Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

36 263 Regels inzake specifieke wettelijke voorzieningen voor het uitvoeren van onderzoeken door de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen (Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma)

Nr. 9 **NOTA NAAR AANLEIDING VAN HET VERSLAG**

Ontvangen 4 september 2023

Inhoudsopgave

I. Algemeen deel 2
1. Inleiding 14
2. Inhoud van het wetsvoorstel op hoofdlijnen 21
2.1 Inleiding 21
2.2 Integrale wijze van onderzoek in het cyberdomein en gegevensverwerking 24
2.2.3 De wijze van verwerking van gegevens 27
2.3 Overzicht van de voorgestelde maatregelen 28
2.4 De verhouding van de Tijdelijke wet tot de Wiv 2017 32
3. De maatregelen nader beschouwd 42
3.1 De reikwijdte van de wet 43
3.2 verkennen van en binnendringen in een geautomatiseerd werk 45
3.2.1 Verkennen van een geautomatiseerd werk 51
3.2.2 Technische risico's 52
3.2.3 Verduidelijking bijschrijfmogelijkheid 53
3.3 Onderzoeksopdrachtgerichte (OOG) interceptie en GDA 56
3.3.1 Het verkennen ten behoeve van OOG-interceptie 65
3.4 Bijschrijfmogelijkheid artikel 47 Wiv 2017 67
3.5 Bijschrijfmogelijkheid artikel 54 Wiv 2017 70
4. Toets en toezicht en de mogelijkheid van beroep op de Afdeling bestuursrechtspraak van de Raad van State 72
4.1 Inleiding 72
4.2 Bindend toezicht door de afdeling toezicht van de CTIVD 77

kst-36263-9
ISSN 0921 - 7371
's-Gravenhage 2023

4.3 Beroep op de Afdeling bestuursrechtspraak 43
5. Grondrechtelijke en mensenrechtelijke aspecten 91
6. Gevolgen verbonden aan de uitvoering van de wet 103
6.1 Algemeen 103
6.2 De uitvoeringsconsequenties voor de TIB, de CTIVD en de Afdeling bestuursrechtspraak van de Raad van State 103
7. Advies en consultatie 107
7.1 Algemeen 107
7.2 De reactie van de TIB 108
7.3 Overige reacties (burgers en NGO's) 108
II. Artikelsgewijze toelichting 109

I. Algemeen deel

Wij hebben met veel belangstelling kennis genomen van de vragen en opmerkingen van de leden van de fracties van de VVD, D66, CDA, SP, PvdA, GroenLinks, PvdD, CU, SGP, Volt en BBB. Wij gaan daar graag op in. Daarbij zal zoveel mogelijk de indeling van het verslag worden gevolgd. Waar dat dienstig is zullen gelijkluidende vragen van de leden van de diverse fracties worden samengenomen en worden beantwoord. Er zijn in het verslag diverse vragen gesteld over de nota van wijziging en de Hoofdlijnennotitie. Deze beide documenten zijn gelijktijdig met deze nota naar aanleiding van het verslag aan de Tweede Kamer aangeboden. Kortheidshalve is naar de inhoud daarvan verwezen.

De leden van de VVD-fractie hebben met veel waardering en interesse kennisgenomen van het wetsvoorstel. Zij benadrukken dat de (digitale) dreiging van landen met een offensief cyberprogramma toeneemt en dat daarmee de Nederlandse (veiligheids)belangen in zowel nationaal als internationaal verband onder druk komen te staan. Zij achten het dan ook noodzakelijk om de juiste randvoorwaarden te scheppen voor de effectieve taakuitvoering van de Nederlandse inlichtingen- en veiligheidsdiensten in het cyberdomein, zodat daarmee de toenemende (digitale) dreigingen het hoofd kunnen worden geboden en de nationale veiligheid beter kan worden gewaarborgd. Zij van mening dat het voorliggende wetsvoorstel de diensten daartoe in staat stelt.

De leden van de D66-fractie geven aan kennis te hebben genomen van het wetsvoorstel en onder andere vragen te hebben over de reikwijdte, technische aspecten, nadere verduidelijking en proportionaliteit van het voorliggende wetsvoorstel.

Zo vernemen deze leden graag van de regering of de dreiging van landen met een offensief cyberprogramma nog even groot is als toen de wet werd aangekondigd. Wij reageren hierop graag als volgt. De dreiging van landen met een offensief cyberprogramma tegen Nederland en Nederlandse belangen is onverminderd groot. In dit verband wordt verwezen naar de jaarverslagen van de AIVD en MIVD over het jaar 2022. De knelpunten die met de Tijdelijke wet opgelost moeten worden, worden groter. De cyberdreigingen zijn in de afgelopen jaren toegenomen, terwijl het zicht op de dreiging van landen met een offensief cyberprogramma verder is afgenomen.[1] Landen als China, Rusland, Iran en Noord-Korea zetten op grote schaal digitale aanvallen in. Deze landen opereren offensief, opportunistisch en houden zich niet aan de rechtstatelijke principes en regels zoals wij dat doen. Doelwitten zijn persoonsgegevens, belangrijke hightech innovaties, politieke standpunten, militaire

[1] AIVD Jaarverslag 2022 (pag. 29) en MIVD Jaarverslag 2022 (pag. 31).

geheimen, kwetsbaarheden van onze vitale infrastructuur, informatie over dissidenten en nog veel meer. Het gaat dus om economische schade, militaire schade, fysieke schade en/of geopolitieke schade veroorzaakt bij zowel Nederlandse organisaties als ook individuele Nederlanders. Bijvoorbeeld doordat routers van Nederlanders worden gebruikt vanuit Rusland door hackers van de GRU. Of doordat persoonsgegevens van Nederlandse burgers worden buitgemaakt. De AIVD zag dit in 2022 gebeuren toen verschillende landen met offensieve cyberprogramma's probeerden data te stelen in de (Europese) reis- en luchtvaartsector (Jaarverslag 2022). Ook hebben de diensten in het afgelopen jaar gezien dat Russische staatshackers een cyberoperatie aan het voorbereiden waren waarbij de website van een Nederlandse overheidsinstelling zou worden misbruikt. De hackers maakten een kopie van deze overheidswebsite om bezoekers daarvan te kunnen infecteren met malware om ze hiermee te kunnen bespioneren. In potentie kunnen de gegevens van Nederlandse burgers die hackers buitmaken gebruikt worden voor allerlei doeleinden. Een ander goed voorbeeld zijn Russische desinformatiecampagnes rond MH17. Voor landen met een offensief cyberprogramma kunnen Nederlandse burgers een middel zijn om bepaalde doelen (beïnvloeding, spionage, sabotage) te bereiken. De Nederlandse infrastructuur is hier bij uitstek in het vizier vanwege het feit dat Nederland in het wereldwijde communicatienetwerk een belangrijk knooppunt is. Landen zetten een offensief cyberprogramma in de vorm van cyberoperaties veelal in als onderdeel van een bredere offensieve strategie, waarbij ook andere – meer klassieke – operaties worden ingezet, teneinde hun geopolitieke doelstellingen te bereiken. Deze operaties vormen ook onderdeel van een militaire strategie. Deze aanpak van die landen wordt ook wel een whole-of-society approach genoemd. Dat vergt van de AIVD en MIVD een integrale wijze van onderzoek naar die landen waar de dreiging vanuit gaat. De diensten doen daarbij onderzoek naar hun doelwitten, intenties, capaciteiten en wijze van aansturing. Om deze vragen te kunnen beantwoorden is het nodig om naar meer dan alleen de specifieke cyberaanval te kijken. Cyberaanvallen worden niet uitgevoerd als doel op zich, maar als onderdeel van een integrale strategie. De diensten moeten dan ook integraal onderzoek doen naar het land achter de aanval, zodat zij zicht krijgen op de herkomst, aansturing, politieke intenties, doelwitten en slachtoffers van de cyberaanvallen. Het is nodig zicht te krijgen op welke infrastructuur cyberactoren gebruiken, welke personen of organisaties daarachter zitten en wat hun modus operandi is. Pas dan kunnen de diensten beter zicht krijgen op de dreiging die van de landen uitgaat. Dat zicht hebben de diensten nu onvoldoende. Deze wet gaat daar een belangrijke bijdrage aan leveren.

Om de AIVD en de MIVD aan hun wettelijke taak te kunnen laten voldoen, is het noodzakelijk bestaande bevoegdheden op een effectieve wijze in te kunnen zetten tegen deze landen. Het huidige wettelijke kader sluit onvoldoende aan bij de cyberdreiging en het type onderzoek naar landen met een offensief cyberprogramma. Zoals ook in de memorie van toelichting aangeven, zijn er een aantal knelpunten die er in de praktijk voor zorgen dat de dreiging die vanuit statelijke actoren uitgaat onvoldoende effectief door de diensten kunnen worden onderkend, onderzocht en tegengegaan. Dat komt omdat een aantal bevoegdheden op een beperkte wijze kunnen worden uitgeoefend. Iedere bevoegdheid die de diensten tot hun beschikking hebben om onderzoek te doen naar dreigingen zijn ieder op zich noodzakelijk en hebben hun eigen, unieke meerwaarde. Zo zijn bulkdatasets noodzakelijk omdat hiermee bijvoorbeeld de koppeling gemaakt kan worden tussen target en telefoonnummer. Of is onderzoek op de kabel nodig om de verborgen dreiging te zien die daar voorbij komt, zoals een aanval van een nog onbekend Russisch target. Het gaat hierbij om de puzzelstukjes die de puzzel

compleet kunnen maken. Zonder deze puzzelstukjes geen goed zicht. In de praktijk blijkt dat als gevolg van de eerdergenoemde knelpunten waardevolle bulkdatasets moeten worden vernietigd, dat hackoperaties hortend en stotend op gang komen en worden uitgevoerd of helemaal niet kunnen worden opgestart en dat OOG-interceptie op de kabel niet goed van de grond komt.

Dat deze bevoegdheden niet effectief kunnen worden ingezet klemt extra, omdat het bij dit soort complexe onderzoeken gaat om de inlichtingenmiddelenmix, waarbij elke bevoegdheid die voor dit soort onderzoeken wordt ingezet, het geheel effectiever maakt. Dat is onderdeel van de eerder genoemde integrale wijze van onderzoek doen. Het één kan niet zonder het ander. Als een bevoegdheid niet kan worden ingezet of wegvalt, kan dat worden vergeleken met het vallen van dominosteen dat effect heeft op het hele onderzoek. Een afnemende effectiviteit van elk van deze middelen heeft een negatieve consequentie voor het werk van de diensten en de combinatie daarvan versterkt dat alleen maar ten negatieve. Zo kunnen bijvoorbeeld bulkdatasets niet worden gebruikt om een koppeling te kunnen maken tussen een target en een kenmerk, waardoor een hackoperatie niet kan worden gestart. Ook kan bijvoorbeeld niet via kabelinterceptie worden opgemerkt dat een bepaald target een kenmerk heeft waardoor deze kan worden gehackt.
De Tijdelijke wet treft enkele regelingen die bovengenoemde knelpunten moet oplossen. Het is deze combinatie van maatregelen en inzet van inlichtingenmiddelen die de diensten effectiever maken in hun onderzoeken naar landen met een offensief cyberprogramma. Alleen dan is het mogelijk zicht op de dreiging van deze landen op te bouwen en de verborgen dreiging gekend te maken. Bij die ongekende of verborgen dreiging weten de inlichtingen- en veiligheidsdiensten dat er een dreiging is, maar is nog niet bekend hoe deze dreiging eruitziet, hoe deze zich technisch manifesteert en welke personen of organisaties te identificeren zijn.

De leden van de D66-fractie vragen voorts of er verschuivingen hebben plaatsgevonden in de landen waar de dreiging vandaan komt sinds de aankondiging van het voorstel. Ook vragen zij of nader uiteengezet kan worden welke landen onder «landen met een offensief cyberprogramma» vallen. Is, aldus deze leden, deze term dynamisch en betekent dit dat eventueel andere dan de in de memorie van toelichting genoemde landen, hieronder kunnen worden geschaard als de omstandigheden daartoe aanleiding geven. In dit kader vragen zij ten slotte voorts of ook NAVO- of EU-landen hier theoretisch onder kunnen (gaan) vallen. Op dit samenhangende complex aan vragen willen we graag als volgt reageren. De specifieke landen met een offensief cyberprogramma waar op dit moment actief onderzoek naar wordt gedaan door de diensten worden genoemd in de staatsgeheim gerubriceerde bijlage bij de Geïntegreerde Aanwijzing (GA). In de memorie van toelichting bij het voorstel van de Tijdelijke wet worden twee voorbeelden genoemd: China en Rusland. In het jaarverslag 2022 van de AIVD worden ook Iran en Noord-Korea genoemd. De diensten doen ook onderzoek naar cyberdreigingen en cyberaanvallen afkomstig van statelijke actoren of (criminele) organisaties die cyberaanvallen uitvoeren als deze direct gericht zijn op Nederland of Nederlandse belangen. Hieronder valt ook de ongekende digitale dreiging gericht tegen Nederland of Nederlandse belangen. Of en, zo ja, welke verschuiving heeft plaatsgevonden kan vanwege het genoemde staatsgeheime karakter ervan – anders dan hetgeen reeds in de openbaarheid is gebracht – niet worden benoemd. Gelet op de – in de woorden van deze leden – dynamisch gekenschetste term, is het zeker mogelijk dat omstandigheden aanleiding kunnen geven om andere – dan de in de toelichting en het jaarverslag genoemde – landen onder de term «landen met een

offensief cyberprogramma» te scharen. Zoals eerder aangegeven, bepaalt de GA naar welke landen met een offensief cyberprogramma de diensten onderzoek doen, maar ook de GA kan op dit punt worden aangepast als omstandigheden daartoe aanleiding geven. De diensten hebben in de GA ook de opdracht gekregen om onderzoek te doen naar de (op dit moment) ongekende dreiging. Dit kunnen dreigingen zijn die nog niet geattribueerd kunnen worden aan een al gekende statelijke actor met een offensief cyberprogramma genoemd in de GA, of dreigingen die komen van statelijke actoren waarvan tot nu toe onbekend was dat zij een dreiging vormden tegen Nederland of Nederlandse belangen. Dit kunnen ook NAVO- of EU-landen zijn, indien deze landen een offensief cyberprogramma hebben dat gericht is op Nederland of Nederlandse belangen en de GA de diensten de opdracht geeft hier onderzoek naar te doen. De Kamer wordt hierover geïnformeerd via de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD).

De leden van de D66-fractie wijzen erop dat volgens de memorie van toelichting het bestaande regime van de Wiv 2017 de inlichtingendiensten belemmert om onderzoek naar landen met een offensief cyberprogramma effectief uit te kunnen voeren. Deze leden verzoeken de regering aan te geven of de inlichtingendiensten met de voorliggende tijdelijke wet dit onderzoek wel effectief kunnen uitvoeren. In het wetsvoorstel zijn diverse elementen opgenomen die deze belemmeringen weg kunnen nemen en de effectiviteit van de inzet vergroten. Bij de totstandkoming van het wetsvoorstel zijn zowel diensten, departementen als de TIB en CTIVD op een constructieve wijze betrokken. Dit geeft vertrouwen dat met dit wetsvoorstel het doel van grotere effectiviteit van de diensten bereikt kan worden. Voor wat betreft uitvoering geldt dat het concept wetsvoorstel op uitvoeringseffecten is getoetst. De uitkomsten hiervan zijn zo goed mogelijk in het uiteindelijke wetsvoorstel verwerkt. Dit geeft ook ten aanzien van de uitvoerbaarheid van het wetsvoorstel het benodigde vertrouwen.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel en onderkennen dat het van groot belang is dat de AIVD en MIVD met adequate bevoegdheden zijn toegerust om onderzoek te doen naar landen met een offensief cyberprogramma. In dat kader herinneren zij aan de motie-Van der Staaij c.s.[2] Deze leden willen meegeven dat wanneer dergelijke landen erin slagen om vertrouwelijke informatie, economische en technologische kennis te bemachtigen, dit niet alleen het vrije maatschappelijk verkeer van onze inwoners schaadt en schendt maar ook een enorme inbreuk op de burgerrechten van onze inwoners betekent. Naar het oordeel van deze leden is het dan ook een valse tegenstelling dat het hier zou gaan om een uitruil tussen burgerrechten en veiligheid. De diensten moeten dan ook zo snel mogelijk in staat worden gesteld te handelen op dreigingen van landen met een offensief cyberprogramma. Wij steunen deze reactie.

De leden van de CDA-fractie wijzen erop dat technologische ontwikkelingen snel gaan en vragen in dat verband in hoeverre deze wet voldoende ruimte voor de veiligheidsdiensten geeft om te kunnen opereren tegen dreigingen uit landen met een offensief cyberprogramma die gebruik maken van nieuwe technologische ontwikkelingen om informatie te vergaren en te verwerken. Wij antwoorden graag als volgt. Dit wetsvoorstel stelt de AIVD en MIVD in staat effectiever onderzoek te doen naar landen met een offensief cyberprogramma. Juist in het cyberdomein zijn wendbaarheid en snelheid cruciaal. De Wiv 2017 biedt – zo blijkt ook uit het ECW-rapport – deze snelheid en wendbaarheid

[2] Kamerstukken II 2021/2022, 36 045, nr. 16.

onvoldoende, waardoor de diensten onvoldoende in staat zijn de cyberdreiging op een adequate manier te onderzoeken en tegen te gaan. Dit wetsvoorstel beoogt die ruimte wel te bieden. De desbetreffende landen opereren steeds geavanceerder en de technische omgeving waarbinnen zij opereren wijzigt constant. Het is daarom van belang de onderzoeksmethoden van de diensten hierop aan te passen en tijdens onderzoeken te kunnen meebewegen in een dynamisch en veranderlijk domein. Dit is nodig om zicht te houden, maar in veel gevallen juist zicht te krijgen op de doelwitten, intenties, technische capaciteiten en wijze van aansturing en daarmee de dreiging van landen met een offensief cyberprogramma.

De leden van de CDA-fractie wijzen erop dat de Afdeling advisering het geen gegeven acht dat met de voorgestelde maatregelen de beoogde operationele snelheid en wendbaarheid zal worden bereikt en dat, gelet daarop, de Afdeling het van groot belang acht dat de maatregelen tijdens de looptijd van de tijdelijke wet gemonitord worden. In reactie hierop heeft de regering gesteld dat gedurende de looptijd van de tijdelijke wet (tussentijds) de uitvoering intern door de diensten zal worden gemonitord en dat de (tussentijdse) resultaten met de stelselpartners (de CTIVD, de TIB en de Afdeling bestuursrechtspraak van de Raad van State) zullen worden gedeeld en besproken. Deze leden vragen op welk moment de Kamer wordt geïnformeerd over de bevinding van de tussentijdse monitoring. Wij antwoorden deze leden graag als volgt. Om te kunnen beoordelen of de Tijdelijke wet functioneert is op dit moment voorzien dat deze 1 jaar na inwerkingtreding (tussentijds) wordt gemonitord, middels een invoeringstoets. Zodra de eerste inzichten beschikbaar zijn, zullen die met de Kamer worden gedeeld.
Deze leden vragen voorts wanneer de Kamer de nota van wijziging tegemoet kan zien, die bij brief van 20 december 2022[3] is aangekondigd. De nota van wijziging, die is voorzien van een uitgebreide toelichting, is gelijktijdig met deze nota naar aanleiding van het verslag aan de Tweede Kamer aangeboden. Tegelijkertijd is ook het nader rapport naar aanleiding van het door de Afdeling advisering van de Raad van State uitgebrachte advies openbaar geworden.

Op de vraag van de leden van de CDA-fractie wat de consequenties voor het functioneren van de diensten kunnen zijn, indien het wetsvoorstel niet voortvarend wordt behandeld, merken wij het volgende op. Wij erkennen dat het wetgevingsproces door diverse factoren, zoals het feit dat wij het wenselijk hebben geacht een nota van wijziging in te dienen en deze voorafgaand daaraan voor advies voor te leggen aan de Afdeling advisering alsmede de tijd die de afstemming met TIB en CTIVD heeft genomen, ten opzichte van de eerder uitgesproken wens van een voortvarende behandeling vertragend heeft gewerkt. De oorzaak daarvan was gelegen in de noodzaak om ook voor de bulkdatasets in overleg met de toezichthouders tot een uitvoerbare oplossing te komen. Een en ander neemt niet weg dat de problematiek waarvoor het wetsvoorstel een oplossing beoogt te bieden, niet weg is en zeker niet is afgenomen; integendeel. De cyberdreigingen zijn in de afgelopen jaren toegenomen, terwijl het zicht op die dreiging is afgenomen. Er dreigt een grotere kloof te ontstaan tussen de ontwikkeling van de dreiging en digitale aanvallen van landen met een offensief cyberprogramma en de weerbaarheid van Nederland daartegen. Dat levert evidente risico's op voor onze nationale veiligheid. De afronding van het wetstraject blijft ons streven. Ook in deze periode achten wij behandeling die niet wacht tot de verkiezingen noodzakelijk gezien de dreiging.

---

[3] Kamerstukken II 2022/2023, 36 263, nr. 5.

De leden van de SP-fractie hebben kennisgenomen van het wetsvoorstel en geven aan daarover nog vele vragen te hebben. Deze leden vragen allereerst waarom de regering ervoor gekozen heeft dit wetsvoorstel incompleet aan de Kamer voor te leggen, voordat de afronding via een nota van wijziging klaar is. Wij antwoorden graag als volgt. Het aan de Kamer voorgelegde wetsvoorstel is niet incompleet. Het heeft zelfstandige betekenis en ook zonder de voorgenomen wijzigingen die zijn opgenomen in de gelijktijdig met deze nota naar aanleiding van het verslag aan de Tweede Kamer aangeboden nota van wijziging, blijft het van het grootste belang dat de daarin opgenomen wettelijke voorzieningen om de diensten in staat te stellen effectief onderzoek te kunnen doen naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen op een zo kort mogelijke termijn beschikbaar komen. Zie voorts hetgeen wij hiervoor in antwoord op de vraag van de leden van de CDA-fractie hebben geantwoord.

De leden van de SP-fractie geven aan verbaasd te zijn dat tijdens de technische briefing van de toezichthouders bleek dat deze een brief inzake het toezicht op de AIVD en MIVD hadden gekregen en dat de nadere informatie die de Kamer in voorbereiding op het verslag vroeg niet is gestuurd. Zij vragen waarom dit zo is en waarom de regering de Tweede Kamer informatie onthoudt over besluiten die zij wel heeft genomen in het kader van dit wetsvoorstel. Wij antwoorden deze leden graag als volgt. De brief waaraan de voorzitter van de TIB tijdens de technische briefing aan refereerde behelsde een antwoord op een vraag in de (niet door de TIB openbaar gemaakte) aanbiedingsbrief van haar consultatiereactie op de ontwerpnota van wijziging. De TIB vroeg daarin om verduidelijking van het door ons in gesprekken met de voorzitter van de TIB ingenomen standpunt inzake de toepasselijke proportionaliteitstoets in het kader van het wetsvoorstel. In die brief, die desgevraagd ook aan de Kamer is gezonden, is die verduidelijking gegeven. Er was geen intentie om de Kamer deze informatie te onthouden.

De leden van de fractie van de SP geven aan dat in de aanloop van dit wetsvoorstel de regering met meerdere fracties in de Tweede Kamer heeft afgesproken om steun te verwerven voor dit wetsvoorstel (Vergaderjaar 2022/23, Aanhangsel van de Handelingen, nr. 1185) en deze leden vragen de regering opnieuw of zij uit wil leggen waarom deze fracties zijn geselecteerd voor dat overleg en welke informatie daar met de fracties is gedeeld. Deze leden hechten er zeer aan dat alle volksvertegenwoordigers een gelijke informatiepositie krijgen van de regering, zeker op het vlak van wetgeving, en verzoeken dus om inhoudelijk antwoord op deze opnieuw gestelde vraag. In reactie hierop merken wij het volgende op. Het is niet ongebruikelijk dat een bewindspersoon de mogelijke steun in de Kamer voor een wetsvoorstel verkent. De gesprekken door de toenmalige Ministers van BZK en van Defensie werden noodzakelijk geacht om een beeld te vormen over het draagvlak voor een tijdelijke wet binnen de Tweede Kamer. Deze gesprekken waarbij een bewindspersoon mogelijke steun voor een wetsvoorstel verkent zijn oriënterend van aard. Het was dan ook niet de intentie om met alle fracties te spreken.

De leden van de SP-fractie willen weten of de regering tijdens deze gesprekken toezeggingen heeft gedaan over dit wetsvoorstel of de werkwijze van de geheime diensten die in een vorm van een «side letter» bestaan. De toenmalige Ministers van BZK en van Defensie hebben destijds gesproken over de aanleiding voor de tijdelijke wet, de toegenomen dreiging vanuit landen met een offensief cyberprogramma en de operationele knelpunten die de AIVD en MIVD ervaren in de onderzoeken naar deze landen. De gesprekken vonden plaats met de portefeuillehouders van de coalitiepartijen, alsmede met de portefeuillehouders van

oppositiepartijen GroenLinks, PvdA, SGP en JA21, en gingen over de aanleiding en over het draagvlak voor de tijdelijke wet. Er zijn in deze gesprekken geen toezeggingen gedaan over het wetsvoorstel en/of de werkwijze van de diensten. Er bestaat dan ook geen «side letter».

Deze leden vroegen voorts of de regering op dit moment gesprekken met Tweede Kamerfracties over dit wetsvoorstel voert buiten het wetstraject om, bijvoorbeeld omdat zij wil onderzoeken welke steun er is in de Eerste Kamer? Het is, zoals hiervoor al is uiteengezet, gebruikelijk dat er rondom wetsvoorstellen verkennend wordt gesproken met verschillende Tweede en Eerste Kamerfracties over steun voor wetsvoorstellen.

De leden van de SP-fractie vragen waarom deze wet het karakter van «spoed» heeft gekregen, zeker nu duidelijk is dat er in 2021 al door (voormalig) bewindspersonen uitgebreid met fracties is gesproken over dit wetsvoorstel en er uit documenten, opgevraagd via de Wet open overheid, blijkt dat er meermaals een plan is gemaakt om de presentatie van het wetsvoorstel «goed te laten landen», bijvoorbeeld via de inzet van «witte jassen» en steunzenders. In reactie hierop merken wij op, dat de dreiging van landen met een offensief cyberprogramma toeneemt en die dreiging is actueel, terwijl het zicht op die dreiging en de weerbaarheid daartegen afneemt. Dat levert directe risico's op voor de nationale veiligheid. De noodzaak en urgentie om de nationale veiligheid te beschermen is dan ook groot. Deze Tijdelijke wet moet er voor zorgen dat de diensten effectief onderzoek kunnen doen naar de cyberdreiging. Een spoedige behandeling en inwerkingtreding van de wet is daarom van belang. De Tijdelijke wet betreft echter een technische en juridische complexe materie waardoor zorgvuldig te werk moet worden gegaan in het voorbereidingstraject. In de communicatie ten aanzien van het voorstel voor een Tijdelijke wet worden personen gesproken die bekend zijn binnen en met het nationale veiligheidsdomein, het werk van de TIB en CTIVD en de diensten, waardoor ze de (technisch) complexe materie die in de Tijdelijke wet wordt geregeld goed begrijpen en feitelijke informatie op dat punt goed over kunnen brengen aan anderen. Er is geen sprake van de inzet van «steunzenders» of «witte jassen» die een positief geluid over het wetsvoorstel kunnen verspreiden. Overigens, zoals ik ook in antwoord op kamervragen van het toenmalig Kamerlid Leijten heb aangegeven[4], is de term witte jassen of steunzenders niet geheel passend en daarom zullen deze termen in het vervolg niet meer worden gebruikt, maar zal worden gesproken over vaktechnische- of inhoudelijk experts. Beoogd is aan genoemde experts feitelijke informatie te verschaffen over nut en noodzaak van het wetsvoorstel die zij vervolgens kunnen overbrengen dan wel toelichten aan anderen indien zij daarnaar worden gevraagd. Het is namelijk in ieders belang dat de discussie omtrent dit wetsvoorstel gevoerd wordt op basis van feiten en met respect voor argumenten voor en tegen.

Ook willen de leden van de SP-fractie graag een heldere uitleg van de regering over wat zij als «nieuw» betitelt in dit wetsvoorstel, omdat bij de Wiv 2017 al een spoedprocedure – waarbij het toezicht van de TIB vooraf wordt uitgesteld – bestaat. Wordt deze spoedprocedure betiteld als onwerkbaar en zo ja, waarom dan precies? In de context van de Wiv 2017 moet spoed enerzijds onderscheiden worden van snelheid en wendbaarheid anderzijds. De spoedprocedure is bedoeld voor onvoorziene en uitzonderlijke situaties waarbij er niet gewacht kan worden met de inzet van middelen om een dreiging te onderzoeken, terwijl in onderzoeken naar landen met een offensief cyberprogramma operationele snelheid en wendbaarheid juist doorlopend van essentieel belang is. Zo

[4] Aanhangsel II 2022/2023, 1185.

moet er bij cyberoperaties snel meebewogen kunnen worden met de aanvaller, bijvoorbeeld door kenmerken bij te schrijven op een hacklast, en is snelheid de norm. Het is daarnaast van belang gedurende een hackoperatie het binnendringen in een geautomatiseerd werk en onderzoek in dit systeem ononderbroken voort te zetten, bijvoorbeeld om onderkenning te voorkomen. Anders komen operaties stil te liggen waardoor inlichtingenposities verloren gaan. Dit proces is iets anders dan spoed. De spoedprocedure uit de Wiv 2017 is daarom niet de geschikte procedure om snelheid en wendbaarheid in deze onderzoeken te bewerkstelligen. Dit wetsvoorstel beoogt oplossingen te bieden om die snelheid en wendbaarheid in de dagelijkse praktijk van de diensten mogelijk te maken. Dit zorgt ervoor dat de wijze waarop de diensten onderzoek doen past bij de dynamiek van de dreiging. Daarom wordt in een gedeeltelijke verschuiving van de statische TIB toets vooraf naar bindend toezicht van de CTIVD gedurende en na afloop van de uitvoering van bepaalde bijzondere bevoegdheden voorzien, bijvoorbeeld ten aanzien van de bijschrijfmogelijkheid bij de bevoegdheid tot het binnendringen in en de bevoegdheid tot het verkennen van geautomatiseerde werken.

De leden van de SP-fractie vragen de regering ook te reageren op de «spoed» claim voor deze wet als het gaat om de korte consultatietermijn die is toegepast voor dit wetsvoorstel en het feit dat er vervolgens na het sluiten van de termijn het nog zeven maanden duurde voordat het wetsvoorstel bij de Kamer werd ingediend. Zij vragen of de regering kan reflecteren op haar werkwijze. Wij lichten de gevolgde werkwijze graag als volgt toe. Bij het opstellen van deze wet zijn verschillende organisaties betrokken. Naast de departementen zijn ook de uitvoeringsorganisaties AIVD en MIVD nauw aangesloten bij dit proces. Daarnaast zijn de TIB en CTIVD, mede op verzoek van uw Kamer, vanaf het begin van het opstellen van deze wet intensief geconsulteerd. Vanwege de taak die aan de Afdeling bestuursrechtspraak van de Raad van State is toebedeeld in de Tijdelijke wet, is ook deze organisatie uitvoerig geconsulteerd. Aangezien elke wijziging in de wet direct effect heeft of kan hebben op de nationale veiligheid en/of het operationele werk van de diensten is er nadrukkelijk aandacht geweest voor de uitvoerbaarheid van het wetsvoorstel. Alle genoemde betrokken organisaties hebben hieraan bijgedragen. Al deze consultatie reacties en inzichten in de uitvoerbaarheid zijn zorgvuldig meegenomen en meegewogen in de aanpassingen van de tekst van het wetsvoorstel en de memorie van toelichting. Dit gehele proces nam veel tijd in beslag, waardoor het inderdaad nog zeven maanden duurde voordat het daadwerkelijk ingediend kon worden.

De leden van de SP-fractie vragen de regering te reageren op de uitspraak van de directeur-generaal van de AIVD, gedaan tijdens het rondetafelgesprek van 5 april 2023, dat de diensten niet bij de totstandkoming van de Wiv 2017 betrokken waren en dat daardoor de implementatie van de Wiv 2017 (zie het rapport van de Algemene Rekenkamer over de slagkracht van de AIVD en MIVD) niet goed is verlopen. Klopt deze uitspraak wel, zo vragen deze leden aan de regering. Zij herinneren zich de actieve rol van de AIVD in de discussies rond het referendum over de Wiv 2017. Ook herinneren zij zich de foutieve informatie die de AIVD over de Wiv 2017 op haar website had (Vergaderjaar 2017/18, Aanhangsel van de Handelingen, nr. 921). Zij vragen of de regering helder kan uitleggen waar de stellige uitspraak van de DG-AIVD vandaan komt. Wij willen hier als volgt op reageren. De uitspraak komt van de praktijkervaring van de diensten met de Wiv 2017, de lessen die de regering daaruit heeft getrokken en de constateringen van de ECW en de ARK in hun rapporten. Eén van de grote verschillen tussen de voorbereiding van de Wiv 2017 destijds en de voorbereiding van de Tijdelijke wet nu is dat er destijds geen goede

uitvoeringstoets is geweest. De Algemene Rekenkamer heeft in haar rapport geconcludeerd dat de uitvoeringseffecten bij de implementatie van de Wiv 2017 meer aandacht hadden moeten krijgen bij de totstandkoming van de wet. Ook constateren zij dat de onmisbare technische en operationele inbreng vanuit de diensten bij de totstandkoming van de wet beperkt was. Ook de ECW heeft in het kader van haar evaluatie van de Wiv 2017 aanbevolen voorafgaand aan de inwerkingtreding van toekomstige wetswijzigingen een impactanalyse uit te voeren en zo in praktische zin de consequenties van de invoering van de wet in beeld te brengen. De ECW doet dan ook de aanbeveling[5] bij een toekomstige wetswijziging tijdig aandacht te hebben voor de implementatie daarvan en een ICT-uitvoeringstoets uit te doen. Ook moet worden opgemerkt dat enkele cruciale punten in de wet pas in een laat stadium van het wetstraject zijn toegevoegd, zoals het gerichtheidscriterium en de oprichting van de TIB, zonder voldoende stil te staan bij de uitvoeringseffecten van die aanpassingen. Wij hebben de aanbevelingen van de ECW en ARK ter harte genomen bij de voorbereiding van de Tijdelijke wet. Bij de voorbereiding van dit wetsvoorstel is doorlopend aandacht geweest voor de uitvoerbaarheid van het wetsvoorstel voor de diensten door verschillende uitvoeringstoetsen uit te voeren. Bij deze uitvoeringstoetsen zijn ook de TIB, CTIVD en Afdeling bestuursrechtspraak van de Raad van State betrokken geweest. De uitkomsten van die uitvoeringstoetsen zijn betrokken bij de totstandkoming van het wetsvoorstel. Ook hebben de diensten reeds de voorbereiding van de implementatie van de Tijdelijke wet gestart, zodat implementatievraagstukken en eventuele knelpunten tijdig worden gesignaleerd.

De leden van de SP-fractie vragen of de regering kan aangeven welke ándere opties dan een wetswijziging onderzocht zijn om de administratieve last van de inzet van bevoegdheden te verminderen. Voordat is besloten over te gaan tot het opstellen van een wetsvoorstel is samen met alle stelselpartners – in casu de TIB, de CTIVD en de betrokken departementen – onderzocht of de Wiv 2017 voldoende ruimte bood om de operationele knelpunten die de diensten in onderzoeken naar landen met een offensief cyberprogramma ervoeren op te lossen. Uit de gesprekken met deze stelselpartners, dus ook de TIB en CTIVD, is de conclusie getrokken dat de problematiek enkel via een wetswijziging kan worden opgelost. Bij de implementatie van de Tijdelijke wet wordt tevens meegenomen hoe de interne processen zo efficiënt mogelijk kunnen worden ingericht, bijvoorbeeld door automatisering van bepaalde processtappen. Het aanpassen van interne processen lost echter niet de geconstateerde operationele knelpunten op. Daarnaast merken wij op dat alhoewel administratieve lastenverlichting gewenst is, de Tijdelijke wet niet primair ten doel heeft de administratieve last van de inzet van bevoegdheden te verminderen. De Tijdelijke wet beoogt een effectieve inzet van bevoegdheden die past bij de snelheid, dynamiek en complexiteit van onderzoeken naar landen met een offensief cyberprogramma en een daarbij passend en robuust stelsel van waarborgen.

De leden van de PvdA-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Deze leden delen de zorg over het feit dat ook Nederland in toenemende mate te maken heeft met dreigingen vanuit diverse landen met een offensief cyberprogramma en dat de inlichtingen- en veiligheidsdiensten de wettelijke mogelijkheden moeten hebben om onderzoek naar dergelijke dreigingen te doen en daar tegen op te kunnen

[5] Aanbeveling 56 luidt: Bij een toekomstige wetswijziging moet tijdig aandacht zijn voor de implementatie daarvan en bij iedere afzonderlijke wetswijziging moet worden overwogen of overgangsrecht nodig is. Aanbeveling 57 luidt: Doe een ICT-uitvoeringstoets bij wijzigingen van de wet.

treden. Dit neemt echter niet weg dat er bij eventuele versterking van de wettelijke mogelijkheden een balans moet worden behouden tussen enerzijds het kunnen optreden tegen die bedreigingen en anderzijds de bescherming van de democratische rechtsstaat. Wij onderschrijven deze benadering, waarbij wij wel opmerken dat het optreden van de diensten tegen de hier bedoelde dreigingen ook plaatsvindt ter bescherming van de democratische rechtsstaat. Een solide wettelijke borging van de bevoegdheden van de diensten achten de leden van de PvdA-fractie noodzakelijk. Deze leden geven aan nog meerdere vragen bij het wetsvoorstel te hebben. Wij hopen dat wij met de beantwoording van de vragen van deze en andere leden hen ervan kunnen overtuigen dat met dit wetsvoorstel de door deze leden noodzakelijk geachte balans en solide wettelijke borging wordt geboden.

De leden van de GroenLinks-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel en onderschrijven het belang van effectieve wetgeving om de diensten in staat te stellen te voorkomen dat landen met een offensief cyberprogramma Nederland schade toebrengen. Zij hechten daarnaast ook veel belang aan goede waarborgen tegen disproportionele inzet van bevoegdheden en aan effectief toezicht van de toezichthouders. Om de passendheid van het wetsvoorstel binnen deze uitgangspunten te kunnen beoordelen geven zij aan nog behoorlijk wat vragen te hebben.

De leden van de PvdD-fractie geven aan met ontstentenis kennis te hebben genomen van het wetsvoorstel. Zij hebben bezwaren tegen het wetsvoorstel en vinden het staatsrechtelijk vreemd dat gelijktijdig met de aanbieding van de wet al een nota van wijziging werd aangekondigd. De leden van de PvdD-fractie verwachten dat de Staten-Generaal deugdelijke wetgeving ontvangt en kan behandelen en niet meteen op aanvullende of reparatiewetgeving moeten rekenen. Anders dan deze leden zien wij geen staatsrechtelijke bezwaren tegen de aankondiging van een nota van wijziging gelijktijdig met de indiening van het wetsvoorstel. Het indienen van nota's van wijziging is immers een normaal onderdeel van het wetgevingsproces. Nu reeds bij de indiening van het wetsvoorstel het voornemen bestond om op het wetsvoorstel een nota van wijziging in te dienen, leek het ons juist wenselijk om de Kamer daarvan op de hoogte te stellen om te voorkomen dat de Kamer zich bij het achterwege laten van een dergelijke mededeling juist daardoor overvallen zou kunnen voelen. Wij verwijzen kortheidshalve naar de brief van 20 december 2022 die wij aan de Kamer hebben gezonden.[6] Het ingediende wetsvoorstel is naar ons oordeel deugdelijk en de nota van wijziging strekt zeker niet tot reparatie van het wetsvoorstel. Het heeft wel een substantieel aanvullend karakter, hetgeen de reden is om de ontwerpnota van wijziging voor advies aan de Afdeling advisering voor te leggen. Dat neemt niet weg dat het wetsvoorstel wel degelijk zelfstandige betekenis heeft. Wij hopen dan ook met de beantwoording van de vragen en opmerkingen van de leden van deze fractie de scepsis die bij deze leden met betrekking tot dit wetsvoorstel leeft weg te kunnen nemen.

De leden van de ChristenUnie-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Ze hebben nog wel enkele vragen daarbij, die zich met name toespitsen op de in artikel 13 geregelde beroepsmogelijkheid bij de Afdeling bestuursrechtspraak van de Raad van State.

De leden van de SGP-fractie hebben met belangstelling van het wetsvoorstel kennisgenomen. Zij vinden het belangrijk dat de diensten snel en wendbaar kunnen reageren op de complexe en wisselende dreigingen die uitgaan van landen. Zij geven aan vragen te hebben over

[6] Kamerstukken II 2022/2023, 36 263, nr. 5.

de wenselijkheid van verschillende toezichtregimes en de relatie tussen het wetsvoorstel en bezinning op de herziening voor de langere termijn. Ook wachten zij de nota van wijziging af. Waar het gaat om de herziening voor de langere termijn verwijzen wij naar de gelijktijdig met deze nota naar aanleiding van het verslag en nota van wijziging aan de Tweede Kamer aangeboden Hoofdlijnennotitie. Daarin is onder meer ingegaan op enkele scenario's die er bestaan met betrekking tot het stelsel van toetsing, toezicht en klachtbehandeling alsmede op de verhouding van onderhavig wetsvoorstel tot de herziening van de Wiv 2017.

De leden van de Volt-fractie hebben kennisgenomen van het wetsvoorstel en hetgeen schriftelijk is voorbereid en toegelicht tijdens het rondetafelgesprek over het wetsvoorstel op 5 april 2023.

Het lid van de BBB-fractie heeft van alle documenten omtrent het wetsvoorstel kennisgenomen en nog een aantal vragen daarover.

Het wetsvoorstel voorziet in een tijdelijk, van de Wiv 2017 afwijkend, regime voor het onderzoek van de AIVD en de MIVD naar landen met een offensief cyberprogramma. Er wordt hier uitgegaan van tijdelijke wetgeving voor de termijn van vier jaar. Het lid van de BBB-fractie wil graag vernemen wat de beweegredenen van de regering zijn om de wet tijdelijk te maken? Zijn de problemen omtrent dit onderwerp, zo stelt dit lid, niet permanent van aard? Wij reageren hierop graag als volgt. Het doel van het onderhavige wetsvoorstel is het op korte termijn treffen van een tijdelijke voorziening om de diensten in staat te stellen om effectief op te kunnen treden tegen de dreigingen van landen met een offensief cyberprogramma tegen Nederland. Daarmee kon niet worden gewacht totdat de eerder aangekondigde herziening van de Wiv 2017 ter opvolging van de evaluatie door de ECW zijn beslag zou hebben gekregen. Die omvat immers een scala aan onderwerpen en vergt een langere voorbereidingstijd. In artikel 17 van het wetsvoorstel is bepaald dat de Tijdelijke wet na vier jaar vervalt. De reden daarvoor is dat de herziening van de Wiv 2017 naar verwachting binnen de werkingsduur van de Tijdelijke wet kan worden bewerkstelligd. Mocht dat onverhoopt niet zo zijn, dan zal bezien moeten worden of een wetstraject tot verlenging van de Tijdelijke wet moet worden ingezet.

Het lid van de BBB-fractie leest dat de inlichtingendiensten 9% en 10% van hun personeelscapaciteit kwijt zijn om te voldoen aan de wet. Dit betreft veel juridische en administratieve capaciteit. Dit lid vraagt wat de regering ervan vindt dat zoveel personeelscapaciteit hier naartoe gaat en of er naar mogelijkheden kan worden gezocht waarbij de diensten niet zoveel tijd kwijt zijn aan bureaucratische werkzaamheden. In reactie hierop antwoorden wij als volgt. Zoals de ARK heeft geconcludeerd lijdt de operationele slagkracht onder structurele administratieve lastenverzwaring als gevolg van de implementatie van de Wiv 2017. De ARK heeft de aanbeveling gedaan om hier passende maatregelen te treffen nu de operationele slagkracht onder druk staat. Wij hechten belang aan een goede implementatie van de wet door de diensten en onderschrijven de aanbeveling van de ARK. Tegelijkertijd wordt onderkend dat de zwaarte van de wettelijke bevoegdheden zorgvuldige besluitvorming vereist op basis van een gedegen, door waarborgen omgeven proces. Het is evident dat dit administratieve capaciteit vergt. Sinds de implementatie van de Wiv 2017 hebben de diensten verder geïnvesteerd in de ICT-capaciteit en het interne toezicht op onder andere de gegevensverwerking. Dit door middel van meer structurele borging van het compliant werken. Dit moet ervoor zorgen dat de administratieve (lasten) verzwaring afneemt.

