep met risico op incidenteel geweld' naar 'een hoog risico beroep´. De bedreiging van politiemensen strekt zich soms ook uit tot de privésituatie. Weerbaarheid heeft de laatste jaren hoog op de agenda gestaan en dat zal naar verwachting zo blijven.

Van politiepersoneel wordt niet meer alleen incasseringsvermogen en veerkracht gevergd, maar ook weldoordachte weerbaarheid en onkreukbaarheid. Integriteit is een kwestie van aanhoudende zorg voor de politie, zeker gezien het reeds vermelde fenomeen ondermijning, en heeft nadrukkelijk raakvlakken met de cultivering van een gedeelde beroepsopvatting binnen de Nationale Politie en de ruimte om binnen de organisatie schendingen van integriteit te bespreken en aan te kaarten. De opmars van digitale communicatie in het persoonlijk leven van burgers en politie stelt nieuwe eisen aan de behandeling van vertrouwelijke informatie.

Taakstelling Nationale Politie: In het realisatieplan heeft het korps zich tot doel gesteld dat het het gezag van de politie in de openbare ruimte wil vergroten, dat wil zeggen haar zichtbaarder en weerbaarder wil maken.

Kennis en leemten in kennis: Er is behoorlijk veel onderzoek gedaan naar geweld tegen politiepersoneel. Naar het gezag van de politie onder de burgers is (veelal kwalitatief) onderzoek gedaan; de laatste jaren ook naar de pendant: de weerbaarheid van het politiepersoneel. Gezien het belang van de veerkracht van politiemedewerkers blijft dat laatste onderwerp van belang. Ook culturele aspecten van het beroep, zoals de uitwisseling van ervaring middels een vertelcultuur op de bureaus, zijn onderzocht. In het verleden is vrij veel onderzoek gedaan naar integriteit en de interne meldingsbereidheid, waaruit grote regionale verschillen naar voren kwamen. De huidige toestand is niet bekend.

Vragen ter oriëntatie:

- Wat zijn de effecten van genomen maatregelen om de veerkracht en de weerbaarheid te vergroten (training, uniform, bewapening, teamvorming, preventie, nazorg)?
- Hoe ontwikkelt zich de bereidheid om integriteitschendingen te bespreken?
- Welke risico's met betrekking tot hun integriteit lopen politiemensen bij samenwerking met externe deskundigen en tolken?

Beoogd resultaat: Onderzoeksrapporten die de politieleiding inzicht geven in de ontwikkeling van de arbeidsomstandigheden, de omgangsvormen en de beroepsopvatting in het nieuwe korps. Daarnaast moet ook bij dit thema worden gezocht naar andere effectieve (bijvoorbeeld audiovisuele) vormen om nieuwe inzichten aan de politiepraktijk over te dragen.

Het beste politiekorps is het korps dat in staat is om te blijven leren

H. Vakkundig optreden

Gesignaleerd probleem: De laatste decennia is de politie verder geprofessionaliseerd. Van een overwegend reactieve dienst is zij een organisatie geworden die op nieuwe ontwikkelingen inspeelt, het eigen optreden – ook als sprake is van integrale samenwerking met andere instanties – evalueert of laat evalueren en dat vervolgens aanpast zodat effectiever tegen criminaliteit en overlast kan worden opgetreden. Het parool is: “Het beste politiekorps is het korps dat in staat is om te blijven leren.” In de politie bestaan reeds veel formele opleidingsprogramma’s: leergangen die leiden tot een bepaalde vorm van certificering voor het politiewerk.

De laatste jaren is er steeds meer aandacht voor informele manieren van leren. Voorbeelden zijn de briefing voorafgaande aan een actie, oefenen met gevaarsbeheersing voorafgaande aan en tijdens een interventie, verhooroefeningen als onderdeel van een concrete zaak, intervisietrajecten in basisteams (blauw vakmanschap), peer reviews van commandanten grootschalig politieoptreden en gezamenlijk werken aan een probleemgerichte aanpak in de basisteams. Deze leervormen krijgen extra betekenis nu het streven is de politieopleiding dichter naar de politiepraktijk te brengen.