Het lid van de BBB-fractie wijst erop dat de TIB en de CTIVD nu een wettelijke grondslag krijgen voor de informatie-uitwisseling. In het verlengde hiervan wordt gevraagd waarom de regering er niet voor kiest om van deze twee organen één orgaan te maken. Deze twee organen lijken op het eerste gezicht op elkaar en daarmee zou de efficiëntie worden bevorderd en de bureaucratie worden verminderd. Dit lid vraagt of de regering dit ook denkt en aan te geven in hoeverre dit mogelijk is. Wij merken allereerst op dat beide organen binnen het bestaande stelsel van toetsing en toezicht twee te onderscheiden functies vervullen. De TIB dient een door de Minister verleende toestemming voor de inzet van bijzondere bevoegdheden op rechtmatigheid te toetsen.[7] Wordt de verleende toestemming onrechtmatig bevonden, dan vervalt deze van rechtswege. De TIB is dan ook in de autorisatiefase voorafgaand aan de inzet van (bepaalde) bijzondere bevoegdheden gepositioneerd. De afdeling toezicht van de CTIVD (hierna ook: de afdeling toezicht) heeft een andersoortige taak en functie en ziet toe op de rechtmatige uitvoering van de Wiv 2017. De vraag of het laten opgaan van beide organen in één nieuw orgaan wenselijk is, is een vraagstuk dat niet in het kader van dit wetsvoorstel dient te worden beantwoord maar in het kader van de herziening van de Wiv 2017. In de Hoofdlijnennotitie wordt hierop – en op andere mogelijke scenario's voor een herinrichting van het stelsel van toetsing, toezicht en klachtbehandeling – ingegaan.

Zowel de AIVD als de MIVD voeren speciale strategische operaties uit. Van een strategische operatie kan sprake zijn als een van de diensten zich positioneert in een netwerk of binnendringt bij een leverancier van software gebruikt door targets. Dit is noodzakelijk om zicht te kunnen krijgen op de activiteiten en intenties van targets zoals landen met een offensief cyberprogramma en hiermee ook een betere inlichtingenpositie te krijgen. Hiermee kunnen we in het kader van de nationale veiligheid cyberoperaties onderkennen en tijdig tegen gaan. Het lid van de BBB-fractie geeft aan dat bevoegdheden hiertoe zijn opgenomen in de Wiv 2017, maar door een gebrek aan toetsingskaders heeft de TIB meerdere aanvragen om te interveniëren afgewezen. Dit lid vindt dit uitermate slecht en aannemelijk is ook dat Nederland hierdoor minder informatie kan vergaren. Dit lid vraagt of hier in de nieuwe wet rekening mee is gehouden zodat het voorgaande niet meer kan gebeuren. Wij antwoorden dit lid graag als volgt. Met de in het wetsvoorstel voorgestelde maatregelen wordt beoogd de thans in de praktijk van de uitvoering van onderzoeken naar landen met een offensief cyberprogramma ondervonden belemmeringen bij de toepassing van de Wiv 2017 te adresseren. In hoofdstuk 2 van de memorie van toelichting is uiteengezet op welke wijze dit is uitgewerkt in het wetsvoorstel. Een belangrijk onderdeel vormt de te introduceren mogelijkheid om tegen oordelen van de TIB beroep in te kunnen stellen bij de Afdeling bestuursrechtspraak. Daarmee wordt – zoals de ECW in haar evaluatierapport aangeeft – een weeffout in het bestaande stelsel van toetsing en toezicht hersteld. Dit biedt de mogelijkheid om in de situatie waar tussen de TIB en de voor een dienst verantwoordelijke Minister verschil van mening bestaat over de uitleg van de wet, zoals bijvoorbeeld over het toetsingskader, bij de Afdeling bestuursrechtspraak een eenduidige en gezaghebbende uitspraak te verkrijgen.

Het lid van de BBB-fractie vraag voorts of de regering kan toezeggen dat aanvragen van veiligheidsdiensten niet meer worden afgewezen omwille van gebrekkige bureaucratische regels. In reactie hierop antwoorden wij als volgt. De inzet van bijzondere bevoegdheden door de diensten, ook die

[7] Dit is vergelijkbaar met de figuur van goedkeuring als bedoeld in afdeling 10.2.1 Algemene wet bestuursrecht.

rondom strategische operaties, gaat altijd gepaard met passende waarborgen. De afwegingen die worden gemaakt en interne procedures die worden gevolgd, te weten vanaf het verzoek om toestemming tot de inzet van de bijzondere bevoegdheid, zorgen er voor dat er sprake is van een grote mate van zorgvuldigheid van voorbereiding tot en met de inzet van de bevoegdheid. Deze zijn ook inzichtelijk voor de CTIVD. Dit is in de Tijdelijke wet niet anders en betekent dat er ook in de Tijdelijke wet sprake zal zijn van enige vorm van bureaucratie. Uit de uitvoeringstoets is echter gebleken dat de Tijdelijke wet in zijn huidige vorm uitvoerbaar is. Hoe de Tijdelijke wet in de praktijk gaat werken is, net zoals de Raad van State constateert, is afhankelijk van het rolvaste gedrag van de stelselpartners. Met de Tijdelijke wet wil de regering het mogelijk maken dat bestaande bijzondere bevoegdheden in samenhang met passende waarborgen kunnen worden ingezet ten behoeve van het beschermen van Nederlandse belangen tegen offensieve cyberdreigingen. De bureaucratie die hierbij hoort moet werkbaar zijn, en is noodzakelijk om de inzet van bijzondere bevoegdheden te laten voldoen aan de waarborgen die daarbij horen.

Het lid van de BBB-fractie wijst tot slot op de risico's verbonden aan de bredere bevoegdheden van de diensten en dat bijvoorbeeld het College voor de Rechten van de Mens (CRvdM) en Bits of Freedom (BoF) kritische reacties hebben gegevens op het wetsvoorstel. In reactie op de vraag van dit lid of de regering deze reactie heeft gelezen, wordt bevestigend geantwoord. In paragraaf 7 van de memorie van toelichting is ingegaan op deze en andere reacties. Daar is ook gereageerd op enkele van de door dit lid aangestipte onderwerpen uit die reacties, met name waar het gaat om de informatieplicht (meldplicht) en de informatie-uitwisseling tussen TIB en CTIVD. Voor zover daarbij de door dit lid aangestipte voorbeelden daarin niet zijn geadresseerd, zullen deze bij de inhoudelijke bespreking van de desbetreffende onderwerpen in deze nota naar aanleiding van het verslag worden betrokken.

1. Inleiding

De leden van de SP-fractie constateren dat het wetsvoorstel een nieuwe werkwijze en vorm van toezicht introduceert voor het inlichtingenonderzoek van de diensten naar landen met een offensief cyberprogramma. Deze leden vragen hoe wenselijk het is om te gaan werken met twee verschillende toezichtsregimes. Wij reageren hierop graag als volgt. Voorop wordt gesteld dat het bestaande toezichtsregime in de Wiv 2017 gewoon geldt, ook waar het gaat om de onderzoeken die onder de werking van de regeling in het wetsvoorstel vallen. Het wetsvoorstel geeft deels een afwijking van en deels een aanvulling op het in de Wiv 2017 neergelegde stelsel, ook waar het gaat om het stelsel van toetsing en toezicht. De afwijking bestaat daaruit dat (1) de toestemming voor verkenning van geautomatiseerde werken (artikel 4, eerste lid) en (2) de toestemming voor geautomatiseerde analyse op metadata verkregen via OOG-interceptie (artikel 8) in het kader van onderzoeken waarop deze wet van toepassing is verklaard niet meer ter toetsing aan de TIB wordt voorgelegd. De aanvulling ten opzichte van de Wiv 2017 bestaat uit twee onderdelen, namelijk de introductie van (1) een bindende toezichtsbevoegdheid voor de afdeling toezicht en (2) de mogelijkheid van beroep op de Afdeling bestuursrechtspraak. In de genoemde gevallen waarbij de TIB-toets komt te vervallen, wordt bindend toezicht door de afdeling toezicht geïntroduceerd. De in het wetsvoorstel getroffen voorzieningen zijn onlosmakelijk verbonden met de andere daarin opgenomen afwijkingen dan wel aanvullingen van de Wiv 2017 ter zake van de bijzondere bevoegdheden van de diensten en zijn ook daartoe beperkt. De keuze voor deze voorzieningen hangt samen met de wens om voor de onderzoeken

en (met name) de daarbij in te zetten bevoegdheden in de sfeer van OOG-interceptie en hacken, te komen tot een vorm van toets en toezicht dat aansluit bij de fase waarin de desbetreffende bevoegdheden moeten worden ingezet en als zodanig ook beter aansluit bij de dynamiek van de uitvoering van die bevoegdheden. Dit standpunt wordt door zowel TIB als CTIVD onderschreven. Het gaat er dan ook uiteindelijk niet om of – zoals deze leden stellen – het wenselijk is met twee toezichtsregimes te werken. Het is inherent aan de gemaakte keuzen in de Tijdelijke wet om de diensten meer mogelijkheden te bieden voor hun onderzoeken in het cyberdomein dat die gepaard dienen te gaan met aanvullende waarborgen, ook in de sfeer van toezicht. Bovendien achten we het stelsel werkbaar, nu immers voorafgaand aan de inzet van bijzondere bevoegdheden door de diensten onder de werking van de Tijdelijke wet altijd aangegeven moet worden dat daarop de Tijdelijke wet van toepassing is. Dit bepaalt ook 1-op-1 of het in het wetsvoorstel opgenomen stelsel van toetsing, toezicht en beroep van toepassing is. Daar kan dus geen rechtsonzekerheid over ontstaan.

Waar het gaat om de vraag van deze leden welk regime de diensten moeten hanteren bij een offensieve aanval van een land dat niet betiteld is als actor die onder dit wetsvoorstel valt, wordt opgemerkt dat het wetsvoorstel betrekking heeft op alle landen met een offensief cyberprogramma tegen Nederland of Nederlands belangen (artikel 2, eerste lid). Indien is vastgesteld dat het niet om een land (statelijke actor) gaat, dan is uitsluitend de Wiv 2017 van toepassing.

De leden van de SP-fractie vragen of de regering helder kan uiteenzetten welke landen zich kwalificeren als landen met offensieve cyberprogramma's tegen Nederland of Nederlandse belangen? Wij verwijzen deze leden naar onze reactie op een vergelijkbare vraag van de leden van de D66-fractie.

De leden van de SP-fractie vragen voorts hoe landen nu precies in aanmerking komen en op welke wijze de kwalificatie vervalt. Wij antwoorden deze leden als volgt. De wettelijke taken van de diensten worden aan de hand van de inventarisatie van de behoeften bij belanghebbende ministeries[8] uitgewerkt in onderzoeksthema's in de Geïntegreerde Aanwijzing (GA). Daarin is ook het onderzoek naar landen met een offensief cyberprogramma opgenomen. Het offensieve cyberprogramma moet gericht zijn op Nederland of Nederlandse belangen. Landen komen in aanmerking voor deze kwalificatie als de diensten en de belanghebbende ministeries aanwijzingen hebben dat deze landen actief een offensief cyberprogramma ontplooien waarmee zij een risico vormen gericht op Nederland en/of Nederlandse belangen. Indien bij actualisering van de GA een thema geen prioriteit meer heeft of er geen onderzoeksbehoefte meer is, kan dat thema vervallen. Bij onderhavig onderzoeksthema is daarvan geen sprake; integendeel. De cyberdreiging neemt alleen maar toe.

Deze leden vragen of de regering ook kan aangeven wat wordt verstaan onder «Nederlandse belangen»? Wij reageren hierop graag als volgt. De Nederlandse belangen waar deze wet naar verwijst, zijn de belangen zoals beschreven in de veiligheidsstrategie voor het Koninkrijk der Nederlanden.[9] Deze nationale veiligheidsbelangen vormen de kern van wat Nederlandse inlichtingen- en veiligheidsdiensten moeten beschermen. Er zijn verschillende dreigingen voor de nationale veiligheid. Als een dreiging één of meer veiligheidsbelangen ernstig aantast, kan dat

[8] Zie artikel 5 Wiv 2017.
[9] Zie Kamerstukken II 2022/2023, 30 821, nr. 178.

maatschappelijke ontwrichting veroorzaken en daarmee de nationale veiligheid schaden. Tegelijkertijd zijn deze dreigingen met elkaar verweven. De ene dreiging heeft invloed op de andere dreiging, waardoor ze elkaar kunnen versterken. De Veiligheidsstrategie legt de nadruk op deze verwevenheid en beschrijft de veiligheidsbelangen als volgt:

- Territoriale veiligheid: Het ongestoord functioneren van het Koninkrijk der Nederlanden en haar EU en NAVO bondgenoten als onafhankelijke staten in brede zin,
- dan wel de territoriale veiligheid in enge zin.
- Fysieke veiligheid: Het ongestoord functioneren van de mens in het Koninkrijk der Nederlanden en zijn omgeving.
- Economische veiligheid: Het ongestoord functioneren van het Koninkrijk der Nederlanden als een effectieve en efficiënte economie.
- Ecologische veiligheid: Het ongestoord blijven voortbestaan van de natuurlijke leefomgeving in en nabij het Koninkrijk der Nederlanden.
- Sociale en politieke stabiliteit: Het ongestoorde voortbestaan van een maatschappelijk klimaat waarin individuen ongestoord kunnen functioneren en groepen mensen
- goed met elkaar kunnen samenleven binnen de verworvenheden van de democratische rechtstaat van het Koninkrijk der Nederlanden en de daarin gedeelde waarden.
- Internationale rechtsorde en stabiliteit: Het goed functioneren van het internationale stelsel van normen en afspraken, gericht op het bevorderen van de internationale vrede en veiligheid, inclusief mensenrechten, en effectieve multilaterale instituties en regimes, alsmede het goed functioneren van staten grenzend aan het Koninkrijk der Nederlanden en in de directe omgeving van de Europese Unie.

De leden van de SP-fractie vinden het beschermen van het Nederlandse bedrijfsleven tegen cyberaanvallen zeer belangrijk maar vragen de regering wel uit te leggen wat precies de rol van de AIVD en MIVD behoort te zijn op dit vlak. Is dat de taak van veiligheidsdiensten, of zou het beter zijn om het bestaande Nationaal Cyber Security Center (NCSC) hier beter op toe te rusten, zo vragen deze leden. Wij beantwoorden deze vraag als volgt. De AIVD en de MIVD hebben in het kader van de nationale veiligheid beiden zowel een veiligheidstaak als een inlichtingentaak. Dat behelst onderzoek, waarbij men – anders dan het NCSC – algemene en bijzondere bevoegdheden mag inzetten om dreigingen tegen de nationale veiligheid te onderkennen. Daarmee kan uniek zicht op de digitale dreiging worden opgebouwd. Daarnaast hebben de diensten ook een veiligheidsbevorderende taak, gericht op rijksoverheid, defensie en vitale sectoren. Het Nationaal Bureau Verbindingsbeveiliging (NBV) van de AIVD maakt daar gebruik van om organisaties te adviseren over het versterken van de digitale weerbaarheid. Vanzelfsprekend wordt daarbij door de diensten nauw samengewerkt met ketenpartners zoals het NCSC. De MIVD doet specifiek onderzoek bij en naar de defensie-industrie en verwerkt in dat kader inlichtingen, waarbij de bescherming van het desbetreffende bedrijfsleven tegen cyberaanvallen een belangrijk aandachtspunt is.

De leden van de SP-fractie geven aan dat zij economische schade van cyberaanvallen uiteraard ook willen terugdringen en voorkomen, maar, zo vragen deze leden, is het grootschalig kunnen afluisteren van de samenleving daarvoor het uitgelezen middel. Zij vragen of de regering hierop een reflectie kan geven. Allereerst merken we op dat we afstand nemen van de door deze leden gehanteerde kwalificatie dat er sprake zou zijn van grootschalig afluisteren van de Nederlandse samenleving. Wat wel gebeurt, maar dat is inherent aan zowel de bevoegdheid tot het verkennen ten behoeve van OOG-interceptie als de bevoegdheid tot OOG-interceptie, is dat in beide gevallen sprake is van het in bulk

intercepteren van gegevens die – in de context van de Tijdelijke wet – bij kunnen dragen aan het beantwoorden van onderzoeksvragen over landen met een offensief cyberprogramma. De Nederlandse bevolking als samenleving valt hier niet onder. Omdat offensieve cyberprogramma's zich voornamelijk via het internet manifesteren en omdat van te voren niet bekend is waar dreigingen vandaan komen of hoe deze eruit zien, is de mogelijkheid om via de hier bedoelde bijzondere bevoegdheden dataverkeer te kunnen verwerven cruciaal. De inzet van deze bevoegdheden voor de interceptie van gegevens die worden getransporteerd via een kabel- of satellietverbinding (ook HF, UHF en VHF) alsmede de opslag en verdere verwerking van de aldus verworven gegevens hebben voornamelijk betrekking op het buitenland. Wij hanteren het begrip «voornamelijk» omdat door de werking van het internet het nimmer uit te sluiten is dat hier ook gegevens van of over burgers uit Nederland in zitten. Het onderzoek van de diensten richt zich echter op het beantwoorden van onderzoeksvragen naar personen en/of organisaties die onderdeel uitmaken van landen met een offensief cyberprogramma. Bij de *verkenning* van de kabel- of satellietverbindingen wordt eerst onderzocht welke gegevens van deze kabel of satelliet wél en welke gegevens niet kunnen bijdragen aan het beantwoorden van onderzoeksvragen. Op deze manier kunnen bij de *interceptie voor het inlichtingenproces* dus alleen die gegevens worden geïntercepteerd en verwerkt waarvan de gerede verwachting is dat deze een bijdrage leveren aan de beantwoording van de onderzoeksvragen. Het betreft hier dan zoals hierboven aangegeven de onderzoeksvragen gericht op de dreiging vanuit landen zoals China en Rusland. Voordat deze bevoegdheden ingezet mogen worden, toetst de TIB of de verleende toestemming voor de inzet van deze bevoegdheden rechtmatig is verleend. Daarbij wordt bezien of voldaan wordt aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit en – voor zover het gaat om OOG-interceptie voor het inlichtingenproces – ook de eis van gerichtheid. De afdeling toezicht van de CTIVD kan te allen tijde hun reguliere toezicht houden op de uitvoering van de betreffende bevoegdheden door de diensten.

De leden van de PvdA-fractie wijzen erop dat na de inwerkingtreding van de Wiv 2017 deze wet door de Evaluatiecommissie Wiv 2017 is geëvalueerd en dat de Algemene Rekenkamer onderzoek heeft gedaan naar de invloed van die wet op de operationele slagkracht van de diensten. Zij geven aan dat de uitkomsten van beide onderzoeken zijn gebruikt bij de onderbouwing van het voorliggende wetsvoorstel. Zij missen echter een beschouwing op het rapport dat op verzoek van de Minister van BZK door de hoogleraren Bovend'Eert, Lawson en Winter is gemaakt. Zij vragen of de regering alsnog uitgebreid op de conclusies van de genoemde hoogleraren in hun rapport kan ingaan en aan kunnen geven in hoeverre die conclusies stroken met de voorstellen in voorliggend wetsvoorstel. Wij reageren hierop graag als volgt. De genoemde rapportages, dus die van de ECW, de Algemene Rekenkamer en van de drie hoogleraren, zijn rapportages die primair van belang zijn bij de herziening van de Wiv 2017. In de Hoofdlijnennotitie die betrekking heeft op de herziening van de Wiv 2017 en die gelijktijdig met deze nota naar aanleiding van het verslag aan de Tweede Kamer is aangeboden, wordt op deze rapportages ingegaan. Wij verwijzen naar hetgeen daar is gesteld. Bij de voorbereiding van voorliggend wetsvoorstel heeft het advies van de drie hoogleraren geen enkele rol gespeeld. Immers het advies is uitgebracht in het kader van de te nemen vervolgstappen ter opvolging van het rapport van de ECW en de daarin gedane voorstellen met betrekking tot het stelsel van toetsing, toezicht en klachtbehandeling gaan het bestek van de Tijdelijke wet te buiten. Dat ligt slechts ten dele anders waar het gaat om het rapport van de ECW, omdat een aantal aanbevelingen van de ECW van direct belang bleken te zijn voor de met het voorliggend wetsvoorstel te adresseren

problematiek. Dat ziet onder meer op de aanbevelingen met betrekking tot de bijschrijfmogelijkheid, de verkenningsbevoegdheid bij OOG-interceptie en het herstel van de door de ECW geconstateerde weeffout[10] in het stelsel van toezicht, namelijk door het openen van de beroepsmogelijkheid bij de Afdeling bestuursrechtspraak.

De leden van de PvdA-fractie wijzen er op dat na de inwerkingtreding van de voorliggende wet er twee wettelijke regimes voor toetsing en toezicht ontstaan en in hoeverre, zo vragen deze leden, vormt dat een extra belasting voor de diensten en de toezichthouders. De extra belasting zal voornamelijk liggen bij de implementatie van de Tijdelijke wet, waarbij door de diensten uitvoeringsbeleid gemaakt moet worden en medewerkers moeten worden opgeleid. Ook voor de TIB en de CTIVD zal een implementatietermijn nodig zijn, zoals de CTIVD in haar reactie op het ontwerpwetsvoorstel ook eerder heeft aangegeven. Met beide instanties is omtrent de benodigde aanvullende capaciteit, onder andere van juridische aard, overleg gevoerd.

Ook vragen deze leden in hoeverre het bestaan van twee wettelijke regimes op zich al niet nadelig is voor de slagkracht van de diensten. Wij willen deze leden allereerst verwijzen naar hetgeen wij eerder in Onderdeel I van deze nota naar aanleiding van het verslag hebben geantwoord op vragen van de leden van de CDA-fractie, waarbij zij vragen of de wet voldoende ruimte aan de diensten geeft om te opereren tegen dreigingen. In aanvulling daarop merken we op dat wij er vertrouwen in hebben dat het wetsvoorstel bij kan dragen aan de effectiviteit van de uitvoering van de taken van de diensten en de mogelijkheid om de verplichtingen die uit het wetsvoorstel voortvloeien goed uit te kunnen voeren.

De leden van de fractie van de PvdA vragen of de regering nog nader kan ingaan op de vraag waarom de bestaande wetgeving niet afdoende zou zijn om op te kunnen treden tegen cyberbedreigingen van statelijke actoren. Ook vinden deze leden ondanks de uitleg in de memorie van toelichting nog niet duidelijk waarom het zo gericht als mogelijk werken voor de diensten belemmerend zou zijn. Ook op dit punt vragen zij of de regering daarop wil ingaan. Zoals we ook al eerder in deze nota naar aanleiding van het verslag hebben gesteld, zijn wendbaarheid en snelheid essentieel bij onderzoeken in het cyberdomein. In het cyberdomein is het immers, in tegenstelling tot het fysieke domein, voor personen en organisaties waar de diensten onderzoek naar doen zeer eenvoudig om snel en vaak te wisselen van locatie, wereldwijd. Het is van belang mee te kunnen bewegen met dergelijke veranderingen. De noodzakelijke wendbaarheid en snelheid kan op dit moment echter binnen de bestaande wettelijke kaders niet worden gerealiseerd. Dit is tevens geconcludeerd door de ECW. Ook heeft de Algemene Rekenkamer in haar rapport over de operationele slagkracht van de diensten geconcludeerd dat de effectiviteit van de diensten onder druk staat. Effectief onderzoek doen naar de dreiging vanuit statelijke actoren was dus al onvoldoende mogelijk binnen de kaders van de Wiv 2017, maar is het urgenter geworden door de toenemende dreiging. De knelpunten die de diensten nu ondervinden in deze onderzoeken kunnen enkel worden opgelost met een wetswijziging. Immers, zonder een adequate inzet van bevoegdheden is het voor beide diensten moeilijk, en soms onmogelijk, op een effectieve wijze uitvoering te geven aan onderzoek naar landen met een offensief cyberprogramma en daarmee zicht te krijgen op de dreiging die daarvan uitgaat. Juist in onderzoeken als hier bedoeld is het van belang de verborgen dreiging te

[10] Zie hetgeen de ECW ter zake heeft gesteld in par. 9.5 (Balans in het stelsel) van haar evaluatierapport.

kunnen onderkennen. Bij de totstandkoming van de Wiv 2017 is onvoldoende onderkend wat dit betekent voor de inzet van bijzondere bevoegdheden. Bij de Wiv 2017 is de targetgerichte benadering (gericht op een – zoveel mogelijk – vooraf gespecificeerde persoon of organisatie), ook waar het gaat om de toepassing van bijzondere bevoegdheden, de dominante benadering geweest. Onderzoek in het cyberdomein vergt echter een grotendeels andersoortige onderzoeksmethodiek, waarbij ook een daarop aangepaste wijze van invulling van wettelijk vastgelegde criteria, zoals bijvoorbeeld de eis van gerichtheid, past.[11] Het wetsvoorstel beoogt dat de AIVD en de MIVD op een effectieve wijze hun wettelijke taak met betrekking tot de dreigingen in het cyberdomein kunnen uitvoeren. Hierbij blijft het niveau van waarborgen gehandhaafd en wordt dat zelfs op punten versterkt, waarbij de aard van het toezicht beter aansluit bij de fase waarin de uitvoering van een bijzondere bevoegdheid zich bevindt. Dat sluit beter aan bij de dynamische praktijk van het cyberdomein en doet tevens recht aan de rolverdeling binnen het stelsel: namelijk die tussen de TIB en de afdeling toezicht van de CTIVD in relatie tot de uitvoeringspraktijk van de diensten.

Waar het gaat om de vraag van deze leden waarom «zo gericht mogelijk» voor de diensten belemmerend zou zijn, merken we het volgende op. Bij de toepassing van de bevoegdheid tot OOG-interceptie gericht op verkennen is de in artikel 26, vijfde lid, Wiv 2017 neergelegde eis dat de bevoegdheid gericht moet worden ingezet naar zijn aard niet toepasbaar. Dit concludeert de CTIVD ook in rapport 75 over de inzet van kabelinterceptie. De bevoegdheid tot verkennen heeft immers als doel om van de beschikbare gegevensstromen vast te stellen welke gegevensstromen bij de uiteindelijke OOG-interceptie ex artikel 48 Wiv 2017 een bijdrage kunnen gaan leveren aan de beantwoording van de onderzoeksvraag. Dit is alleen mogelijk door gegevensstromen te intercepteren en om vervolgens door middel van technisch onderzoek te bepalen of en op welke wijze een gegevensstroom mogelijk een bijdrage levert aan de beantwoording van onderzoeksvragen. Dit technisch onderzoek richt zich onder andere op het onderzoeken van de aanwezigheid van voor de onderzoeksvragen van de diensten van belang zijnde communicatie, het vaststellen van de aard van deze communicatie en de gebruikte technische protocollen. Verkenning heeft dus tot doel om het verzoek om toestemming voor OOG-interceptie voor inlichtingenonderzoek te onderbouwen. In een verzoek om toestemming om de bijzondere bevoegdheid tot OOG-interceptie als bedoeld in artikel 48 Wiv 2017 in te kunnen zetten dient volgens artikel 7 van de Tijdelijke wet – als nadere duiding van de in artikel 26, tweede en vijfde lid, Wiv 2017 neergelegde proportionaliteits- en gerichtheidseis – een indicatie te worden gegeven welke gegevensstromen worden geïntercepteerd. De uitkomsten van de verkenning bieden daarvoor de noodzakelijke informatie.

De leden van de PvdA-fractie wijzen op de spoedprocedure zoals die in artikel 37 Wiv 2017 is opgenomen. Daarin wordt bepaald dat indien er sprake is van onverwijlde spoed een bevoegdheid ook al mag worden gebruikt zonder dat de TIB ex ante heeft getoetst; die toetsing vindt dan achteraf plaats. Deze leden hebben een aantal vragen. Allereerst willen zij vernemen hoe vaak die spoedprocedure wordt gebruikt. Wij wijzen op hetgeen in het jaarverslag 2022 van de TIB is opgenomen, namelijk dat er in 2021 111 spoedprocedures zijn aangevraagd en in 2022 129 spoedprocedures. Deze leden vragen voorts waarom de spoedprocedure niet voldoende mogelijkheden biedt voor slagvaardig optreden van de diensten en of daarvoor een Tijdelijke wet nodig is. Ook vragen zij of deze spoedprocedure aangepast kan worden om de slagvaardigheid van de

[11] Zie ook hetgeen daaromtrent is gesteld in Kamerstukken II 2022/2023, 36 263, nr. 3, p. 4 e.v.

diensten te bevorderen, en zo ja, waarom een Tijdelijke wet dan nog beter is. En, zo nee, waarom niet. Wij willen deze leden allereerst verwijzen naar hetgeen we hiervoor in reactie op vragen van de leden van de SP-fractie hebben gesteld over de spoedprocedure. In aanvulling daarop merken we nog het volgende op. Een aanpassing van de spoedprocedure wordt niet passend geacht, aangezien de spoedprocedure naar haar aard bedoeld is om in uitzonderingssituaties snel te kunnen handelen. De Tijdelijke wet ziet niet op uitzonderingssituaties, waar bijvoorbeeld een spoedprocedure voor ingezet kan worden, maar op een tijdelijke reguliere oplossing voor de al eerder benoemde knelpunten die aan de orde van de dag zijn bij onderzoeken naar cyberdreigingen van statelijke actoren, mét daarbij een adequaat stelsel van toetsing en toezicht.

De leden van de GroenLinks-fractie constateren dat het voorliggende wetsvoorstel in 2021 is aangekondigd en nu pas in de Kamer voorligt ter behandeling, terwijl de regering destijds heeft aangegeven, vooruitlopend op de bredere herziening van de Wiv 2017, vanwege spoedeisende omstandigheden met een tijdelijke wet te komen. Zij vragen of de regering kan aangeven waarom de tijd tussen de aankondiging van de tijdelijke wet en de daadwerkelijke indiening bij de Kamer zo relatief lang heeft geduurd voor een wet die aangekondigd was met spoed ingevoerd te moeten worden? Deze leden verwijzen wij voor onze reactie op een vergelijkbare vraag van de leden van de SP-fractie naar hetgeen daar is gesteld.

De leden van de fractie van GroenLinks vragen naar de stand van zaken van de aangekondigde nota van wijziging. De nota van wijziging is gelijktijdig met deze nota naar aanleiding van het verslag bij de Tweede Kamer ingediend.

De leden van de fractie van de PvdD-fractie vragen of de behandeling van deze wet niet stilgelegd kan worden en de aandacht niet beter besteed kan worden aan de herziening van de Wiv 2017. Wat hen betreft gaan we niet aan de slag met dit soort tijdelijke wetgeving, met erg veel onduidelijkheden, maar zetten we in op een herziening van de Wiv 2017. Daarbij moet, aldus deze leden, echt aandacht besteed worden aan en informatie gedeeld worden over op welke schaal er momenteel al data (van burgers) verzameld wordt door de veiligheidsdiensten, en hoort een deugdelijke impactanalyse. Daarnaast moeten vragen beantwoord worden als: wat kan er momenteel wel en niet op basis van bevoegdheden? Wat zijn de knelpunten? Deze leden zouden het liefst zien dat de herziening in één keer goed gedaan wordt en niet met, zoals sommige experts het noemden, «experimenteerwetgeving» komen waarbij geëxperimenteerd wordt met de data van miljoenen mensen. In reactie op de vragen en opmerkingen van deze leden, merken wij op dat huidige Wiv 2017 aan herziening toe is. In dit kader wordt mede verwezen naar de rapporten van de ECW en ARK. De ECW constateert immers dat de Wiv 2017 niet op alle punten heeft gebracht wat was beoogd en de ARK constateert dat de slagkracht van de diensten fors onder druk staat. Echter, het stilleggen van de behandeling van de Tijdelijke wet is niet wenselijk aangezien de diensten nog steeds aangeven dat ze op dit moment in onvoldoende mate in staat zijn Nederland te beschermen tegen offensieve cyberdreigingen. De urgentie van de problemen waar de Tijdelijke wet oplossingen voor biedt is dermate hoog, dat het onwenselijk is om deze oplossingen uit te stellen tot het moment waarop de gehele herziening van de Wiv 2017 is afgerond. De structurele herziening van de Wiv 2017 zal naar zijn aard omvangrijker zijn en meer voorbereidingstijd vragen dan de Tijdelijke wet. In de Hoofdlijnennotitie wordt hier meer uitgebreid op ingegaan. Inzichten die voortvloeien uit de (evaluatie van de) werking van de Tijdelijke wet worden meegenomen in het wetvoorstel voor de structurele herziening.

Wat de suggestie over het experimenteren met data van miljoenen mensen betreft, kan worden opgemerkt dat de inzet van bijzondere bevoegdheden voor het verkrijgen, bewerken, analyseren en/of opslaan van data ten alle tijde voorzien zijn van passende waarborgen, bijvoorbeeld op het gebied van privacy. Hierbij dient te worden opgemerkt dat de diensten in het kader van de Tijdelijke wet deze gegevens verwerven en verwerken enkel in het kader van hun opdracht onderzoek te doen naar de dreiging die uitgaan van landen met een offensief cyberprogramma gericht op Nederland en Nederlandse belangen. Deze onderzoeken zijn dus altijd gericht op de dreigingen vanuit het buitenland, namelijk vanuit landen als Rusland, China, Iran en Noord-Korea. In de Tijdelijke wet worden de waarborgen voor de bescherming van data van Nederlandse burgers niet afgeschaald. Op bepaalde bevoegdheden verschuift het toezicht vooraf door de TIB naar toezicht tijdens of achteraf door de afdeling toezicht. deze afdeling kan dan tijdens en na de inzet van een bevoegdheid bindend toezicht houden en kan meekijken tijdens (bijvoorbeeld) het uitvoeren van een hackoperatie. Indien er sprake is van een onrechtmatigheid, kan de afdeling via de voorgestelde procedure in de Tijdelijke wet de inzet van de bevoegdheid direct stopzetten en de verwerkte gegevens na de inzet van die bevoegdheid laten verwijderen en vernietigen. Er is dan ook in het geheel niet sprake van experimenteren en ook niet van experimenteerwetgeving.

2. Inhoud van het wetsvoorstel op hoofdlijnen

2.1 Inleiding

De leden van de D66-fractie merken op dat het beoogde doel van de wet, namelijk meer operationele snelheid en wendbaarheid mogelijk te maken, terwijl het niveau van toezicht gelijk blijft, door de Afdeling advisering niet als gegeven wordt geacht. In reactie op dit advies stelt de regering, aldus deze leden, dat de Afdeling advisering dit terecht signaleert en dat het succes in sterke mate zal afhangen van de bereidheid van de betrokken instanties tot rolvaste en constructieve samenwerking. Deze leden vragen de regering hoe zij het succes van het bereiken van dit doel inschat en ook of zij in dit verband nader kan ingaan op die constructieve samenwerking en aangeven waar dit in het verleden wellicht niet geheel volgens wens verliep. Hoe is dat, zo vragen deze leden ten slotte, met dit wetsvoorstel opgelost. Het beoogde doel van de wet zal inderdaad in sterke mate afhangen van de bereidheid van betrokkenen tot rolvaste en constructieve samenwerking. In de Tijdelijke wet wordt een aantal wettelijke voorzieningen getroffen die tezamen met de uitleg in de memorie van toelichting en hetgeen voorts in de parlementaire behandeling ter zake wordt gewisseld meer duidelijkheid zal bieden over de inzet van bepaalde bijzondere bevoegdheden, niet alleen voor de diensten maar ook waar het gaat om de toetsende taak van de TIB dan wel de toezichthoudende taak van de afdeling toezicht in de onderscheiden fasen van inzet van bijzondere bevoegdheden alsmede de reikwijdte van de uitoefening van de hen toekomende bevoegdheden. In het verleden bestond er met betrekking tot bepaalde bijzondere bevoegdheden soms onduidelijkheid over de mogelijkheden voor het inzetten van deze bevoegdheden. Dit kon dan resulteren in verschillen van inzicht tussen betrokkenen, waardoor impasses ontstonden in de toepassing van bevoegdheden. De Tijdelijke wet verschaft naar ons oordeel de helderheid over de inzet van bepaalde cruciale bevoegdheden die eerder ontbrak. Indien er toch geschillen ontstaan tussen de afdeling toezicht van de CTIVD of TIB enerzijds en de verantwoordelijke Minister anderzijds biedt de Tijdelijke wet de mogelijkheid deze voor te leggen aan de Afdeling Bestuursrechtspraak van de Raad van State. Daarmee kunnen impasses worden doorbroken en

wordt voorzien in eenduidige en gezaghebbende uitleg van de betreffende wettelijke bepalingen.

De leden van de D66-fractie vragen de regering nader in te gaan op de spoedeisendheid van het voorliggende wetsvoorstel. Het feit dat gekozen is voor een tijdelijke wet impliceert dat niet tot een algehele herziening van de Wiv 2017 kan worden gewacht. Zij missen een omschrijving van de spoedeisendheid in de memorie van toelichting, met name waarom het wetsvoorstel nu geboden is en niet gewacht kan worden tot de algehele herziening van de Wiv 2017. De toegenomen dreiging vanuit landen met een offensief cyberprogramma en de operationele knelpunten die de AIVD en MIVD ervaren in de onderzoeken naar deze landen vormen de aanleiding voor de Tijdelijke wet. Langer wachten met het oplossen van deze knelpunten belemmert de diensten bij het adequaat beschermen van de belangen van Nederlandse burgers, bedrijven, militairen en bondgenoten. De noodzaak om de desbetreffende knelpunten op te lossen wordt bevestigd door de rapporten van de Evaluatiecommissie Wiv en de Algemene Rekenkamer. Het ligt in de lijn der verwachting dat de oplossingen voor de knelpunten die in de Tijdelijke wet zijn opgenomen ook onderdeel zijn van de algehele herziening van de Wiv 2017. Echter het herzieningstraject zal naar verwachting nog enkele jaren vergen en het is niet verantwoord om voor het onderzoek naar landen met een offensief cyberprogramma gericht tegen Nederland op de afronding van dat traject te wachten.

Waar het gaat om de vraag van deze leden of met betrekking tot de nota van wijziging nog spoedadvies bij de Afdeling advisering is gevraagd, verwijzen wij naar het antwoord op een vergelijkbare vraag van de leden van de fractie van de SP.

De leden van de CDA-fractie lezen dat de Tijdelijke wet bedoeld is om bedreigingen vanuit diverse landen met een offensief cyberprogramma het hoofd te bieden, waarbij zij aangegeven dat de landen die met name genoemd worden China, Rusland, Iran en Noord-Korea zijn. Deze leden vragen of de Tijdelijke wet nu expliciet er op toeziet dat alleen aanvallen uit deze landen het hoofd wordt geboden of geeft de wet voldoende mogelijkheden om te kunnen ingrijpen wanneer andere landen buiten deze vier een offensief cyberprogramma gaan ontwikkelen. In reactie hierop merken wij op dat de wet is ook van toepassing is op het moment dat er sprake is van cyberdreiging en cyberaanvallen door andere landen dan die welke door deze leden worden genoemd. Wij verwijzen deze leden voor het overige naar hetgeen wij aan het begin van onderdeel I (Algemeen deel) van deze nota naar aanleiding van het verslag in reactie op vragen van de leden van de D66-fractie hebben uiteengezet over de wijze waarop het onderzoek van de diensten zich ook op andere landen kan gaan richten.

De leden van de CDA-fractie lezen dat de acties van de hiervoor genoemde landen los moeten worden gezien van eveneens schadelijke, maar met een crimineel oogmerk verrichte aanvallen. Betekent dit nu, aldus deze leden, dat deze wet niet ingezet kan worden op gelijksoortige aanvallen maar dan van criminelen, niet gelieerd aan een land met een offensief cyberprogramma. Waarom, zo vragen deze leden, wordt de vertrouwelijke informatie, economische en technologische kennis die door criminelen wordt verzameld bij een aanval en daarna doorverkocht aan een land met een offensief cyberprogramma niet op dezelfde wijze beoordeeld als een aanval van land met een offensief cyberprogramma. Het gaat er volgens deze leden toch om dat vertrouwelijke informatie, en economische en technologische kennis wordt beschermd, niet op welke wijze een land met een offensief cyberprogramma deze verzamelt. Zij

vernemen graag waarom de regering dit onderscheid maakt. Wij merken hier het volgende over op. De reikwijdte van de Tijdelijke wet is gericht op onderzoek naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen. Wanneer deze landen in het kader van hun offensieve cyberprogramma ook gebruik maken van bedrijven of groeperingen, vormen deze bedrijven en groeperingen daarmee een dreiging voor de nationale veiligheid en kan onderzoek daarnaar ook plaatsvinden binnen de reikwijdte van deze wet. Het is daarbij niet bepalend of het gaat om criminelen of niet. Daarbij moet het vermoeden bestaan dat de aanval te linken is aan een statelijke actor. Indien dat niet zo, of tijdens het onderzoek dit vermoeden wordt ontkracht, valt het onderzoek niet meer onder de reikwijdte van de Tijdelijke wet. In dat geval kunnen de diensten het onderzoek eventueel vervolgen onder de Wiv 2017. Verder sluit dit ook niet uit dat andere aanvallen die een dreiging van de nationale veiligheid inhouden, wel degelijk door de diensten in onderzoek kunnen worden genomen op grond van de Wiv 2017.

De leden van de SP-fractie zijn niet overtuigd van de noodzakelijkheid van de Tijdelijke wet en vinden een periode van vijf jaar (bedoeld zal zijn vier jaar) ook niet tijdelijk en vragen waarom er geen horizonbepaling in de wet zit als deze tijdelijk zou zijn. Deze leden wijs ik op artikel 17 van het wetsvoorstel, waarin is voorzien dat de Tijdelijke wet vier jaren na het tijdstip van inwerkingtreding vervalt.

De leden van de SP-fractie geven aan dat in de technische briefings en het rondetafelgesprek werd gesproken over een experimenteerwet. Zij vragen of de regering kan aangeven waar het karakteriseren van het wetsvoorstel als een experimenteerwet vandaan komt en of de regering het met deze karakterisering eens is. In reactie hierop merken wij op dat in de technische briefing die is gegeven door de diensthoofden en directeur CZW deze wet niet als een experimenteerwet is aangemerkt. Het is een tijdelijke wet die voor een nijpend probleem van de diensten bij het verrichten van onderzoeken naar landen met een offensief cyberprogramma een oplossing moet bieden, een en ander in afwachting van de brede herziening van de Wiv 2017. In het algemeen deel van de memorie van toelichting, met name de paragrafen 1 en 2, is op nut en noodzaak van de in het wetsvoorstel opgenomen voorzieningen ingegaan, die de mogelijkheden tot effectieve inzet van de bijzondere bevoegdheden die voor onderzoeken naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen van cruciale betekenis zijn, vergroten, waarbij tegelijkertijd de waarborgen waarmee die inzet moet zijn omgeven op een hoog niveau blijven. De Tijdelijke wet is een tijdelijke oplossing totdat de herziening van de Wiv 2017 zijn beslag krijgt.

De leden van de SGP-fractie vragen een motivering van de keuze van de verschillende onderdelen van het wetsvoorstel, in het licht van het feit dat nog een Hoofdlijnennotitie volgt en een algehele herziening van de Wiv 2017. Wij antwoorden deze leden graag als volgt. De toegenomen dreiging vanuit landen met een offensief cyberprogramma en de operationele knelpunten die de AIVD en MIVD ervaren in de onderzoeken naar deze landen vormen de aanleiding voor de Tijdelijke wet. Langer wachten met het oplossen van deze knelpunten belemmert de diensten bij het adequaat beschermen van de belangen van Nederlandse burgers, bedrijven, militairen en bondgenoten. De noodzaak om de desbetreffende knelpunten op te lossen wordt bevestigd door de rapporten van de ECW en de Algemene Rekenkamer. Het ligt in de lijn der verwachting dat de oplossingen voor de knelpunten die in de Tijdelijke wet zijn opgenomen ook onderdeel kunnen uitmaken van de algehele herziening van de Wiv 2017. Daarom wordt de werking van de Tijdelijke wet ook periodiek gemonitord en worden de resultaten daarvan bij de voorgenomen

herziening van de Wiv 2017 betrokken. In de Hoofdlijnennotitie die gelijktijdig met deze nota naar aanleiding van het verslag aan de Tweede Kamer is aangeboden, wordt nader ingegaan op de hoofdlijnen van de algehele herziening van de Wiv 2017.

De leden van de SGP-fractie lezen dat de regering met het wetsvoorstel operationele knelpunten wil verhelpen. Zij vragen zich af waarom in dat licht ook onderwerpen als geschillenbeslechting zijn opgenomen, terwijl zulke thema's beter passen in het vervolgtraject aangezien het fundamentele systeemkeuzes betreft die uitgebreid doordenking vergen. Deze leden vragen waarom niet met andere, tijdelijke oplossingen in de sfeer van geschillenbeslechting kan worden volstaan om tegemoet te komen aan de zorgen die op dit punt leven. Wij reageren hierop graag als volgt. Ervan uitgaande dat deze leden met hun vragen beogen aan te geven dat herziening van het stelsel van toetsing en toezicht een fundamentele systeemkeuze betreft, dan onderschrijven wij dat. Dat is een vraagstuk dat bij de herziening van de Wiv 2017 aan de orde zal komen en waarop in de Hoofdlijnennotitie ook wordt ingegaan. Dat er in dit wetsvoorstel reeds een voorstel voor geschillenbeslechting is opgenomen hangt echter samen met de wens om operationele knelpunten die de diensten op dit moment bij hun onderzoeken in het cyberdomein ervaren, te verhelpen, nu immers een deel van die knelpunten zijn terug te voeren op verschillen van inzicht met de TIB over de uitleg en toepassing van diverse wettelijke bepalingen, ook waar het gaat om de (rol)invulling van de TIB bij de uitvoering van haar rechtmatigheidstoets. De ECW wijt dit onder meer aan een systeemfout in de Wiv 2017, namelijk het ontbreken van de mogelijkheid om geschillen op dit vlak aan een rechter te kunnen voorleggen. Waar het gaat om de introductie van het bindend toezicht voor de afdeling toezicht van de CTIVD, hangt dat samen met het feit dat de Kamer in de aanvaardde motie van het lid Van Baarle[12] heeft aangegeven dat – kort gezegd – er bij verschuivingen in het toezichtstelsel geen afschaling van toezicht in de verwerkingsfase mag optreden. Hoewel de motie primair ziet op de herziening van de Wiv 2017 is de daarin neergelegde notie ook bij de voorstellen inzake de beperking van de ex-ante toets van de TIB in een aantal gevallen in acht genomen, door in plaats daarvan bindend toezicht voor de afdeling toezicht te introduceren. Daarnaast is bindend toezicht ook voorzien op de toepassing van de bijschrijfmogelijkheden zoals voorzien in de Tijdelijke wet. Met de thans gemaakte keuzes wordt niet vooruitgelopen op keuzes die bij de herziening van de Wiv 2017 zullen worden gemaakt, zij het dat het beroep op de Afdeling bestuursrechtspraak ook bij de herziening zal terugkomen. In dat kader zal onder meer bezien worden of het mogelijk is om aansluiting te zoeken bij de beroepsprocedure in de Algemene wet bestuursrecht. De tijdelijke aanpassingen in het stelsel van toetsing en toezicht zullen na inwerkingtreding van de Tijdelijke wet worden gemonitord en mede op basis van de daarmee opgedane ervaringen zal een besluit inzake een andere inrichting van het stelsel van toetsing en toezicht, waarbij ook de klachtbehandeling zal worden betrokken, worden genomen. In de Hoofdlijnennotitie wordt nader geschetst hoe wij dat traject voor ons zien. In de Hoofdlijnennotitie worden ook meerdere scenario's voor de herinrichting van dat stelsel geschetst.

2.2 Integrale wijze van onderzoek in het cyberdomein en gegevensverwerking

De leden van de SP-fractie vragen of zij goed begrijpen dat de verworven gegevens onder deze tijdelijke wet, gericht op landen met een offensief cyberprogramma, burgers in Nederland kunnen betreffen. Zij vragen of de

[12] Kamerstukken II 2020/2021, 29 924, nr. 218.

regering kan uitleggen hoe dat precies werkt. Voor zover deze vraag ziet op OOG-interceptie, is deze bevoegdheid per definitie een bulkbevoegdheid met een grote mate van inherente ongerichtheid bij het verzamelen van gegevens. Allereerst moet worden opgemerkt dat alle onderzoeken waar OOG-interceptie wordt ingezet of waar verzoeken daartoe zijn gedaan door de diensten deze gericht zijn op het buitenland. In het kader van de Tijdelijke wet zal dat immers altijd het geval zijn: de onderzoeken zijn naar landen met een offensief cyberprogramma. Het is op voorhand, door de werking van het internet, niet uit te sluiten dat daarbij ook gegevens van burgers uit Nederland worden verworven. Gegevensstromen over het wereldwijde internet zijn niet af te bakenen op geografische grenzen. Er is geen evident «Nederlands» verkeer of «Russisch» verkeer. Gegevensstromen worden dynamisch gerouteerd waarbij bijvoorbeeld sprake kan zijn van keuzes op basis van prijs of snelheid. De werking van dit systeem kan dus betekenen dat bijvoorbeeld een mail verzonden vanaf een account van een persoon in Amsterdam naar een account van een persoon in Breda niet uitsluitend over de binnenlandse infrastructuur wordt gerouteerd, maar deels via buitenlandse infrastructuur en als gevolg daarvan bij OOG-interceptie wordt verworven. Dat is een technische realiteit van hoe het internet functioneert die onder ogen moet worden gezien. Dergelijke gegevens zullen echter in vrijwel alle gevallen niet voor het inlichtingenproces gebruikt mogen worden en niet verder worden verwerkt.

De leden van de SP-fractie vragen of zij het goed lezen dat de verworven gegevens onder de Tijdelijke wet ingezet mogen worden voor andere opsporingsactiviteiten. Wij reageren hierop graag als volgt. Allereerst wordt opgemerkt dat de diensten geen opsporingsactiviteiten (mogen) verrichten (zie artikel 13 Wiv 2017); de diensten verrichten onderzoeken in het kader van de nationale veiligheid. Wel is het zo dat gegevens die onder toepassing van de Tijdelijke wet door een dienst worden verworven, ook gebruikt kunnen worden voor andere lopende onderzoeken van die dienst. Er is geen enkele reden om op dit aspect af te wijken van hetgeen uit de (toepasselijke) Wiv 2017 voortvloeit. De gegevens die onder toepassing van de bevoegdheid tot verkennen als bedoeld in artikel 6, eerste lid, van het wetsvoorstel worden verworven, mogen echter *uitsluitend* worden gebruikt voor het daarin geformuleerde doel, namelijk om vast te stellen op welke gegevensstromen een verzoek om toestemming als bedoeld in artikel 48, tweede lid, Wiv 2017 betrekking dient te hebben. En dat betreft dan uitsluitend een verzoek om toestemming tot inzet van die bevoegdheid in het kader van de uitvoering van een onderzoek waarop de Tijdelijke wet betrekking heeft. De in het kader van de verkenning verworven gegevens mogen dus niet voor het inlichtingenproces worden gebruikt en mogen dus ook niet voor andere doeleinden of onderzoeken worden gebruikt. Waar het gaat om de wijze waarop het toezicht in dit geval plaatsvindt, antwoorden wij deze leden graag als volgt. Voor de uitoefening van de bevoegdheid tot verkenning als bedoeld in artikel 6, eerste lid, van de Tijdelijke wet dient de voor de dienst verantwoordelijke Minister toestemming te geven. Deze toestemming dient voor een bindende rechtmatigheidstoets te worden voorgelegd aan de TIB (artikel 6, derde lid). Daarmee wordt dus niet afgeweken van de regeling in de Wiv 2017, zoals die geldt voor de uitoefening van artikel 48 Wiv 2017. Daarnaast blijft op de uitvoering van de bevoegdheid het reguliere toezicht door de afdeling toezicht van de CTIVD, zoals geregeld in de Wiv 2017, gewoon van toepassing. Er vindt dan ook geen afschaling van het toezicht plaats.

De leden van de SP-fractie zouden graag een volledige lijst zien van de geautomatiseerde data-analyse zoals die in artikel 60 is bedoeld. Wij reageren hierop graag als volgt. In artikel 60, eerste lid, Wiv 2017 staat dat

de diensten bevoegd zijn om geautomatiseerde data-analyse (GDA) uit te voeren. Alle vormen van data-analyse kunnen onder deze bevoegdheid worden begrepen. De wet geeft geen definitie van het begrip GDA en dus ook geen scherpe afbakening van wat wel en niet onder GDA kan worden verstaan. Het tweede lid noemt een drietal vormen van GDA die bij de voorbereiding van de Wiv 2017 illustratief waren voor geautomatiseerde data-analyse. De opsomming is niet limitatief omdat de wet geschreven is met als doel om ook de toepassing van eventuele nieuwe methoden en technieken mogelijk te maken. Het is bovendien technisch gezien niet mogelijk om een dergelijke volledige lijst van vormen van geautomatiseerde data-analyse, zoals bedoeld in artikel 60 Wiv 2017, op te stellen, omdat voortdurend nieuwe methoden en technieken worden ontwikkeld die vaak bestaande methoden en technieken weer vervangen.

De leden van de SP-fractie geven aan dat het toezicht op verzamelde bulkdata goed moet kunnen inschatten wat de algoritmes die de data gaan onderzoeken precies doen en zoeken. Zij vragen of de regering kan aangeven of dit vormgegeven is op zo een wijze dat de geautomatiseerde analyse van data geen uitkomsten kent waarmee principes als de onschuldpresumptie worden ondermijnd. Hoe, zo vragen deze leden, wordt er gewaakt voor tunnelvisie via algoritmes en wellicht het missen van signalen. Deze leden zijn niet gerust op de mogelijkheid goed toezicht te houden op de automatische data-analyse als dit niet zo transparant mogelijk kan gebeuren. Zij vragen hierop een reactie van de regering. Wij reageren hierop als volgt. Artikel 60 van de Wiv 2017 geeft in algemene zin een regeling voor de toepassing van geautomatiseerde data-analyse van de diensten. Voor alle vormen van geautomatiseerde data-analyse geldt dat deze slechts toegepast mogen worden in het kader van een goede taakuitvoering van de diensten. Daarbij gelden de algemene bepalingen van gegevensverwerking uit de Wiv 2017 (artikelen 17 tot en met 24). In het bijzonder speelt de zorgplicht voor de rechtmatigheid van gegevensverwerking (artikel 24 Wiv 2017) een belangrijke rol bij geautomatiseerde data-analyse. De diensten moeten maatregelen treffen voor een zorgvuldige ontwikkeling, toepassing en beheer van geautomatiseerde data-analyses. Bovendien moet er samenwerking zijn tussen de ontwikkelaars en beheerders van geautomatiseerde data-analyses en de gebruikers. Zo wordt ervoor gezorgd dat het algoritme steeds passend is voor de situatie waarin het wordt gebruikt, voorzien van de meest actuele waarborgen. Een belangrijke waarborg bij de toepassing van GDA door de diensten is dat het de diensten niet is toegestaan om maatregelen jegens een persoon te bevorderen of te treffen uitsluitend gebaseerd op de resultaten van GDA. Er moet altijd sprake zijn van menselijke validatie, weging en tussenkomst. De afdeling toezicht houdt toezicht op de ontwikkeling en uitvoering van geautomatiseerde data-analyses. De afdeling heeft in het kader van hun toezichthoudende taak dan ook toegang tot de systemen van de diensten. Hierover publiceert de CTIVD ook in haar toezichtsrapporten, zoals rapport 69.[13] In de Tijdelijke wet wordt daarnaast geregeld dat de afdeling toezicht, binnen de reikwijdte van het wetsvoorstel, bindend kan oordelen over de toepassing van GDA op OOG-metadata. Tot slot wordt opgemerkt dat het principe van onschuldspresumptie een rol speelt in het kader van de opsporing en vervolging van strafbare feiten. De Nederlandse inlichtingen- en veiligheidsdiensten zijn daar niet mee belast. Het principe van onschuldspre-

[13] De CTIVD publiceerde de eerste twee jaar na inwerkingtreding van de Wiv 2017 in halfjaarlijkse rapportages over de implementatie van de wet door de diensten. In het afsluitende halfjaarlijkse rapport, rapport 69, oordeelt dat de implementatie van GDA op dat moment leidt tot een gemiddeld risico op onrechtmatigheden. Zie CTIVD nr. 69, Voortgangsrapportage IV over de implementatie van de Wiv 2017, p. 18.

sumptie is dan ook niet van toepassing in het domein van de inlichtingen- en veiligheidsdiensten.

2.2.3 De wijze van verwerking van gegevens
De leden van de PvdA-fractie lezen dat het toezicht een dynamisch karakter moet krijgen en dat daardoor ook gemonitord kan worden of de wet rechtmatig wordt uitgevoerd en of de in de wet voorziene waarborgen in verband met de bescherming van de persoonlijke levenssfeer adequate invulling krijgen. Deze leden vragen wat de gevolgen zijn indien gedurende deze monitoring blijkt dat de rechtmatige toepassing problematisch is of de waarborgen tekortschieten. Wordt, aldus deze leden, de wet dan aangepast en, zo ja, gaat dat dan meteen gebeuren; zo nee, waarom niet. In antwoord op deze vragen reageren wij graag als volgt. Het monitoren waarnaar deze leden verwijzen, heeft betrekking op het dynamische toezicht door de afdeling toezicht (monitoren van de rechtmatige uitvoering) en moet dan ook worden onderscheiden van het monitoren dat plaatsvindt met betrekking tot de toepassing van de Tijdelijke wet als zodanig en dat in reactie op een daartoe strekkend advies van de Afdeling advisering in het nader rapport is aangekondigd. Waar het gaat om het «monitoren», lees: de uitvoering van het dynamische toezicht door de afdeling toezicht, geldt juist dat die ertoe strekt om erop toe te zien dat de diensten de Tijdelijke wet op een rechtmatige wijze uitvoeren en daarbij de waarborgen in verband met de bescherming van de persoonlijke levenssfeer – niet alleen zoals die zijn voorzien in de Tijdelijke wet maar ook in de Wiv 2017 – in acht nemen. Indien bij de uitvoering van dit toezicht blijkt dat de wet door de diensten niet rechtmatig wordt uitgevoerd of dat men de waarborgen niet in acht neemt, dan staan de afdeling toezicht de reguliere toezichtsbevoegdheden ter beschikking die voortvloeien uit de Wiv 2017 aangevuld met die uit de Tijdelijke wet. Dit laatste ziet dan op de in artikel 12 van de Tijdelijke wet voorziene mogelijkheid om in de daar aangegeven gevallen (artikel 12, eerste lid) bindend toezicht uit te oefenen. Zoals hiervoor aangegeven zal de toepassing van de wet in brede zin worden gemonitord en de daarmee opgedane ervaringen zullen worden betrokken bij de brede herziening van de Wiv 2017, waarop in de Hoofdlijnnotitie wordt ingegaan. Er is dan ook niet voorzien in een tussentijdse aanpassing van de Tijdelijke wet.

Waar het gaat om de vraag van de leden van de PvdA-fractie of er alsnog een formeel tussentijds ijkmoment in de Tijdelijke wet kan worden opgenomen, naar wij aannemen bedoelt men daarmee een tussentijdse evaluatie, achten wij dat niet wenselijk. Zoals in reactie op het advies van de Afdeling advisering is opgemerkt (onderdeel 3), is in artikel 17 van het wetsvoorstel erin voorzien dat de wet na vier jaren vervalt. In die vier jaren zal de herziening van de Wiv 2017 niet alleen voorbereid moeten worden maar ook tot stand dienen te worden gebracht. Een formeel ijkpunt halverwege die periode zal, zeker indien dat een vorm krijgt van een formele evaluatie, vertragend gaan werken op de herziening. Immers een dergelijke evaluatie kost tijd – niet alleen om uit te voeren, maar ook om voor te bereiden – en heeft alleen betekenis, indien de resultaten daarvan worden afgewacht en worden meegenomen bij de herziening. Vandaar dat is aangegeven dat de Tijdelijke wet gedurende de looptijd zal worden gemonitord. Daartoe zal onder meer een jaar na inwerkingtreding een invoeringstoets worden uitgevoerd, maar ook daarna zullen de effecten van de werking van de wet op de daadwerkelijke praktijk worden bezien.

2.3 Overzicht van de voorgestelde maatregelen

De leden van de D66-fractie lezen dat de diensten uiterlijk binnen drie dagen een oordeel van de afdeling toezicht moeten uitvoeren. Drie dagen kunnen, aldus deze leden, onder omstandigheden erg lang maar ook erg kort zijn. Deze leden vragen of de diensten binnen die termijn een operatie (tijdelijk) stopzetten. Ook vragen zij of die termijn inhoudt dat de diensten binnen drie dagen de activiteit gestaakt moet hebben of de activiteit direct moet staken, en dit uiterlijk binnen drie dagen afgerond moet hebben. Tot slot vragen zij of de toezichthouder toezicht houdt op het staken van de activiteit en zou de termijn hiertoe niet proportioneel moeten zijn tegenover hoe snel dat realistisch en wenselijk is. Dit wetsvoorstel introduceert een bindende vorm van toezicht voor de afdeling toezicht van de CTIVD. Indien de afdeling toezicht van oordeel is dat sprake is van een onrechtmatige situatie is het zaak zo spoedig mogelijk gevolg te geven aan dit oordeel, zodat de door de afdeling toezicht als onrechtmatig aangemerkte situatie niet langer dan nodig blijft bestaan. De afdeling toezicht komt niet lichtvaardig tot een oordeel van onrechtmatigheid. Hieraan gaat een onderzoek en een proces van hoor- en wederhoor vooraf. Een onrechtmatigheidsoordeel zal – gelet op de doorlopende informatie-uitwisseling en constructieve dialoog tussen diensten en CTIVD – voor de diensten naar verwachting niet als een verrassing komen. Een termijn van drie dagen wordt, gelet op de technische en organisatorische handelingen die het beëindigen van een onrechtmatig aangemerkte situatie vergen, redelijk geacht.

De leden van de D66-fractie hebben kennisgenomen van de wijzigingen op het gebied van kabelinterceptie. Zij vragen of de regering een voorbeeldcasus kan schetsen voor wat er nodig is om de inzet van de bevoegdheid tot verkennende kabelinterceptie als omschreven in artikel 6 te rechtvaardigen. Is, zo vragen deze leden, de wens om in een vervolgstadium OOG-interceptie toe te passen afdoende. Als antwoord op deze vragen reageren wij als volgt. Zoals genoemd in artikel 6 van de Tijdelijke wet kan de desbetreffende bevoegdheid, namelijk verkennend onderzoek ten behoeve van OOG-interceptie, ingezet worden met het uitsluitende doel om vast te stellen op welke gegevensstromen een verzoek om toestemming voor OOG-interceptie ten behoeve van het inlichtingenproces betrekking dient te hebben. Indien de diensten OOG-interceptie op de kabel voor het inlichtingenproces willen inzetten om zicht te krijgen op het offensieve cyberprogramma van een statelijke actor, zullen zij eerst moeten weten hoe en over welke gegevensstromen deze actor communiceert. Deze informatie kan onder meer verkregen worden door gegevens op te vragen bij aanbieders van communicatiediensten op grond van artikel 52 Wiv 2017 of door intern onderzoek. Hieruit kunnen aanwijzingen volgen die gebruikt worden bij een verzoek om toestemming voor de inzet van het verkennend onderzoek ten behoeve van OOG-interceptie, namelijk bijvoorbeeld dat dit verkennende onderzoek gericht zal zijn op internationaal verkeer en mogelijk antwoord zal geven op de onderzoeksopdracht waarvoor wordt verkend. Met de inzet van deze verkennende bevoegdheid wordt beter zicht gecreëerd op eventuele activiteiten/aanwezigheid van de statelijke actor op deze gegevensstromen. Deze opbrengsten zullen vervolgens uitsluitend gebruikt worden om het verzoek om toestemming voor OOG-interceptie ten behoeve van het inlichtingenproces te onderbouwen. De opbrengsten van de verkennende bevoegdheid komen dus niet beschikbaar voor het inlichtingenproces. Voor de verdere uitwerking van OOG-interceptie ten behoeve van het inlichtingenproces verwijzen wij naar paragraaf 3.3.

Deze leden vragen voorts of de regering een indicatie kan geven van de mogelijke schaal van de dataverzameling op basis van de voorgestelde bevoegdheid tot ongerichte kabelinterceptie. Wij merken ter zake het volgende op. Het doel van de verwerving van de gegevens op grond van artikel 6 van de Tijdelijke wet, het verkennen ten behoeve van OOG-interceptie, is om met deze kennis het verzoek voor OOG-interceptie ex artikel 48 Wiv 2017 zo goed mogelijk te kunnen onderbouwen. Als belangrijke waarborg verbiedt dit wetsvoorstel de opbrengst van de verkenning te gebruiken voor inlichtingendoeleinden. Het algemeen of cijfermatig aangeven van een schaal van de dataverzameling van gegevens op basis van deze bevoegdheid is niet mogelijk aangezien de inzet per keer enorm kan verschillen.

De leden van de D66-fractie vragen of de regering in een limitatieve lijst kan opsommen waarvoor de via verkennende kabelinterceptie verkregen gegevens allemaal verwerkt mogen worden. Hierop antwoorden wij als volgt. Het doel van de verwerking van de gegevens is om met deze kennis het uiteindelijke toestemmingsverzoek, met daarin de aspecten genoemd in artikel 7 van de Tijdelijke Wet, voor OOG-interceptie ex artikel 48 Wiv 2017 te kunnen onderbouwen. Als belangrijke waarborg verbiedt het wetsvoorstel de opbrengst van de verkenning te gebruiken voor inlichtingendoeleinden. Gegevens mogen dus enkel worden verwerkt om de toestemmingsverzoeken voor OOG-interceptie naar landen met een offensief cyberprogramma te kunnen onderbouwen. De verzoeken zijn altijd gebaseerd op de aandachtsgebieden van de diensten zoals geformuleerd in de GA.

Deze leden vragen voorts of de regering kan aangeven waarom de toestemming tot verkennende kabelinterceptie een jaar geldig is en waarom deze termijn niet dusdanig wordt verkort in overeenstemming met het doel van de bevoegdheid of verlengd waar nodig met een verzwaarde toets. In artikel 48, tweede lid, van de Wiv 2017 is bepaald dat de toestemming voor de uitoefening van de bijzondere bevoegdheid tot OOG-interceptie door de Minister kan worden verleend voor een periode van ten hoogste een jaar. Bij de uitwerking van de regeling voor de verkenningsbevoegdheid, die immers gerelateerd is aan de uitoefening van de bevoegdheid ex artikel 48, eerste lid, van de Wiv 2017, is bij die systematiek aangesloten. Zoals uit de formulering blijkt gaat het om een maximumtermijn en bestaat de mogelijkheid om voor een kortere termijn toestemming te verkrijgen. Daarnaast kan, indien dat noodzakelijk is, na afloop van de periode waarvoor toestemming is verleend, een nieuwe toestemming worden aangevraagd. De verleende toestemming wordt door de TIB op rechtmatigheid getoetst.

De leden van de D66-fractie vernemen dat met de ongerichte interceptiebevoegdheid op de kabel gegevens kunnen worden verworven en met buitenlandse «collegadiensten» mogen worden gedeeld voor technisch onderzoek. In dit verband vragen deze leden of de regering kan aangeven wie wel en wie niet «collegadiensten» zijn en welke criteria zijn daaraan zijn verbonden en welke rol de wegingsnotities hierin spelen. Wij antwoorden deze leden graag als volgt. Collegadiensten zijn inlichtingen- en veiligheidsdiensten van andere landen waar een samenwerkingsrelatie mee is. In artikel 88 Wiv 2017 is het aangaan van samenwerkingsrelaties met de inlichtingen- en veiligheidsdiensten genormeerd. Wegingsnotities spelen hierin een belangrijke rol, aangezien die de basis vormen voor de besluitvorming door de Minister of met een dienst van een ander land kan worden samengewerkt en zo ja, wat de aard en intensiteit van die samenwerking kan zijn (de voorwaarden voor samenwerking). Bij de uit te voeren weging spelen in ieder geval de volgende aspecten een rol:
– De democratische inbedding van de dienst in het desbetreffende land;

– De eerbiediging van de mensenrechten door het desbetreffende land;
– De professionaliteit en betrouwbaarheid van de desbetreffende dienst;
– De wettelijke bevoegdheden en mogelijkheden van de dienst in het desbetreffende land;
– Het door de desbetreffende dienst geboden niveau van gegevensbescherming.

De verstrekking van de gegevens waarop de leden van de D66-fractie in hun vraagstelling op duiden, is dan ook alleen mogelijk indien dat past binnen de op grond van de weging vastgestelde voorwaarden van samenwerking. Indien deze niet voorziet in de verstrekking van gegevens, dan kunnen daaraan ook niet de gegevens ten behoeve van technisch onderzoek worden verstrekt.

De leden van de D66-fractie vragen of het klopt dat zowel de verstrekking als de naleving van de gemaakte afspraken zich onttrekken aan bindende toezichtsbevoegdheden van de TIB en de CTIVD. Hierover merken we op dat ook onder de Wiv 2017 de bindende ex ante toets van de TIB zich niet uitstrekt over de verstrekking van gegevens die met de inzet van bijzondere bevoegdheden zijn verworven. Die toets is immers beperkt tot de door de Minister verleende toestemmingen voor de inzet van bijzondere bevoegdheden in de sfeer van de verwerving van gegevens (enkele uitzonderingen daargelaten) en niet op de verdere verwerking van de daarmee verworven gegevens. Dat valt immers onder de reguliere – niet bindende – toezichtsbevoegdheid van de afdeling toezicht. Dit wordt niet anders onder de werking van de Tijdelijke wet.

Waar het gaat om het toezicht op de naleving op de gemaakte afspraken tussen de collegadiensten en de Nederlandse diensten, waarnaar deze leden aansluitend informeren, en of de situatie kan ontstaan dat gegevens of toepassingen die niet door de Nederlandse inlichtingendiensten mogen worden gebruikt wel kunnen worden gebruikt bij buitenlandse diensten, merken we het volgende op. Voor het verstrekken van gegevens aan buitenlandse diensten bestaat een zorgvuldig stelsel met bijbehorende waarborgen, waarop de CTIVD toezicht houdt. De AIVD en MIVD kunnen samenwerken met buitenlandse diensten waarvoor een wegingsnotitie is opgesteld als bedoeld in artikel 88 Wiv 2017. In een wegingsnotitie wordt een weging gemaakt waarbij in ieder geval de volgende criteria dienen te worden betrokken: de eerbiediging van de mensenrechten, democratische inbedding en de professionaliteit en betrouwbaarheid van de dienst. In een wegingsnotitie kunnen tevens aanvullende waarborgen voor samenwerking worden opgenomen. Een voorbeeld daarvan is dat bepaalde gegevens – bijvoorbeeld ongeëvalueerde gegevens – niet met een bepaalde dienst mogen worden gedeeld. Voor het delen van gegevens met een buitenlandse dienst moet altijd eerst toestemming worden gegeven. Afhankelijk van de aard van de gegevens en de uitkomst van de uitgevoerde weging van de buitenlandse dienst zijn er verschillende toestemmingsniveau 's voorzien, tot aan de betrokken Minister. De AIVD en MIVD stellen in voorkomende gevallen voorwaarden aan het gebruik van de gegevens. In het kader van technisch onderzoek van gegevens verworven door middel van OOG-interceptie ten behoeve van verkennen onder de Tijdelijke wet zal expliciet die voorwaarde worden toegevoegd. Voor deze voor de AIVD en MIVD soms noodzakelijke ondersteuning mag de desbetreffende partnerdienst enkel op de aangegeven gronden, dus voor technisch onderzoek, de verstrekte gegevens gebruiken. Tevens geldt de zogenaamde derde partij-regel: verstrekte gegevens mogen nooit zonder toestemming van de AIVD of MIVD aan derden worden verstrekt. Ook wordt als voorwaarde gesteld dat door de AIVD en MIVD verstrekte gegevens niet mogen worden gebruikt ten behoeve van handelingen die in strijd zijn met internationale recht. De

naleving van gemaakte afspraken met een buitenlandse collegadienst is onderworpen aan de (ongeschreven) vertrouwensregel die in de samenwerking tussen inlichtingen- en veiligheidsdiensten van toepassing is. Indien geconstateerd wordt dat een dienst van een ander land zich niet aan de gestelde voorwaarde(n) houdt, zal de samenwerkingsrelatie met die dienst opnieuw worden gewogen. Afhankelijk van de uitkomst wordt besloten of de samenwerkingsrelatie moet worden voortgezet en, zo ja, wat dan de aard en de intensiteit van die relatie – mede in het licht van de geconstateerde vertrouwensbreuk – moet zijn. Dat kan betekenen dat met de desbetreffende buitenlandse dienst geen gegevens meer mogen worden gedeeld. Schending van het wederzijdse vertrouwen is namelijk een «doodzonde» in de internationale samenwerking tussen inlichtingen- en veiligheidsdiensten.

De leden van de SP-fractie zouden graag willen weten hoe en wanneer de TIB om een toestemmingsaanvraag wordt gevraagd als het gaat om een bijschrijving van een server waar veel burgers gebruik van maken. Hierop antwoorden wij als volgt. In het algemeen geldt dat de diensten de Minister verzoeken om toestemming voor de inzet van bepaalde bijzondere bevoegdheden, zoals de bevoegdheid tot binnendringen in een geautomatiseerd werk. Hiervoor worden toestemmingsverzoeken geschreven door de diensten, die – na een interne juridische toets en na toestemming van het diensthoofd – vervolgens aan de verantwoordelijke Minister worden voorgelegd. Wanneer de Minister toestemming verleent, wordt de door de Minister verleende toestemming voor de inzet van de bevoegdheid op rechtmatigheid getoetst door de TIB. Daarbij wordt geoordeeld aan de hand van de criteria noodzaak, proportionaliteit, subsidiariteit en gerichtheid. De TIB wordt dus niet gevraagd om toestemming maar beoordeelt de door de Minister verleende toestemming op rechtmatigheid. Dat oordeel is bindend. Op grond van artikel 5, tweede lid, is de reeds in artikel 45, achtste lid, Wiv 2017 voorziene bijschrijfmogelijkheid verduidelijkt. Deze bijschrijfmogelijkheid zorgt ervoor de diensten effectief onderzoek kunnen doen dat past bij de dynamische dreiging en operationele praktijk. Juist in het cyberdomein zijn snelheid en wendbaarheid – het mee kunnen bewegen met een actor – cruciaal. Hierbij staat het gebruik van het kenmerk door de actor centraal. Gedurende de toestemmingsperiode kunnen dus ook (na interne autorisatie) geautomatiseerde werken zoals servers die behalve door de actor ook door burgers of andere derden worden gebruikt, worden bijgeschreven. Hierbij blijven de vereisten van noodzaak, proportionaliteit en subsidiariteit onverkort gelden. Bij de toepassing daarvan is dus geen (aanvullende) toestemming van de Minister voorzien en dus ook geen TIB-toets. Deze leden zien het dan ook goed dat binnendringen op een aldus bijgeschreven geautomatiseerd werk bij een door de Minister verleende toestemming tot verlenging van de uitoefening van de bevoegdheid door de TIB getoetst kan worden, afhankelijk van de vraag of hetgeen is bijgeschreven ook in de verlengingsaanvraag terug komt. Een en ander betekent niet dat er geen toezicht op de toepassing van deze bijschrijfmogelijkheid bestaat. In het wetsvoorstel is dit immers onderworpen aan het bindend toezicht van de afdeling toezicht van de CTIVD. Er is dus sprake van een sluitend stelsel van toetsing en toezicht op de inzet en uitvoering van de bevoegdheid tot het binnendringen in een geautomatiseerd werk, inclusief op de in het wetsvoorstel voorziene bijschrijfmogelijkheid.

De leden van de SP-fractie vragen hoe is geregeld dat de verworven gegevens die niet relevant zijn voor het onderzoek ook daadwerkelijk zullen worden vernietigd. Hierop antwoorden wij als volgt. Het vernietigen van gegevens omdat deze niet-relevant zijn verklaard zal op eenzelfde

wijze geschieden als de beide diensten kennen onder de Wiv 2017. De CTIVD houdt toezicht op de daadwerkelijke uitvoering hiervan.

Tot slot vragen deze leden de regering om aan te geven hoe lang de diensten gegevens die via een bijschrijving zijn verkregen kunnen onderzoeken zonder dat daarvoor enige toets op proportionaliteit heeft plaatsgevonden. Dit is naar ons oordeel niet mogelijk. Wij wijzen erop dat intern bij de diensten bijschrijvingen worden getoetst aan de wettelijke vereisten, zoals onder meer de in paragraaf 3.1 van de Wiv 2017 opgenomen algemene bepalingen die gelden voor elke vorm van gegevensverwerking door de diensten. De toets op proportionaliteit maakt daar deel van uit. En ook hier geldt dat de CTIVD toezicht houdt op de uitvoering van de bevoegdheid tot binnendringen in een geautomatiseerd werk en de verwerking van de daarmee verkregen gegevens.

2.4 De verhouding van de Tijdelijke wet tot de Wiv 2017

De leden van de VVD-fractie hebben vernomen dat voorliggend wetsvoorstel een tijdelijke wet betreft met een horizonbepaling van vier jaar. Zij vragen of de regering het traject tot herziening van de Wiv 2017 kan concretiseren dat binnen de werkingsduur van de Tijdelijke wet moet worden bewerkstelligd. Voorts vragen deze leden welke concrete stappen worden de komende tijd genomen om dit traject te bestendigen en hoe deze stappen en plannen zich verhouden tot voorbereiding van de Tijdelijke wet. Tot slot vragen deze leden op welke wijze de regering voornemens is vertraging in dit traject tot aanpassing van de wet te voorkomen zonder daarbij de voortvarendheid van het wetstraject van de tijdelijke wet uit het oog te verliezen. Hierop antwoorden wij als volgt. De Tijdelijke wet beoogt tijdelijke voorzieningen te treffen om een urgent probleem met betrekking tot het kunnen verrichten van onderzoeken door de AIVD en MIVD naar cyberdreigingen tegen Nederland en Nederlandse belangen op korte termijn te adresseren. Herziening van de Wiv 2017 is een naar aard en omvang ingrijpender wetstraject, dat veel meer voorbereidingstijd vraagt en bovendien een goede afstemming met diverse betrokken stelselpartners – waaronder ook de toezichthouders – vergt. De hoofdlijnen van de in gang te zetten herziening zijn geschetst in de Hoofdlijnennotitie. Na bespreking daarvan met de Tweede Kamer, zal het wetstraject worden ingezet. In afwachting daarvan zullen reeds verkennende studies plaatsvinden, bijvoorbeeld naar de toepasselijkheid van de Algemene wet bestuursrecht, de aspecten verbonden aan een bulkdataregeling en een regeling voor gegevensverwerking, opdat het wetstraject – concreet de uitwerking in een wetsvoorstel met toelichting – vervolgens met voortvarendheid kan starten. Het is onze inschatting dat dit in een periode van vier jaar (de looptijd van de Tijdelijke wet) kan worden gerealiseerd. Inzichten die gaande het wetstraject worden opgedaan met de toepassing van de Tijdelijke wet zullen daarbij worden betrokken.

De leden van de D66-fractie vragen of de regering kan aangeven in hoeverre het beschermen van economische belangen verdisconteerd is in het belang van de nationale veiligheid. In antwoord op deze vraag willen wij in algemene zin het volgende opmerken. Economische belangen kunnen ingeval daarbij tevens nationale veiligheidsbelangen in het geding zijn onder de taakstelling van de diensten vallen en – via de GA – door de verantwoordelijke Ministers in onderzoeksopdrachten worden vervat. Het begrip nationale veiligheid zoals dat in de Wiv 2017 wordt gehanteerd komt overeen met hetzelfde begrip zoals dat wordt gehanteerd in het EVRM, met name in artikel 8 EVRM waar het als één van de doelcriteria geldt die een beperking op het recht op bescherming van de persoonlijke levenssfeer (private and family life) legitimeert, en volgt de uitleg die

daaraan door het EHRM wordt gegeven.[14] Er bestaat geen formele definitie van nationale veiligheid. Uit de jurisprudentie van het EHRM komt het beeld naar voren dat het begrip ruim wordt uitgelegd. Aan de bij het EVRM aangesloten staten wordt een «wide margin of appreciation» gelaten. Afhankelijk van maatschappelijke omstandigheden en de bijbehorende mogelijke bedreigingen is het mogelijk het begrip nationale veiligheid nader in te vullen. De invulling van het begrip vindt in de Nederlandse praktijk met name plaats door de wetgever, die in de taakartikelen van de AIVD en de MIVD in de Wiv 2017 en de daarbij gegeven toelichting al enige richtinggevende uitspraken heeft gedaan, en in de uitwerking van de taakstelling in de Geïntegreerde Aanwijzing (GA) ex artikel 6 Wiv 2017.

De leden van de fractie van D66 vragen – meer concreet – in hoeverre het beschermen van bedrijven een belangrijk aspect is bij de voorliggende wet. Ook vragen zij of het beschermen van economische belangen een doel op zich is. Tot slot vragen deze leden welke mate of schaal van economische schade de regering verwacht te voorkomen met voorliggend voorstel. Hierop antwoorden wij als volgt. De diensten hebben de wettelijke taak om onderzoek te doen naar activiteiten van statelijke en andere actoren die een dreiging kunnen vormen voor de economische veiligheid van Nederland voor zover daarbij ook sprake is van nationale veiligheidsbelangen. Immers de diensten mogen alleen onderzoek verrichten in het kader van de nationale veiligheid. Een dergelijke dreiging kan zich voordoen in de vorm van ongewenste kennis- of technologieoverdracht en onwenselijke strategische afhankelijkheden. Zoals gesteld in het Dreigingsbeeld Statelijke Actoren (november 2022) staat de economische veiligheid van Nederland onder druk. Zo zijn vitale processen kwetsbaar voor spionage, sabotage en ook, als gevolg van bijvoorbeeld investeringen en overnames, voor ongewenste invloed en strategische afhankelijkheid van statelijke actoren. Tegelijkertijd is er sprake van een toename van misbruik van die risicovolle strategische afhankelijkheden. De Europese afhankelijkheid van Russisch gas heeft dat recent duidelijk gemaakt. Ook ongewenste kennisoverdracht vormt een dreiging voor de economische veiligheid van Nederland. Zo zijn Nederlandse bedrijven, kennisinstellingen en wetenschappers op grote schaal doelwit van (digitale) actoren die hoogwaardige technologie proberen buit te maken, bijvoorbeeld door middel van cyberspionage of het omzeilen van exportrestricties. Diefstal en het weglekken van kennis brengt het risico van oneerlijke concurrentie en ongewenst eindgebruik voor bijvoorbeeld militaire doeleinden met zich mee. De diensten verwachten niet dat deze dreiging op korte of middellange termijn minder wordt. De kwetsbaarheid van nationale veiligheidsbelangen is niet alleen afhankelijk van de dreiging door statelijke actoren, maar ook van de weerbaarheid van Nederland. Twee specifieke taken van de AIVD die bijdragen aan een weerbare overheid en bedrijfsleven zijn de zogeheten naslagtaak[15] en het werk dat de diensten in het kader van hun beveiligingsbevorderende taak. Onder de veiligheidsbevorderende taak valt het in het kader van de nationale veiligheid bevorderen van maatregelen ter bescherming van het voortbestaan van de democratische rechtsorde, de veiligheid of andere gewichtige belangen van de staat. Daaronder vallen ook maatregelen ter beveiliging van gegevens waarvan de geheimhouding door de nationale veiligheid wordt geboden en van die onderdelen van de overheid en van het bedrijfsleven die van vitaal belang zijn voor de instandhouding van het maatschappelijk leven en voor de MIVD van de krijgsmacht.[16] Een integrale aanpak van weerbaarheid vraagt ook breed maatschappelijk

[14] Kamerstukken II 1999/2000, 25 877, nr. 9, p. 13 e.v.
[15] Taak ex artikel 8, tweede lid, onder f, (AIVD) en 10, tweede lid, onder g, (MIVD) Wiv 2017.
[16] Taak ex artikel 8, tweede lid, onder c, (AIVD) en 10, tweede lid, onder d, MIVD) Wiv 2017.

bewustzijn van de economische dreigingen tegen Nederland. De AIVD droeg ook daar in 2022 met partners aan bij. Door in gesprek te gaan met vitale sectoren en topsectoren en adviezen te geven. En door bedrijven en burgers bewuster te maken van het bestaan van economische spionage en de gevolgen daarvan. Ook zetten de diensten zich in om (defensie)bedrijven en kennisinstellingen bewuster te maken van risico's op spionage en ongewenste kennisoverdracht. Dat doen de diensten vaak samen met de betrokken ministeries. Op de vraag van deze leden in welke mate of op welke schaal de regering verwacht economische schade te voorkomen met voorliggend wetsvoorstel, antwoorden wij, dat het niet mogelijk is om op voorhand daarvan een inschatting te maken.

De leden van de D66-fractie vragen voorts of de regering kan aangeven of zij ten aanzien van het voorkomen van economische schade de inbreuken op privacyrechten van burgers gerechtvaardigd achten conform dezelfde proportionaliteitsafwegingen zoals op het vlak van nationale veiligheid. Hierop antwoorden wij als volgt. De diensten hebben in het belang van de nationale veiligheid mede als taak onderzoek te doen om de economische veiligheid en kennisveiligheid van Nederland te waarborgen. Dit is conform hetgeen staat gesteld in de Nationale Veiligheidsstrategie. De Nederlandse economische- en kennisveiligheid worden ook bedreigd door landen met een offensief cyberprogramma. In het Dreigingsbeeld Statelijke Actoren, opgesteld door de AIVD, MIVD en NCTV, is de dreiging van statelijke actoren tegen de economische veiligheid van Nederland en haar bondgenoten de afgelopen jaren duidelijker naar voren gekomen. Wanneer deze veiligheid, als onderdeel van de nationale veiligheid, in het geding komt en mogelijk economische schade voor Nederland en Nederlandse belangen als gevolg heeft, bijvoorbeeld aan vitale sectoren, hebben de diensten dezelfde bevoegdheden tot hun beschikking om in te zetten in het onderzoek naar de dreiging, als naar andere dreigingen gericht tegen de nationale veiligheid. In ieder onderzoek van de diensten wordt per bevoegdheid en per casus een proportionaliteitsafweging gemaakt, waarbij het onderzoeksbelang voor de nationale veiligheid wordt afgewogen tegen de privacy-inbreuk die de bevoegdheid met zich meebrengt.