Taakstelling Nationale Politie: Een van de twee hoofddoelstellingen van de Nationale Politie is vergroting van de ruimte voor professioneel politieoptreden. Dit moet worden bereikt door medewerkers meer centraal te stellen, het leiderschap dichter naar het operationele optreden te brengen en bovenal het vakmanschap van het politiepersoneel te vergroten. Nadrukkelijk wordt ook onderkend dat het personeelsbeleid het bereiken van deze doelstelling moet ondersteunen. De opleiding zal dichter naar de praktijk worden gebracht.

Kennis en leemtes in kennis: Grootschalig politieoptreden dat maatschappelijke beroering heeft gewekt, wordt vaak geëvalueerd. Door middel van peer reviews, after-action reviews en leer- arena’s wordt voor overdracht van ervaring gezorgd. Dergelijk onderzoek is van blijvend belang maar in hoeverre ook op langere termijn sprake is van lessons learned is onduidelijk. In de opsporing worden – mede uit vrees voor tunnelvisie – onderzoekers als tegensprekers ingezet. In beide gevallen is onduidelijk welke impact dit leren heeft op de langere termijn.
Er is recent onderzoek naar de briefing, naar verhalende ervaringsoverdracht en naar de impact van schietvaardigheidstraining.

Vragen ter oriëntatie:

- Hoe kan leren op de werkplek het meest efficiënt en effectief vorm krijgen? In hoeverre maakt de politie bij het probleemgerichte optreden gebruik van de resultaten van wetenschappelijk onderzoek (evidence based policing)?
- Hoe staat het met de kwaliteit van de processenverbaal en hoe kan deze worden verbeterd?
- Wat zijn de effecten van de invoering van flex-ME?
- Hoe kan op de werkvloer meer profijt worden getrokken uit onderzoeksresultaten?
- Hoe snel kan nu kennis voor de praktijk worden gemobiliseerd en hoe kan de organisatie daarvan worden verbeterd?

Beoogd resultaat: Observatiestudies naar de implementatie van best practices. Evaluatiestudies van de impact van lessons learned op de langere termijn.
Voorts zou kunnen worden onderzocht of de peer review methode buiten het domein van het grootschalig optreden een effectieve vorm van ervarings- en kennisoverdracht is.

5

Doorwerking van de agenda

Diverse werkvormen moeten de overdracht van kennis naar onderwijs en praktijk bevorderen

a. Uitvoering

De Strategische Onderzoeksagenda voor de Politie is opgesteld door de Politieacademie en wordt vastgesteld door de minister van Veiligheid en Justitie, na advies over de thema's te hebben ingewonnen bij de Politieonderwijsraad.[11] De Politieacademie werkt daarop de agenda jaarlijks uit in een onderzoeksprogramma. Dat programma wordt vastgesteld door de directeur van de Politieacademie. De lectoren en onderzoekers van de Politieacademie zullen, op basis van de aldaar aanwezige kennis en kunde, een deel van het programma uitvoeren.

Het resterende deel zal door middel van een jaarlijkse call worden uitbesteed aan onderzoekers buiten de Politieacademie. De Commissie Kennis en Onderzoek van de Politieonderwijsraad verzorgt de uitbesteding en begeleidt de uitvoering en de oplevering van deze onderzoeken. Omdat bij de lectoraten en in de programmering van de Commissie een aantal eerder gestarte onderzoeken nog doorlopen en de Call 2014 wordt uitgebracht voordat de Onderzoeksagenda formeel is vastgesteld, zal 2015 een overgangsperiode zijn.

b. Valorisatie

De Strategische Onderzoeksagenda beoogt het toepassingsgericht wetenschappelijk onderzoek naar en voor de politie te bevorderen en de doorwerking van de uit dit onderzoek opgedane kennis naar (politie) praktijk en onderwijs sterk te verbeteren. Dat laatste thema is complex en heeft al langer de aandacht van bestuurders, politieleiding en onderzoekers, in Nederland en in het buitenland. Een moderne politie kan niet goed functioneren zonder begeleidend onderzoek, maar het aantal significante vernieuwingen die voortkwamen uit (wetenschappelijk) onderzoek en vervolgens breed ingang vonden in de politie, is beperkt. Meestal was sprake van onderzoekers die gelijk optrokken met vernieuwers in de politie en een verkennende, begeleidende en evaluerende rol speelden. Volharding bleek veelal onontbeerlijk. Voorbeelden van dergelijke vernieuwingen zijn de introductie van de wijkteams, de de-escalerende aanpak van grootschalige ordeverstoringen, de bestrijding van georganiseerde misdaad en de aandacht voor slachtoffers. Hoewel iedere kennisvraag zijn eigen onderzoeksdesign met zich meebrengt, zal de Politieacademie zich, vanwege haar unieke positie dicht tegen de politiepraktijk aan, sterk richten op het uitvoeren van op toepassing gericht wetenschappelijk onderzoek in en in samenwerking met de politiepraktijk.