De leden van de D66-fractie vragen of de regering kan schetsen hoe er bij samenloop van verschillende onderzoekstaken van de diensten wordt bepaald of en waarop het nieuwe toezichtstelsel van toepassing is. Hierop antwoorden wij als volgt. In artikel 2, tweede lid, van het wetsvoorstel is bepaald dat op de uitvoering van de in artikel 2, eerste lid, bedoelde taak de Wiv 2017 van toepassing is met inachtneming van het bepaalde in deze wet. Dat geldt dus ook voor het stelsel van toetsing en toezicht; wat in de Wiv 2017 ter zake is bepaald geldt met inachtneming van het bepaalde in de Tijdelijke wet. De onderzoeken die de diensten dienen te verrichten worden op grond van artikel 6 Wiv 2017 in de GA geformuleerd en geprioriteerd en dat geldt niet anders voor onderzoeken naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen. Daarmee is nog niet gezegd dat dus altijd de Tijdelijke wet van toepassing is. De toepasselijkheid van de Tijdelijke wet wordt immers binnen het stelsel van de Tijdelijke wet telkens ad hoc bepaald en wordt in het verzoek om toestemming voor de inzet van een bijzondere bevoegdheid aangegeven. Ingeval een target van de dienst in verschillende onderzoeken van de dienst is betrokken, waaronder een onderzoek naar landen met een offensief cyberprogramma, en vanuit die verschillende onderzoeken de inzet van een bijzondere bevoegdheid jegens dat target wordt overwogen, dan zal een ad hoc afweging dienen plaats te vinden voor welk onderzoek de inzet van die bijzondere bevoegdheid en de daarmee te verkrijgen gegevens het grootste belang heeft oftewel waar het zwaartepunt van het onderzoek naar het target ligt. Als dat zwaar-

tepunt bij het onderzoek naar landen met een offensief cyberprogramma ligt, dan kan de toepasselijkheid van de Tijdelijke wet worden ingeroepen. Daarvoor geldt de volgende werkwijze:

- Waar het gaat om de toepassing van alle bijzondere bevoegdheden als bedoeld in paragraaf 3.2.5 van de Wiv 2017 geldt dat op grond van artikel 2, derde lid, dient te worden aangegeven of daarbij uitvoering wordt gegeven aan de Tijdelijke wet.
- Voor zover het een bijzondere bevoegdheid betreft waarop de Tijdelijke wet van toepassing is verklaard en die is onderworpen aan de ex ante toetsing door de TIB geldt dat de TIB die toetst conform het bepaalde in de Wiv 2017 met inachtneming van het bepaalde in de Tijdelijke wet.
- Indien de TIB van oordeel is dat met betrekking tot de aan haar voorgelegde toestemming ten onrechte is bepaald dat daarmee toepassing wordt gegeven aan de Tijdelijke wet, deelt zij dit terstond mede aan de Minister. De TIB toetst vervolgens de toestemming zonder toepassing van het bepaalde in de Tijdelijke wet. Uitsluitend de Wiv 2017 is dan van toepassing. Tegen het oordeel van de TIB dat in casu de Tijdelijke wet niet van toepassing is staat voor de Minister beroep open bij de Afdeling bestuursrechtspraak. Ingeval de TIB een onder toepassing van de Tijdelijke wet verleende toestemming goedkeurt, deelt zij dit terstond mede aan de afdeling toezicht van de CTIVD. Indien de TIB onder toepassing van de Tijdelijke wet de goedkeuring weigert, vervalt de toestemming van rechtswege. Tegen het oordeel van de TIB staat voor de Minister beroep open bij de Afdeling bestuursrechtspraak.
- Voor zover het gaat om bijzondere bevoegdheden die op grond van de Tijdelijke wet zijn onttrokken aan de ex ante toetsing van de TIB, geldt nog steeds dat in de aanvraag voor toestemming bepaald dient te zijn dat de Tijdelijke wet van toepassing is. Van de verleende toestemming in deze gevallen dient terstond mededeling te worden gedaan aan de afdeling toezicht van de CTIVD.
- Waar het gaat om de bijschrijfmogelijkheden bij toepassing van artikel 47 en 54 Wiv 2017 (de artikelen 9 en 10) geldt dat van de toepassing daarvan terstond mededeling dient te worden gedaan aan de afdeling toezicht van de CTIVD. Deze bijschrijfmogelijkheden bestaan uitsluitend indien ten aanzien van de bijzondere bevoegdheid die het betreft (artikel 47 en 54) overeenkomstig artikel 2, derde lid, is bepaald dat toepassing wordt gegeven aan de Tijdelijke wet.
- De afdeling toezicht van de CTIVD krijgt in het kader van de toepassing van de Tijdelijke wet in aanvulling op het bepaalde in de Wiv 2017 in een limitatief aantal gevallen (artikel 12, eerste lid) de bevoegdheid bindende oordelen te geven en te bepalen of ze daaraan – eveneens limitatief bepaalde (artikel 12, tweede lid) – gevolgen verbindt. Tegen de bindende oordelen van de afdeling toezicht en de daaraan verbonden gevolgen staat voor de Minister de mogelijkheid van beroep op de Afdeling bestuursrechtspraak open.

Resumerend: het vaststellen of de Tijdelijke wet toepassing moet vinden – ook ingeval van samenloop van onderzoeken naar een zelfde target – vindt primair plaats in het kader van de toestemmingverlening voor een bijzondere bevoegdheid, secundair – voor zover een TIB-toets is voorgeschreven – door de TIB en – ingeval de TIB de Tijdelijke wet niet van toepassing acht – uiteindelijk door de Afdeling bestuursrechtspraak bij een eventueel tegen dat oordeel ingesteld beroep.

De leden van de D66-fractie verzoeken de regering nader uiteen te zetten waarom de huidige spoedprocedure volgens hen niet toereikend is. Ook vragen zij of de regering kan aangeven hoe vaak er van de huidige spoedprocedure – uitgesplitst per jaar – gebruik is gemaakt sinds de inwerkingtreding van de Wiv-2017 en of uitgesplitst kan worden welk

percentage dit van het volledige aantal verzoeken per jaar vormt. In dit verband wordt verwezen naar de beantwoording op soortgelijke vragen van de SP-fractie en PvdA-fractie. In onderstaande tabel wordt het door deze leden gevraagde overzicht verstrekt.

Jaar	Totaal aantal verzoeken[1]	spoedprocedure	Percentage spoedverzoeken op volledige aantal verzoeken
2022	2.902	129	4.4%
2021	3.071	111	3.6%
2020	2.784	86	3.1%
2019	2.355	68	2.9%
2018	2.159	112	5.2%

[1] **Boven genoemde cijfers komen uit de jaarverslagen van de TIB**

In het jaar 2023 tot en met de maand juli heeft de AIVD 1.579 verzoeken aan de TIB voorgelegd, waarop 72 de spoedprocedure van toepassing was. Het percentage spoedverzoeken op het volledige aantal verzoeken dat op rechtmatigheid is getoetst door de TIB komt voor de AIVD van 1 januari tot en met 31 juli 2023 uit op 4,6%.

De leden van de CDA-fractie vragen wat de stand van zaken is met betrekking tot de toegezegde Hoofdlijnennotitie inzake de voorgenomen wijziging van de Wiv 2017. De Hoofdlijnennotitie is gelijktijdig met de aanbieding van deze nota naar aanleiding van het verslag aan de Tweede Kamer aangeboden.

De leden van de SP-fractie willen graag weten hoe de geheime diensten zullen bepalen welke wet – de Tijdelijke wet of de Wiv 2017 – van toepassing is bij samenloop van verschillende onderzoekstaken en voorts wat nu precies de voorliggende keuze wordt bij inlichtingenactiviteiten richting landen met een offensief cyberprogramma. Deze leden verwijzen we naar hetgeen hiervoor in antwoord op een (deels) vergelijkbare vraag van de leden van de fractie van D66 is geantwoord.

Naar aanleiding van de vraag van deze leden hoe de regering erop toeziet dat de diensten niet onnodig het lichtere toezichtsregime van de Tijdelijke wet inzetten, willen we opmerken dat van een lichter toezichtsregime geen sprake is. Integendeel. Waar de ex ante TIB-toets in een beperkt aantal gevallen is beperkt, is ter compensatie voorzien in ex durante bindend toezicht door de afdeling toezicht van de CTIVD, omdat dat beter past bij het dynamische karakter van de uitvoering van de desbetreffende bevoegdheden door de diensten. En ook overigens is het toezichtinstrumentarium van de afdeling toezicht in het kader van de Tijdelijke wet ten opzichte van de regeling in de Wiv 2017 met extra bindende oordeelsbevoegdheden uitgebreid. Er is vanuit toezichtsoptiek dan ook geen enkele reden te veronderstellen dat de diensten de Tijdelijke wet onnodig inzetten. Zowel intern (via de reguliere verantwoordingslijn vanuit de diensten naar de Minister) als extern (door de TIB en de afdeling toezicht) bestaan er mechanismen die een juiste toepassing van de Tijdelijke wet borgen.

De leden van de SP-fractie vragen ten slotte op welke wijze er afspraken zijn gemaakt met de toezichthouders en de diensten dat altijd gekozen zal worden voor het minst ingrijpende onderzoeksmiddel, in plaats van de meest vergaande. Wij beantwoorden deze vraag als volgt. Er zijn met de TIB of de CTIVD ter zake geen afspraken gemaakt. Dat is ook niet nodig, nu immers uit artikel 26, eerste lid, van de Wiv 2017 voortvloeit dat de

diensten het zogeheten subsidiariteitsvereiste dienen toe te passen. De TIB en de CTIVD zien ieder vanuit hun taak toe op de toepassing daarvan door de diensten.

De leden van de PvdA-fractie lezen dat het aan de TIB is om te beoordelen of de bevoegdheden van de Tijdelijke wet mogen worden ingeroepen dan wel dat de bestaande Wiv 2017 van toepassing is. Daarbij geldt dat een bevoegdheid alleen op grond van de Tijdelijke wet mag worden ingezet als het zwaartepunt van de inzet op onderzoeksopdrachten binnen de reikwijdte van deze wet valt. Deze leden vragen hoe en op grond waarvan dat zwaartepunt wordt bepaald. Wij beantwoorden deze vraag als volgt. Het kan inderdaad voorkomen dat vanuit verschillende lopende onderzoeken van de dienst aandacht is voor een bepaald(e) target(organisatie). In die gevallen kan een bevoegdheid alleen onder toepassing van de Tijdelijke wet worden ingezet als het zwaartepunt van de inzet betrekking heeft op onderzoeksopdrachten die binnen de reikwijdte van deze wet vallen. De wijze waarop dit zwaartepunt wordt bepaald is zeer afhankelijk van de omstandigheden van de specifieke casus. Voor de inzet van een bijzondere bevoegdheid onderbouwen de diensten de onderzoeksvragen die bijdragen aan de beantwoording van onderzoeksopdrachten zoals vastgesteld in de GA. Er zijn enkele criteria die richting geven aan het bepalen van het zwaartepunt. Deze criteria zijn bijvoorbeeld ten behoeve van welk inlichtingenteam de bevoegdheid wordt ingezet en voor welke onderzoeksopdracht de meeste opbrengst door de inzet van de bevoegdheid wordt verwacht. De Minister geeft al dan niet toestemming voor de onderbouwing dat ofwel het Tijdelijke wet-regime ofwel het Wiv 2017-regime van toepassing is. De TIB toetst deze toestemming op rechtmatigheid.

De leden van de PvdA-fractie lezen dat als het om de reikwijdte van de wet gaat (paragraaf 3.1) het voor de diensten niet altijd mogelijk is om een cyberaanval aan een specifiek land te linken en te beoordelen of er al dan niet sprake is van een statelijke actor. En ook of er sprake is van een offensief cyberprogramma. Kortom, zo stellen deze leden, hoe kan op voorhand duidelijk worden of de Tijdelijke wet van toepassing is? De reikwijdte van deze Tijdelijke wet is beperkt tot onderzoeken van de diensten naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen. Welke landen dat zijn wordt bepaald aan de hand van de GA. Daarnaast bepaalt de GA dat de diensten onderzoek moeten doen naar cyberdreigingen en cyberaanvallen enkel vanwege het feit dat deze op Nederland of Nederlandse belangen zijn gericht en dat het vermoeden bestaat dat deze te attribueren is aan een statelijke actor. In die gevallen is de Tijdelijke wet ook van toepassing. Zowel de TIB als de CTIVD zijn bekend met de inhoud van de GA. In een verzoek tot toestemming voor de inzet van een bijzondere bevoegdheid wordt onderbouwd waarom de deze onder de Tijdelijke wet valt. Ook als niet (direct) een digitale aanval te attribueren is aan een land, maar er wel een vermoeden is dat deze te attribueren is aan een statelijke actor wordt dat onderbouwd. Op basis van deze onderbouwing wordt toestemming gegeven door de Minister, welke toestemming op rechtmatigheid wordt getoetst door de TIB.

De leden van de PvdA-fractie vragen hoe de Tijdelijke wet gebruikt wordt om de strengere voorwaarden van de Wiv 2017 te vermijden. Wij verwijzen deze leden naar hetgeen ik hiervoor op eenzelfde vraag van de leden van de SP-fractie heb geantwoord.

Tot slot vragen de leden van de PvdA-fractie hoe kan worden voorkomen dat gegevens van onschuldige personen die voor de diensten niet interessant (zijn) – laat staan voor buitenlandse diensten – door gebruik-

making van de Tijdelijke wet toch breder beschikbaar komen. Wij merken daarover op dat de Tijdelijke wet niet tot doel heeft en ook geen specifieke of afwijkende regeling bevat ten opzichte van de Wiv 2017 om gegevens van personen die niet relevant zijn voor onderzoeken van de diensten breder beschikbaar te stellen. De in de Wiv 2017 neergelegde waarborgen die gelden als het gaat om internationale samenwerking zijn onverkort van toepassing.

De leden van de GroenLinks-fractie merken op dat in aanloop naar de invoering van de Wiv 2017 een uitgebreide parlementaire behandeling heeft plaatsgevonden. Ook vond er een uitgebreide maatschappelijke discussie plaats in aanloop naar het raadgevend referendum over het wetsvoorstel. Zowel tijdens de parlementaire behandeling als tijdens de discussie in de campagne voor het referendum kwam de gerichtheid van het zogenoemde sleepnet uitgebreid aan de orde. Het uitgangspunt dat geformuleerd werd was dat bevoegdheden zo gericht mogelijk moeten worden ingezet om te voorkomen dat onnodig gegevens van burgers worden verzameld die geen doel van het specifieke noodzakelijke onderzoek zijn. Deze leden hechten sterk aan dit uitgangspunt en zijn van mening dat ook bij een gewijzigde wet de bijzondere bevoegdheden die de diensten hebben zo gericht mogelijk moeten worden ingezet. Zij vragen of de regering hierop kan reflecteren. Ook wij hechten aan dat uitgangspunt, en het vereiste dat bijzondere bevoegdheden door de diensten zo gericht mogelijk moeten worden ingezet blijft ook in de Tijdelijke wet gelden; ook bij de bevoegdheid tot kabelinterceptie ten behoeve van het inlichtingenonderzoek. De Tijdelijke wet maakt daarop één uitzondering, namelijk bij de bevoegdheid tot OOG-interceptie ten behoeve van verkennen. Bij deze bevoegdheid die juist dient om vast te stellen waarop de toepassing van artikel 48 Wiv 2017 (OOG-interceptie), waarbij sprake is van verwerving van gegevens ten behoeve van het inlichtingenproces, zich dient te richten, is de eis van gerichtheid bij de uitoefening van de verkenningsbevoegdheid naar zijn aard niet toepasbaar. Dit wordt tevens door de CTIVD in rapport 75 naar inzet van kabelinterceptie toegelicht.[17] Het is daarbij van belang te benadrukken dat deze bevoegdheid dient als opstap naar het indienen van interceptie ten behoeve van het inlichtingenproces. Deze gegevens mogen dan ook alleen gebruikt worden ten behoeve van het indienen van die aanvraag. Voor deze interceptie ten behoeve van het inlichtingenproces geldt de eis van gerichtheid onverkort.

De leden van de GroenLinks-fractie vragen hoe het gerichtheidscriterium sinds de inwerkingtreding van de Wiv 2017 in de praktijk is toegepast en op welke wijze dit criterium onder de Tijdelijke wet wordt vormgegeven. Voorts vragen deze leden hoe de toezichthouders hier zo adequaat mogelijk toezicht op blijven houden. Wij beantwoorden deze vraag als volgt. Bevoegdheden die de diensten inzetten om gegevens te verzamelen moeten zo gericht mogelijk door de diensten worden ingezet. De diensten doen wat redelijkerwijs in hun vermogen ligt om reeds bij verwerving van gegevens de niet voor het onderzoek noodzakelijke gegevens tot een minimum te beperken en motiveren dit in hun aanvraag tot de inzet van een bevoegdheid. De invulling van het gerichtheidscriterium is sterk afhankelijk van de bevoegdheid die wordt ingezet, de omstandigheden van een specifieke operatie en de fase waarin het onderzoek zich bevindt. Ook wordt rekening gehouden met de inlichtingencontext, bijvoorbeeld of het inzetten van de bevoegdheid dient tot onderzoek naar een gekend contraterrorisme-target of een ongekende statelijke dreiging. De Tijdelijke wet wijzigt het gerichtheidscriterium op zichzelf niet. Bij een aanvraag tot toestemming voor OOG-interceptie ten behoeve van het inlichtingen-

[17] Toezichtsrapport over de inzet van kabelinterceptie door de AIVD en de MIVD (CTIVD nr. 75).

proces wordt in de Tijdelijke wet nader gespecificeerd welke aspecten met name – en daarmee het zwaarwegendst – moeten worden betrokken bij de invulling van de eisen van gerichtheid en proportionaliteit en de toets daarop (artikel 7 van het wetsvoorstel). Bij de bevoegdheid tot verkennen ten behoeve van OOG-interceptie heeft het gerichtheidsvereiste geen betekenis, gelet op de aard en het doel van de bevoegdheid (artikel 6, vierde lid van het wetsvoorstel). In de praktijk motiveren de diensten bij de aanvraag van een bevoegdheid tot het verzamelen van gegevens op welke wijze de bevoegdheid zo gericht mogelijk wordt ingezet. Op deze manier kan de TIB bij haar rechtmatigheidstoets op de door de Minister verleende toestemming toetsen op welke wijze de diensten voornemens zijn de desbetreffende bevoegdheid zo gericht mogelijk in te zetten. De afdeling toezicht kan tijdens haar onderzoeken inzicht krijgen in de manier waarop de diensten invulling hebben gegeven aan het gerichtheidsvereiste tijdens de uitvoering van een bevoegdheid en daarop toezicht houden.

De leden van de GroenLinks-fractie constateren dat er zorgen en verwarring is ontstaan over de vraag of het toezicht door de TIB en de CTIVD nu wel of niet wordt ingeperkt. Zij vragen om in een helder schematisch overzicht het huidig toezicht te schetsen en in ditzelfde schema aan te geven hoe dit toezicht in de tijdelijke wet wordt gewijzigd en of daarbij sprake is van een versterking of inperking. Wij bieden graag deze verduidelijking en willen benadrukken dat met het voorliggend voorstel geen sprake is van inperking van het toezicht op het handelen van de diensten.

Huidig stelsel van toetsing en toezicht in de Wiv 2017	**Wijzigingen op grond van de Tijdelijke wet**	**Compenserende maatregel**	**Effect**
TIB toetst ex ante de toestemmingen voor de in artikel 32 Wiv 2017 gespecificeerde bijzondere bevoegdheden	Ex ante toets door de TIB van verleende toestemmingen vervalt met betrekking tot: – De verkenning van geautomatiseerde werken ex artikel 45, eerste lid, onder a, Wiv 2017 (artikel 4 Tijdelijke wet); – Geautomatiseerde data-analyse (GDA) op met OOG-interceptie verkregen metadata ex artikel 50, vierde lid, Wiv 2017 (artikel 8 Tijdelijke wet).	In plaats van bindend ex ante toets door de TIB komt bindend toezicht ex durante (gedurende de uitoefening van de bevoegdheid) en ex post (na afloop van de uitoefening van de bevoegdheid) door de afdeling toezicht van de CTIVD in de plaats.	Verschuiving van bindende toets ex ante naar bindend toezicht ex durante en ex post. Sluit beter aan bij fase van uitvoering onderzoek door de diensten en is daarmee effectiever. Aanpassingen zoals voorgesteld worden door zowel TIB als CTIVD ondersteund.

Huidig stelsel van toetsing en toezicht in de Wiv 2017	Wijzigingen op grond van de Tijdelijke wet	Compenserende maatregel	Effect
De afdeling toezicht van de CTIVD is op grond van artikel 97, derde lid, jo. paragraaf 7.2.2 Wiv 2017 belast met rechtmatig toezicht op de uitvoering van de Wiv 2017	Taak blijft ongewijzigd en wordt aangevuld met de mogelijkheid tot het geven van bindende oordelen met betrekking tot de in artikel 12, eerste lid, Tijdelijke wet gespecificeerde handelingen.	Verduidelijking bijschrijfmogelijkheden worden gecompenseerd door bindend toezicht door de afdeling toezicht.	Is versterking van het ex durante en ex post toezicht door de afdeling toezicht
	Mogelijkheid van beroep tegen oordelen van de TIB en de afdeling toezicht bij de Afdeling bestuursrechtspraak van de Raad van State	Herstel weeffout (ECW)	Versterking van het stelsel doordat Afdeling bestuursrechtspraak in geschillen tussen Minister en TIB of afdeling CTIVD inzake de uitleg of toepassing van de Tijdelijke wet definitief uitsluitsel kan geven (draagt bij aan doorbreken impasses).

De regering schrijft dat de voorliggende wet nadrukkelijk een tijdelijk karakter heeft. De leden van de GroenLinks-fractie vragen de regering nader in te gaan op het tijdelijke karakter van de voorliggende wet. Ook vragen zij op welke wijze de tijdelijke wijzigingen zullen worden geëvalueerd. Kan hierbij, aldus deze leden, ook aangegeven worden waarom bij het voorliggende wetsvoorstel gekozen is voor vier jaar en bijvoorbeeld niet voor een periode van twee jaar, zodat na twee jaar beoordeeld kan worden of verlenging noodzakelijk is of dat dan de herziening van de gehele Wiv 2017 gereed kan zijn. Wij beantwoorden deze vraag als volgt. De reden dat er voor een looptijd van vier jaar is gekozen, is dat na het uitbrengen aan de Kamer van de Hoofdlijnennotitie, het traject van de structurele herziening van de Wiv 2017 kan worden ingezet. De verwachting is dat de herziening binnen vier jaar zijn beslag moet kunnen krijgen. Een termijn van twee jaar is voor een herzieningstraject dat een bredere reikwijdte heeft dan de Tijdelijke wet niet realistisch. Mocht blijken dat de herziening van de Wiv 2017 eerder klaar is dan de looptijd van de Tijdelijke wet, dan kan deze ook eerder vervallen. Tot slot wordt opgemerkt dat om te kunnen beoordelen of de Tijdelijke wet functioneert zoals wordt beoogd, deze na inwerkingtreding (tussentijds) zal worden gemonitord. De resultaten daarvan zullen ook met de Kamer worden gedeeld. Deze zullen ook worden meegenomen in het bredere herzieningstraject.

De leden van de SGP-fractie vragen de regering om vanuit het perspectief van de uitvoeringspraktijk in te gaan op het dubbele regime van toetsing en toezicht dat ontstaat door het naast elkaar bestaan van de Wiv 2017 en de Tijdelijke wet. Zij vragen of het voldoende werkbaar is om rekening te houden met de verschillende regimes die door het wetsvoorstel ontstaan en ook wat dit betekent dat voor de administratieve belasting. Wij verwijzen deze leden naar ons antwoord op vergelijkbare vragen van de leden van de PvdA-fractie in onderdeel 1. Inleiding van deze nota naar aanleiding van het verslag.

De leden van de SGP-fractie vragen in het licht van de constatering van de Afdeling advisering dat het stelsel van toezicht in complexiteit toeneemt en dat het de vraag is of de beoogde doelen van het wetsvoorstel worden

bereikt, waarom de regering toch geen nut ziet in eenduidiger alternatieven. Wij hebben kennis genomen van de zorgen van de Afdeling advisering, zoals door deze leden geschetst. De Afdeling advisering geeft daarnaast echter ook aan dat men, gelet op de dreiging die uitgaat van landen met een offensief cyberprogramma, het niettemin begrijpelijk acht om thans, vooruitlopend op een definitieve wetswijziging, een aangepast regime voor een beperkt deel van de taken en bevoegdheden te beproeven. Daarbij is volgens de Afdeling advisering van belang dat veel van de in de Tijdelijke wet gekozen oplossingen corresponderen met de grondig gemotiveerde aanbevelingen van de ECW. De praktijk zal moeten uitwijzen of de met het wetsvoorstel beoogde doelen worden bereikt. Overeenkomstig het advies van de Afdeling advisering zullen dan ook de ervaringen met de voorgestelde maatregelen worden gemonitord en die zullen vervolgens worden betrokken bij de herziening van de Wiv 2017. Daarop zijn we eerder in deze nota naar aanleiding van het verslag al ingegaan. Bij de voorbereiding van het wetsvoorstel is uiteraard bezien hoe de problematiek waarvoor op korte termijn een oplossing moest worden gevonden, het beste kon worden geadresseerd en zijn ook alternatieven bezien. Daarbij was het van belang om de balans tussen enerzijds de verbetering van de mogelijkheden voor de diensten om onderzoek te doen naar dreigingen vanuit landen met een offensief cyberprogramma en anderzijds daarop te voorzien in adequaat en effectief toezicht een continu aandachtspunt. Erkend is dat er tijdelijk twee stelsels, ook waar het gaat om toezicht, naast elkaar bestaan. Maar zoals hiervoor reeds is uiteengezet is dit vanuit het perspectief van de diensten werkbaar.

De leden van de Volt-fractie merken op dat met de komst van de Tijdelijke wet een poging wordt gedaan om acute knelpunten te verhelpen. Ook wijzen ze erop dat de regering in de memorie van toelichting aangeeft dat de brede wetswijziging van de Wiv 2017 binnen de vervaltermijn van de Tijdelijke wet wordt afgerond. Deze leden vragen of de regering verwacht dat de inzet van de bevoegdheden uit de Tijdelijke wet over vier jaar niet langer nodig is of is het waarschijnlijk dat de wet dan verlengd wordt. Uit de memorie blijkt immers niet, aldus deze leden, dat de dreiging van tijdelijke aard is en dus vragen zij de regering waarom dan toch voor een tijdelijke wet is gekozen. Op basis waarvan acht de regering het waarschijnlijk dat de Wiv 2017 binnen vier jaar herzien is en welke manier gaat de regering ervoor zorgen dat de herziening van de Wiv 2017 binnen vier jaar zal plaatsvinden. Wij willen deze leden allereerst verwijzen naar onze reactie op (deels) vergelijkbare vragen van de leden van de GroenLinks-fractie waar het gaat om het tijdelijke karakter van de wet. In aanvulling daarop merken we nog het volgende op. Het is correct te veronderstellen dat de oplossingen die de Tijdelijke wet biedt voor de geconstateerde knelpunten- deels in aanvulling en deels in afwijking op het bepaalde in de Wiv 2017 – langer dan vier jaar nodig zijn. Voorzien is dat de oplossingen voor deze knelpunten daarom moeten worden meegenomen in het wetsvoorstel dat zal worden voorbereid in het kader van het traject van de herziening van de Wiv 2017.

De leden van de Volt-fractie vragen tot slot of het tijdelijke karakter van de wet een impact heeft op de rechtsbescherming van burgers. Voor de rechtsbescherming van de burgers heeft de Tijdelijke wet geen gevolgen. De mogelijkheden die de burgers hebben in het kader van rechtsbescherming op grond van de Wiv 2017 blijven immers onverkort van toepassing.

3. De maatregelen nader beschouwd

De leden van de PvdA-fractie lezen dat de diensten onderzoek doen naar cyberdreigingen en cyberaanvallen waarbij enkel het vermoeden dat deze te linken zijn aan een statelijke actor afdoende is om dat onderzoek te kunnen doen. Op grond waarvan, zo vragen deze leden, kunnen diensten een dergelijk vermoeden krijgen en hoe wordt dit afgebakend. Voorts vragen zij of degenen die toestemming moeten geven en gedurende het onderzoek dit moeten monitoren inzicht krijgen in de achtergrond van een vermoeden dat er sprake is van een statelijke actor. Wij beantwoorden deze vraag als volgt. Alle onderzoeken van de AIVD en MIVD vinden hun grondslag in de in artikel 8 onderscheidenlijk artikel 10 Wiv 2017 geregelde taakstelling en de ter uitvoering daarvan op grond van artikel 6 Wiv 2017 vastgestelde GA. De GA geeft de diensten de expliciete opdracht onderzoek te doen naar cyberdreigingen en cyberaanvallen vanwege het feit dat deze op Nederland of Nederlandse belangen zijn gericht en het vermoeden bestaat dat deze dreiging of aanval te attribueren is aan een statelijke actor. Dit vermoeden is altijd gebaseerd op bestaande informatie en inlichtingen.[18] De afbakening dat het vermoeden moet bestaan dat het om een statelijk actor gaat is van belang, omdat het taakveld van de inlichtingen- en veiligheidsdiensten in het geval van cyberdreiging zich daarop richt. In de aanvragen voor de inzet van bijzondere bevoegdheden worden de vermoedens onderbouwd en moet ook onderbouwd worden hoe de verzochte inzet bijdraagt aan de beantwoording van de onderzoeksvragen. Dat betekent dus inderdaad dat degene die toestemming geeft voor de inzet van een bevoegdheid – veelal de Minister – inzicht heeft in de onderbouwing van het vermoeden van een statelijke actor. Datzelfde geldt voor de TIB die de rechtmatigheid van de door de Minister gegeven toestemming toetst – voor zover de inzet van een bijzondere bevoegdheid aan haar toets onderworpen is – alsook de afdeling toezicht die toezicht houdt op het rechtmatig handelen van de diensten.

De leden van de SGP-fractie vragen of de regering meer concreet inzichtelijk kan maken wat de beoogde maatregelen kunnen betekenen voor de omvang en intensiteit van verzamelen van gegevens, mede met het oog op de maatschappelijke gevoeligheid van de thematiek. Deze leden vragen bijvoorbeeld aandacht voor de zorg dat volledige steden en woonwijken worden afgetapt, en dat bij intercepties gegevens van miljoenen burgers verzameld worden. Graag zouden zij op basis van de huidige ontwikkelingen vernemen welke verwachtingen reëel zijn als het gaat om frequentie en intensiteit. Wij gaan er bij onze beantwoording van uit dat de vraagstelling van deze leden specifiek betrekking heeft op de bevoegdheid tot OOG-interceptie in het kader van de Tijdelijke wet, immers daarover zijn de door deze leden genoemde zorgen geuit. Het is van belang om allereerst te benadrukken dat de diensten OOG-interceptie op de kabel niet zullen inzetten om een beeld te krijgen van de digitale handelingen van (Nederlandse) burgers. Kabelinterceptie betreft het intercepteren van getransporteerde gegevens over kabelgebonden infrastructuur. Anders dan bijvoorbeeld een gerichte internet- of telefoontap, welke gericht is op een apparaat van een persoon en/of organisatie en betrekking heeft op alle communicatie (inhoud en metadata)[19] die daarmee plaatsvindt waardoor een vollediger beeld van

[18] Dat is niet anders bij andere onderzoeken. Zie de a-taak van de AIVD, ter uitvoering waarvan het onderzoek als bedoeld in de Tijdelijke wet plaatsvindt, waarbij de dienst onder meer onderzoek moet verrichten naar organisaties en personen die door de doelen die zijn nastreven dan wel door hun activiteiten aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat.

[19] Tenzij het gaat om een stomme tap, waarbij uitsluitend verkeers- en locatiegegevens in real time worden verworven.

deze persoon en/of organisatie kan worden verkregen, is kabelinterceptie gericht op communicatiestromen. Deze communicatiestromen bevatten slechts gedeelten (fragmenten) van de communicatie van personen en organisaties in het digitale domein. Het levert – anders dan bij gerichte interceptie – geen volledig (en ononderbroken) beeld op van de communicatie van een persoon of organisatie. De diensten richten zich op communicatiestromen die internationaal gegevensverkeer bevatten. Zoals eerder in deze nota naar aanleiding van het verslag is uiteengezet, is vanwege de technische inrichting van het internet en de wijze waarop gegevensstromen daarop plaatsvinden, het nimmer uit te sluiten dat daarin ook gedeelten van gegevens van communicatieverkeer van Nederlandse burgers in zitten. De interceptie is daarop ook niet gericht. Waar het gaat om de betekenis van de beoogde maatregelen voor de omvang en intensiteit van OOG-interceptie merken we het volgende op. Een doel van de Tijdelijke wet is dat de diensten meer gegevensstromen kunnen verkennen (artikel 6) en aan de hand van een analyse van die gegevens beter kunnen bepalen via welke datastromen vervolgens de bevoegdheid tot OOG-interceptie (artikel 48 Wiv 2017) kan worden ingezet voor onderzoeken naar landen met een offensief cyberprogramma. Met deze aangepaste werkwijze wordt bewerkstelligd dat ten opzichte van de huidige situatie zowel de omvang als de frequentie voor het inzetten van de bevoegdheid tot OOG-interceptie ex artikel 48 Wiv 2017 kan worden vergroot en de effectiviteit van het onderzoek. Daarbij wordt opgemerkt dat ook voor de inzet van de verkennende bevoegdheid de normen van noodzaak, proportionaliteit en subsidiariteit onverkort van toepassing zijn. De TIB zal dus een rechtmatigheidsoordeel over een door de Minister verleende toestemming voor de inzet van de verkennende bevoegdheid moeten geven. De gegevens die worden geïntercepteerd onder artikel 6 worden overigens niet gebruikt voor inlichtingenonderzoek.

3.1 De reikwijdte van de wet

De leden van de VVD-fractie begrijpen dat de toegenomen cyberdreiging vanuit statelijke actoren een belangrijke aanleiding vormt voor het voorliggende wetsvoorstel. Hoewel deze leden met de regering van oordeel zijn dat de toegenomen cyberdreiging voor een substantieel deel wordt veroorzaakt door de agressie van diverse landen met een offensief cyberprogramma, staan de Nederlandse (veiligheids)belangen niet louter onder druk door statelijke actoren. In 2022 werd in het Cyber Security Beeld Nederland, een gezamenlijk document van het Nationaal Cyber Security Centrum en de AIVD en MIVD, gesteld dat ransomware aanvallen (van criminele groeperingen) inmiddels een bedreiging vormen voor de nationale veiligheid. Deze leden vragen welke rol de regering ziet voor de inlichtingen- en veiligheidsdiensten, in het bijzonder in het kader van voorliggend wetsvoorstel, in het tegengaan van bedreigingen voor de nationale veiligheid wanneer die uitgaan van criminele groeperingen. Wij beantwoorden deze vraag als volgt. De inlichtingen- en veiligheidsdiensten voeren hun taak uit in het kader van de nationale veiligheid. Als criminele actoren een dreiging vormen voor de nationale veiligheid en hun activiteiten een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of andere gewichtige belangen van de staat, heeft de AIVD de wettelijke taak daar onderzoek naar te doen. In het kader van voorliggend wetvoorstel is het van belang op te merken dat deze zich beperkt tot onderzoeken naar landen met een offensief cyberprogramma. Dit onderzoek richt zich dan ook primair op statelijke dreigingen tegen de rijksoverheid, defensie en vitale organisaties. Indien (criminele) organisaties in opdracht van of gelieerd zijn aan statelijke actoren die vallen onder de reikwijdte van de Tijdelijke wet, doen de diensten daar tevens in het kader van deze wet onderzoek naar. Zoals is vastgesteld in bijvoorbeeld het Cybersecurity-

beeld Nederland 2021 kunnen digitale aanvallen van criminele groeperingen echter ook een bedreiging vormen voor de nationale veiligheid. In dat geval vindt het onderzoek uitsluitend op grond van de Wiv 2017 plaats.

De leden van de GroenLinks-fractie lezen dat de regering niet vooraf kan bepalen welke landen gerekend zullen worden tot de categorie landen met een offensief cyberprogramma en geven aan dit op zichzelf te begrijpen. Zij vragen dan ook een nadere toelichting op hoe precies bepaald wordt wanneer er sprake is van een statelijke actor waarop de tijdelijke wet van toepassing is. Wij verwijzen deze leden allereerst graag naar onze reactie op een grotendeels zelfde vraag van de leden van de D66-fractie in het begin van het Algemeen deel van deze nota naar aanleiding van het verslag, waarin zij vragen welke landen onder de categorie landen met een offensief cyberprogramma vallen. In aanvulling daarop merken we nog het volgende op. Bij de dreiging van statelijke actoren hoeft de dreiging niet direct afkomstig te zijn van een regeringsapparaat, inlichtingendienst of krijgsmacht. Deze dreigingen en aanvallen kunnen zich ook manifesteren via bedrijven, groeperingen of instellingen die zich laten inzetten door statelijke actoren maar daar niet direct aan gelinkt kunnen worden. Het is aan de AIVD en MIVD om te onderzoeken of er bij dergelijke cyberaanvallen sprake is van een statelijke actor – en er dus een link is met een land – die dergelijke bedrijven en organisaties direct of indirect aanstuurt.

De leden van de SGP-fractie constateren dat de reikwijdte van de wet op twee punten een enigszins onbepaald karakter heeft, namelijk het vereiste dat het optreden van niet-statelijke actoren onderdeel en uitvloeisel moet zijn het handelen van landen en bovendien het criterium van de Nederlandse belangen. Deze leden vragen hoe de regering omgaat met het risico dat het bereik van de wet (gaandeweg) op oneigenlijke wijze kan worden opgerekt. Specifiek vragen zij een meer concrete duiding te geven van de Nederlandse belangen. Klopt het, zo vragen deze leden, dat hieronder bijvoorbeeld niet begrepen wordt het beschermen van individuele, grote bedrijven, maar dat de ernst hierbij altijd te maken moet hebben met de taken die de diensten op grond van de Wiv 2017 hebben in het belang van de nationale veiligheid. Wij beantwoorden deze vraag als volgt. Voor een nadere toelichting op het begrip Nederlandse belangen, verwijzen wij graag naar het antwoord dat wij eerder op een vraag van de leden van de SP-fractie hebben gegeven. Het beschermen van individuele, grote bedrijven kan een Nederlands belang zijn in het kader van bescherming van de economische veiligheid, waar de diensten op grond van hun wettelijke taken onderzoek naar moeten doen. Bij de inzet van een bevoegdheid moeten de diensten een toestemmingsverzoek schrijven. Dit verzoek geschiedt in het kader van een of meer onderzoeksopdrachten waarbij ze ook moeten aangeven of naar het oordeel van de diensten de Tijdelijke wet van toepassing is. Het is primair de verantwoordelijkheid van de diensten om binnen het juiste wettelijke kader te handelen. De TIB zal, ingeval in de verleende toestemming is bepaald dat de Tijdelijke wet van toepassing is, dit bij haar rechtmatigheidstoets kunnen betrekken. De TIB kan aldus erop toezien dat de verleende toestemming binnen het bereik van de wet past. Bij verschil van mening tussen de Minister en de TIB kan dit aan de Afdeling bestuursrechtspraak worden voorgelegd.

De leden van de SGP-fractie vragen voorts een toelichting op de stelling dat de wet ook van toepassing is op situaties waarin het vermoeden bestaat dat dreigingen te attribueren zijn aan een statelijke actor. Deze leden constateren dat het vermoeden niet duidelijk op te maken valt uit de Wiv 2017. Zo spreekt artikel 8, tweede lid, onderdeel d, slechts expliciet

over het verrichten van onderzoek betreffende landen. Waarom, zo vragen deze leden, heeft de regering geen aanleiding gezien om het criterium van het vermoeden duidelijker te verankeren in het wetsvoorstel. De leden van de SGP-fractie vragen ten slotte of de regering uitgebreider kan duiden wanneer sprake is van een vermoeden en op welke wijze dat vermoeden door de diensten aannemelijk dient te worden gemaakt. Wij merken naar aanleiding van deze vragen het volgende op. In artikel 2, eerste lid, van het wetsvoorstel is het onderzoek waarop onderhavig wetsvoorstel specifiek ziet nadrukkelijk als een uitwerking van de bestaande taakstelling van de diensten in artikel 8 (AIVD) en 10 (MIVD) van de Wiv 2017 geformuleerd. Dat is breder dan de inlichtingentaak buitenland van de AIVD en MIVD, zoals neergelegd in artikel 8, tweede lid, onder d, Wiv 2017, waarnaar deze leden verwijzen. Veeleer is relevant de taak van de diensten om onderzoek te doen naar dreigingen, zoals die onder meer in artikel 8, tweede lid, onder a, Wiv 2017 voor de AIVD is neergelegd. Aldaar is expliciet gesteld dat dit onderzoek betrekking heeft op organisaties en personen die door de doelen die zij nastreven, dan wel door hun activiteiten aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat. Maar ook al zou het aspect vermoeden niet zijn benoemd, het is inherent aan het onderzoek van de diensten dat men niet alleen onderzoek doet naar gekende dreigingen die te attribueren zijn aan gekende personen en organisaties, maar juist ook om ongekende dreigingen te onderkennen en te achterhalen welke persoon of organisatie (in casu statelijke actor) daarachter zit. Dat is het domein van de vermoedens. De specifieke landen met een offensief cyberprogramma waarnaar op dit moment door de AIVD en MIVD actief onderzoek wordt gedaan, worden genoemd in de staatsgeheim gerubriceerde bijlage bij de Geïntegreerde Aanwijzing (GA). Zoals hiervoor uiteengezet doen de diensten ook naar (op dit moment) ongekende dreigingen. Dit kunnen dreigingen zijn die nog niet geattribueerd kunnen worden aan een al gekende statelijke actor met een offensief cyberprogramma genoemd in de GA, of dreigingen die komen van statelijke actoren waarvan tot nu toe onbekend was dat zij een dreiging vormden tegen Nederland of Nederlandse belangen. De GA geeft de diensten namelijk de expliciete opdracht onderzoek te doen naar cyberdreigingen en cyberaanvallen vanwege het feit dat deze op Nederland of Nederlandse belangen zijn gericht en het vermoeden bestaat dat deze dreiging of aanval te attribueren is aan statelijke actor. Dit vermoeden is altijd gebaseerd op bestaande informatie en inlichtingen. Om vast te kunnen stellen of er sprake is van een statelijke actor moet uit het onderzoek van de inlichtingen- en veiligheidsdiensten blijken dat het offensieve cyber programma gefaciliteerd, gestuurd en/of gedoogd wordt door de overheid van de betreffende staat. Het is daarom van belang inzicht te krijgen in de doelstellingen, intenties en aansturing van landen waar de diensten onderzoek naar doen. Bij de dreiging van statelijke actoren hoeft de dreiging niet direct afkomstig te komen van een regeringsapparaat, inlichtingendienst of krijgsmacht. Deze dreigingen en aanvallen kunnen zich ook manifesteren via bedrijven, instellingen of meer diffuse proxy-organisaties. Het is aan de AIVD en MIVD om te onderzoeken of er bij dergelijke cyberaanvallen sprake is van een statelijke actor – en er dus een link is met een land – die dergelijke bedrijven en organisaties direct of indirect aanstuurt.

3.2 Verkennen van en binnendringen in een geautomatiseerd werk

De leden van de D66-fractie vragen of de regering kan bevestigen dat de rol van de TIB bij het verkennen van geautomatiseerde werken volledig verdwijnt, maar voor het binnendringen nog steeds geldt. Wij kunnen bevestigen dat in het kader van de Tijdelijke wet de bindende ex ante toets

van de TIB bij de uitoefening van de bijzondere bevoegdheid tot het *verkennen* van een geautomatiseerd werk wordt geschrapt en wordt vervangen door bindend toezicht van de afdeling toezicht gedurende de uitoefening van deze bevoegdheid alsmede achteraf (artikel 4 resp. 12, eerste lid, onder a).

Waar het gaat om de technische risico's die de TIB bij de uitoefening van de ex ante toets op het *binnendringen* van een geautomatiseerd werk kan betrekken, merken wij – naar aanleiding van een vraag van deze leden ter zake – het volgende op. Het wetsvoorstel voorziet er allereerst in dat bij een verzoek om toestemming om binnen te dringen in een geautomatiseerd werk niet meer de plicht bestaat om een omschrijving te geven van de technische risico's die verbonden zijn aan de uitoefening van de desbetreffende bevoegdheid. Deze eis leidt in de uitvoeringspraktijk immers tot onduidelijkheid: naast bekende technische risico's worden daar – door de TIB – ook de mogelijke technische risico's verbonden aan mogelijke handelingen in het kader van de uitvoering van de bevoegdheid onder begrepen. Zoals in de memorie van toelichting is uiteengezet[20], is het echter niet mogelijk om voorafgaand aan een toestemmingsperiode van drie maanden te voorspellen welke handelingen precies nodig zijn om gedurende die periode het met de inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk beoogde doel te bereiken. De eventuele technische risico's die gekoppeld zijn aan deze handelingen zijn daarom van tevoren ook niet te voorzien.[21] Het schrappen van de wettelijke eis om bij de aanvraag om toestemming voor het binnendringen in een geautomatiseerd (altijd) de technische risico's te vermelden, betekent niet dat er geen technische risico's meer worden vermeld in het verzoek om toestemming. Het vermelden van technische risico's dient – ook zonder een wettelijke plicht daartoe – nog steeds plaats te vinden, maar is beperkt tot de op het moment van aanvraag van de toestemming bekende risico's. Die zijn en blijven immers relevant voor de oordeelsvorming van de voor de dienst verantwoordelijke Minister. De toetsing van de TIB ziet op de door de Minister verleende toestemming en voor zover het gaat om de technische risico's is deze dan ook beperkt tot de bekende technisch risico's. Gezien de dynamische en onvoorzienbare aard van operaties waarbij wordt binnengedrongen in een geautomatiseerd werk zal deze toets een hoger abstractieniveau hebben. De afdeling toezicht houdt vervolgens toezicht op de uitvoering van de bevoegdheid en dus ook op de wijze waarop bekende en nieuwe technische risico's zich tijdens de uitvoering concreet voordoen. Daarmee verschuift de bindende ex ante toets voor andere risico's dan die welke op moment van toestemmingverlening bekend zijn naar de fase van dynamisch toezicht door de afdeling toezicht. Ingevolge artikel 12, eerste lid, onder b, van het wetsvoorstel is ook dat toezicht bindend voor zover dat betrekking heeft op de aan de uitoefening van de bevoegdheid verbonden technische risico's. Zoals in de brief aan de voorzitter van de TIB door ons is aangegeven, is er geen enkele intentie geweest om de wijze waarop de TIB de proportionaliteitstoets uitvoert in te perken, maar wel om via de toelichting duidelijk te maken dat waar het gaat om de beoordeling van de technische risico's in de nieuwe systematiek het domein van de TIB ophoudt en die van de afdeling toezicht van de CTIVD begint.[22] Het voorgaande geldt mutatis mutandis voor het gebruik van onbekende kwetsbaarheden door de diensten. Daarmee beantwoorden wij ook de vraag van de leden van de D66-fractie om wat bij de afdeling toezicht van de CTIVD komt te liggen en welke rol de TIB op dit vlak nog heeft.

---

[20] Paragraaf 3.2.4.1.

[21] Zie onder meer de inbreng van oud-technisch lid van de TIB, Ronald Prins, bij het rondetafelgesprek over de Tijdelijke wet.

[22] Zie bijlage bij Kamerstukken II 2022/2023, 36 263, nr. 6.

Deze leden horen graag via welk afwegingskader de diensten besluiten wel of niet gebruik te maken van onbekende kwetsbaarheden (ook wel zero-days genaamd). Het gebruik door de diensten van een onbekende kwetsbaarheid – indien daar technische risico's mee gepaard gaan – zal moeten vallen binnen de in het kader van een verzoek om toestemming gemaakte proportionaliteitsafweging. De AIVD en MIVD maken tevens gebruik van het «Beleid AIVD en MIVD over omgang met «onbekende kwetsbaarheden» in het geval dat er gebruik is gemaakt van een onbekende kwetsbaarheid. Dit beleid is openbaar[23]. In dit beleid is het uitgangspunt van «melden, tenzij» vastgelegd. Factoren waaraan wordt getoetst zijn risico's, wettelijke beperkingen, noodzaak en geheimhouding.

Deze leden vragen ten slotte of de regering kan aangeven of het enkel kwalificeren van onbekende kwetsbaarheden als technische risico's voldoende de maatschappelijke risico's meeweegt, zoals bij de gevolgen van de WannaCry aanvallen. En, zo ja, of de regering hier een voorbeeld bij kan schetsen. Wij beantwoorden deze vraag als volgt. Er dient onderscheid te worden gemaakt tussen technische risico's en maatschappelijke risico's. In een toestemmingsverzoek voor een specifieke inzet van deze bevoegdheid dient er (ingevolge artikel 26 van de Wiv 2017) in het kader van de proportionaliteit een afweging plaats te vinden tussen het onderzoeksbelang en het nadeel voor de betrokkene. In de memorie van toelichting bij de Wiv 2017 is verduidelijkt dat onder «betrokkene» moet worden verstaan degene jegens wie de bevoegdheid wordt ingezet. Dit betekent dus dat maatschappelijke risico's niet passen bij de te maken proportionaliteitsafweging in een toestemmingsverzoek dat gericht is op een specifiek persoon of specifieke organisatie. Dat betekent natuurlijk niet dat de diensten geen oog hebben voor maatschappelijke risico's, nu de diensten de verwezenlijking daarvan – net zo goed als bij technische risico's – wil voorkomen. De maatschappelijke risico's maken onderdeel uit van de afweging die wordt gemaakt bij de keuze om over te gaan tot het schrijven en indienen van een toestemmingsverzoek. Het maakt onderdeel uit van de proportionaliteitstoetsing die daarbij dient te worden uitgevoerd.
De Afdeling advisering adviseert in het wetsvoorstel te regelen dat data die wordt verkregen door middel van een verkennende bevoegdheid (inzake OOG interceptie) niet mogen worden uitgewisseld met buitenlandse diensten. De leden van de CDA-fractie vragen de regering wat de consequenties voor het functioneren van de diensten zou zijn als deze aanbeveling van de Afdeling advisering zou worden opgevolgd. Klopt het, zo vragen deze leden, dat er in dit stadium geen sprake is van uitwisseling van gegevens, maar juist van verkenning van de mogelijkheden voor onderzoek, en dat Nederland voor onderzoek soms afhankelijk is van kennis of technische mogelijkheden van buitenlandse diensten. Tot slot vragen deze leden in hoeverre opvolging van deze aanbeveling de samenwerking bemoeilijkt van onze diensten met buitenlandse diensten uit landen met gelijke waarden. Wij beantwoorden deze vragen graag als volgt. Voordat gegevens uit OOG-interceptie bruikbaar zijn voor het inlichtingenproces moeten deze technisch verwerkt en van betekenis worden voorzien. In sommige gevallen kan dit een buitengewoon complexe aangelegenheid zijn. In het kader van dit technisch onderzoek is het soms noodzakelijk ondersteuning te krijgen van een buitenlandse collegadienst. Artikel 90 van de Wiv 2017 biedt de wettelijke grondslag voor de AIVD en de MIVD om in het kader van een goede taakuitvoering een verzoek te doen aan een buitenlandse dienst tot het verlenen van technische of andere vormen van ondersteuning, waartoe ook de ondersteuning als hier bedoeld kan worden begrepen. In onderhavig

[23] https://www.aivd.nl/documenten/publicaties/2018/05/01/beleid-omgang-met-onbekende-kwetsbaarheden

geval worden – ingeval de buitenlandse dienst bereid is de gevraagde ondersteuning te verlenen – de voor dat technisch onderzoek benodigde gegevens aan de desbetreffende collegadienst verstrekt. De desbetreffende collegadienst kan dan technische informatie geven over hoe deze gegevens het beste verwerkt kunnen worden. Indien met behulp van de buitenlandse diensten de verstrekte gegevens van betekenis kunnen voorzien en daarmee bruikbaar worden voor het doel waarvoor ze zijn verworven, dan kan dit bijdragen aan een gerichtere formulering van het verzoek om toestemming voor OOG-interceptie ex artikel 48 Wiv 2017. Indien de mogelijkheid tot het verstrekken van gegevens aan een buitenlandse dienst voor technisch onderzoek zou ontbreken, betekent dat de desbetreffende gegevens uiteindelijk niet voor het doel gebruikt kunnen worden waarvoor ze zijn verworven.

De leden van de SP-fractie vragen de regering waarom zij juist ingebouwde waarborgen die tegemoet kwamen aan de tegenstemmers in het «sleepwet-referendum» nu wettelijk schrapt. Wij beantwoorden deze vraag als volgt. De regering heeft de Tweede Kamer bij brief van 6 april 2018 geïnformeerd dat naar aanleiding van het referendum over de invoering van de Wiv 2017 een zestal aanvullende waarborgen worden toegepast bij de inwerkingtreding van de Wiv 2017. Deze waarborgen blijven intact, met uitzondering van één specifieke aanpassing met betrekking tot het vereiste van een zo gericht mogelijke inzet van bevoegdheden. Het is sinds de inwerkingtreding van de Wiv 2017 gebleken dat de bevoegdheid tot OOG-interceptie op de kabel zich met name bij de verkenningsfase moeizaam verhoudt tot het vereiste om gegevens zo gericht mogelijk te verwerven. Deze problematiek is eveneens onderkend door de ECW. In de verkenningsfase (waarvoor artikel 6 van het wetsvoorstel een regeling geeft) dienen de diensten immers juist de ruimte te hebben om te onderzoeken welke gegevensstromen voor de diensten relevante gegevens bevatten. Een zo gericht mogelijke inzet is in die fase niet mogelijk aangezien de diensten dan nog over onvoldoende inlichtingen beschikken om te bepalen op welke gegevensstromen de bevoegdheid dient te worden ingezet. Daarvoor dient juist de verkenningsbevoegdheid, teneinde de daadwerkelijke interceptie ten behoeve van het inlichtingenproces wel zo gericht mogelijk te kunnen toepassen. Om die reden is in het wetsvoorstel opgenomen dat het vereiste van een zo gericht mogelijke inzet niet van toepassing is bij verkenning ten behoeve van OOG-interceptie. De bevoegdheid tot verkenning dient uiteraard wel te voldoen aan de vereisten van noodzaak, proportionaliteit en subsidiariteit en is onderworpen aan een voorafgaande TIB-toets en toezicht door de CTIVD. Daarnaast mogen de met de verkenningsbevoegdheid verworven gegevens niet gebruikt worden voor het inlichtingenproces, en geldt een maximale bewaartermijn van 6 maanden voor deze gegevens. Bij de reguliere OOG-interceptie ex artikel 48 (ten behoeve van het inlichtingenproces) geldt uiteraard wel het gerichtheidsvereiste.

De leden van de PvdD-fractie lezen dat het toezicht en de inschatting van de technische risico's van de ex ante toetsing bij de TIB komt te vervallen en wordt ondergebracht bij ex durante toezicht door de CTIVD. Dat de CTIVD bindende bevoegdheden krijgt achten deze leden een goed teken. Zij achten het ook begrijpelijk dat niet alle technische risico's evenals alle door de AIVD en de MIVD noodzakelijk geachte handelingen vooraf bekend zijn, maar ze snappen niet waarom de ex ante toetsing komt te vervallen. Zij geven aan in het kader van deugdelijk toezicht ex ante en ex durante toezicht wat hen betreft het beste zou zijn en zouden van de regering graag vernemen waarom niet voor gecombineerd toezicht wordt gekozen. Deze leden zouden wij willen verwijzen naar de uiteenzetting die wij aan het begin van deze paragraaf hebben gegeven naar aanleiding van

vragen van de leden van de D66-fractie. Daaruit blijkt dat de ex ante toetsing op technische risico's bij het binnendringen in geautomatiseerde werken geenszins komt te vervallen, maar dat deze beperkt wordt tot de op dat moment bekende technische risico's. Het toezicht op deze en nieuwe technische risico's tijdens de uitvoering van de bevoegdheid (ex durante) ligt bij de afdeling toezicht van de CTIVD en is bindend. In het door deze leden gewenste gecombineerde toezicht is dus voorzien.

De leden van de PvdD-fractie vragen voorts hoe een en ander verhoudt tot de vereisten van het EHRM en of het klopt dat deze stelt dat er een ex ante toestemming moet worden verleend. Wij beantwoorden deze vraag als volgt. Het EHRM stelt slechts in enkele gevallen (namelijk bij interceptie van communicatie en de toepassing van categorieën van selectoren op in bulk geïntercepteerde gegevens) de eis van een voorafgaande bindende toets of toestemming door een onafhankelijke instantie, waarbij men de voorkeur heeft voor een rechter maar dat mag ook een onafhankelijke bestuurlijke autoriteit zijn (zoals de TIB). Met betrekking tot het binnendringen van geautomatiseerde werken wordt de eis van een bindende toestemming vooraf dus niet gesteld. Voor het overige zal de regeling voor bijzondere bevoegdheden, waaronder de inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk, dienen te voldoen aan de eisen die het EVRM en de jurisprudentie van het EHRM stelt aan wetgeving waarin de activiteiten van inlichtingen- en veiligheidsdiensten worden gereguleerd. Kortheidshalve wordt gewezen naar hetgeen is gesteld in hoofdstuk 5 van de memorie van toelichting bij onderhavig wetsvoorstel en voor de Wiv 2017 naar hoofdstuk 9 van de memorie van toelichting op het daaraan ten grondslag liggende wetsvoorstel.[25]

Deze leden hebben voorts diverse vragen over de bijschrijfmogelijkheid. Uit de toelichting maken zij op dat het bijschrijven juridisch makkelijker wordt gemaakt, en dat er minder toetsing op rechtmatigheid nodig gaat zijn. Zij vragen of hun analyse klopt. Wij beantwoorden deze vraag als volgt. In artikel 5, tweede lid, van het wetsvoorstel wordt verduidelijkt wat de bijschrijfmogelijkheid in artikel 45, achtste lid, Wiv 2017 precies behelst, namelijk dat niet is vereist dat er sprake dient te zijn van exclusief gebruik (uitleg TIB) van een geautomatiseerd werk door een persoon of organisatie waarop de bevoegdheid wordt ingezet. Dit betekent niet dat sprake is van het makkelijker maken van bijschrijven. Zoals in de memorie van toelichting is aangegeven geldt dat voor het bijschrijven een interne toestemming is vereist. De vereisten van noodzaak, proportionaliteit, subsidiariteit en gerichtheid blijven daarbij onverkort gelden. De afdeling toezicht van de CTIVD houdt bindend toezicht op dit bijschrijfproces tijdens de uitvoering van de bevoegdheid tot binnendringen in een geautomatiseerd werk (artikel 12, eerste lid, onder c, van het wetsvoorstel).

Daarnaast vragen deze leden of het klopt dat wanneer de geheime diensten een server bijschrijven waar veel burgers gebruik van maken zij de gegevens die daar op staan kunnen binnenhalen en deze voor andere onderzoeken gebruiken, en dat de TIB pas bij de verlenging van de toestemmingsaanvraag deze specifieke hack kan toetsen. Wij beantwoorden deze vraag als volgt. De diensten kunnen niet zonder meer een server bijschrijven waar veel burgers gebruik van maken. De bijschrijfmogelijkheid kan alleen gebruikt worden indien er sprake is van kenmerken/infrastructuur die wordt gebruikt door een persoon of organisatie waar de dienst onderzoek naar doet. Zoals hiervoor is aangegeven, dient daarvoor interne toestemming te worden verkregen waarbij getoetst wordt aan de eisen van de noodzakelijkheid, proportionaliteit, subsidiariteit en

[25] Kamerstukken II 2016/2017, 34 588, nr. 3, p. 190 e.v.

gerichtheid. De afdeling toezicht kan op grond van het wetsvoorstel bindend toezicht houden op de rechtmatigheid van de bijschrijving. Waar het gaat om de gegevens die langs deze weg door de diensten worden verworven, geldt dat ingevolge artikel 27, eerste lid, Wiv 2017, deze zo spoedig mogelijk op relevantie moeten worden beoordeeld en indien niet relevant dienen te worden vernietigd. Met andere woorden: als gegevens van burgers die niks met statelijke actoren te maken hebben worden verzameld, worden ze gewist. En voordat ze gebruikt mogen worden is een nadere analyse nodig. Voor zover het gaat om bulkdatasets wordt verwezen naar hetgeen in de ingediende nota van wijziging ter zake wordt voorgesteld. De TIB kan oordelen over de bijgeschreven geautomatiseerde werken die in de door de Minister verleende toestemming waarmee de inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk wordt verlengd zijn opgenomen. Dat betreft echter de toestemming tot verlenging en niet de bijschrijving als zodanig (dat valt immers onder de competentie van de afdeling toezicht).

De leden van de PvdD-fractie vragen in dit kader ten slotte of het klopt dat pas na vaststelling dat deze gegevens voor geen van de onderzoeken relevant is ze zullen worden vernietigd. De verplichting van art. 27, eerste lid, Wiv 2017 blijft hier onverkort van toepassing. Dat betekent dat gegevens zo spoedig mogelijk op hun relevantie voor het onderzoek waarvoor de gegevens zijn verworven dan wel enig ander lopend onderzoek van de dienst, zoals in artikel 27 nader gespecificeerd, dienen te worden onderzocht en indien niet relevant bevonden ze dienen te worden vernietigd. Voor dit onderzoek staat een jaar, waarna – tenzij van de verlengingsmogelijkheid met zes maanden van artikel 27, derde lid, is gebruik gemaakt – de gegevens zonder meer moeten worden vernietigd. Voor zover het gaat om bulkdatasets wordt verwezen naar hetgeen in de ingediende nota van wijziging ter zake wordt voorgesteld.

De leden van de SGP-fractie vragen of de regering de interne autorisatie bij bijschrijvingen wil toelichten. Wie, zo vragen deze leden, verstrekt die autorisatie en welke procedures gelden daarbij. We reageren als volgt op deze vraag. Een bijschrijving is het toevoegen van een kenmerk aan een lopende toestemming voor de inzet van de desbetreffende bevoegdheid. Dit wordt gedaan door het inlichtingenteam dat gemotiveerd omschrijft waarom het nieuwe kenmerk past in de verleende toestemming en of dit noodzakelijk, proportioneel, subsidiair en gericht is. Deze motivatie wordt eerst getoetst door de leidinggevende van dat inlichtingenteam en, indien deze akkoord is, verleent deze toestemming voor de bijschrijving. Vervolgens wordt die toestemming bij MIVD bezien door afdeling juridische zaken en bij de AIVD door het unithoofd. Indien daaruit geen bezwaren naar voren komen, kan de bijschrijving worden geëffectueerd. De beslissing wordt intern vastgelegd, zodat de CTIVD te allen tijde de overwegingen die ten grondslag hebben gelegen voor de autorisatie van de bijschrijving kan toetsten.

De leden van de Volt-fractie vragen of de regering kan toelichten wat er precies terechtkomt van het verplaatsen van de toetsing vooraf door de TIB naar toezicht van de CTIVD tijdens de inzet van de bevoegdheid. Deze leden zouden wij willen verwijzen naar onze reactie op vragen van de GroenLinks-fractie inzake de in hun ogen ontstane verwarring over het wel of niet inperken van het toezicht van de TIB en CTIVD (zie paragraaf 3.1) alsmede de antwoorden die aan het begin van onderhavige paragraaf zijn gegeven naar aanleiding van vragen van de leden van de D66-fractie. Met name laatstgenoemde antwoorden adresseren naar onze mening ook de vraag die deze leden hebben met betrekking tot de invulling van de proportionaliteitstoets en het toezicht dat wordt gehouden.

Deze leden vragen voorts of de regering tevens kan aangeven hoe de toets van het hoofd van de dienst eruit ziet? Welke kaders gelden er voor het diensthoofd bij het al dan niet verlenen van toestemming? Wij beantwoorden deze vraag als volgt. Het toestemmingsniveau van verkennen wordt in de Tijdelijke wet bij het hoofd van de dienst belegd. Het diensthoofd maakt de afweging en verleent toestemming op basis van de vereisten van noodzaak, proportionaliteit, subsidiariteit en gerichtheid en de onderbouwing van die vereisten. Indien het diensthoofd toestemming verleent voor het verkennen geldt een meldplicht bij de afdeling toezicht, die daarop vervolgens – de in het wetsvoorstel geïntroduceerde bevoegdheid tot – bindend toezicht kan uitoefenen. Het diensthoofd maakt de afweging en verleent toestemming op basis van de vereisten van noodzaak, proportionaliteit, subsidiariteit en gerichtheid en de onderbouwing van die vereisten.

De leden van de Volt-fractie vragen tot slot welke gevolgen het verschuiven van de toets voor de invulling van de proportionaliteitstoets en het toezicht dat wordt gehouden heeft. Deze leden verwijzen wij naar onze reactie op een vergelijkbare vraag van de leden van de D66-fractie aan het begin van deze paragraaf.

3.2.1 Verkennen van een geautomatiseerd werk

De leden van de PvdA-fractie wijzen erop dat wordt voorgesteld om het verlenen van voorafgaande toestemming tot het verkennen van een geautomatiseerd werk bij de TIB weg te halen en te verleggen naar (bindend) toezicht achteraf door de CTIVD. In dat kader vragen deze leden of ze het goed begrijpen dat het voorafgaande toetsen op rechtmatigheid door de TIB in deze komt te vervallen maar dat de TIB nog wel op proportionaliteit mag blijven toetsen, en, zo nee, wat begrijpen deze leden dan niet goed. Wij antwoorden deze leden graag als volgt. In artikel 32 Wiv 2017 is vastgelegd dat de TIB belast is met het toetsen van de rechtmatigheid van een door de verantwoordelijke Minister verleende toestemming. Deze rechtmatigheidstoets omvat onder andere een toets op de vereisten van noodzaak, proportionaliteit, subsidiariteit en gerichtheid. Ten aanzien van de bevoegdheid tot het verkennen van een geautomatiseerd werk wordt in het voorliggende wetsvoorstel de voorafgaande TIB toets vervangen door bindend toezicht door de afdeling toezicht tijdens de inzet en achteraf (artikel 4, eerste lid, onderscheidenlijk 12, eerste lid, onder a). Daarmee komt de rol van de TIB voorafgaand aan de inzet van deze bijzondere bevoegdheid te vervallen, en zal zij derhalve ook geen toets op de gerichtheid of de proportionaliteit meer kunnen uitvoeren. Het toezicht op het voldoen aan deze criteria zal deel uitmaken van het bindend toezicht door de afdeling toezicht op uitoefening van de bevoegdheid door de diensten. De TIB heeft in haar consultatiereactie op het wetsvoorstel aangegeven zich in deze aanpassing te kunnen vinden gelet op de zeer beperkte inbreuk die deze bijzondere bevoegdheid oplevert. Met een voorafgaande toestemming van de Minister en toetsing daarvan door de TIB is die bevoegdheid naar het oordeel van de TIB in het huidige stelsel te zwaar belegd.[26] Nu de overige vragen van de leden van de PvdA-fractie betrekking hebben op de situatie dat de TIB wel blijft toetsen op proportionaliteit, kan de beantwoording hiervan achterwege blijven.

Het is deze leden overigens niet duidelijk waarom niet ook het verkennen, zelfs al gaat het dan niet om het binnendringen van een geautomatiseerd werk, niet toch zo gericht als mogelijk zou kunnen plaatsvinden. Zij vragen of de regering hierop kan ingaan. Wij willen erop wijzen dat het niet zo is

[26] Zie de reactie van de TIB op het concept-voorstel van Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma d.d. 14 april 2022.

dat de eis van gerichtheid bij het verkennen van een geautomatiseerd werk vervalt. Wel is het zo dat geautomatiseerde werken zeer omvangrijke en complexe systemen zijn. In veel gevallen gaat het om netwerken die bestaan uit honderden of duizenden wereldwijd verspreide servers of computers. In deze context is voordat wordt verkend in principe de samenstelling, omvang en gelaagdheid van een dergelijk (net)werk onbekend, waarmee minder gericht te werk kan worden gegaan dan bij het daadwerkelijk binnendringen van een geautomatiseerd werk. Dat is dus wel een factor om mee te wegen bij de invulling van de gerichtheidseis. Met de resultaten van de verkenning kunnen de diensten een verzoek om toestemming tot het binnendringen van een geautomatiseerd werk beter motiveren en – mits de verleende toestemming is verkregen en de TIB deze rechtmatig heeft beoordeeld – vervolgens ter uitvoering van de verleende toestemming gericht, efficiënt en zorgvuldig in relevante geautomatiseerde werken binnendringen.

3.2.2 Technische risico's

De leden van de PvdA-fractie merken op dat voorgesteld wordt om het toezicht op technische risico's bij inzet van de hackbevoegdheid van ex ante bij de TIB te verleggen naar ex durante toezicht door de CTIVD. Deze leden vragen in hoeverre dit toezicht effectief kan zijn in het geval het technisch risico zich in de praktijk daadwerkelijk gaat voordoen of reeds heeft voorgedaan. Is, aldus deze leden, het toezicht gedurende de operatie dan niet te laat. Wij beantwoorden deze vraag als volgt, met dien verstande dat wordt veronderstelt dat daarmee wordt gedoeld op de situatie waarin een technisch risico zich daadwerkelijk verwezenlijkt.
Op het moment dat het toestemmingsverzoek wordt geschreven wordt er door de diensten een inschatting gemaakt van de technische risico's, zodat dit kan worden meegenomen in het kader van de proportionaliteitstoets. Het maken van die inschatting kan alleen ten aanzien van hetgeen op dat moment bekend is over de voorgenomen inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk. In het scenario waarin ten tijde van het schrijven van het verzoek bekend is dat een risico zich zal verwezenlijken (hetgeen zeer sporadisch zal voorkomen, omdat dit veelal zal indruisen tegen het heimelijke karakter van de inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk), dan zal dit kunnen worden vermeld in het verzoek om toestemming en, indien de Minister toestemming heeft verleend, worden meegenomen in de toets door de TIB. Een ander scenario waarin een risico zich verwezenlijkt is dat dit gebeurt gedurende de uitvoering van de bevoegdheid, terwijl dat ten tijde van het opstellen van het toestemmingsverzoek niet werd voorzien. Door het vooraf zorgvuldig inschatten van de technische risico's en het zo nodig nemen van mitigerende maatregelen wordt de kans daarop zo klein mogelijk gemaakt. Mocht dit zich evenwel voordoen, dan geldt een incidentenprotocol binnen de diensten en wordt het incident zo nodig ook actief aan de CTIVD gemeld. Op de omgang daarmee kan de afdeling toezicht van de CTIVD toezicht houden, ook doordat zij toegang hebben tot de systemen van de diensten waarin de handelingen die tijdens de uitvoering van de bevoegdheid tot binnendringen in een geautomatiseerd werk worden verricht via logging worden vastgelegd. Hierbij verdient ook opmerking dat de afdeling toezicht niet alleen toezicht houdt op specifieke operaties, maar ook op het geheel van beleid en werkinstructies en de opvolging hiervan door de diensten. Dit betekent dat nog voordat sprake is van specifieke inzet de risico's op onrechtmatigheden of andere risico's worden beperkt. Over het geheel genomen zijn wij van oordeel dat hiermee sprake is van een evenwichtige en effectieve manier van toetsing en toezicht op technische risico's, en dat er geen sprake is van toezicht dat te laat is.

Voorts vragen deze leden wat de gevolgen zijn voor het lopend onderzoek van een dienst als de CTIVD een dreigend risico ziet, of constateert dat er al een technisch probleem is ontstaan. Wij reageren hierop als volgt. Als hiervan sprake is kunnen de diensten hierop door de CTIVD worden geattendeerd en kan worden bezien of de risico's kunnen worden gemitigeerd en indien dat niet mogelijk is kan dat ertoe leiden dat de inzet van de bevoegdheid wordt beëindigd. Dit kan betekenen dat een dienst daarmee zijn informatiepositie in een lopend onderzoek kwijtraakten daarmee het zicht verliest of verdwijnt op de activiteiten en de dreiging die uitgaat van landen met een offensief cyberprogramma. Dat kan daarmee ook betekenen dat niet kan worden voldaan aan de opdrachten die door de betrokken behoeftestellers zijn vastgesteld in de GA.

Ook vragen deze leden zich af hoe de Minister, als niet meer van tevoren duidelijk hoeft te worden gemaakt wat de technische risico's zijn, dan kan beoordelen of een hackoperatie verantwoord is en toegestaan kan worden. Wij beantwoorden deze vraag als volgt. Het is een onjuiste veronderstelling dat technische risico's bij een verzoek om toestemming – dus tevoren – niet meer duidelijk hoeven te worden gemaakt. Bij het opstellen van een verzoek om toestemming zullen de op dat moment *bekende* technische risico's wel degelijk dienen te worden geschetst, omdat voor de Minister in het kader van de toestemmingverlening relevante, mee te wegen aspecten zijn. Het gaat om de bekende risico's, omdat het voor de diensten niet mogelijk is om vooraf precies te voorspellen of voorzien welke handelingen wel of niet nodig zullen zijn om uiteindelijk te kunnen binnendringen. De Minister kan de beschrijving van de bekende technische risico's meenemen in de beoordeling en of een operatie tot binnendringen in een geautomatiseerd werk verantwoord is en dus toegestaan kan worden. De verleende toestemming wordt vervolgens door de TIB getoetst op rechtmatigheid en de TIB kan de bekende technische risico's, zoals hiervoor uiteengezet, in haar proportionaliteitstoets meewegen. De afdeling toezicht ziet vervolgens toe op de rechtmatige uitoefening van de bijzondere bevoegdheid.

3.2.3 Verduidelijking bijschrijfmogelijkheid

De leden van de PvdA-fractie lezen dat de voorliggende wet voorstelt om de mogelijkheid tot bijschrijven te verduidelijken. Volgens deze leden gaat het echter om verruiming van die mogelijkheid en vragen of de regering deze mening deelt. En zo niet, waarom dan niet.

Wij zien de voorgestelde regeling (artikel 5, tweede lid) niet als een verruiming, maar als een verduidelijking van een bestaande bevoegdheid in artikel 45 Wiv 2017. Het is immers altijd de bedoeling geweest dat (op voorhand nog niet bekende) infrastructuur die *gebruikt* wordt door partijen waarop de bevoegdheid tot binnendringen in een geautomatiseerd werk wordt ingezet, moet kunnen worden bijgeschreven. Met de voorgestelde tekst wordt beoogd – op wettelijk niveau – duidelijkheid te geven over de reikwijdte van die bijschrijfmogelijkheid. Zoals in de memorie van toelichting is uiteengezet legt de TIB, in het kader van de uitvoering van haar rechtmatigheidstoets op de door de Minister verleende toestemming, het feit dat in artikel 45, achtste lid, Wiv 2017 gesproken wordt van een geautomatiseerd werk *van* een persoon of organisatie, zodanig uit dat het hier dient te gaan om een geautomatiseerd werk dat *exclusief* aan die persoon of organisatie toebehoort. De TIB maakt daarbij onderscheid tussen systemen die in eigendom zijn van, exclusief bezit zijn van of exclusief gebruikt worden door personen of organisaties enerzijds, en anderzijds systemen waarbij naast de personen of organisaties waarvoor de oorspronkelijke toestemming is verleend sprake is van medegebruik door anderen van dat systeem. Bij deze laatste categorie moet gedacht worden aan een gedeelde server of een door de actor gehackt systeem. De uitleg van de TIB is problematisch omdat

cyberactoren vaak gebruik maken van een gedeelde infrastructuur. Dit maakt bijschrijven in een dergelijke situatie in de praktijk vrijwel onmogelijk. De bijschrijfmogelijkheid wordt aldus nader verduidelijkt. De leden van de PvdA-fractie lezen dat met artikel 5, tweede lid, het mogelijk wordt om geautomatiseerde werken die behalve door de actor zelf ook door anderen gebruikt worden als onderdeel van een onderzoek kunnen worden bijgeschreven. Betekent dat, aldus deze leden, dan dat een server waarop naast gegevens van een actor ook gegevens van anderen staan bijgeschreven kunnen worden, of dat er op een dergelijke server mogelijk duizenden websites gehost worden. En, zo ja, of dat dan wil zeggen dat de diensten zonder voorafgaand (extern) toezicht hierop onderzoek kunnen doen. In artikel 5, tweede lid, van het wetsvoorstel wordt verduidelijkt wat de bijschrijfmogelijkheid in artikel 45, achtste lid, Wiv 2017 precies behelst, namelijk dat niet is vereist dat er sprake dient te zijn van exclusief gebruik (uitleg TIB) van een geautomatiseerd werk door een persoon of organisatie waarop de bevoegdheid wordt ingezet. Deze bijschrijfmogelijkheid zorgt ervoor de diensten effectief onderzoek kunnen doen dat past bij de dynamische dreiging en operationele praktijk. Juist in het cyberdomein zijn snelheid en wendbaarheid – het mee kunnen bewegen met een actor – cruciaal. Dit betekent niet dat sprake is van het makkelijker maken van bijschrijven. Zoals in de memorie van toelichting is aangegeven geldt dat voor het bijschrijven een interne toestemming is vereist. De vereisten van noodzaak, proportionaliteit, subsidiariteit en gerichtheid blijven daarbij onverkort gelden. De afdeling toezicht van de CTIVD houdt bindend toezicht op dit bijschrijfproces tijdens de uitvoering van de bevoegdheid tot binnendringen in een geautomatiseerd werk (artikel 12, eerste lid, onder c, van het wetsvoorstel). De diensten kunnen niet zonder meer een server bijschrijven waar veel burgers gebruik van maken. De bijschrijfmogelijkheid kan alleen gebruikt worden indien er sprake is van kenmerken/infrastructuur die wordt gebruikt door een persoon of organisatie waar de dienst onderzoek naar doet. Hierbij staat het gebruik van het kenmerk door de actor centraal. Gedurende de toestemmingsperiode kunnen dus ook (na interne autorisatie) geautomatiseerde werken zoals servers die behalve door de actor ook door burgers of andere derden worden gebruikt, worden bijgeschreven. Waar het gaat om de gegevens die langs deze weg door de diensten worden verworven, geldt dat ingevolge artikel 27, eerste lid, Wiv 2017, deze zo spoedig mogelijk op relevantie moeten worden beoordeeld en indien niet relevant dienen te worden vernietigd. Met andere woorden: als gegevens van burgers die niks met statelijke actoren te maken hebben worden verzameld, worden ze gewist. En voordat ze gebruikt mogen worden is een nadere analyse nodig. Voor zover het gaat om bulkdatasets wordt verwezen naar hetgeen in de ingediende nota van wijziging ter zake wordt voorgesteld. De TIB kan oordelen over de bijgeschreven geautomatiseerde werken die in de door de Minister verleende toestemming waarmee de inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk wordt verlengd zijn opgenomen. Dat betreft echter de toestemming tot verlenging en niet de bijschrijving als zodanig (dat valt immers onder de competentie van de afdeling toezicht). Samengevat is er dus sprake van een sluitend stelsel van toetsing en toezicht op de inzet en uitvoering van de bevoegdheid tot het binnendringen in een geautomatiseerd werk, inclusief op de in het wetsvoorstel voorziene bijschrijfmogelijkheid.

Deze leden vragen ook of het mogelijk is dat indien een cyberactor gelinkt aan een statelijke actor voor een aanval gebruik maakt van routers van families dat die door de diensten dan gehackt of getapt mogen gaan worden en dat daarvoor dan ook geen voorafgaande externe toestemming voor nodig is. Zo ja, dan vragen deze leden of de regering dit proportioneel acht in verhouding tot de behoefte van de diensten om

snel te kunnen handelen. Wat kunnen burgers en bedrijven doen om hier bezwaar tegen aan te tekenen? Zo nee, wat is er dan niet waar? En deelt de regering de mening dat het voor de CTIVD op zijn minst moeilijk zal zijn gedurende een hack of tap (ex durante) of achteraf (ex post) te kunnen beoordelen of dit geoorloofd was? Wij reageren op dit geheel aan vragen als volgt. De diensten moeten voor de inzet van de bevoegdheid een onderbouwde toestemmingsverzoek schrijven en na toestemming van de Minister toetst de TIB de verleende toestemming op rechtmatigheid. Indien de TIB de toestemming voor de inzet rechtmatig acht, mogen de diensten de bevoegdheid tot bijschrijven inzetten, voor een periode van maximaal drie maanden. Een bijschrijving moet passen in de afwegingen die in het rechtmatig geachte toestemmingsverzoek zijn gemaakt. Op de bijschrijving vindt intern bij de diensten wel degelijk een toets plaats op noodzaak, proportionaliteit, gerichtheid en subsidiariteit. De diensten hebben daarnaast een inspanningsverplichting om te onderzoeken of sprake is van andere gebruikers. Aan de hand daarvan kan worden bepaald of de motiveringen in het verzoek passen bij deze eventuele andere gebruikers. Indien er een bijschrijving heeft plaatsgevonden, wordt dit gemeld bij de afdeling toezicht van de CTIVD. De afdeling toezicht kan bindend toezicht houden op de bijschrijving. Indien zij de bijschrijving niet binnen de kaders van de verleende toestemming achten, kunnen zij – met inachtneming van de in artikel 12 neergelegde procedure – de inzet van de bevoegdheid doen beëindigen of de gegevens die zijn verworven met deze bevoegdheid, laten vernietigen. Naar ons oordeel is de afdeling toezicht zeer wel in staat om de geoorloofdheid van de bijschrijving te beoordelen. De uitoefening van de bijzondere bevoegdheid door de dienst vindt op een heimelijke wijze plaats en is – om onderkenning van het feit dat de diensten een onderzoek doen gericht op het voorkomen, te voorkomen dat de personen of organisaties die het betreft daartegen maatregelen kunnen nemen en daarmee de effectiviteit van het onderzoek kunnen schaden – niet kenbaar bij betrokkenen. Er bestaat dan ook niet de mogelijkheid om daartegen bezwaar aan te tekenen.[27] Mocht een persoon of organisatie – en dus ook familie – het vermoeden hebben dat door de diensten gebruik is gemaakt van (mede) aan hen toekomende routers, dan kunnen ze altijd een klacht indienen bij de afdeling klachtbehandeling van de CTIVD. Deze kan effectief onderzoek naar de klacht doen en uiteindelijk tot een bindend oordeel komen.

Tot slot vragen deze leden of de regering nader kan ingaan op wie (intern) toestemming tot bijschrijving moet geven en hoe het interne toezicht daarop wordt ingericht. Wij reageren als volgt op deze vraag. Een bijschrijving is het toevoegen van een kenmerk aan een lopende toestemming voor de inzet van de desbetreffende bevoegdheid. Dit wordt gedaan door het inlichtingenteam dat gemotiveerd omschrijft waarom het nieuwe kenmerk past in de verleende toestemming en of dit noodzakelijk, proportioneel, subsidiair en gericht is. Dit wordt vervolgens getoetst door de leidinggevende van dat inlichtingenteam en indien deze akkoord is verleent deze toestemming voor de bijschrijving. Deze toestemming wordt bij de MIVD bezien door afdeling juridische zaken en bij de AIVD door het unithoofd. Indien daaruit geen bezwaren naar voren komen, kan de bijschrijving worden geëffectueerd. De beslissing wordt intern vastgelegd, zodat de CTIVD te allen tijde de overwegingen die ten grondslag hebben gelegen voor de autorisatie van de bijschrijving kan toetsen.

[27] De Algemene wet bestuursrecht is hier niet van toepassing.

De leden van de VVD-fractie onderschrijven het grote belang van het identificeren van bekende en onbekende dreigingen. Deze leden delen het uitgangspunt van de regering dat het hebben van de juiste bevoegdheden een randvoorwaarde is voor het effectief uitvoeren van deze taak door de diensten. Zij begrijpen dan ook dat het inzetten van kabelinterceptie voor deze taak als noodzakelijk wordt geacht. Deze leden vragen of de regering het toetsingskader (artikel 7) bij deze specifieke bevoegdheden nader kan toelichten en concretiseren hoe, met inbegrip van dit toetsingskader, het uitoefenen van de kabelinterceptie als operationele meerwaarde voor de diensten wordt geborgd. Wij lichten dit graag toe. De dreigingen, en zeker die in het cyberdomein, vinden vooral plaats via het wereldwijde communicatienetwerk. De computers en servers in deze netwerken zijn met elkaar verbonden via datakabels en satellieten. Om inzicht te krijgen op de cyberdreiging is het daarom cruciaal om gegevensstromen van deze kabels en satellieten te intercepteren. De diensten hebben zeer beperkte mogelijkheden om gegevens over personen en organisaties – gerelateerd aan landen met een offensief cyberprogramma – te verzamelen in het buitenland. Het middel dat daarvoor bij uitstek geschikt is, is kabelinterceptie. De inzet van kabelinterceptie wordt gerechtvaardigd door de ernst van de dreiging die van statelijke actoren met offensieve cyberprogramma's uitgaat en de unieke meerwaarde die het middel heeft voor de inlichtingenposities van de diensten over de dreiging van die landen. De informatie die het middel opbrengt is uniek en cruciaal als het gaat om informatie over bijvoorbeeld de werkwijze van de landen, hun intenties en doelwitten, bijvoorbeeld door deze vast te kunnen stellen of te verifiëren. Het zorgt voor de noodzakelijke puzzelstukjes die niet op een andere wijze kunnen worden verkregen, waardoor het zicht op de dreiging wordt versterkt of juist zelfs de dreiging aan het licht komt. Kabelinterceptie is hét middel om onderzoek te doen naar dit soort dreigingen, en meer specifiek naar de ongekende dreiging. Hierbij is het van belang dat de invulling van de proportionaliteit en de gerichtheid niet beperkt is tot (technische) kenmerken die zijn gerelateerd aan een lopende operatie tot binnendringen in een geautomatiseerd werk of aan gekende targets, maar is de operationele meerwaarde van kabelinterceptie juist dat deze ook kan worden ingezet ten behoeve van de verborgen dreiging en het identificeren van targets. Voor deze onderbouwing van de gerichte en proportionele toepassing van OOG-interceptie is in het toetsingskader van artikel 7 in de Tijdelijke wet aansluiting gezocht bij de dynamiek van cyberdreigingen en de wijze waarop gegevens over het wereldwijde communicatienetwerk worden gerouteerd.
Voor de inzet van bijzondere bevoegdheden binnen het kader van de Wiv 2017 dient in beginsel aan vier voorwaarden te zijn voldaan. Getoetst wordt of de inzet van de bijzondere bevoegdheid (1) noodzakelijk is, of wordt voldaan aan de vereisten van (2) proportionaliteit en (3) subsidiariteit en (4) de inzet zo gericht mogelijk plaatsvindt. Artikel 7 van dit wetsvoorstel geeft een nadere invulling van het toetsingskader voor OOG-interceptie. Binnen het gegeven toetsingskader moeten twee aspecten met name worden gemotiveerd ter concretisering van de gerichtheid en proportionaliteit. Het betreft (1) een indicatie van de gegevensstromen en (2) een indicatie van de reductie van de gegevens. Uit praktijkervaring blijkt dat actoren gebruik maken van veel verschillende protocollen en technieken om hun offensieve cyberprogramma uit te voeren en hun activiteiten te verhullen. Tevens innoveren deze actoren voortdurend hun werkwijze om hun offensieve doelen beter te bereiken en niet te worden onderkend. Het toetsingskader voor OOG-interceptie in de Tijdelijke wet zorgt voor meer houvast bij de invulling van de vereisten van gerichtheid en proportionaliteit die past bij de aard van de bevoegdheid. De invulling van die vereisten moet immers passen bij het

onderzoek naar – veelal – de ongekende dreiging en het bulkkarakter van de bevoegdheid. Hierbij beschikken de diensten in de eerste, verwervende fase, niet over concrete technische kenmerken van gekende targets of targetorganisaties waarop de inzet zich kan richten. In die fase, waarbij de verleende toestemming voor de daarbij in te zetten bijzondere bevoegdheid is onderworpen aan het rechtmatigheidsoordeel van de TIB, kan een indicatie worden gegeven van de te intercepteren gegevensstromen, veelal onderbouwd door de verkennende bevoegdheid ten behoeve van OOG-interceptie. Ook het geven van een indicatie van de wijze waarop de reductie van gegevens binnen de gehele keten van verwerving invulling krijgt, geeft invulling aan de vereisten van gerichtheid en proportionaliteit dat past bij de aard van de bevoegdheid en dynamiek van de operationele praktijk. Hierbij is het van belang op te merken bulkinterceptie verschillende stappen kent, waarbij bij elke stap een andere mate van inbreuk op de privacy gepaard gaat: het graduele proces van inbreuk bij bulkinterceptie. Bij de eerste verwervende fase zal een indicatie kunnen worden gegeven van de wijze waarop gegevensreductie zal plaatsvinden. De gegevensstromen die worden geïntercepteerd zijn dynamisch van aard en wijzigen voortduren. Tijdens de uitvoering van de bevoegdheid moeten de filters die data reduceren daarop worden aangepast, zodat de gegevens die worden geïntercepteerd, worden verworven voor het doel waarvoor de inzet plaatsvindt. Het aanbrengen van filterkaders is derhalve ook een dynamisch proces. Op de uitvoering van de bevoegdheid, en de wijze waarop gegevensreductie plaatsvindt, houdt de CTIVD toezicht.
Op basis van bovenstaande specifieke punten uit het toetsingskader kunnen de diensten het potentieel van kabelinterceptie (lees: identificeren van bekende en onbekende dreigingen) meer benutten. Juist in de identificatie van de onbekende dreiging zit de operationele meerwaarde van kabelinterceptie voor de diensten. Op die manier kunnen (cyber)dreigingen inzichtelijk worden gemaakt. Kabelinterceptie is hierbij cruciaal, omdat de diensten zeer beperkte mogelijkheden hebben om gegevens over personen en organisaties – gerelateerd aan landen met een offensief cyberprogramma – te verzamelen in het buitenland.
In paragraaf 2.3 van deze nota naar aanleiding van het verslag is in reactie op vragen van de leden van de D66-fractie ingegaan op de verkennende bevoegdheid in het kader van OOG-interceptie (artikel 6), waarbij wordt aangegeven dat deze verkennende bevoegdheid er toe dient om de aanvraag voor OOG interceptie als bedoeld in artikel 7 Tijdelijke wet en artikel 48 Wiv 2017, te kunnen onderbouwen.
Artikel 7 van dit wetsvoorstel geeft een nadere invulling van het toetsingskader voor OOG-interceptie. Binnen het gegeven toetsingskader moeten twee aspecten met name, en daarmee het zwaarwegendst, worden gemotiveerd ter concretisering van de gerichtheid en proportionaliteit. Deze twee aspecten zijn een indicatie van de gegevensstromen en een indicatie van de reductie van de gegevens.