De lectoraten van de Politieacademie hebben in de afgelopen jaren diverse werkvormen ontwikkeld om de overdracht van kennis naar de politiepraktijk en het onderwijs te bevorderen zoals peer review trajecten in het crowd management, actie-onderzoek in het basispolitiewerk, lectorale colleges in het politieonderwijs en het opzetten van modules, het maken van lesbrieven en de formulering van een canon van de professionele literatuur voor politiedocenten. Niettemin bleek uit de visitaties van de lectoraten dat de transfer van kennis, in het bijzonder naar het onderwijs, voor verbetering vatbaar is. In de programmatische uitwerking van de Strategische Onderzoeksagenda zal hier daarom expliciet aandacht aan worden besteed. Daarbij wordt gedacht aan promotieonderzoek naar verbetering voor deze transfer, aan structurele participatie van docenten in onderzoek van de lectoraten, aan onderzoekers van de universiteiten en onderzoeksinstituten die embedded toetsend onderzoek in de politie verrichten en aan alternatieven voor de publicatie van onderzoeksresultaten in traditionele boekvorm.

11 Kamerstukken II, 2012/13, 29 628, nr. 388, blz. 8.

Colofon

Uitgave :	Politieacademie
Datum :	Juni 2015
Oplage :	200 exemplaren
Productiebegeleiding :	Communicatie & Marketing, Politieacademie
Vormgeving :	CLIC-design bv, Enschede
Fotografie :	Hollandse Hoogte, Amsterdam Beeldbank Politie
Drukwerk :	De Bondt, Barendrecht
Voor reacties, vragen of exemplaren :	directie.oko@politieacademie.nl

0388

www.politieacademie.nl

« waakzaam en dienstbaar »

15-049-03

Van: 10.2.e
Verzonden: dinsdag 9 mei 2017 23:44
Aan: Plas, Theo van der (T.G.)10.2.e @politie.nl>
Onderwerp: FW: Stukken onderzoekslijn Technologie en Informatiegebruik

Neem aan dat jij deze misschien al hebt?

Groet,

10.2.e

10.2.e
9
Staf KL, Directie Operatiën
Nieuwe Uitleg 1, 2514 BP Den Haag
Postbus 17107, 2502 CC Den Haag

Van: Plas, Theo van der (T.G.)
Verzonden: dinsdag 9 mei 2017 23:48
Aan: 10.2.e
Onderwerp: RE: Stukken onderzoekslijn Technologie en Informatiegebruik

Hallo10.2.e ik ken het niet en 12-14
. Zal ik met Marjolein bespreken ? groeten, Theo

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

Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20301 2500 EH Den Haag

de Nationale politie
Postbus 17107
2502 CC Den Haag

Staf Korpsleiding politie
DIV
Docnr. .....
Ingekomen 11 MEI 2017
Zaaknr. .....-002103
TJZ
CC Cors

Directie Wetgeving en Juridische Zaken
Sector straf- en sanctierecht

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

Contactpersoon
9
Raadadviseur

M +31 6 10.2.e
9 @minvenj.nl

Ons kenmerk
2068042

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

Datum 10 mei 2017
Onderwerp Ontwerp- besluit onderzoek in een geautomatiseerd werk

Hierbij zend ik u ter advisering toe het ontwerp- besluit onderzoek in een geautomatiseerd werk.

Uw reactie op het ontwerp- besluit onderzoek in een geautomatiseerd werk ontvang ik zowel schriftelijk als elektronisch graag vóór 7 juli 2017. Mocht ik voor deze datum geen advies van u hebben ontvangen, dan ga ik ervan uit dat u geen prijs stelt op advisering over het voorstel.

Omdat het advies op internet wordt gepubliceerd, verzoek ik u in verband met de privacy om geen persoonlijke gegevens in het advies of bij de referentiegegevens op te nemen.

Ik zie uw reactie met belangstelling tegemoet.

De Staatssecretaris van Veiligheid en Justitie,
namens deze,

10.2.e

Directeur Wetgeving en Juridische Zaken

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