De uitoefening van OOG-interceptie betreft een gefaseerd model dat we hieronder nader toelichten:
1) interceptie en opslag van gegevens (verwerving van gegevens);
2) doorzoekbaar maken van gegevens;
3) onderzoeken van de gegevens;
4) het verder verwerken en gebruiken van de gegevens in het inlichtingendomein.

Binnen fase 1 richten de beide diensten zich op communicatiedragers (zoals kabels of satellietlinken) die gegevensstromen transporteren die vooral betrekking hebben op het buitenland. Het is niet uitgesloten dat deze communicatiedragers, door de werking van het internet, ook gegevensstromen van Nederlandse burgers transporteren. De communi-

catiedragers waarop geïntercepteerd wordt, zijn resultaten van het verkennend onderzoek zoals bedoeld in artikel 6 Tijdelijke wet. Het doel in fase 1 is om mogelijk relevant internationaal verkeer voor het betreffende onderzoek te intercepteren en op te slaan. In deze fase is er nog geen sprake van inlichtingenonderzoek, het betreft enkel het intercepteren en opslaan van grote hoeveelheden gegevens die mogelijk relevant internationaal verkeer bevat in het onderzoek naar landen met een offensief cyberprogramma.

Binnen fase 2 en 3 start het «search» gericht op selectie oftewel identificatieonderzoek. In dit onderzoek gaan de diensten op zoek naar gegevens van personen en/of organisaties die onderdeel zijn van landen met een offensief cyberprogramma. Deze fase kan gezien worden als de start van het onderzoeken of personen en/of organisaties in aanmerking komen voor verder onderzoek gezien een mogelijke betrokkenheid bij statelijke actoren, die ook een offensief cyberprogramma uitvoeren. De gegevens van personen en/of organisaties die potentieel in aanmerking komen voor verdere onderzoeken kunnen ter beschikking komen voor de inlichtingenteams in fase 4.

De leden van de D66-fractie hebben kennisgenomen van de wijzigingen op het gebied van kabelinterceptie. Zij stellen in dat kader diverse vragen, die identiek zijn met de vragen die zij in paragraaf 2.3 van het verslag (Overzicht van de voorgestelde maatregelen) hebben gesteld. Wij verwijzen dan ook kortheidshalve naar onze antwoorden op die vragen in paragraaf 2.3 van deze nota naar aanleiding van het verslag.

De leden van de D66-fractie vragen of de methoden die de inlichtingendiensten gebruiken om de data te analyseren (GDA) onder de algoritmewetgeving van Europa gaan vallen. Indien dat niet het geval is, willen deze leden vernemen op basis van welke uitzonderingen dat dan het geval is. Wij beantwoorden deze vraag als volgt. De concept AI-verordening van de EU is niet van toepassing op de ontwikkeling en het gebruik van AI systemen voor het doel van nationale veiligheid. Nationale veiligheid blijft krachtens artikel 4 lid 2 van het EU-Verdrag[28] immers de uitsluitende verantwoordelijkheid van de lidstaten. De toepassing van GDA door de diensten is gereguleerd door de bepalingen inzake gegevensverwerking uit de Wiv 2017, en in het bijzonder artikel 60 van de Wiv 2017.

De leden van de CDA-fractie merken op dat de regering stelt, dat de bevoegdheid tot onderzoeksopdrachtgerichte interceptie tot op heden slechts beperkt is ingezet ten behoeve van het inlichtingenproces vanwege de onduidelijkheid met betrekking tot de wijze waarop het gerichtheidsvereiste bij de inzet van deze bevoegdheid moet worden geïnterpreteerd en de verschillende zienswijzen ter zake van de Ministers en de TIB nog niet tot een oplossing hebben geleid. Daardoor kunnen bepaalde onderzoeken in het cyberdomein nog niet worden opgestart. Deze leden vragen de regering in dit verband ook te reflecteren op de uitspraak van prof. dr. Bart Jacobs en mr. drs. Rowin Jansen in het rondetafelgesprek over het voorliggende wetsvoorstel: «Uiteindelijk zal het van de opstelling van de diensten én van de toezichthouders afhangen of dit nieuwe «dynamisch toezicht» succesvol is.» Deze leden vragen, op

[28] Artikel 4, tweede lid, van het EU verdrag luidt: De Unie eerbiedigt de gelijkheid van de lidstaten voor de Verdragen, alsmede hun nationale identiteit die besloten ligt in hun politieke en constitutionele basisstructuren, waaronder die voor regionaal en lokaal zelfbestuur. Zij eerbiedigt de essentiële staatsfuncties, met name de verdediging van de territoriale integriteit van de staat, de handhaving van de openbare orde en de bescherming van de nationale veiligheid. Met name de nationale veiligheid blijft de uitsluitende verantwoordelijkheid van elke lidstaat.

welke wijze de regering de (bereidheid tot) constructieve samenwerking van alle betrokkenen denkt te bevorderen. In paragraaf 2.1 van deze nota naar aanleiding van het verslag zijn wij naar aanleiding van vragen van de leden van de D66-fractie ingegaan op wat wij bedoelen met constructieve samenwerking. Kortheidshalve verwijzen wij deze leden daarnaar.

De leden van de SP-fractie stellen dat onderzoeksopdrachtgerichte onderschepping ongericht mogelijk en techniek onafhankelijk wordt gemaakt. Zij vragen of de regering kan aangeven op basis van welke informatie dit onderdeel is geworden van het wetsvoorstel. Ook vragen deze leden of het klopt dat hier geheel de wens van de geheime diensten wordt gevolgd of dat hier op basis van uitgebreide evaluatie en gesignaleerde knelpunten een wetsaanpassing wordt voorgesteld. Ook vragen zij of de motivering tot verkennen van een kabel gelijk is aan een OOG-interceptie en, zo nee, waarom niet. Voorts willen zij vernemen waarom naar het oordeel van de regering een OOG-interceptie risicovoller – en daardoor met meer waarborgen omkleed – is dan snapshotten. In antwoord op de vragen van deze leden, willen we als volgt reageren. Reeds in de voorloper van de Wiv 2017, te weten de Wiv 2002, was voorzien in de mogelijkheid tot ongerichte interceptie van niet-kabelgebonden telecommunicatie (artikel 27 Wiv 2002). De koppeling van de bevoegdheid aan het feit dat het uitsluitend betrekking mocht hebben op niet-kabelgebonden telecommunicatie (lees: etherverkeer) maakte dat die bevoegdheid techniekafhankelijk was geformuleerd. Op advies van de Commissie Dessens, die de Wiv 2002 heeft geëvalueerd, bevat de Wiv 2017 thans een techniekonafhankelijke regeling voor OOG-interceptie: de regeling voor zowel ether- als kabelinterceptie van bulkgegevens. De Tijdelijke wet volgt deze techniekonafhankelijk bepaling voor OOG-interceptie. In aanvulling op de Wiv 2017 voorziet artikel 6 van de Tijdelijke wet in een zelfstandige juridische grondslag voor het verkennend onderzoek ten behoeve van OOG-interceptie. Daarmee wordt tevens uitvoering gegeven aan een aanbeveling van de CTIVD en de ECW.[29] Ook de TIB ziet een aparte, zelfstandige wettelijke regeling als een welkome wijziging.[30]
De verkennende bevoegdheid heeft tot doel om een verzoek tot toestemming voor OOG-interceptie beter te kunnen onderbouwen. Deze stap gaat vooraf aan de toepassing van OOG-interceptie ten behoeve van het inlichtingenproces en dus het onderzoeken van de daadwerkelijke dreiging vanuit landen met een offensief cyberprogramma. De bevoegdheid tot verkennen ten behoeve van OOG-interceptie en de bevoegdheid tot OOG-interceptie ten behoeve van het inlichtingenproces dienen beide een ander doel, hetgeen tot uitdrukking komt in de motivering voor de inzet van betreffende bevoegdheid; die zijn dan ook verschillend. Beide bevoegdheden zijn voorzien met waarborgen die passen bij de aard van de bevoegdheid. Een belangrijke waarborg die geldt voor het verkennende onderzoek is dat geïntercepteerde gegevens met dat doel niet mogen worden gebruikt voor inlichtingendoeleinden. Vanuit privacy-perspectief is de daarmee gepaard gaande inbreuk geringer dan bij het gebruik van gegevens voor inlichtingendoeleinden, nu in het laatste geval immers de inhoud van de geïntercepteerde communicatie in een inlichtingenonderzoek kan worden gebruikt. In die zin is laatstgenoemd gebruik als risicovoller aan te merken. Voor beide bevoegdheden – verkennen en OOG-interceptie – geldt dat deze niet mogen worden ingezet zonder toestemming van de Minister en

[29] Zie CTIVD-rapport nr. 75 en aanbeveling 19 van de ECW (die overigens spreekt van «metingen» doen bij bepaalde aanbieders).
[30] Brief van 14 april 2022 van de TIB aan de Ministers van BZK en Defensie met reactie TIB op concept wetsvoorstel Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma.

goedkeuring door de TIB in het kader van de aan haar opgedragen rechtmatigheidstoets. De afdeling toezicht kan regulier toezicht op de uitvoering van beide bevoegdheden uitoefenen.

De leden van de SP-fractie vragen de regering te erkennen dat het mogelijk is om een hele wijk of stad af te tappen. Wij beantwoorden deze vraag als volgt en verwijzen hier tevens naar de beantwoording van de Kamervragen van het lid Arib, d.d. 9 juni 2022, en de Kamervragen van het lid Leijten, d.d. 23 december 2022[31]. Het is voor de inlichtingendiensten technisch niet mogelijk om hele wijken of steden in Nederland af te luisteren. De inrichting van communicatienetwerken (zowel internet als telefonie) maken het integraal aftappen op wijk- of stadniveau in de praktijk technisch onmogelijk. Daar speelt mee dat de inrichting van de interceptieketen, zoals hierboven reeds is aangegeven, niet is ingericht op dergelijke interceptie. De interceptie wordt gericht op internationaal verkeer (omdat de diensten een onderzoek uitvoeren gericht op dreigingen vanuit het buitenland richting Nederland) waarbij door de inrichting van communicatienetwerken niet geheel kan worden uitgesloten dat verkeer met oorsprong en bestemming in Nederland wordt verworven.

In dat kader is het ook aangewezen om de door de (toenmalige) Ministers van BZK en Defensie gedane toezegging inzake de inzet van kabelinterceptie voor onderzoek naar communicatie met oorsprong en bestemming in Nederland te verhelderen. In de kamerbrief van april 2018 [32] is door de Ministers aangegeven dat het vrijwel uitgesloten is dat OOG-interceptie op de kabel de komende jaren wordt ingezet voor onderzoek naar communicatie met oorsprong en bestemming in Nederland (met uitzondering van onderzoek in het kader van cyber defence, omdat bij digitale aanvallen misbruik wordt gemaakt van de Nederlandse digitale infrastructuur en OOG-interceptie op de kabel noodzakelijk kan zijn om dit te ontdekken). Dit volgt uit het feit dat het lichtst mogelijke middel moet worden ingezet (subsidiariteit) en dat het middel in verhouding moet staan tot de dreiging (proportionaliteit). Indien de inlichtingendiensten in Nederland een inlichtingenonderzoek uitvoeren gericht op personen in een wijk of stad in Nederland, zijn daar lichtere middelen voor beschikbaar dan kabelinterceptie, en zou men bijvoorbeeld toestemming kunnen vragen voor een gerichte telefoontap of voor de bevoegdheid tot binnendringen in een geautomatiseerd werk. De CTIVD geeft in haar rapport aan dat de precieze strekking van de gedane toezegging niet eenduidig is maar dat geconcludeerd kan worden dat het zwaartepunt van de toezegging gericht is op onderzoek naar gegevens met oorsprong en bestemming Nederland en niet op de interceptie van gegevens met oorsprong en bestemming Nederland. [33] Interceptie van gegevens met oorsprong en bestemming Nederland is door de werking van het internet op voorhand niet uit te sluiten. Het inlichtingenonderzoek, zoals hierboven genoemd, zal de toets op het gebied van subsidiariteit en proportionaliteit om deze redenen niet doorstaan. De waarborg die voortvloeit uit de gedane toezegging door de Ministers dient op een manier gelezen te worden dat het vrijwel uitgesloten is dat de diensten OOG-interceptie zullen inzetten voor inlichtingenonderzoeken naar gegevens met oorsprong en bestemming Nederland met uitzondering van de onderzoeken binnen cyber defence.

---

[31] Zie Aanhangsel Handelingen II 2021/2022, nr. 3070 en Aanhangsel Handelingen II 2022/2023, nr. 1185.

[32] Kamerstukken II 2017/18, 34 588, nr. 70, p. 3.

[33] Toezichtsrapport over de inzet van kabelinterceptie door de AIVD en de MIVD (CTIVD nr. 75, p. 41).

De leden van de SP-fractie vragen tenslotte aan de regering om uit te leggen waarom dit moment is gekozen om het toezicht vooraf op de toepassing van algoritmes op bulk-geïntercepteerde data af te schaffen. Zou de komst van ChatGPT en soortgelijke algoritmes niet juist pleiten voor sterker toezicht. Zij vragen of de regering bereid is om artikel 8 ter herzien. Wij zijn niet bereid om artikel 8 te herzien gelet op het volgende. In artikel 8 van het wetsvoorstel wordt voorgesteld de ex ante toets van de TIB op de door de Minister verleende toestemming voor GDA op OOG-metadata te laten vervallen en die te vervangen door bindend toezicht door de afdeling toezicht. Het is op voorhand niet te voorspellen welke vorm van GDA op welk moment met welke gegevens gebruikt gaan worden bij de onderzoeken van de diensten. Bij het verrichten van data analyses kunnen bij elke handeling nieuwe inzichten worden verkregen en moeten nieuwe hypotheses worden getoetst. Dit alles gebeurt in een omgeving waarbij de beschikbare en bruikbare gegevens zeer veranderlijk zijn. De regering acht het wenselijk dat er goed en effectief toezicht plaatsvindt op de wijze waarop de diensten gegevens verwerken, ook gelet op de ontwikkelingen rondom AI en algoritmes. De afdeling toezicht heeft inzicht in de systemen van de diensten en kan meekijken met de wijze waarop GDA op OOG-metadata tijdens onderzoeken wordt toegepast en is daarom de aangewezen instantie om effectief toezicht te houden. De ECW concludeerde in haar rapport ook dat het verwerken van gegevens een dynamisch proces is en zich daarom minder goed leent voor een statische ex ante toets door de TIB.[34] In de Tijdelijke wet krijgt de afdeling toezicht de bevoegdheid om bindend te oordelen over de wijze waarop de diensten GDA op metadata uit kabel- of etherinterceptie toepassen (artikel 12, eerste lid, onder d). De TIB schrijft in haar reactie op het conceptwetsvoorstel dat deze verschuiving van toezicht verdedigbaar wordt geacht, gelet op de aard van de bevoegdheid die meer het karakter heeft van verdere verwerking van gegevens.[35]

De leden van de GroenLinks-fractie merken op dat in de samenleving en in de Kamer ook tijdens de behandeling van de Wiv 2017 veel aandacht is geweest voor het delen van gegevens met buitenlandse diensten. Zij wijzen erop dat ze al vaker aandacht hebben gevraagd voor het toezicht op het delen van informatie met buitenlandse diensten. Zij vragen of de regering nauwkeurig kan aangeven wat er met voorliggend voorstel concreet gaat veranderen ten aanzien van het delen van gegevens met buitenlandse diensten. Wij beantwoorden deze vraag als volgt. Het voorliggend wetsvoorstel brengt geen veranderingen aan ten aanzien van het delen van gegevens met buitenlandse diensten. De Wiv 2017 is en blijft onverkort van toepassing. Wel is in de toelichting op artikel 6 geëxpliciteerd dat de diensten de gegevens die zijn verkregen ten behoeve van verkennend onderzoek met het oog op toepassing van artikel 48 Wiv 2017 met andere diensten kunnen delen om ondersteuning te krijgen bij het technisch onderzoek van die gegevens. Bij de verstrekking van de gegevens voor dit doel moet dan ook expliciet als voorwaarde worden gesteld dat de verstrekte gegevens niet voor andere doeleinden, bijvoorbeeld voor inlichtingenonderzoek, mogen worden gebruikt door de ontvangende dienst.

---

[34] Paragraaf 9.3 van het rapport van de ECW.

[35] «In het wetsvoorstel wordt daarnaast voorgesteld de TIB niet langer voorafgaand bindend te laten toetsen over de toestemming voor geautomatiseerde data-analyse op gegevens verkregen met kabelinterceptie. Deze verschuiving van toezicht verdedigbaar, gelet op de aard van de bevoegdheid die meer het karakter heeft van verdere verwerking van gegevens. De CTIVD zal hier bindend toezicht op houden.« (brief van de TIB met reactie op het wetsvoorstel d.d. 14 april 2022).

De leden van de GroenLinks-fractie vragen of de regering ook kan aangeven op welke manier nu het toezicht op het delen van gegevens met buitenlandse diensten is geregeld en wat er met het voorliggend voorstel op dit vlak concreet zal veranderen. Om met de laatste vraag te beginnen: het wetsvoorstel brengt geen wijziging aan in het toezicht waar het gaat om de uitoefening van de bevoegdheid van de diensten om gegevens met inlichtingen- en veiligheidsdiensten van andere landen te delen. Daarvoor geldt de bestaande regeling in de Wiv 2017. Dat betekent dat uitoefening van die bevoegdheid is onderworpen aan het rechtmatigheidstoezicht door de afdeling toezicht van de CTIVD. Nu het hier gaat om de verstrekking van ongeëvalueerde gegevens zal altijd toestemming van de voor de dienst verantwoordelijke Minister moeten worden verkregen en dient de CTIVD van een verleende toestemming terstond op de hoogte te worden gesteld. De afdeling toezicht kan beoordelen of aan de wettelijke vereisten voor verstrekking van gegevens wordt voldaan en zal, zeker waar het gaat om verstrekking van gegevens als bedoeld in artikel 6, eerste lid, van het wetsvoorstel, daarbij de in de memorie van toelichting gedane uitspraken van de regering ter zake betrekken. Dat ziet dan in het bijzonder op de mededeling dat bij de verstrekking door de dienst van de hier bedoelde gegevens aan een buitenlandse dienst het expliciete verbod is gesteld deze gegevens te gebruiken voor inlichtingendoeleinden. Ook zal de afdeling toezicht kunnen toetsen of er inderdaad van een situatie sprake is dat voor het technisch onderzoek van de gegevens het noodzakelijk is de hulp in te roepen van een buitenlandse dienst.

De leden van de GroenLinks-fractie vragen op welke wijze voorkomen wordt dat gegevens die door Nederland met buitenlandse diensten gedeeld worden vervolgens door die diensten weer gedeeld worden met diensten waar Nederland geen gegevens mee zou willen delen. Wij beantwoorden deze vraag als volgt. Op grond van artikel 65, tweede lid, Wiv 2017 zijn de diensten verplicht om in alle gevallen waarbij sprake is van verstrekking van gegevens aan inlichtingen- en veiligheidsdiensten van andere landen de voorwaarde te stellen dat degene aan wie de gegevens worden verstrekt, deze gegevens niet aan anderen mag verstrekken (de zogeheten derde partijregel[36]). Uitsluitend de voor de dienst verantwoordelijke Minister of namens deze het hoofd van de dienst kan aan de ontvangende dienst alsnog toestemming verlenen om de gegevens aan andere personen of instanties te verstrekken, waaraan voorwaarden kunnen worden verbonden (artikel 66, derde lid, Wiv 2017). De naleving van deze voorwaarde(n) door de desbetreffende dienst berust op de (ongeschreven) vertrouwensregel die in de samenwerking tussen inlichtingen- en veiligheidsdiensten geldt. Indien geconstateerd wordt dat een dienst van een ander land zich niet aan de gestelde voorwaarde(n) houdt, zal de samenwerkingsrelatie met die dienst opnieuw worden gewogen. Afhankelijk van de uitkomst wordt besloten of de samenwerkingsrelatie moet worden voortgezet en, zo ja, wat dan de aard en de intensiteit van die relatie – mede in het licht van de geconstateerde vertrouwensbreuk – moet zijn. Schending van het wederzijdse vertrouwen is namelijk een «doodzonde» in de internationale samenwerking tussen inlichtingen- en veiligheidsdiensten. Tot slot wordt opgemerkt dat verstrekking van gegevens aan diensten waarmee geen samenwerkingsrelatie bestaat weliswaar in artikel 64 Wiv 2017 is toegestaan, maar die mogelijkheid is gereserveerd voor situaties waarin een dringende of gewichtige reden daartoe noodzaakt.

[36] Dit ter onderscheiding van de derde landregel, waarbij men de ontvangen gegevens niet aan andere landen mag door verstrekken maar wel aan personen en instanties binnen het eigen land.

De leden van de GroenLinks-fractie constateren dat niet precies duidelijk is wat er gebeurd is met de analyse en de aanbevelingen van de commissie Bovend'Eert ten aanzien van het toezicht en zouden graag willen vernemen op welke wijze deze zijn betrokken bij de totstandkoming van voorliggend wetsvoorstel. Wij beantwoorden deze vraag als volgt. Waar het gaat om voorliggend wetsvoorstel hebben de analyse en de aanbevelingen van deze commissie geen rol gespeeld. Immers het verzoek van de Minister van BZK dat heeft geleid tot de rapportage van deze hoogleraren stond in het teken van de herziening Wiv 2017 en de te nemen vervolgstappen ter zake. De analyse en aanbevelingen zullen worden betrokken bij de voorgenomen herziening van de Wiv 2017, waarbij ook het gehele stelsel van toetsing, toezicht en klachtbehandeling zal worden bezien. In de Hoofdlijnennotitie wordt op de analyse en aanbevelingen van de commissie Bovend'Eert ingegaan.

De leden van de PvdD-fractie lezen dat de in het kader van artikel 6 van het wetsvoorstel verworven gegevens met buitenlandse diensten gedeeld mogen worden, waarbij deze gehouden worden aan hetzelfde verbod om de gegevens voor inlichtingendoeleinden te gebruiken als de Nederlandse diensten. Deze leden vragen hoe de regering kan garanderen dat buitenlandse diensten deze gegevens niet gebruiken voor inlichtingen-doeleinden. Hiervoor hebben wij een vraag van de leden van de GroenLinks-fractie beantwoord waar het gaat om het voorkomen dat een buitenlandse dienst de verstrekte gegevens worden gedeeld met diensten waar Nederland geen gegevens mee zouden willen delen. Het aldaar gegeven antwoord is ook van toepassing op de situatie die door de leden van de PvdD-fractie wordt aangekaart, zodat we kortheidshalve daarnaar verwijzen.

De leden van de PvdD-fractie vinden het bevreemdend dat veiligheids-diensten internationaliseren, maar dat er nauwelijks toezicht bestaat op de samenwerking en wat er met data gebeurt. Deze leden zouden van de regering willen vernemen wat voor toezicht er op dit punt gaat zijn. En ook hoe wordt voorkomen dat buitenlandse diensten geen misbruik maken van de verkregen informatie. Klopt het, aldus deze leden, dat zowel de verstrekking als de naleving van de daarbij gemaakte afspraken zich onttrekken aan bindende toezichtsbevoegdheden van beide toezicht-houders. In dat kader vragen zij ook wat voor sanctieregime moet garanderen dat buitenlandse diensten op de in de memorie van toelichting bedoelde manier met informatie omgaan. In reactie op deze vragen verwijzen wij naar hetgeen wij hiervoor op vragen van de leden van de GroenLinks-fractie, waarbij dezelfde problematiek aan de orde is gesteld, hebben geantwoord. In aanvulling daarop bevestigen we dat zowel de verstrekking als de naleving van de daarbij gemaakte afspraken zich onttrekken aan de *bindende* toezichtsbevoegdheden van TIB en CTIVD. Wel is het zo dat de TIB een bindende ex ante toets uitoefent op de door de verleende toestemming voor de toepassing van de bevoegdheid als bedoeld in artikel 6, eerste lid, van het wetsvoorstel (artikel 6, derde lid). Het gaat hier echter om de *toepassing* van de bevoegdheid (de verwerving van de gegevens) en niet om de verdere verwerking van de daarmee verworven gegevens. Op de verdere verwerking, waaronder *de verstrekking* aan buitenlandse diensten, ziet immers de afdeling toezicht van de CTIVD toe. Van die verstrekking wordt overeenkomstig artikel 89, tweede lid, Wiv 2017 terstond mededeling gedaan aan de afdeling toezicht. De in artikel 6, derde lid, van het wetsvoorstel opgenomen mededelingsplicht van de TIB aan de afdeling toezicht van een rechtma-tigheidsoordeel alsmede hetgeen in artikel 11 is geregeld, strekken ertoe dat de overgang van de ex ante toetsing door de TIB naar het ex durante en ex post toezicht door de afdeling toezicht op een goede manier kan plaats vinden.

De leden van de PvdD-fractie vragen voorts waarom er in artikel 6 lid 2 gekozen wordt om voor de periode van een jaar toestemming te verlenen tot het met een technisch hulpmiddel aftappen, ontvangen, opnemen en afluisteren van elke vorm van telecommunicatie of gegevensoverdracht. Zoals wij eerder in antwoord op een vraag van de leden van de fractie van D66 hebben aangegeven, is in artikel 48, tweede lid, van de Wiv 2017 bepaald dat de toestemming voor de uitoefening van de bijzondere bevoegdheid tot OOG-interceptie door de Minister kan worden verleend voor een periode van ten hoogste een jaar. Bij de uitwerking van de regeling voor de verkenningsbevoegdheid in artikel 6 van het wetsvoorstel, die immers gerelateerd is aan de uitoefening van de bevoegdheid ex artikel 48, eerste lid, van de Wiv 2017, is bij die systematiek aangesloten.

De leden van de PvdD-fractie vragen aansluitend waarom deze toestemming «telkens op een daartoe strekkend verzoek kan worden verlengd voor eenzelfde periode». Wat is, zo vragen deze leden, de maximale duur om data te intercepteren. Want zoals deze leden het nu in de wet lezen kan deze onbeperkt verlengd worden, terwijl de memorie van toelichting het laat lijken dat dit tot «ten hoogste» een jaar kan. Zij vragen of de regering hier duidelijkheid over kan geven. Wij beantwoorden deze vraag als volgt. Na een verkregen toestemming voor de uitvoering van de bevoegdheid tot intercepteren ten behoeve van verkennen als bedoeld in artikel 6 van het wetsvoorstel kunnen de diensten maximaal één jaar lang uitvoering geven aan deze bijzondere bevoegdheid. Indien bij afloop van deze termijn blijkt dat het noodzakelijk is om de uitoefening van de bevoegdheid voor het onderzoek voort te zetten, kunnen de diensten een verzoek bij de Minister indienen om toestemming te vragen voor verlenging van de duur waarvoor de bevoegdheid mag worden uitgeoefend. Bij het indienen van een toestemmingsverzoek tot verlenging is er sprake van eenzelfde besluitvormingsproces als bij het eerste verzoek voor het mogen uitoefenen van die bevoegdheid. Een dergelijk verzoek moet voldoen aan de eisen van artikel 29, tweede lid, Wiv 2017, waarbij – hier relevant – in onderdeel g is bepaald dat voor zover het een verzoek om verlenging van de toestemming betreft, daarin een aanduiding van de met de uitoefening van de desbetreffende bevoegdheid behaalde resultaten moet zijn opgenomen. Dat is – naast de noodzaak tot het onderbouwen van de noodzakelijkheid, proportionaliteit en subsidiariteit van het verlengingsverzoek – dus een relevant feit bij de beoordeling door de Minister of opnieuw toestemming moet worden verleend. Een door de Minister verleende toestemming wordt vervolgens onderworpen aan de rechtmatigheidstoets door de TIB die het hiervoor genoemde aspect daarbij kan betrekken.

De leden van de Volt-fractie merken op dat met betrekking tot de verwerving, het gebruik en verwerking van bulkdatasets de regering aangeeft dat de wet voldoende waarborgen bevat om hiervan op een verantwoorde manier gebruik te maken. Zij vragen of de regering aan de hand van een concreet voorbeeld kan toelichten waarom zij van oordeel is dat het gebruik van bulkdatasets, zoals bedoeld in de Tijdelijke wet, voldoet aan de eisen die daaraan worden gesteld in de jurisprudentie van het EHRM en de Grondwet. En ook of daarbij in het bijzonder in kan worden in gegaan op de beoogde bewaartermijnen en de wijze waarop die kunnen worden verlengd. Om met laatstgenoemde vraag te beginnen, merken we op dat in de nota van wijziging is voorzien in een regeling inzake termijnen voor het gebruik van bulkdatasets verworven met bijzondere bevoegdheden. Wij verwijzen deze leden graag naar hetgeen ter toelichting daarop is gesteld, waarmee ook de door hen gestelde vragen ter zake worden beantwoord. Waar het gaat om de vraag inzake het gebruik van bulkdatasets in relatie tot de eisen van het EHRM en de

Grondwet, hebben we in de memorie van toelichting gewezen op jurisprudentie in relatie tot bulkinterceptie (via OOG-interceptie verworven bulkdatasets) en de aan de Kamer toegezonden analyse van recente jurisprudentie van het EHRM (Big Brother Watch e.a. tegen het VK; Centrum för Rätvissa tegen Zweden) van de directie Constitutionele Zaken en Wetgeving van het Ministerie van BZK. De conclusie is dat de Wiv 2017 in algemene zin aan de eisen van het EVRM (en de Grondwet) voldoet. De in genoemde uitspraken gegeven oordelen van het EHRM zien specifiek op bulkdatasets verworven via bulkinterceptie en hoe die bevoegdheid is gereguleerd (inclusief de verstrekking aan en verkrijging van buitenlandse diensten). Die bevindingen die zijn gerelateerd aan de verwerking van bulkdatasets verworven met bulkinterceptie kunnen niet 1-op-1 op de verwerking van bulkdatasets verworven met andere bevoegdheden (zoals de bevoegdheid tot het binnendringen van een geautomatiseerd werk) worden getransponeerd. Daarvoor gelden dus – in afwachting van de herziening van de Wiv 2017, waarbij het voornemen bestaat met een specifieke regeling voor de verwerking van bulkdatasets te komen -de in de Wiv 2017 opgenomen algemene bepalingen inzake de verwerking van gegevens (artikelen 17 e.v. Wiv 2017). Dat neemt niet weg, dat gelet op het bijzondere karakter van bulkdatasets, specifieke voorzieningen wenselijk kunnen zijn. In dit kader wijzen we onder meer op de Tijdelijke regeling verdere verwerking gegevens bulkdatasets.

3.3.1 Het verkennen ten behoeve van OOG-interceptie
De leden van de PvdA-fractie merken op dat om toestemming te krijgen voor OOG-interceptie zo duidelijk mogelijk dient te worden omschreven welke gegevensstromen worden geïntercepteerd. Daarvoor is eerst technisch onderzoek nodig om duidelijk te krijgen welke gegevensstromen over welke kabels gaan en op welke wijze deze gegevensstromen mogelijk een bijdrage leveren bij de beantwoording van de onderzoeksvragen van de diensten. Voor dit technisch onderzoek kan het nodig zijn gegevens met een buitenlandse collegadienst te delen. Die mag dan expliciet geen gebruik van die gegevens maken voor inlichtingendoeleinden. Deze leden vragen of de regering hun mening deelt, dat het delen van dergelijke gegevens met buitenlandse diensten extra waarborgen vergt. En, zo ja, hoe kan daar op worden toegezien. Ook vragen zij welke waarborgen en welk toezicht er bestaat op het verder gebruik van deze gegevens. Wij delen de mening van deze leden dat voor het delen van gegevens als hier bedoeld waarborgen dienen te bestaan, maar dat geldt in feite voor elke vorm van uitwisseling van gegevens met buitenlandse diensten. Of en, zo ja, met welke diensten mag worden samengewerkt, wat de aard en intensiteit van die samenwerking is – waaronder dus ook of er gegevens aan verstrekt mogen worden – wordt vastgesteld aan de hand van de wettelijke voorgeschreven weging van de (voorgenomen) samenwerkingsrelatie aan de hand van diverse, deels ook wettelijk vastgelegde, criteria (artikel 89 Wiv 2017), en dient ten slotte door de Minister te worden goedgekeurd. Deze weging bepaalt de parameters waarbinnen de samenwerking met een buitenlandse dienst kan plaatsvinden. Aan de verstrekking van gegevens aan een buitenlandse dienst stelt de wet in ieder geval de eis van toepassing van de derde-partijregel en voorts zal de Minister toestemming moeten geven voor de verstrekking van ongeëvalueerde gegevens aan een buitenlandse dienst (artikel 89, tweede lid, Wiv 2017). Een extra waarborg die bij de verstrekking van gegevens als hier bedoeld ten behoeve van een technische analyse, is dat dit doel bij de verstrekking nadrukkelijk als voorwaarde dient te worden gesteld: de ontvangende dienst mag de gegevens niet voor andere (eigen) doeleinden aanwenden. Op de wijze waarop op de naleving van deze voorwaarde wordt toegezien, zijn we in paragraaf 2.3 van deze nota naar aanleiding van het verslag in antwoord op vragen van de leden van de D66-fractie reeds ingegaan. Kortheidshalve wordt daarnaar verwezen.

Tot slot vragen de leden van de PvdA-fractie in hoeverre de TIB weet of dergelijke gegevens met buitenlandse diensten worden gedeeld en kan het de toestemming[37] voor een technisch onderzoek daarvan mede afhankelijk maken. Wij beantwoorden deze vraag als volgt. De TIB is uitsluitend belast met het beoordelen op rechtmatigheid van door de Minister verleende toestemmingen voor de inzet van bijzondere bevoegdheden. De TIB heeft een rol in de autorisatiefase. Het delen van gegevens door de diensten met inlichtingen- en veiligheidsdiensten van andere landen zit in de fase van verdere verwerking van de met de hiervoor bedoelde bijzondere bevoegdheden verworven gegevens. De wetgever heeft het toezicht daarop belegd bij de CTIVD. De TIB heeft met andere woorden hier wettelijk gezien geen rol.

De leden van de SGP-fractie ontvangen graag nadere toelichting waarom in artikel 7 gekozen is voor de toevoeging «met name» voor de twee centrale aspecten bij de toetsing van OOG-interceptie, waarvan in de toelichting wordt gezegd dat deze aspecten het zwaarwegendst zijn. Zij vragen in hoeverre het noodzakelijk is om deze toevoeging op te nemen. Zijn er situaties denkbaar, zo vragen deze leden, waarin aan andere dan de centrale aspecten toch een doorslaggevend belang toekomt en zo nee, waarom is deze toevoeging dan niet gewoon achterwege gelaten. Het bevreemdt deze leden dat, ervan uitgaande dat de toevoeging relevant is, een duiding van de toevoeging ontbreekt. Wij beantwoorden deze vraag als volgt. Het toevoegen van «met name» heeft tot doel om aan te geven dat deze twee aspecten als het zwaarwegendst dienen te worden betrokken bij de invulling van de toets op gerichtheid en proportionaliteit. Daarmee wordt dus beoogd richting te geven aan de uit te voeren toets ter zake, waarbij de in de memorie van toelichting gegeven toelichting op de in artikel 7 genoemde aspecten dient te worden betrokken. Een en ander is noodzakelijk gebleken omdat de bevoegdheid tot OOG-interceptie tot op heden slechts beperkt is ingezet ten behoeve van het inlichtingenproces vanwege de onduidelijkheid met betrekking tot de wijze waarop deze vereisten bij de inzet van deze bevoegdheid moet worden geïnterpreteerd en de verschillende zienswijzen ter zake van de Ministers en de TIB nog niet tot een oplossing heeft geleid. Daardoor kunnen bepaalde onderzoeken in het cyberdomein nog niet worden opgestart.

De leden van de SGP-fractie vragen of de regering kan aangeven welke afspraken en waarborgen er zijn voor zorgvuldige omgang gegevens door buitenlandse collegadiensten, bijvoorbeeld als het gaat om het vernietigen van gegevens. Welk belang komt toe aan het onderscheid tussen het verstrekken van gegevens aan buitenlandse diensten en benutten van buitenlandse expertise om de Nederlandse gegevens te analyseren? In hoeverre bestaat bovendien inzicht en wordt richting de Nederlandse diensten rekenschap gegeven of afspraken worden nageleefd? Klopt het dat geen rol voor toetsing en toezicht is weggelegd als het gaat om de samenwerking met buitenlandse collegadiensten? In antwoord op de vragen van deze leden verwijzen wij allereerst naar hetgeen we aan het begin van deze paragraaf in antwoord op vragen van de leden van de PvdA-fractie hebben gesteld, waar het gaat om het aspect van waarborgen. Naast de voorwaarde dat de verstrekte gegevens door de desbetreffende buitenlandse dienst uitsluitend in het kader van de gevraagde technische analyse mogen worden gebruikt, kunnen daarbij uiteraard ook andere voorwaarden worden gesteld, zoals dat men de gegevens na die analyse dient te vernietigen. Aan het vragen van ondersteuning van de buitenlandse dienst bij technische analyse als hier bedoeld is inherent dat er gegevens verstrekt worden en in dat opzicht is

[37] De TIB verleent geen toestemming, dat doet immers de Minister. De TIB beoordeelt de rechtmatigheid van de door de Minister verleende toestemming.

er dus geen onderscheid, behalve dat dit plaatsvindt onder strikte doelbinding. Waar het de overige vragen van deze leden betreft wordt verwezen naar hetgeen in paragraaf 2.3 – in antwoord op vragen van de leden van de D66-fractie – en in paragraaf 3.3 – in antwoord op vragen van de leden van de PvdD-fractie is gesteld, met name waar het gaat om het aspect toetsing en toezicht als het gaat om samenwerking met buitenlandse diensten.

3.4 Bijschrijfmogelijkheid artikel 47 Wiv 2017

Voorafgaand aan de beantwoording van de vragen van de leden van de fracties van de VVD, PvdA en D66 merken wij op dat gelet op de inhoud van de vragen van deze leden het ons voorkomt dat deze – uitgezonderd de eerste vraag van de leden van de VVD-fractie – betrekking hebben op de bijschrijfmogelijkheid in het kader van de toepassing van artikel 45 Wiv 2017 (de bevoegdheid tot binnendringen in een geautomatiseerd werk) en niet de bijschrijfmogelijkheid in het kader van artikel 47 Wiv 2017 (gericht tappen). De beantwoording van hun vragen heeft dan ook betrekking op de toepassing van de bijschrijfmogelijkheid van artikel 45 Wiv 2017.

De leden van VVD-fractie lezen dat bij de bijschrijfmogelijkheid krachtens artikel 47 naast de wettelijk vereiste toestemming sprake moet zijn van een geldige interne toestemming. Deze leden vragen of de regering de geschetste interne toestemming nader kan toelichten, onder meer bij wie die is belegd. De interne toestemmingsprocedure voor bijschrijven is dezelfde als die welke eerder geschetst is bij artikel 45 (bijschrijven in het kader van de bevoegdheid tot binnendringen in een geautomatiseerd werk). De diensten moeten voor de inzet van de tapbevoegdheid een onderbouwd toestemmingsverzoek schrijven en na toestemming van de Minister toetst de TIB de verleende toestemming op rechtmatigheid. Indien de TIB de toestemming voor de inzet rechtmatig acht, mogen de diensten de bevoegdheid tot bijschrijven inzetten, voor een periode van maximaal drie maanden. Een bijschrijving is het toevoegen van een kenmerk aan een lopende toestemming voor de inzet van de desbetreffende bevoegdheid. Dit wordt gedaan door het inlichtingenteam dat gemotiveerd omschrijft waarom het nieuwe kenmerk past in de verleende toestemming en of dit noodzakelijk, proportioneel, subsidiair en gericht is. Deze motivatie wordt eerst getoetst door de leidinggevende van dat inlichtingenteam en, indien deze akkoord is, verleent deze toestemming voor de bijschrijving. Vervolgens wordt die toestemming bij MIVD bezien door afdeling juridische zaken en bij de AIVD door het unithoofd. Indien daaruit geen bezwaren naar voren komen, kan de bijschrijving worden geëffectueerd. De beslissing wordt intern vastgelegd, zodat de CTIVD te allen tijde de overwegingen die ten grondslag hebben gelegen voor de autorisatie van de bijschrijving kan toetsen.

De leden van de VVD-fractie achten het positief dat lopende onderzoeken kunnen worden uitgebreid met apparaten via de wettelijke bijschrijfmogelijkheden met de nodige waarborgen. Gelet op het feit dat cyberaanvallen steeds geraffineerder en grootschaliger georganiseerd kunnen worden via de inzet van de brede digitale infrastructuur en specifiek via digitale apparaten van derden (bijvoorbeeld via botnets) achten zij deze bevoegdheid noodzakelijk. Deze leden vragen hoe de bijschrijfmogelijkheid van artikel 45 kan bijdragen aan het effectief bestrijden van botnetaanvallen. Wij beantwoorden deze vraag graag als volgt. Cyberactoren maken gebruik van snel wisselende infrastructuur voor het uitvoeren van hun offensieve cyberstrategie. De verduidelijking van de mogelijkheid tot bijschrijving op grond van artikel 47, zevende lid, van de Wiv 2017 en artikel 45, achtste lid, van de Wiv 2017 in respectievelijk artikel 9, eerste lid, van de Tijdelijke wet en artikel 5, tweede lid van de

Tijdelijke wet zorgt ervoor dat de diensten snel en effectief onderzoek kunnen doen, doordat bewegingen van cyberactoren in het digitale domein beter of überhaupt gevolgd kunnen worden en in kaart gebracht kunnen worden. Het voorgaande geldt in algemene zin voor alle onderzoeken in het cyberdomein, en dus ook voor (eventuele) onderzoeken naar actoren die gebruik maken van botnets. Waarbij opgemerkt moet worden dat een botnet slechts een middel of wijze van opereren van een cyberactor is. Vanuit het perspectief van de diensten zijn daarom niet zozeer de geautomatiseerde werken die deel uitmaken van het botnet op zichzelf interessant, maar meer de beheersinfrastructuur daarachter waarmee aanvallen worden aangestuurd, de wijze waarop dit gebeurt, met welke intentie en uiteraard welke actor hierachter zit.

De leden van de D66-fractie vragen de regering aan te geven of de voorbeelden die zij onder hoofdstuk 3.3.4.1 (GDA) van de memorie van toelichting geeft, een limitatieve opsomming is van de inzet van GDA. Indien dit geen limitatieve opsomming is, kan de regering dan aangeven wat de grenzen zijn van wat er onder GDA wordt verstaan? Zoals wij ook eerder in antwoord op vragen van de leden van de SP-fractie hebben aangegeven (paragraaf 2.2 van deze nota naar aanleiding van het verslag) bestaat er geen limitatieve lijst met vormen van GDA. Het is een open begrip dat diverse bestaande en nog te ontwikkelen vormen van GDA moet kunnen omvatten. Bij de herziening van de Wiv 2017 zal overigens de bestaande regeling inzake GDA opnieuw tegen het licht worden gehouden, waarbij ook hetgeen de ECW ter zake heeft opgemerkt zal worden betrokken.

Deze leden horen graag van de regering hoe de proportionaliteit van het bijschrijfsysteem gewaarborgd is. Wij beantwoorden deze vraag als volgt. Voor de toepassing van de bijschrijfmogelijkheid geldt dat de interne toestemmingsprocedure moet worden gevolgd. Evenals bij een regulier verzoek om toestemming aan de Minister om de bijzondere bevoegdheid ex artikel 47 Wiv 2017 (gericht tappen) in te mogen zetten, zal het verzoek om toestemming dienen te voldoen aan de vereisten van noodzaak, proportionaliteit, subsidiariteit en gerichtheid. Wordt de interne autorisatie verleend, dan wordt de afdeling toezicht daarvan terstond mededeling gedaan. De afdeling kan dan beoordelen of de autorisatie rechtmatig is verleend en toezien op de wijze waarop aan de bijschrijfbevoegdheid uitvoering wordt gegeven.

Voorts vragen deze leden hoe ruim «een derde» wordt opgevat en hoeveel sneller «derden» voortaan kunnen worden bijgeschreven dan nu de praktijk is. Wij beantwoorden deze vraag als volgt. Een derde is een partij die technisch te relateren is aan het target. Daarbij moet onder andere gedacht worden aan een partij die een netwerk aansluit, een dienst levert, software levert of technische kennis levert. Een derde kan niet worden bijgeschreven. Zodra in een lopend onderzoek een nieuwe derde in beeld komt, dient een nieuw toestemmingsverzoek te worden ingediend. Geautomatiseerde werken van een derde die al in het toestemmingsverzoek vermeld staat kunnen wel worden bijgeschreven. Dit is overigens onder de Wiv 2017 ook al het geval.

De leden van de D66-fractie vragen of de regering nader kan uiteenzetten wat zij precies verstaat onder dat geen sprake hoeft te zijn van exclusief gebruik voor geautomatiseerde werken die behalve door de actor zelf ook door anderen worden gebruikt, voor zover dat noodzakelijk is voor het doel waarvoor de oorspronkelijke toestemming is aangevraagd, om te kunnen bijschrijven. Ook vragen zij of hierbij voorbeelden uit de praktijk bij worden gegeven. Wij beantwoorden deze vragen graag als volgt. De mogelijkheid tot bijschrijven zorgt ervoor dat de diensten snel en effectief

onderzoek kunnen doen. Cyberactoren maken gebruik van geautomatiseerde werken, die vaak in een complexe keten aan elkaar gekoppeld worden, hun zogenoemde digitale aanvalsinfrastructuur, voor het uitvoeren van hun offensieve cyberstrategie. Om de herleidbaarheid van hun activiteiten te verkleinen, wisselen targets snel van geautomatiseerde werken en werkmethodes. Ook hacken cyberactoren geautomatiseerde werken van anderen om die te gebruiken voor het uitvoeren van hun offensieve cyberprogramma. Cyberactoren maken gebruik van gedeelde infrastructuur of hacken geautomatiseerde werken om dit onderdeel te maken van hun aanvalscampagne. Dit maakt bijschrijven in een dergelijke situatie in de praktijk vrijwel onmogelijk. Er kan enkel een kenmerk worden bijgeschreven indien het past binnen de reikwijdte van de betreffende toestemming. Een kenmerk bij een geautomatiseerd werk is een technische aanduiding, waarmee wordt aangeduid op welke geautomatiseerd werk een bijzondere bevoegdheid betrekking heeft, in dit geval de bevoegdheid tot het binnendringen in een geautomatiseerd werk. Een voorbeeld hiervan is een IP-adres. Indien een toestemming gericht is op een bepaalde cyberactor dan kunnen enkel kenmerken worden bijgeschreven die gebruikt worden door de cyberactor. Deze kenmerken kunnen exclusief en niet-exclusief in gebruik zijn bij de cyberactor. Op het moment dat een cyberactor meerdere geautomatiseerde werken gebruikt ten behoeve van een aanvalscampagne die zowel exclusief en niet-exclusief in gebruik zijn, kunnen de diensten de cyberactor niet snel genoeg volgen als de niet-exclusieve kenmerken niet bijgeschreven kunnen worden. Hier dient namelijk een procedure gevolgd te worden die minstens een week in beslag neemt. Het is noodzakelijk om deze niet-exclusieve kenmerken wel bij te schrijven om efficiënt en effectief onderzoek te doen naar activiteiten van cyberactoren die de nationale veiligheid van Nederland kan schaden. Het ontbreken van zicht op deze activiteiten schaadt Nederland en Nederlandse belangen en kan uiteindelijk schadelijk zijn voor Nederland als geheel maar ook voor burgers en bedrijven die direct geraakt kunnen worden door deze activiteiten. Het is derhalve noodzakelijk om zowel kenmerken die exclusief in gebruik zijn als kenmerken die niet-exclusief in gebruik zijn om activiteiten van cyberactoren te kunnen volgen zodat de dreiging voor de nationale veiligheid op tijd geduid kan worden. Vanzelfsprekend zijn de beginselen van noodzakelijkheid, gerichtheid, proportionaliteit en subsidiariteit alsmede de reikwijdte van de eerder verleende toestemming waaraan de bijschrijving moet zijn gerelateerd van toepassing.

Deze leden vragen ten slotte of de regering een mogelijk risico ziet in het ontbreken van een nadere afbakening van wie of wat er wel bijgeschreven mag worden en of de regering hierop kan reflecteren en daarbij ingaan op de waarborgen die er met het voorliggende voorstel bestaan tegen (praktisch) ongelimiteerd bijschrijven. Ook vragen zij of er een limiet is aan op welke schaal kan worden bijgeschreven en, zo ja, of hiervan een voorbeeld kan worden gegeven. In reactie hierop merken we het volgende op. De TIB toetst of de door de Minister verleende toestemming rechtmatig is. Bij de beoordeling van de rechtmatigheid worden noodzaak, proportionaliteit, subsidiariteit en gerichtheid meegewogen. Binnen de reikwijdte van de verleende toestemming mag worden bijgeschreven. Dit is nu al mogelijk als het gaat om kenmerken die *exclusief* toebehoren aan een persoon of organisatie waar de diensten onderzoek naar doen. Het (kunnen) bijschrijven van kenmerken is aldus niet nieuw en is dus een bestaande praktijk, waarop de afdeling toezicht van de CTIVD toezicht kan houden. Het onderhavige wetsvoorstel verduidelijkt slechts dat ook kenmerken die *niet exclusief* toebehoren aan de persoon of organisatie waar de diensten onderzoek naar doen kunnen worden bijgeschreven. De afbakening wordt bepaald door de door de Minister verleende toestemming en wel in het bijzonder de persoon of organisatie waarop de

bevoegdheid mag worden ingezet. De bijschrijving dient daaraan gerelateerd te zijn en hoe vaak daarvan gebruik moet worden gemaakt is op voorhand niet aan te geven, immers dat is afhankelijk van het gedrag van de desbetreffende persoon of instantie. Het is ook niet wenselijk om (op voorhand) een limiet daaraan te stellen. Naar ons oordeel kan in deze worden volstaan met de op de toepassing van artikel 5, tweede lid, van het wetsvoorstel voorziene mogelijkheid van bindend toezicht door de afdeling toezicht (artikel 12, eerste lid, onder c). Voor het overige geldt dat de algemene waarborgen uit de Wiv 2017 van toepassing zijn in het kader van de zorgplicht en de verdere gegevensverwerking. Deze waarborgen zorgen ervoor dat niet-relevante gegevens zo spoedig mogelijk worden vernietigd en niet verder worden verwerkt in het inlichtingenproces. Met de huidige waarborgen zijn wij van oordeel dat sprake is van een sluitend stelsel van waarborgen.

De leden van de GroenLinks-fractie wijzen erop dat de regering (in de toelichting op artikel 9 van het wetsvoorstel) schrijft dat gedurende de toestemmingsperiode nummers dan wel technische kenmerken worden bijgeschreven voor zover dat noodzakelijk is voor het doel waarvoor de oorspronkelijke toestemming is verleend. Deze leden vragen de regering op dit punt nader in te gaan op wat hier «noodzakelijk» betekent en welke criteria hierbij gebruikt worden om te bepalen of het noodzakelijk is. Om een kenmerk te mogen bijschrijven is het vereist dit kenmerk ook noodzakelijk, proportioneel, subsidiair en zo gericht mogelijk is en dat dezelfde afwegingen gelden zoals in de verleende toestemming zijn omschreven en die door de TIB rechtmatig zijn beoordeeld.

3.5 Bijschrijfmogelijkheid artikel 54 Wiv 2017

Voorafgaand aan de beantwoording van de vragen van de leden van de SP-fractie merken wij op dat gelet op de inhoud van de vragen van deze leden het ons voorkomt dat deze betrekking hebben op de bijschrijfmogelijkheid in het kader van de toepassing van artikel 45 Wiv 2017 (de bevoegdheid tot binnendringen in een geautomatiseerd werk) en niet de bijschrijfmogelijkheid in het kader van artikel 54 Wiv. De beantwoording van hun vragen heeft dan ook betrekking op de toepassing van de bijschrijfmogelijkheid van artikel 45 Wiv 2017.

De leden van de SP-fractie vragen de regering wat de AIVD en MIVD in de technische briefing bedoelden met de claim dat er nooit IP-adressen van nieuwe servers «bijgeschreven» kunnen worden en of kan worden aangegeven of dit nooit gebeurt of hoe vaak dit nu wel gebeurt. Wij beantwoorden deze vraag als volgt. Technische kenmerken, zoals IP-adressen, die niet exclusief in gebruik zijn bij de actor worden nu niet bijgeschreven maar zijn onderdeel van een reguliere aanvraag voor de uitvoering van een bijzondere bevoegdheid zoals geregeld in de artikelen 45 (bevoegdheid tot binnendringen in een geautomatiseerd werk) en 47 (gerichte interceptie) Wiv 2017. Dit komt voort uit een strikte interpretatie van het bijschrijfcriterium.

Deze leden wijzen erop dat het wetsvoorstel de mogelijkheid uitbreidt tot bijschrijven van non-targets en deze leden vragen zich af waarom de indruk is gewekt dat bijschrijven geheel onmogelijk was tot nu toe. Wij reageren graag als volgt. Het klopt dat tijdens de technische briefing is toegelicht dat er op dit moment geen bijschrijvingen gedaan kunnen worden indien er sprake is van kenmerken die niet exclusief in gebruik zijn bij de actor. Het voorstel zorgt er juist voor dat de diensten effectief onderzoeken kunnen doen dat past bij de snelheid en dynamiek van de dreiging in het cyberdomein. Het maakt het mogelijk om kenmerken die in gebruik zijn bij een actor, bijvoorbeeld bij aanvalsinfrastructuur, ten

behoeve van bijvoorbeeld een aanvalscampagne bij te kunnen schrijven onder een lopende toestemming tot binnendringen in een geautomatiseerd werk of taptoestemming die gericht is op de betreffende actor. Dit voorstel voorziet niet in de mogelijkheid om kenmerken van non-targets bij te schrijven. Non-targets zijn namelijk personen of organisaties die niet onder de aandacht van de diensten staan, maar wel over gegevens of informatie beschikken over of van een target. In casu gaat het over kenmerken die ofwel toebehoren aan zowel een actor als een legitieme gebruiker (omdat er bijvoorbeeld sprake is van gedeeld gebruik van een server), ofwel een kenmerk dat toebehoort aan een legitieme gebruiker maar feitelijk onder controle staat van de actor (omdat er bijvoorbeeld een geautomatiseerd werk van een legitieme gebruiker gehackt is). In deze gevallen moeten de diensten in staat zijn om deze kenmerken bij te schrijven om zicht te houden op de actor en omdat bij deze kernmerken het gebruik van het kenmerk door de actor centraal staat. Vanzelfsprekend zullen de diensten gegevens die niet toebehoren aan de actor niet meenemen in het inlichtingenonderzoek.

De leden van de SP-fractie vragen voorts toe te lichten waarom het toetsen van bijschrijven kan vervallen. Hoe wordt, aldus deze leden, een bijschrijving bij het verschoven toezicht zichtbaar en daarmee toetsbaar. Wij antwoorden deze leden als volgt. Het is een onjuiste conclusie dat de toets op bijschrijven vervalt onder het voorstel. Het toezicht op bijschrijvingen wordt onder het voorstel juist verstevigd vanwege het bindend toezicht van de afdeling toezicht op bijschrijvingen. Indien er sprake is van een lopende toestemming kunnen de diensten onder artikel 45 Wiv 2017 en artikel 47 Wiv 2017, en na inwerkingtreding Tijdelijke wet ook bij artikel 54 Wiv 2017, overgaan tot het bijschrijven van kenmerken die gebruikt worden door de actor die onderwerp is van de verleende toestemming. Bij beide diensten is er sprake van een interne toets op het bijschrijven van kenmerken. Bij een eventueel door de Minister verleende toestemming waarbij de uitoefening van de bevoegdheid wordt verlengd, kan de TIB kennisnemen van de resultaten van een bijgeschreven kenmerk op de eerder verleende toestemming indien het kenmerk onderdeel uitmaakt van de aan de TIB-toets onderworpen toestemming. De bijschrijfmogelijkheid wordt in het nieuwe voorstel wel verduidelijkt waardoor ook kenmerken die niet exclusief in gebruik zijn bij de actor bijgeschreven kunnen worden. Ten allen tijde blijven de beginselen van gerichtheid, noodzakelijkheid, proportionaliteit en subsidiariteit alsmede de reikwijdte van het verzoek onverminderd van toepassing.

Deze leden vragen de regering ten slotte om toe te lichten of door de CTIVD geformuleerde criteria (CTIVD toezichtsrapport nr. 53) voor het hacken van non-targets onverkort van kracht blijven bij toepassing van artikel 5 in het voorliggend wetsvoorstel. En gelden deze criteria ook voor de artikelen 10 en 11 in relatie tot artikelen 47 en 54 van de bestaande wet? Het begrip non-targets zoals de diensten en de CTIVD het begrip omschrijven is hier niet van toepassing. Een non-target is een persoon of een organisatie die niet onder de aandacht van de diensten staat maar wel over gegevens of informatie beschikt van een target. Bij een inzet op non-target staat het non-target centraal met bijbehorende waarborgen. Bij een inzet op een kenmerk dat niet exclusief in gebruik is bij een actor staat de actor en dus het target centraal. Dit betekent ook meteen dat de gegevens die niet bij de actor horen niet verder worden verwerkt in een inlichtingenonderzoek. Het rapport van de CTIVD is onverkort van toepassing maar heeft geen invloed op het bijschrijven van kenmerken die niet exclusief in gebruik zijn bij de actor onder bijvoorbeeld artikel 45 Wiv 2017, 47 Wiv 2017 en artikel 54 Wiv 2017.

4. Toets en toezicht en de mogelijkheid van beroep op de Afdeling bestuursrechtspraak van de Raad van State

4.1 Inleiding

De leden van de SP-fractie willen graag nadere uitleg over wat er bedoeld wordt bij de accentverschuiving van het toezicht en willen graag een overzicht krijgen welk bindend toezicht vooraf vervalt en wordt verschoven. In reactie op deze vraag merken wij op dat accentverschuiving betekent dat waar thans het accent ligt op een bindende toets ex ante door de TIB dat verschuift naar een bindende toets ex durante (of ex post) naar de afdeling toezicht van de CTIVD. Wij hebben dat inzichtelijk gemaakt in een schematisch overzicht dat we eerder in deze nota naar aanleiding van het verslag (paragraaf 2.5) als reactie op vragen van de GroenLinks-fractie hebben opgenomen.

In reactie op de vraag van de leden van SP-fractie of het klopt dat er geen sprake meer is van bindend toezicht op de bevoegdheden voor kabelinterceptie, antwoorden wij dat dat onjuist is. Zowel waar het gaat om de in artikel 6 van dit wetsvoorstel geregelde bevoegdheid tot verkennen als de reguliere OOG-interceptie ex artikel 48 Wiv 2017 blijft de ex ante toets door de TIB bestaan. Er verandert in dat opzicht dus niets. Wel is het zo dat voor de bevoegdheid tot verkennen enkele specifieke voorzieningen zijn getroffen. Zo komt de eis van gerichtheid ex artikel 26, vijfde lid, Wiv 2017 te vervallen, is de uitoefening strikt doelgebonden, mogen alleen daartoe aangewezen medewerkers van de diensten van de desbetreffende gegevens kennisnemen en is de bewaartermijn voor de in het kader van verkennen verworven gegevens voor zover die niet bijdragen aan het doel van de verwerving verkort van drie jaar[38] naar zes maanden.

Deze leden vragen aansluitend of de Kamer dus fout is geïnformeerd tijdens het rondetafelgesprek. Zoals uit voorgaand antwoord blijkt, blijft de bindende toetsing ex ante bij kabelinterceptie bestaan. Bindend toezicht achteraf door de afdeling toezicht van de CTIVD bestaat thans niet en wordt in het wetsvoorstel ook niet bij kabelinterceptie voorzien. Dit alles blijkt uit de memorie van toelichting.[39] Wij zien dan ook niet in hoe de Kamer «dus fout» kan zijn geïnformeerd bij het rondetafelgesprek.

De leden van de fractie van de PvdA vragen of de Afdeling bestuursrechtspraak over de benodigde kennis en vaardigheden beschikt om de in het wetsvoorstel aan deze afdeling opgedragen taak, namelijk tot het oordelen over geschillen tussen de verantwoordelijke Ministers enerzijds en de TIB en afdeling toezicht van de CTIVD anderzijds over de rechtmatigheid van de door de TIB dan wel afdeling toezicht op grond van de Tijdelijke wet genomen oordelen, uit te voeren. Ook vragen zij of de Afdeling bestuursrechtspraak over capaciteit daarvoor beschikt. In reactie hierop merken wij het volgende op. Zoals in de memorie van toelichting is aangegeven, is de keuze voor de Afdeling bestuursrechtspraak in de eerste plaats ingegeven door de volledige onafhankelijkheid van de Afdeling als rechterlijk orgaan en voorts doordat de Afdeling bestuursrechtspraak als hoogste bestuursrechter veel ervaring heeft met de beslechting van geschillen waarin overheidshandelen centraal staat, ook in het licht van constitutionele en mensenrechtelijke vraagstukken. De Afdeling bestuursrechtspraak kan ook met gezag opereren en de keuze voor dit orgaan doet recht aan het grote maatschappelijke belang dat bij oordeelsvorming omtrent de rechtmatigheid van de activiteiten van de

[38] Zie artikel 48, vijfde lid, Wiv 2017.
[39] Zie paragraaf 3.3.2 en in de artikelsgewijze toelichting op artikel 6 van de memorie van toelichting.

inlichtingen- en veiligheidsdiensten aan de orde is. Daarbij komt dat Afdeling bestuursrechtspraak ook nu reeds als hoogste bestuursrechter optreedt bij geschillen over de toepassing van de Wiv 2017 en de Wet veiligheidsonderzoeken.[40] Ook in die zaken kan de Afdeling bestuursrechtspraak van staatsgeheime informatie kennis nemen. Voor zover, gelet op de aard van de geschillen die op grond van de Tijdelijke wet aan de Afdeling bestuursrechtspraak kunnen worden voorgelegd, de Afdeling bestuursrechtspraak het noodzakelijk acht de benodigde technische kennis op te doen, is in het wetsvoorstel erin voorzien dat zij deskundigen kan raadplegen maar ook dat een staatsraad in buitengewone dienst met de benodigde technische kennis kan worden benoemd die onderdeel uitmaakt van een meervoudige kamer. Gelet hierop hebben wij geen enkele twijfel erover dat op het moment dat de beroepsmogelijkheid in werking treedt en wordt toegepast, de Afdeling bestuursrechtspraak over de door de leden van de PvdA-fractie genoemde kennis en ervaring zal beschikken, voor zover men dat nu al niet heeft. Uiteraard zullen bij de Afdeling bestuursrechtspraak de daarvoor benodigde randvoorwaarden in personele, organisatorische, technische en financiële zin dienen te worden gerealiseerd. Over de implementatie van het wetsvoorstel wordt reeds met de Afdeling bestuursrechtspraak van de Raad van State overleg gevoerd.

De leden van de PvdA-fractie wijzen de regering op de kanttekeningen die de commissie Bovend'Eert bij de beroepsmogelijkheid bij de Afdeling bestuursrechtspraak plaatst, namelijk dat de beroepsmogelijkheid wel openstaat voor de Ministers, maar niet voor de burgers of bedrijven die wensen op te komen tegen het inzetten van een bevoegdheid waarmee zij in hun persoonlijke levenssfeer of bedrijfsvoering worden geraakt. Daarom stelde deze commissie voor om een onafhankelijk vertegenwoordiger van de burger of een belangenorganisatie aan te stellen die in de gevallen die het opportuun acht namens de burger beroep instelt. Deze leden wijzen op het feit dat de amicus curiae onlangs een wettelijke basis heeft gekregen en wellicht tot inspiratie kan dienen. In reactie hierop zouden wij het volgende willen opmerken. De beslissingen waartegen beroep bij de Afdeling bestuursrechtspraak kan worden opengesteld, betreffen beslissingen inzake operationele activiteiten van de diensten. Dergelijke activiteiten hebben uit de aard der zaak een staatsgeheim karakter en zijn niet openbaar. Mede in verband daarmee is in artikel 145 Wiv 2017 bepaald dat (onder meer) de Algemene wet bestuursrecht niet van toepassing is.[41] Immers de in de Algemene wet bestuursrecht geldende bepalingen inzake de voorbereiding en totstandkoming van besluiten en de mogelijkheid van bezwaar en beroep kunnen geen toepassing vinden waar sprake is van een heimelijke uitoefening van bevoegdheden tegen personen, waarbij het publiekelijk bekendraken daarvan – met name bij die personen – negatieve gevolgen heeft voor het slagen van die toepassing maar ook dat daarmee het actuele kennisniveau van de dienst in het geding komt. Daarmee wordt de nationale veiligheid ernstig geschaad. De idee van aanstelling van een onafhankelijke vertegenwoordiger voor de burger of een belangenorganisatie die in de gevallen waarin deze het opportuun acht, beroep namens de burger instelt, is om een aantal redenen niet uitvoerbaar. Om beroep in te kunnen stellen, zal een dergelijke onafhankelijke vertegenwoordiger kennis moeten hebben van alle (onder de toepasselijke regeling vallende)

[40] Vgl. de besluiten inzake kennisneming van door de diensten verwerkte gegevens op grond van de Wiv 2017 en de weigeringen of intrekkingen van verklaringen van geen bezwaar op basis van de Wet veiligheidsonderzoeken.

[41] Overigens zal in het kader van de herziening Wiv 2017 worden onderzocht of en, zo ja, op onder welke condities (onderdelen van) de Algemene wet bestuursrecht van toepassing kan worden verklaard.

operationele besluiten die door (of namens) de Minister worden genomen. Los van het feit dat zelfs binnen de diensten kennis over operationele besluiten niet mag worden gedeeld met andere personen dan die welke daar in het kader van een goede taakuitvoering kennis van moeten kunnen nemen (wettelijk vastgelegd need to know-beginsel), is een integraal overzicht daarvan niet beschikbaar en – al zou dat er wel zijn – is het ook vanuit het feit dat het om uiterst gevoelige en kwetsbare informatie gaat niet wenselijk dat deze aan een derde beschikbaar wordt gesteld om aan de hand daarvan te bezien of deze het *opportuun* acht beroep in te stellen. Dat is dus iets anders dan de figuur van de *amicus curiae*, die thans in Afdeling 8.1.2b van de Algemene wet bestuursrecht is geregeld. Daarbij wordt aan de hoogste bestuursrechtelijke colleges, waaronder aan de Afdeling bestuursrechtspraak van de Raad van State, de mogelijkheid geboden om anderen dan partijen in de gelegenheid stellen binnen een door het college te bepalen termijn schriftelijke opmerkingen te maken (artikel 8:12b, eerste lid). In de opgenomen regeling voor beroep bij de Afdeling bestuursrechtspraak is niet in deze mogelijkheid voorzien. In het kader van de herziening van de Wiv 2017 zal worden onderzocht of en, zo ja, op welke wijze (delen van) de Awb van toepassing kunnen worden, onder meer waar het gaat om de beroepsprocedure. Daarbij zal – zo zeggen wij toe – ook de mogelijkheid van toepassing van de figuur van de *amicus curiae* worden betrokken.

De leden van de PvdA-fractie vragen in hoeverre de voorgestelde beroepsmogelijkheid bij de Afdeling bestuursrechtspraak, ondanks de spoedprocedure of de voorlopige voorziening, kan gaan leiden tot vertraging voor de diensten. Belemmert dit, aldus deze leden, de operationele slagkracht van de diensten en hoe verhoudt zich dat tot de belemmering van die slagkracht die nu nog veroorzaakt zou worden door het nu nog bestaande toezicht door de TIB. Voor ons en de diensten is het belangrijkste dat door het instellen van beroep tegen oordelen van de TIB dan wel de afdeling toezicht onder meer duidelijkheid kan worden verkregen over de uitleg van de wet. Dat er enige vertraging kan optreden bij de uitvoering van onderzoeken door de diensten is daaraan inherent, maar te prefereren boven de bestaande situatie dat – in geval van onrechtmatigheidsoordelen van de TIB – een bevoegdheid niet (meer) kan worden ingezet en de toestemmingsprocedure opnieuw moet worden ingezet. Dat levert immers ook vertraging op. Met de beroepsmogelijkheid kan een eenduidige en gezaghebbende uitspraak over de uitleg van de wet worden verkregen, die ertoe kan bijdragen dat (vertragende) discussies over de uitleg van de wet tussen de diensten en de TIB dan wel afdeling toezicht van de CTIVD voor de toekomst worden voorkomen en uiteindelijk juist tot meer snelheid in het proces van het al dan niet kunnen inzetten van bijzondere bevoegdheden door de diensten kan leiden.

De leden van de SGP-fractie vragen de regering te reflecteren op de consequenties van de keuzes inzake toetsing en toezicht voor het uitoefenen van de ministeriële verantwoordelijkheid. Zij vragen daarbij ook aandacht te geven aan de argumenten die door de regering dienaangaande zijn aangevoerd bij de behandeling van de Wiv 2017 en waarom bepaalde keuzes in de huidige omstandigheden nu anders gewogen worden. Zij vragen de regering of deze voorbeelden kan geven van andere beleidsvelden waar de bevoegdheid in ernstige situaties die de openbare orde en het landsbelang raken beperkt worden door bindende toetsing en bindend toezicht. Wij reageren graag als volgt op de door deze leden gemaakte opmerkingen. De leden van de SGP-fractie snijden met hun vragen een wezenlijke kwestie aan. Het borgen van de nationale veiligheid is immers een wezenlijke staatstaak waarvoor de ter zake verantwoordelijke Ministers over de volle breedte verantwoordelijkheid moeten kunnen dragen en aan het parlement verantwoording af moeten kunnen leggen.

Een onafhankelijke toezichthouder – of die nu wel of niet bindende bevoegdheden heeft – kan die verantwoordelijkheid niet «overnemen». Dat neemt niet weg dat op veel beleidsterreinen sprake is van toezicht met bindende bevoegdheden, waarbij we wijzen op het toezicht dat bijvoorbeeld door de Autoriteit Persoonsgegevens (AP) op grond van de Algemene Verordening Gegevensbescherming (AVG) en de daaraan gerelateerde uitvoeringsregelgeving wordt gehouden op de rechtmatige verwerking van persoonsgegevens. Een vergelijkbare rol vervult de afdeling toezicht van de CTIVD maar dan in het domein van de inlichtingen- en veiligheidsdiensten en – tot op heden – met niet bindende bevoegdheden. Daarnaast bestaan er vormen van bindend toezicht in de financiële sector (vergelijk het toezicht door de DNB en AFM), op het vlak van consumentenbescherming (vgl. ACM) e.d.; veelal ter uitvoering van Europese regelgeving. Het is ook vaak toezicht door een bepaalde instantie op een specifiek aspect van de activiteiten van de onder toezichtgestelden, zoals de verwerking van persoonsgegevens of de bescherming van consumentenbelangen. In de praktijk hebben onder toezichtgestelden dan ook vaak met meerdere – gespecialiseerde – toezichthouders te maken. Verder dient opgemerkt te worden dat het domein van de inlichtingen- en veiligheidsdiensten gekenmerkt wordt door een taakuitvoering die zich niet in de openbaarheid afspeelt en waarin dus (in tegenstelling tot andere beleidsterreinen) geen volledige openbare parlementaire of media controle plaatsvindt. Op grond van de huidige Wiv 2017 is het toezichtsmandaat van de afdeling toezicht van de CTIVD breed geformuleerd, namelijk de rechtmatige (niet: de doelmatige) uitvoering van de Wiv 2017 en de Wet veiligheidsonderzoeken. Nu het daar gaat om niet-bindend toezicht en dit toezicht kan uitmonden in onderzoeksrapporten met niet bindende aanbevelingen, heeft dat als zodanig geen (beperkende) invloed op de ministeriële verantwoordelijkheid. Waar het gaat om de TIB die wel een bindende toetstaak heeft, is indertijd door de Afdeling advisering van de Raad van State gesteld dat met de introductie van de bindende rechtmatigheidstoets door de TIB afbreuk kan worden gedaan aan de ministeriële verantwoordelijkheid. Daarop is van de zijde van de regering geantwoord dat de Afdeling – in zijn advies – er terecht op wijst dat de beslissing om de diensten een onderzoek te laten starten niet uitsluitend een juridisch oordeel vereist, maar samenhangt met beleidsmatige afwegingen. De regering heeft daarop – samengevat[42] – gereageerd door te stellen dat voor zover het gaat om de beleidsmatige afwegingen, dat die niet onderworpen zijn aan de toets van de TIB of het rechtmatigheidstoezicht door de CTIVD. De Minister draagt voor die beslissing de volle ministeriële verantwoordelijkheid. Bij de inzet van bevoegdheden van de diensten zullen naast rechtmatigheidsaspecten ook beleidsaspecten een rol spelen en die beleidsaspecten kunnen doorwerking hebben in de invulling van criteria als noodzakelijkheid, proportionaliteit en subsidiariteit. Maar uiteindelijk wordt wel gekozen voor de inzet van een bepaalde bevoegdheid die de rechtmatigheidstoets dient te doorstaan; het gaat immers om toepassing van wettelijk vastgelegde eisen. De Minister is volledig verantwoordelijk voor het uiteindelijk door hem genomen besluit. Dat een bindende toets door de TIB leidt tot een inperking van de ministeriële bevoegdheid en daarmee ook een inperking van de ministeriële verantwoordelijkheid en de daarmee samenhangende mogelijkheid tot parlementaire controle is, zoals de regering indertijd in reactie op het advies van de Afdeling advisering heeft aangegeven, voor discussie vatbaar. Indien de TIB een verleende toestemming onrechtmatig acht, kan de Minister altijd een nieuw besluit nemen, waarbij gepoogd kan worden de door de TIB geconstateerde gebreken op het vlak van rechtmatigheid (onvoldoende noodzaak aangetoond, disproportioneel of een te zwaar middel als er een

[42] De volledige reactie is te vinden in Kamerstukken II 2016/17, 34 588, nr. 4, p. 23–24.

lichter alternatief voorhanden is) weg te nemen. Of de Minister daarvoor kiest is ook aan de Minister en ook daarvoor is hij verantwoordelijk. Voorts is de Minister volledig verantwoordelijk voor de uiteindelijke uitvoering van de bijzondere bevoegdheid. De parlementaire controle blijft intact. Het antwoord op de vraag of er wel of niet sprake is van een inperking van de ministeriële verantwoordelijkheid bij bindende toetsing – maar dat zal niet anders liggen bij bindend toezicht – is voor discussie vatbaar. Naar ons oordeel dient de wetgever – regering en beide kamers der Staten-Generaal – bij de introductie van een bindende bevoegdheid voor de afdeling toezicht van de CTIVD zoals bijvoorbeeld nu in het wetsvoorstel wordt voorgesteld dan ook nadrukkelijk stil te staan bij de betekenis daarvan voor de ministeriële verantwoordelijkheid. Immers het raakt direct aan de parlementaire controletaak. Het voorstel voor een bindende toezichtsbevoegdheid van de afdeling toezicht van de CTIVD, zoals dat er thans ligt, waarbij deze beperkt is tot specifiek aangewezen besluiten, achten we vanuit ons oogpunt aanvaardbaar. Bij de herziening van de Wiv 2017, waarbij in brede zin naar het stelsel van toetsing en toezicht zal worden gekeken en diverse scenario's denkbaar zijn, zal voor elk scenario de gevolgen daarvan voor de ministeriële verantwoordelijkheid nader in kaart gebracht dienen te worden. We verwijzen naar hetgeen in de Hoofdlijnennotitie is gesteld. Wel zijn reeds een aantal noties te onderkennen, die daarbij een rol dienen te spelen. Allereerst dat – aansluitend bij het door de Afdeling advisering gemaakte onderscheid in het kader van de TIB-toets – het toezicht, indien dat bindend is, zich tot rechtmatigheidsvraagstukken dient te beperken en niet kan zien op beleidsmatige vraagstukken of beleidsmatige aspecten niet zijnde beleidsjuridische aspecten bij de uitoefening van de taken door de inlichtingen- en veiligheidsdiensten. Dat betekent naar ons oordeel dat de invulling van de taakstelling van de diensten (zoals met name neergelegd in de GA), dat bij uitstek een beleidsmatige aangelegenheid betreft, buiten het rechtmatigheidstoezicht valt. Dat geldt naar ons oordeel evenzeer voor de besluiten aangaande de samenwerking met inlichtingen- en veiligheidsdiensten van andere landen, nu dat immers uiteindelijk een beleidsmatige en geen louter juridische afweging is, waarbij ook aspecten van belang zijn die raken aan de betrekkingen van Nederland met andere landen. Ergo: het nationale veiligheids- en buitenlands *beleid* van Nederland behoort tot het domein van de politiek. Voor deze beleidsmatige kwesties dient de Minister ten volle verantwoordelijkheid te dragen en verantwoording aan het parlement af te (kunnen) leggen. Daarin kan een toezichthouder niet treden. Bij de herziening van de Wiv 2017 en de vormgeving van het stelsel van toetsing en toezicht, zal dan ook – voor zover sprake is van de invoering van bindend toezicht (anders dan de bestaande TIB-toets) – nadrukkelijk stil dienen te worden gestaan bij de reikwijdte van dergelijk toezicht en de oordelen die uitgesproken kunnen worden.

De leden van de SGP-fractie lezen dat de beroepsprocedure volgens de regering een tijdelijk karakter heeft en dat deze ook meer fundamenteel en in zijn geheel zal worden bezien. Betekent dit, aldus deze leden, dat het een reële optie is om straks te kiezen voor een alternatief voor de voorgestelde beroepsprocedure of is het risico behoorlijk dat wordt voortgegaan op een pad dat onder tijdsdruk is ingeslagen en dat mogelijk niet optimaal is. In reactie op hetgeen deze leden opmerken, willen we als volgt reageren. De Tijdelijke wet heeft een looptijd van vier jaren en alle daarin opgenomen voorzieningen, waaronder de beroepsprocedure bij de Afdeling bestuursrechtspraak delen in die tijdelijkheid. De verwachting is dat binnen die vier jaar de brede herziening van de Wiv 2017 zijn beslag kan krijgen. De in de Tijdelijke wet opgenomen mogelijkheid van beroep bij de Afdeling bestuursrechtspraak zal echter bij de brede herziening worden gehandhaafd. Zoals de ECW terecht heeft geconstateerd bevat de huidige Wiv 2017 een weeffout en met de beroepsmogelijkheid bij de

Afdeling bestuursrechtspraak wordt die weeffout hersteld; in paragraaf 4.3 van de memorie van toelichting zijn we daarop uitgebreid ingegaan. Wel is het zo dat in het kader van de herziening van de Wiv 2017 de ervaringen die met de Tijdelijke wet worden opgedaan, dus ook waar het gaat om de beroepsprocedure, – voor zover voorhanden – daarbij zullen worden betrokken. Zoals in de memorie van toelichting echter ook is aangegeven, is de thans voorgestelde regeling inzake beroep (en de voorlopige voorziening) een regeling *sui generis*, waarbij elementen zijn ontleend aan de Algemene wet bestuursrecht. De Algemene wet bestuursrecht is thans niet van toepassing op – kort gezegd – de operationele besluitvorming van de diensten en al hetgeen daarmee samenhangt; zie artikel 145 Wiv 2017. In het kader van de herziening van de Wiv 2017 zal nadrukkelijk worden onderzocht of en, zo ja, op welke wijze de Algemene wet bestuursrecht toch – waarschijnlijk met diverse uitzonderingen – toepassing kan vinden in het operationele domein van de diensten. Maar ook of voor het beroep op de Afdeling bestuursrechtspraak aansluiting kan worden gevonden bij de regeling van (hoger) beroep in de Algemene wet bestuursrecht. In de Hoofdlijnennotitie wordt daarop nader ingegaan. Het gaat ons echter te ver om dit te kwalificeren als een fundamentele herziening.

4.2 Bindend toezicht door de afdeling toezicht van de CTIVD

De leden van de D66-fractie vragen aan de regering om aan te geven of er sprake is van bindend toezicht door de CTIVD op bevoegdheden voor kabelinterceptie. Dat is niet het geval. Zoals deze leden hebben geconstateerd ontbreekt immers in artikel 12 van het wetsvoorstel, waarin het bindend toezicht door de afdeling toezicht is geregeld, de mogelijkheid om bindend toezicht uit te oefenen op de toepassing van artikel 6 van het wetsvoorstel en artikel 48 Wiv 2017. De reden daarvoor is, dat het bestaande toetsings- en toezichtsstelsel met betrekking tot de uitoefening van deze bevoegdheid zoals is neergelegd in de Wiv 2027 in essentie ongewijzigd blijft. Zowel voor de thans expliciet in artikel 6 van het wetsvoorstel geregelde bevoegdheid tot verkenning met het oog op OOG-interceptie als de interceptie ex artikel 48 Wiv 2017 voor het inlichtingenproces blijft immers een bindende TIB-toets ex ante van de door de Minister verleende toestemmingen vereist en kan de CTIVD op de uitvoering van die bevoegdheden niet bindend rechtmatigheidstoezicht uitoefenen.

De leden van de D66-fractie vragen of de regering een voorbeeldcasus kan geven waarin de TIB op basis van haar toetsing tot een onrechtmatigheidsoordeel kan komen van de door de Minister gegeven toestemming voor de inzet van verkenning op de kabel. In algemene zin kunnen wij het volgende erover opmerken. Een verzoek om toestemming voor het verkennen ten behoeve van OOG-interceptie wordt onderbouwd aan de hand van de eisen van noodzaak, proportionaliteit, subsidiariteit. Een op basis van een dergelijk verzoek verleende toestemming van de voor de dienst verantwoordelijke Minister wordt voor een rechtmatigheidsoordeel aan de TIB voorgelegd. Daarbij zal de TIB als onafhankelijke instantie toetsen of de Minister de toestemming rechtmatig heeft verleend. In het geval de TIB de onderbouwing op één of meerdere van de hiervoor genoemde eisen onvoldoende acht kan de TIB tot een onrechtmatigheidsoordeel komen. De TIB benoemt in haar openbare jaarverslagen ook de juridische gronden waarop verzoeken voor toestemmingen van de Minister voor OOG-interceptie in de verslagperiode onrechtmatig zijn geacht.

De leden van de D66-fractie wijzen erop dat in de Kamerbrief van 31 maart 2023[43] de Minister van Binnenlandse Zaken en Koninkrijksrelaties schrijft dat zij eraan hecht te benadrukken dat er geen enkele intentie is om de wijze waarop de TIB thans de proportionaliteitstoets uitvoert in te perken. Daarbij is aangegeven dat de aanpassing in de toelichting bij de beoordeling van technische risico's is doorgevoerd met als doel te verduidelijken waar (in de nieuwe systematiek) het domein van de TIB ophoudt en het domein van de CTIVD begint en voorts dat zodra zich een geschikte gelegenheid voordoet, zij dit in het kader van de parlementaire behandeling van het wetsvoorstel ook zal verduidelijken. Deze leden vragen of de regering die verduidelijking in de beantwoording van deze vragen kan geven? En, zo niet, of de regering dan kan aangeven wanneer uiterlijk deze verduidelijking kan worden verwacht. Wij antwoorden deze leden graag als volgt. De toetsing van de TIB ziet op de door de Minister verleende toestemming en voor zover het gaat om de technische risico's is deze dan ook beperkt tot de bekende technisch risico's. Deze *bekende* technische risico's kunnen dan ook door de TIB in de door haar uit te voeren proportionaliteitstoetsing worden betrokken. De afdeling toezicht houdt vervolgens toezicht op de uitvoering van de bevoegdheid en dus ook op de wijze waarop bekende en nieuwe technische risico's zich tijdens de uitvoering concreet voordoen. Daarmee verschuift de bindende ex ante toets voor andere risico's dan die welke op moment van toestemmingverlening bekend zijn naar de fase van dynamisch toezicht door de afdeling toezicht. Ingevolge artikel 12, eerste lid, onder b, van het wetsvoorstel is ook dat toezicht bindend voor zover dat betrekking heeft op de aan de uitoefening van de bevoegdheid verbonden technische risico's. Zoals in de brief aan de voorzitter van de TIB door ons is aangegeven, is er geen enkele intentie geweest om de wijze waarop de TIB de proportionaliteitstoets uitvoert in te perken, maar wel om via de toelichting duidelijk te maken dat waar het gaat om de beoordeling van de technische risico's in de nieuwe systematiek het domein van de TIB ophoudt en die van de afdeling toezicht van de CTIVD begint.[44] De leden van de SP-fractie vragen de regering of het verschuiven van delen van toetsing vooraf naar toezicht tijdens een operatie door de CTIVD een vermindering van administratieve lasten in zal houden. Deze leden zien een verschuiving van vooraf naar tijdens niet als een wijziging in waarop toezicht wordt gehouden en hoe de diensten hun inzet moeten verantwoorden en daarmee zien zij niet hoe dit de gewraakte bureaucratische last vermindert. Zij vragen of de regering kan uitleggen hoe dit zit. De Tijdelijke wet zorgt slechts in een beperkt aantal gevallen voor een verschuiving van een ex ante toets door de TIB naar bindend toezicht door de afdeling toezicht ex durante. Zoals we ook in de memorie van toelichting hebben uiteengezet past dit beter bij de dynamische aard van onderzoeken naar landen met een offensief cyberprogramma. De administratieve last die verbonden is aan het voorleggen van door de Minister verleende toestemmingen aan de TIB en het beantwoorden van de vragen die door de TIB worden gesteld komt met de verschuiving te vervallen. Dat levert evident minder administratieve lasten op. Na verleende toestemming door de Minister kan de uitvoering van de bevoegdheid direct plaatsvinden. De afdeling toezicht kan ex durante de rechtmatigheid daarvan monitoren en waar ze een onrechtmatigheid meent te constateren dit op uitvoeringsniveau aan de orde stellen en in overleg met de dienst tot een oplossing daarvoor komen.[45] Omdat de afdeling toezicht in het kader van haar toezichthoudende taak rechtstreeks toegang heeft tot de informatie bij de diensten kan zij in eerste instantie zelf de hiervoor benodigde informatie verza-

[43] Kamerstukken II 2022/2023, 36 263, nr. 6.
[44] Zie bijlage bij Kamerstukken II 2022/2023, 36 263, nr. 6.
[45] Pas als dit niet tot een oplossing leidt, komt het instrumentarium van een bindend oordeel met daarbij eventueel aangegeven welke gevolgen daaraan worden verbonden in beeld.

melen. De administratieve lasten zijn in dat geval dan ook naar verwachting lager dan bij een TIB-toets.

De leden van de SP-fractie vragen waarom de regering niet eerlijk aangeeft dat de CTIVD geen bindend toezicht krijgt op bulkinterceptie-operaties. Het lijkt ons dat uit het wetsvoorstel en de daarop gegeven toelichting blijkt dat de afdeling toezicht van de CTIVD ter zake geen bindend toezicht kan uitoefenen. Voor zover de vraag van deze leden erop ziet waarom dat niet zo is, verwijzen we naar ons antwoord op de vragen ter zake van de leden van de D66-fractie aan het begin van deze paragraaf.

De leden van de PvdA-fractie valt het op dat in artikel 12 van het wetsvoorstel, waarin de bindende toezichtsbevoegdheid van de afdeling toezicht is geregeld, staat dat indien de CTIVD van mening is dat er sprake is van onrechtmatigheid het de Minister «kan» informeren. Betekent dit, aldus deze leden, dat de CTIVD er ook voor kan kiezen om onrechtmatigheden niet te melden en in stand te laten. Voorts vragen zij wat dat betekent als een bevoegdheid onrechtmatig is gebruikt, op grond van welke overwegingen een onrechtmatigheid niet gemeld hoeft te worden en waarom de CTIVD onrechtmatigheden niet moet melden. In antwoord op deze set met elkaar samenhangende vragen, merken wij het volgende op. Het klopt dat ingeval de afdeling toezicht een (vermeende) onrechtmatigheid bespeurt, die niet verplicht hoeft te melden aan de voor de dienst verantwoordelijke Minister. Dat is niet zo vreemd. Toezichthouders hebben immers over het algemeen een zekere vrijheid bij de uitvoering van de hen opgedragen toezichthoudende taak en kunnen daar – binnen de grenzen die de wetgever stelt – ook een eigen beleid in ontwikkelen. Dat is bij het rechtmatigheidstoezicht in het kader van de toepassing van de Wiv 2017 en de Wet veiligheidsonderzoeken niet anders. Zoals ook in de artikelsgewijze toelichting op artikel 12 is aangegeven, zal in de praktijk naar verwachting pas tot een mededeling aan de Minister van een geconstateerde onrechtmatigheid komen indien niet in de reguliere contacten tussen de toezichthouder en de diensten op werkniveau een geconstateerde onrechtmatigheid kan worden weggenomen.[46] Daar komt bij dat er onrechtmatigheden in gradaties kunnen optreden en het zou te ver voeren indien reeds een kleine overtreding van een regel door de AIVD of de MIVD al tot een mededeling als bedoeld in artikel 12, eerste lid, van de wet zou moeten leiden. Toepassing van artikel 12, eerste lid, brengt immers ook een hele procedure op gang: eerst voorlopig oordeel uitbrengen, al dan niet met vermelding van de daaraan te verbinden gevolgen, reactie van de Minister, vaststellen definitief oordeel en de daaraan te verbinden gevolgen en – mogelijk – ook nog een gang naar de Afdeling bestuursrechtspraak. Deze procedure, waarbij ook veel beslag wordt gelegd op de capaciteit van de toezichthouder als de diensten, moet naar ons oordeel gereserveerd blijven voor onrechtmatigheden die enige substantie hebben; uiteraard ter beoordeling aan de afdeling toezicht.

De leden van de GroenLinks-fractie lezen dat het toezicht enigszins verschuift van de TIB naar de CTIVD. Om deze verschuiving ten opzichte van de huidige wet beter te kunnen begrijpen vragen deze leden de regering om ten aanzien van deze aanpassingen binnen het toezicht een concreet (fictief) voorbeeld te beschrijven zoals het toezicht nu verloopt, waar de concrete knelpunten in de praktijk worden ervaren en hoe in hetzelfde (fictieve) voorbeeld het toezicht onder de voorliggende wet zal verlopen en op welke wijze hierbij de in de praktijk ervaren knelpunten worden opgelost.
Een van de terreinen waarop is beoogd een verschuiving van toezicht te realiseren is op het gebied van de beschrijving van technische risico's die

[46] Kamerstukken II 2022/2023, 36 263, nr. 3, p. 61.

gepaard gaan met de inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk. Op dit moment is er een spanningsveld ontstaan tussen de dynamiek van de uitvoering van de bevoegdheid tot binnendringen in een geautomatiseerd werk en de statische ex ante toetsing van de TIB voorafgaand aan de inzet van deze bevoegdheid. Er worden door de TIB eisen gesteld aan de voorafgaande beschrijving van de technische risico's waar de diensten niet aan kunnen voldoen. Hierdoor hebben de diensten operaties niet kunnen uitvoeren of kunnen voortzetten. Voorafgaand aan een toestemmingsperiode van drie maanden is het niet mogelijk om te voorspellen welke handelingen precies nodig zullen zijn om het met de inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk beoogde doel te bereiken. Ook is vooraf vaak nog onbekend binnen welke context zal moeten worden geopereerd, bijvoorbeeld of er sprake is van een target dat veiligheidsbewust is en maatregelen neemt waarmee de diensten bij de uitvoering van de bevoegdheid rekening moeten houden teneinde risico's te beperken dan wel te mitigeren. Doordat zowel de benodigde handelingen als de context vooraf niet of slechts zeer beperkt vooraf bekend zijn, is het niet mogelijk op basis daarvan de technische risico's concreet te omschrijven in een verzoek om toestemming. Voornoemde beperkingen brengen met zich mee dat de omschrijving van de technische risico's voorafgaand aan de inzet van de bevoegdheid een beperkte waarborgfunctie toekomt. Tot deze conclusie kwamen zowel de CTIVD als de Evaluatiecommissie van de Wiv 2017 al eerder. De beschrijving zal beperkt moeten blijven tot hetgeen op het moment van schrijven van het verzoek om toestemming bekend is, en zal geen (technische) details kunnen bevatten, maar op een passend abstract niveau moeten worden geformuleerd. Een ander concreet knelpunt komt voort uit de invulling van de rechtmatigheidstoets door de TIB op het gebied van de technische risico's. Reeds eerder is in de parlementaire behandeling van de Wiv 2017 aangegeven dat het niet de taak is van de TIB om de risico's van grootschalige, abstract aangeduide en technisch complexe operaties in te schatten. Een dergelijke inschatting behoort tot de operationele verantwoordelijkheid van de diensten en de daarvoor verantwoordelijke Ministers. In de praktijk zal deze inschatting aan de orde komen bij de vraag of de bijzondere bevoegdheid voor uitoefening in aanmerking komt gelet op de operationele, veiligheidsrisico's die daaraan verbonden zijn; dat is een andere afweging dan die waarvoor de TIB zich gesteld ziet, die immers de rechtmatigheid toetst indien – naar aanleiding van de hiervoor geschetste afweging – tot de uitoefening van een bijzondere bevoegdheid is besloten.[47] Concreet betekent dit, dat de Ministers zullen moeten worden voorzien van informatie zodat zij in staat worden gesteld om de ingeschatte risico's mee te wegen. De TIB toetst vervolgens of de betrokken Minister op basis van de gegeven inschatting en het laten meewegen daarvan in het kader van de proportionaliteit op rechtmatige wijze tot het geven van toestemming heeft kunnen komen. De voornoemde invulling van de rechtmatigheidstoets en de beperkte waarborgfunctie van de vooraf te geven beschrijving van de technische risico's brengen met zich mee dat het uitoefenen van toezicht op de inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk en de inschatting van en de omgang met de technische risico's beter past bij een ex durante toets.

De leden van de PvdD-fractie lezen dat bij de constatering van een onrechtmatigheid er – op grond van artikel 12, tweede lid – twee opties bestaan, namelijk beëindiging van de desbetreffende bevoegdheid en/of de verwijdering en vernietiging van de bij de uitvoering daarvan verwerkte gegevens. Zij hebben hier enkele vragen over. Allereerst of de aanname klopt dat het alleen om verwerkte gegevens gaat en – aldus deze

[47] Eerste Kamer, vergaderjaar 2016–2017. 34 588, E, p.5

leden – bulkdata buiten beschouwing blijft. Naar wij aannemen is deze vraag ingegeven door hetgeen in de artikelsgewijze toelichting is gesteld met betrekking tot het bindend toezicht op GDA op OOG-metadata, namelijk dat de verwijdering en vernietiging niet ziet op de in de GDA betrokken gegevens maar uitsluitend op de uit de toegepaste GDA-methodiek voortvloeiende gegevens (de resultaten).[48]Die aanname is juist. De bulkdata die bij GDA op OOG-metadata worden betrokken, zijn allereerst de metadata verkregen via een rechtmatig bevonden OOG-interceptie ex artikel 48 Wiv 2017 en voorts de bulkdatasets die door toepassing van andere aan de dienst toekomende bevoegdheden (algemeen en bijzonder, dan wel via verkrijging van een collegadienst) zijn verworven. Het bindend toezicht heeft geen betrekking op de verwerving van die bulkdatasets. Het bindend toezicht heeft uitsluitend betrekking op de toegepaste methodiek van GDA. Is die methodiek (bevoegdheid) onrechtmatig bevonden en heeft de afdeling toezicht daaraan het gevolg verbonden dat die bevoegdheid dient te worden beëindigd, dan kan het daaraan te koppelen gevolg – namelijk de verwijdering en vernietiging van bij de uitvoering verwerkte gegevens – alleen betrekking hebben op de gegevens die door toepassing van de betreffende GDA zijn gegenereerd; dus niet op de daarbij gebruikte bulkdatasets. Artikel 50, vierde lid, Wiv 2017 waarop het bindend toezicht binnen de reikwijdte van het wetsvoorstel betrekking heeft ziet immers uitsluitend op het verkrijgen van toestemming van de Minister voor de *toepassing* van een nader aan te duiden vorm van GDA met een aanduiding van de daarbij te betrekken bulkdatasets (gegevensbestanden). Het bindend toezicht komt hier in de plaats van de ex ante bindende toets door de TIB, welke zich bij haar toetsing ook tot het object van toestemming – namelijk het mogen toepassen van GDA – dient te beperken. De leden van de fractie van de PvdD-fractie vragen voorts wat dit betekent voor data die mogelijk al met buitenlandse diensten is gedeeld. Het antwoord op deze vraag luidt dat het geen betekenis heeft. Immers, dat valt niet onder de reikwijdte van het bindend toezicht in artikel 12 van het wetsvoorstel. Op de verstrekking door de AIVD en MIVD van gegevens, al dan niet in de vorm van bulkdata, geldt het reguliere rechtmatigheidstoezicht door de afdeling toezicht op grond van de Wiv 2017. Dat toezicht is beperkt tot wat onder Nederlandse jurisdictie valt en dus niet op de (verdere) verwerking van de ontvangen bulkdatasets door de desbetreffende buitenlandse diensten. Immers omgekeerd geldt hetzelfde: buitenlandse toezichthouders hebben ook geen jurisdictie met betrekking tot de verwerking van bulkdatasets door de AIVD of MIVD die deze van een dienst van het land waarin de desbetreffende toezichthouder jurisdictie heeft, heeft verkregen.

De leden van de SGP-fractie vragen waarom het wetsvoorstel slechts facultatief regelt dat de afdeling toezicht een oordeel over onrechtmatigheid kan melden aan de Minister. Waarom, aldus deze leden, zou in situaties van onrechtmatigheid niet een verplichting tot melden moeten gelden. Voor het antwoord op deze vraag verwijzen we deze leden naar ons antwoord op een vergelijkbare vraag van de leden van de fractie van de PvdA. Waar het gaat om hun vraag hoe het contrast te verklaren is met de regeling voor de TIB, die bepaalt dat deze terstond het oordeel dient te melden dat de toestemming ten onrechte is verleend, merken we het volgende op. Wij nemen aan dat deze leden met hun vraag doelen op het bepaalde in artikel 3, eerste lid, van het wetsvoorstel, waarbij de TIB met betrekking tot de aan haar voorgelegde toestemming haar oordeel dat met betrekking tot die toestemming ten onrechte is bepaald *dat daarmee uitvoering wordt gegeven aan de Tijdelijke wet*, terstond mededeling dient te doen aan de desbetreffende Minister. Allereerst ziet het hier bedoelde oordeel van de TIB niet op de toestemmingverlening als zodanig maar op

[48] Kamerstukken II 2022/2023, 36 263, nr. 3, p. 61–62.

het feit dat in dat kader tevens is bepaald dat de Tijdelijke wet van toepassing is (zie ook artikel 2, derde lid). Aan dat oordeel verbindt de wet het rechtsgevolg dat de Tijdelijke wet niet van toepassing is en de TIB bij de door haar uit te voeren rechtmatigheidstoets het bepaalde in de Tijdelijke wet buiten toepassing laat. Indien vervolgens de verleende toestemming door de TIB rechtmatig wordt geoordeeld kan de dienst de betreffende bevoegdheid uitsluitend uitvoeren overeenkomstig het bepaalde in de Wiv 2017 en derhalve zonder toepassing van de in de Tijdelijke wet voorziene aanvullingen en afwijkingen ten opzichte van de Wiv 2017. Dat werkt direct door in de mogelijkheden van de dienst bij het verrichten van onderzoek. Gelet op het feit dat de TIB belast is met een bindende *ex ante* toets, waarbij een rechtmatigheidsoordeel voorwaardelijk is voor het kunnen toepassen van een bevoegdheid, is het voor de dienst van belang dat ze terstond wordt geïnformeerd door de TIB indien deze de Tijdelijke wet niet van toepassing acht opdat – indien de Minister dat aangewezen acht – tegen het oordeel van de TIB beroep bij de Afdeling bestuursrechtspraak kan worden ingesteld. Het is immers van het grootste belang dat zo snel mogelijk duidelijkheid komt over de toepasselijkheid van de Tijdelijke wet en daarmee het toepasselijke wettelijke kader waarbinnen de diensten hun onderzoek en bevoegdheden kunnen uitoefenen. Dat is ook van belang voor toezicht door de afdeling toezicht die immers ook duidelijkheid moet hebben of de regeling inzake het bindend toezicht zoals voorzien in de Tijdelijke wet van toepassing is.

De leden van de Volt-fractie merken op dat het bindend toezicht – zoals bedoeld in de Tijdelijke wet – een grote verandering is ten opzichte van de huidige toezichtspraktijk. In beginsel zijn deze leden van mening dat het toezicht vooraf beter is, voor zover het mogelijk is om effectief toezicht te houden vooraf. Door het weghalen van het toezicht vooraf ontstaat, aldus deze leden, de situatie waarin mogelijk gegevens worden verzameld of praktijken worden uitgehaald die niet rechtmatig zijn. Dat kun je volgens deze leden dan stopzetten en/of laten verwijderen, maar dan is het kwaad al geschied. Deze leden vragen of de regering van mening is dat het toezicht met deze wet zo is ingericht dat de diensten daadwerkelijk en onverwijld gestopt kunnen worden door de toezichthouder als de toezichthouder van oordeel is dat de bevoegdheid onrechtmatig, ondoelmatig of buitenproportioneel wordt ingezet. Allereerst zouden wij willen opmerken dat de ex ante toets door de TIB – wat deze leden aanduiden als toezicht vooraf – in het kader van de Tijdelijke wet op een zeer beperkt aantal gevallen komt te vervallen en wordt vervangen door de mogelijkheid van bindend toezicht op de uitoefening van de desbetreffende bevoegdheden door de diensten door de afdeling toezicht van de CTIVD (toezicht ex durante).[49] Dat bindend toezicht is rechtmatigheidstoezicht, waarvan proportionaliteit een onderdeel vormt. Ondoelmatigheid maakt geen onderdeel uit van de rechtmatigheidstoets en daarop ziet de afdeling toezicht dan ook niet toe. De uitoefening van het bindend toezicht door de afdeling toezicht dient op zorgvuldige wijze plaats te vinden gelet op de effecten die het kan hebben op de taakuitvoering van de diensten. Vandaar dat in artikel 12 van het wetsvoorstel is opgenomen dat indien de afdeling toezicht tot het voorlopige oordeel komt dat de toepassing door de diensten van de in artikel 12, eerste lid, bevoegdheden, onrechtmatig is, deze – met de gevolgen die de afdeling daaraan wil verbinden – aan de

[49] De TIB heeft in haar reactie op het concept-voorstel van een Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma aangegeven dat waar het gaat om het scannen (lees: verkennen) van geautomatiseerde werken de TIB zich kan vinden in deze wijziging, gelet op de zeer beperkte inbreuk die het scannen oplevert, en waar het gaat om de verschuiving van de ex ante toets door de TIB naar bindend toezicht door de afdeling toezicht acht zij deze verdedigbaar, gelet op de aard van de bevoegdheid die meer het karakter heeft van verdere verwerking van gegevens.

verantwoordelijke Minister kan worden medegedeeld. De Minister wordt daarmee in de gelegenheid gesteld om daarop binnen een korte termijn van drie dagen te reageren, waarna de afdeling toezicht het oordeel en de daaraan te verbinden gevolgen definitief kan vaststellen. Binnen drie dagen na ontvangst van het vastgestelde oordeel dient de Minister daaraan uitvoering te geven. Tegen het oordeel staat beroep open bij de Afdeling bestuursrechtspraak, maar dat beroep heeft geen schorsende werking. Wel kan een voorlopige voorziening worden aangevraagd. Kort en goed: het bindend toezicht heeft als effect dat er daadwerkelijk bij onrechtmatig handelen van de diensten kan worden ingegrepen en dat onrechtmatig handelen dus kan worden gestopt, maar dat dit vanwege de zorgvuldigheid van de besluitvorming ter zake niet onverwijld kan plaatsvinden.

Deze leden vragen ten slotte of de regering in het kader van het vorige punt concrete informatie heeft over hoeveel tijd de wijziging zal besparen en of de regering kan aangeven hoeveel tijd er nu, zonder Tijdelijke wet, wordt verloren. De voorgestelde wijzigingen beogen dat bijzondere bevoegdheden effectiever kunnen worden ingezet, zodat de noodzakelijke snelheid en wendbaarheid in het cyberdomein wordt bewerkstelligd. Zo wordt die snelheid en wendbaarheid onder meer gehaald met de voorgestelde maatregelen met betrekking tot de bijschrijfmogelijkheden, nu die ertoe leiden dat – anders dan thans het geval is – niet telkens eerst een toestemmingstraject met toets door de TIB dient te worden afgelegd. Het stelsel van toets en toezicht moet daarop aansluiten. Met de voorgestelde wijzigingen in het stelsel van toetsing en toezicht gaat het niet primair om de vraag of daarmee effectiviteitswinst wordt behaald, maar om de voorgestelde tijdelijke voorzieningen in aanvulling op dan wel in afwijking van de Wiv 2017 met adequate waarborgen te omgeven. Zoals eerder in deze nota naar aanleiding van het verslag is aangegeven zal bij de verschuiving van bepaalde onderdelen van de fase van ex ante toets naar die van ex durante er aan de voorkant sprake zijn van minder administratieve lasten. Hier staat tegenover dat er een toename van administratieve lasten zal zijn vanwege de toenemende rol van de CTIVD in het kader van de uitvoering van dynamisch en bindend toezicht.

4.3 Beroep op de Afdeling bestuursrechtspraak

De leden van de D66-fractie vragen waarom niet is gekozen voor de mogelijkheid om een prejudiciële vraag te stellen aan de Afdeling bestuursrechtspraak in plaats van een volledige rechtsgang bij de Afdeling bestuursrechtspraak. Ook vragen zij welke voor- en nadelen de regering daarbij in overweging heeft genomen. Meer specifiek vragen deze leden waarom het stellen van prejudiciële vragen niet afdoende is als de weeffout – volgens de memorie van toelichting – vooral in de uitleg van begrippen, criteria en de wijze waarop toezichthouders daaraan toetsen, ligt. Zoals in de memorie van toelichting reeds is aangegeven, zijn in het kader van de ex ante toets door de TIB de afgelopen jaren meermaals soms fundamentele verschillen van inzicht ontstaan over de uitleg en reikwijdte van wettelijke begrippen maar ook over de wijze waarop de vereisten van noodzaak, proportionaliteit, subsidiariteit en gerichtheid in de aanvragen moeten worden beschreven. Op dit moment heeft de TIB hierin het laatste woord en is niet voorzien in een vorm van (rechterlijk) beroep. De ECW ziet dit als een weeffout in het stelsel van toezicht[50]. De uitleg van wettelijke begrippen, de invulling van toetsingsnormen en de intensiteit van de toetsing is bij uitstek een rechterlijke taak. Wij hebben dit standpunt in onze (eerste) reactie op het rapport van de

[50] Zie paragraaf 9.5 van het rapport van de ECW.

ECW onderschreven en geven daaraan in dit wetsvoorstel (reeds) uitwerking.

Waar het gaat om de prejudiciële procedure merken we het volgende op. Een prejudiciële procedure bestaat thans alleen in het civiele recht en wat het bestuursrecht betreft alleen in het belastingrecht.[51] Kern van de prejudiciële procedure is – kort gezegd – het in een rechterlijke procedure versneld verkrijgen van een finaal rechterlijk standpunt van de hoogste rechter over een rechtsvraag die vervolgens in zaken waarin dezelfde rechtsvraag speelt, toegepast kan worden. Het belangrijkste bezwaar tegen de invoering van een prejudiciële procedure in het Wiv-domein is het gegeven dat in een prejudiciële procedure een lagere *rechter* in een bij hem aanhangige zaak een oordeel kan vragen aan de hoogste rechter. Zowel de Minister als de TIB en de CTIVD zijn geen rechterlijke instanties en kunnen om deze reden dus geen prejudiciële vragen stellen. Het inrichten van een prejudiciële procedure zou dus een herbezinning vergen van bestaande taken, bevoegdheden en positionering van de betrokken partijen alsmede de beroepsgang en daarmee feitelijk van het gehele stelsel van toetsing en toezicht en de inrichting van de rechtsbescherming. Dat gaat het bestek van dit wetsvoorstel te buiten. Met een prejudiciële procedure kunnen parallelle procedures bij meerdere instanties met vergelijkbare rechtsvragen worden voorkomen. Daarmee wordt rechtsongelijkheid beperkt en rechtseenheid bevorderd. In de procedures op grond van dit wetsvoorstel spelen deze argumenten geen rol. Er is geen sprake van een procedure in meerdere instanties en het aantal procespartijen is zeer beperkt: het betreft twee Ministers en de TIB en CTIVD. Dit is wezenlijk anders in het algemene bestuursrecht en het civiele recht waar zaken in beginsel bij elke rechtbank en bij elke rechter aangebracht kunnen worden en waar de mogelijkheid op verschillende uitkomsten in vergelijkbare zaken groter is. Al deze aspecten, leiden tot de conclusie dat de thans voorgestelde beroepsprocedure het best aansluit bij de wens om te voorzien in een vorm van een rechterlijke toets waar het gaat om de oordelen die in het kader van het bindend toezicht door de afdeling toezicht van de CTIVD tot stand komen en de oordelen van de TIB op grond van dit wetsvoorstel zonder dat hiervoor fundamentele wijzigingen in de aard en de positie van de betrokken organisaties nodig zijn. Bij de herziening van de Wiv 2017 zal het gehele stelsel van toetsing en toezicht opnieuw bezien worden. Daarbij zullen ook de ervaringen die worden opgedaan bij de toepassing van de beroepsprocedure worden betrokken.

De leden van de D66-fractie vragen tot slot ook in te gaan op de uitspraak dat het voorstel een beperkte rechtsstatelijke betekenis heeft, nu de burger dezelfde rechtsgang niet kan bewandelen. Hoewel het beroep in de regel zal gaan om de uitoefening van bevoegdheden die een inbreuk maken op de persoonlijke levenssfeer van burgers, is de burger geen (proces)partij. Vanwege het staatsgeheime karakter van de werkzaamheden van de diensten, zullen burgers ook niet op de hoogte zijn van het feit dat zij (mogelijk) onderwerp zijn van onderzoek. De beroepsprocedure voorziet primair in de wens om relatief snel een finaal rechterlijk oordeel te krijgen over bepaalde bindende oordelen van de TIB en de CTIVD en beoogt geen (aanvullende) vorm van rechtsbescherming te bieden. Wel bestaat op grond van de Wiv 2017 voor de burger de mogelijkheid om een klacht in te dienen bij de afdeling klachtbehandeling van de CTIVD die is belast met het onderzoeken en beoordelen van klachten en van meldingen van vermoedens van misstanden. De afdeling klachtbehandeling is een

[51] Wel heeft de bestuursrechter op grond van de Tijdelijke wet Groningen de mogelijkheid tot het stellen van prejudiciële vragen aan de Afdeling bestuursrechtspraak of de Hoge Raad. Hiervan is tot op heden geen gebruik gemaakt.

onafhankelijke en zelfstandige klachtinstantie die diepgaand onderzoek kan doen en bindende oordelen kan geven.

De leden van de CDA-fractie vragen of de regering het eens is met prof. mr. P.P.T. Bovend'Eert dat een procedure in twee instanties de positie van de TIB in het stelsel van toezicht aanzienlijk zou verzwakken. Ook vragen zij hoe de regering de suggestie beoordeelt om bij een verschil van inzicht met de TIB een prejudiciële vraag voor te leggen aan de Afdeling bestuursrechtspraak, die deze vraag dan bindend beantwoordt. Wij merken hier het volgende over op. In het stelsel dat prof. Bovend'Eert c.s. heeft voorgesteld wordt de TIB als een rechterlijke instantie gepositioneerd en is met de mogelijkheid van beroep van de Afdeling bestuursrechtspraak derhalve sprake van een procedure in twee instanties. De TIB is echter geen rechterlijke instantie en dus van een procedure in twee instantie is in dat opzicht geen sprake. Ook zien we niet in dat de beroepsprocedure als zodanig gevolgen heeft voor de positie van de TIB. De TIB kan nog steeds bindend oordelen en een onrechtmatigheidsoordeel betekent nog steeds dat de bevoegdheid niet kan worden uitgeoefend of voortgezet. Het beroep heeft immers geen schorsende werking. Het beroep voorziet in een thans ontbrekende vorm van geschillenbeslechting waarin de rechter het laatste woord krijgt bij verschillen van inzicht tussen de Ministers en de TIB of de CTIVD. Onafhankelijke rechterlijke geschillenbeslechting is een belangrijk kenmerk van een democratische rechtsstaat en doet op geen enkele wijze afbreuk aan de positie van de betrokken partijen.

Zoals hiervoor aangegeven in antwoord op de vraag van de leden van de D66-fractie, is een prejudiciële procedure niet mogelijk omdat in de procedures op grond van de Wiv 2017 (in samenhang met de Tijdelijke wet) de rechter geen rol heeft. Het inrichten van een prejudiciële procedure zou een herbezinning vergen van het gehele stelsel van toetsing en toezicht en dat gaat het bestek van dit wetsvoorstel te buiten. Tot slot is het aantal betrokken partijen minimaal waardoor de bevordering van de rechtseenheid, een belangrijk kenmerk van een prejudiciële procedure, geen rol speelt.

De leden van de SP-fractie vragen of bij een beroep van de diensten bij een afwijzing door de TIB opnieuw alle informatie die hoort bij een operatie moet worden overlegd aan de Afdeling bestuursrechtspraak van de Raad van State en hoe in deze procedure het staatsgeheime karakter van de informatie die wordt gedeeld wordt gewaarborgd. Bij de indiening van het beroepsschrift worden alle relevante gegevens (vertrouwelijk) aan de Afdeling bestuursrechtspraak verstrekt. De betreffende Minister bepaalt als indiener van het beroepsschrift in eerste instantie welke gegevens dit zijn. De TIB ontvangt een afschrift van deze stukken en kan bij indiening van het verweerschrift eventuele aanvullende gegevens verstrekken. Daarnaast kan ook de Afdeling beide partijen verzoeken om aanvullende gegevens te verstrekken. Op deze manier wordt gewaarborgd dat alle relevante gegevens onderdeel uitmaken van het dossier. Om het staatsgeheime karakter van de gegevens te waarborgen, zullen technische en organisatorische maatregelen worden getroffen. Overigens heeft de Afdeling bestuursrechtspraak reeds ervaring met AIVD- en MIVD-gerelateerde zaken en de omgang met staatsgeheime informatie die daaraan inherent verbonden is. Dit is een belangrijk argument om de Afdeling bestuursrechtspraak te belasten met de geschillenbeslechting zoals thans voorgesteld.

Ook vragen de leden van de SP-fractie of de met het beroep beoogde helderheid over afwegingskaders voor de inzet van bevoegdheden niet uit de wet en de bedoeling van de wetgever zou moeten volgen. De Wiv 2017

schept de kaders waarbinnen de diensten opereren waarbij de documenten uit de wetsgeschiedenis, zoals de in het kader van de parlementaire behandeling gewisselde stukken en de memorie van toelichting in het bijzonder, behulpzaam kunnen zijn bij eventuele interpretatiekwesties. Deze documenten moeten immers beschouwd worden als standpunt van de wetgever ten tijde van de totstandkoming. De wetgever kan op onderdelen van het wetsvoorstel in deze stukken voorzien in uitleg, context en duiding of deze juist open laten. Als de invulling of concretisering niet rechtstreeks uit de wet valt af te leiden en de wetsgeschiedenis geen aanknopingspunten biedt, wordt de concrete invulling overgelaten aan de praktijk. Daarbij kunnen (juridische) verschillen van inzicht ontstaan waarbij het gebruikelijk is om de rechter daarin het laatste woord te geven. De rechter zal dan uiteindelijk via zijn uitleg zelf de wet (nader) concretiseren, aanvullen of verfijnen alvorens hij deze kan toepassen. Dit proces van rechtsvorming waarborgt ook dat de rechter kan meebewegen met toekomstige ontwikkelingen. De wetgever kan immers niet alle toekomstige situaties overzien, laat staan regelen.

De leden van de SP-fractie geven aan het niet alleen een rare maar ook onwenselijke figuur te vinden dat de Raad van State uitspraken kan doen in een soort «hoger beroep» inzake een afwijzing. Hiermee zou, aldus deze leden, de regering het doen voorkomen dat de TIB onzorgvuldig te werk zou gaan. Zij vragen welke aanwijzingen de regering daarvoor heeft en of de TIB volgens de regering teveel verzoeken afwijst. Ook vragen zij welk percentage afwijzingen de regering wenselijk zou vinden. Wij zijn niet van opvatting dat de TIB onzorgvuldig te werk gaat. Zoals de ECW heeft aangegeven kent het huidige stelsel van toetsing en toezicht een weeffout. Momenteel hebben de toezichthouders niet alleen het laatste woord in een concrete casus, maar ook wat betreft de uitleg van begrippen en criteria, en de wijze waarop zij hieraan toetsen. Dat heeft in de afgelopen jaren verschillende malen tot knelpunten geleid. In de context van onderzoeken naar landen met een offensief cyberprogramma heeft dat geleid tot knelpunten aangaande de inzet van met name de bijzondere bevoegdheden ex artikel 45 (bevoegdheid tot binnendringen in een geautomatiseerd werk) en 48 (OOG-interceptie) van de Wiv 2017. Daarom regelt dit wetsvoorstel een beroepsprocedure bij de Afdeling bestuursrechtspraak van de Raad van State (artikel 13). Zo kan tot een gezaghebbende en eenduidige wetsuitleg worden gekomen. Er is voorts geen aanleiding te veronderstellen dat de TIB te veel verzoeken afwijst. Uit het meest recente jaarverslag van de TIB blijkt dat de TIB in 2022 in 2,3% van de gevallen een onrechtmatigheidsbeslissing heeft genomen. Er kunnen echter geen conclusies verbonden worden aan aantallen of percentages. Een onrechtmatigheidsoordeel kan immers tot gevolg hebben dat onderzoeken niet kunnen worden opgestart, niet kunnen worden voortgezet of zelfs dat bepaalde toestemmingen helemaal niet meer aangevraagd worden. Juist in die gevallen heeft de beroepsprocedure toegevoegde waarde.

De leden van de SP-fractie vinden het logisch dat bij een geschil over de uitleg van de wet en de bevoegdheden van de diensten juist de Minister of regering een oordeel velt en vragen waarom niet voor die werkwijze is gekozen in plaats van de Afdeling bestuursrechtspraak partij te maken. Vooropgesteld wordt dat bij een geschil over de uitleg van de wet de verantwoordelijke Minister altijd eerst in overleg zal treden met de TIB of de CTIVD zoals dat nu ook gebruikelijk is. Echter bij het geschil dat ontstaat over de uitleg van de wet is de Minister, immers als verantwoordelijke voor een van de diensten, ook partij en de wetgever heeft er niet in voorzien dat de Minister in die gevallen dan de uitleg van de wet vaststelt. Dat doet in de praktijk de TIB (of de CTIVD) en, zoals de ECW ook heeft geconcludeerd en de praktijk uitwijst, leidt dit tot impasses met gevolgen

voor de taakuitvoering door de diensten en daarmee voor de nationale veiligheid. Om die impasses te doorbreken is beroep op – in casu – de Afdeling bestuursrechtspraak aangewezen. Daarmee wordt, zoals de ECW aangeeft, een weeffout in de Wiv 2017 hersteld. Zoals hiervoor aangegeven in antwoord op de vraag van de leden van de CDA-fractie is het een belangrijk rechtstatelijk beginsel dat een uiteindelijk oordeel over de uitleg of toepassing van de wet is voorbehouden aan de onafhankelijke rechter. Dit laat onverlet dat de Minister altijd het initiatief kan nemen om de wet te wijzigen om (meer) duidelijkheid te creëren. Echter, voor de dynamische operationele praktijk van de diensten is een langdurig wetgevingsproces vaak niet de meest gewenste oplossing.

De leden van de SP-fractie vragen ook een uitgebreide toelichting over welke kennis en expertise de Afdeling bestuursrechtspraak bezit op het gebied van cyberoperaties van derde landen. Wij willen deze leden allereerst verwijzen naar ons antwoord op de vraag van de leden van de PvdA-fractie naar de bij de Afdeling bestuursrechtspraak aanwezige kennis en vaardigheden voor de aan haar opgedragen taak (zie paragraaf 4.1 van deze nota naar aanleiding van het verslag). In aanvulling daarop merken wij nog het volgende op. De Afdeling bestuursrechtspraak zal naar verwachting vooral oordelen over de toepassing van de wet en de uitleg van wettelijke begrippen. Dit gebeurt weliswaar in de context van inlichtingenonderzoeken naar landen met een offensief cyberprogramma, maar specifieke kennis en expertise van de cyberoperaties van de desbetreffende landen is daarvoor niet (altijd) noodzakelijk. De beroepsregeling voorziet overigens in de mogelijkheid om externe deskundigen te benoemen en een persoon als deskundig lid toe te voegen aan de meervoudige kamer die het beroep behandelt. Op deze wijze kan de Afdeling beschikken over alle kennis en expertise die zij nodig acht voor de behandeling van de zaak.

De leden vragen tevens naar wat is besproken tijdens het vooroverleg met de voorzitter van de Afdeling bestuursrechtspraak over dit wetsvoorstel, welke randvoorwaarden zijn afgestemd, welke toezeggingen zijn gedaan en met welke argumenten de regering een beroep heeft gedaan op de Raad van State voor deze rol in operaties van de geheime diensten. Zoals aangegeven in de beantwoording van de Kamervragen van het lid Leijten[52] heeft in de voorbereidende fase overleg plaatsgevonden met de voorzitter van de Afdeling bestuursrechtspraak omdat in het voorstel voor de Tijdelijke wet een nieuwe beroepsprocedure bij de Afdeling bestuursrechtspraak wordt geïntroduceerd. Daarbij is het (destijds meest recente) concept van de beroepsregeling besproken en toegelicht waarbij de Afdeling bestuursrechtspraak (procesrechtelijke) suggesties heeft gedaan voor aanvulling of verduidelijking. Ook is in algemene zin gesproken over de eventuele financiële en organisatorische gevolgen. Met uitzondering van enkele procedurele afspraken over het vervolgproces zijn geen toezeggingen gedaan.

Tot slot vragen deze leden te reageren op de analyse van de commissie Bovend'Eert over het externe toezicht en zij vragen waarom de regering wél tot het oordeel komt dat de huidige vormgeving voldoet aan de vereisten van de Europese rechtspraak. Wij merken ter zake het volgende op. In hun advies concluderen de hoogleraren Bovend'Eert, Lawson en Winter dat de huidige inrichting van het stelsel van toezicht in de Wiv 2017 in het algemeen voldoet aan de vereisten in de rechtspraak van het EHRM. Hoewel er geen dwingendrechtelijke aanleiding voor is, zien zij wel aanleiding om op onderdelen tot aanpassingen te komen. Het advies en de daaraan verbonden aanbevelingen zullen tezamen met de aange-

[52] Aanhangsel Handelingen 2022/2023, nr. 1185.

nomen moties over toetsing en toezicht worden betrokken bij de herziening van de Wiv 2017. Zie ook hetgeen is gesteld in de Hoofdlijnennotitie.

De leden van de ChristenUnie-fractie vragen de regering of er bij de totstandkoming van de Wiv 2017 of daarna is gesproken over de introductie van een dergelijke beroepsmogelijkheid of op een ander moment is overwogen deze te introduceren. Indien het antwoord bevestigend is, vragen deze leden in te gaan op de overwegingen waarom daarvan is afgezien en het moment waarop de behoefte ontstond om een dergelijke beroepsmogelijkheid in het leven te roepen. Bij de totstandkoming van de Wiv 2017 is – voor zover kon worden nagegaan – de introductie van de mogelijkheid van beroep tegen de bindende oordelen van de TIB bij de Afdeling bestuursrechtspraak niet aan de orde geweest. Dat was blijkbaar geen issue en er zijn dan ook geen bijzondere overwegingen te geven waarom daarvan is afgezien. Pas na de totstandkoming van de Wiv 2017 is gelet op de opgedane ervaringen met de TIB-toets de wenselijkheid van beroep tegen de bindende oordelen van de TIB manifest geworden. De ECW staat daar in het rapport ook bij stil.

Ook vragen deze leden hoe vaak de afgelopen jaren gebruik zou zijn gemaakt van het instrument als dat reeds had bestaan. Het is onmogelijk aan te geven hoe vaak gebruik zou zijn gemaakt van de beroepsmogelijkheid als deze zou hebben bestaan onder de Wiv 2017. In algemene termen valt wel op te merken dat de ECW een aantal fundamentele verschillen van interpretatie heeft onderkend. Bij dergelijke gevallen van uiteenlopende interpretaties zou tussenkomst van de Afdeling bestuursrechtspraak uitkomst hebben kunnen bieden. De verwachting is dan ook dat de beroepsmogelijkheid met name zal baten in geval van dergelijke specifieke fundamentele interpretatieverschillen.

De leden van de ChristenUnie-fractie constateren dat het onderzoeksrapport van de hoogleraren Bovend'Eert, Lawson en Winter niet terugkomt in de memorie van toelichting, maar dat ter zake slechts wordt verwezen naar de aangekondigde Hoofdlijnennotitie. Zij vragen waarom de regering niet uitgebreider heeft stilgestaan bij de conclusies uit het rapport nu de voorliggende wet een relatief grote wijziging van het toezicht inhoudt en waarom de regering hier pas op wil reflecteren na de voorliggende wetsbehandeling. Zoals hiervoor aangegeven op vragen van de leden van de SP-fractie, zal het advies van de hoogleraren Bovend'Eert, Lawson en Winter en de daaraan verbonden aanbevelingen tezamen met de aangenomen moties over toetsing en toezicht worden betrokken bij de herziening van de Wiv 2017. Zie ook hetgeen is gesteld in de Hoofdlijnennotitie. Hoewel door de drie hoogleraren geconcludeerd wordt dat de huidige inrichting van het stelsel van toezicht in het algemeen voldoet aan de vereisten in de rechtspraak van het EHRM, achten de hoogleraren aanpassingen op enkele onderdelen noodzakelijk. Zo zou de TIB als rechterlijke instantie en de CTIVD als zelfstandig bestuursorgaan (ZBO) moeten worden aangemerkt. Dergelijke wijzigingen zijn naar aard en inhoud echter zeer fundamenteel en vergen een herbezinning van het hele stelsel van toetsing en toezicht. Daarmee is het een vraagstuk dat in het kader van de herziening van de Wiv 2017 aan de orde moet komen en niet bij een Tijdelijke wet als de onderhavige, waarbij voor een urgent probleem – in afwachting van de herziening van de Wiv 2017 – die tijdelijke maatregelen moeten worden getroffen die nodig zijn om dat probleem te adresseren.

Ook vragen deze leden hoe de regering het standpunt van de hoogleraren dat een procedure in twee instanties (toetsing TIB en beroep Afdeling bestuursrechtspraak) niet effectief en niet nodig is en het voorgestelde

alternatief (bindend antwoord op een prejudiciële vraag over de wetsuitleg door de Afdeling bestuursrechtspraak) beoordeelt en hoe de inhoud van het rapport zich verhoudt tot de voorgestelde wijzigingen. Zoals hiervoor aangegeven in antwoord op de vraag van de leden van de D66-fractie, is een prejudiciële procedure niet mogelijk omdat in de procedures op grond van de Tijdelijke wet de rechter geen rol heeft. Het inrichten van een prejudiciële procedure zou een herbezinning vergen van het gehele stelsel van toetsing en toezicht en dat gaat het bestek van dit wetsvoorstel te buiten.

Voorts vragen deze leden in hoeverre het gebrek aan specialistische kennis bij de Afdeling bestuursrechtspraak een beperkende factor kan zijn bij het beroep, evenals de eenzijdigheid van de beroepsmogelijkheid (enkel in te roepen door de Minister). Ook vragen deze leden of het wetsvoorstel niet nadelig is voor de belangen van de burger binnen het toezicht en of de (privacy)belangen van burgers in beroepsprocedures behartigd zouden kunnen worden door speciaal daarvoor aangewezen deskundigen (amici curiae), bijvoorbeeld op grond van artikel 13 lid 10. Zoals aangegeven in antwoord op vragen van de leden van de fracties van D66 en de SP, voorziet de beroepsregeling in voldoende mogelijkheden voor de Afdeling om te beschikken over noodzakelijke deskundigheid die zij nodig acht voor de behandeling van de zaak. Voor zover met de eenzijdigheid van de beroepsmogelijkheid gedoeld wordt op een ontbrekende mogelijkheid voor de burger om beroep in te stellen, wordt opgemerkt dat het belang van de burger en diens privacy wel indirect wordt vertegenwoordigd. Zowel de diensten als de TIB en de CTIVD wegen het belang van de bescherming van de persoonlijke levenssfeer af tegen het belang van de nationale veiligheid. De burger is geen procespartij en kan dat ook niet zijn. In lijn met de suggestie van de Afdeling advisering, zullen de mogelijkheden om de privacybelangen van burgers meer of beter te betrekken bij de procedure, bijvoorbeeld door een amicus curiae, onderzocht worden bij de voorgenomen herziening van de Wiv 2017. Met artikel 13, lid 10, wordt overigens primair bedoeld op deskundigen met expertise die van belang is voor de inhoudelijke beoordeling van het geschil, dus bijvoorbeeld op het terrein van techniek.

De leden van de ChristenUnie-fractie vragen ook, onder verwijzing naar artikel 121 van de Grondwet op grond waarvan uitspraken van rechters openbaar moeten zijn, in hoeverre de uitspraak uit de beroepsprocedure openbaar is en wat er dan precies openbaar is. De beroepsregeling schrijft voor dat de uitspraak van de Afdeling bestuursrechtspraak openbaar gemaakt wordt met uitzondering van staatsgeheime informatie zoals bedoeld in artikel 12, derde lid, van de Wiv 2017. Het gaat dan om informatie inzake door de dienst aangewende middelen in concrete aangelegenheden, door de dienst aangewende geheime bronnen en het actuele kennisniveau van de dienst. Met inachtneming van genoemde beperkingen aan de openbaarheid, kan aldus door de uitspraken van de Afdeling bestuursrechtspraak duidelijkheid worden gegeven over de wijze waarop de wet dient te worden uitgelegd; het kan daarbij gaan om kwesties als de uitleg van wettelijke begrippen, de reikwijdte van de bevoegdheden van de diensten, maar ook de reikwijdte van de bevoegdheden van de TIB en de CTIVD. Daarbij is het niet noodzakelijk om in te gaan op de specifieke staatsgeheime details van de casus.

Ook vragen deze leden wat voor zaken naar verwachting zullen worden voorgelegd in de beroepsprocedure en of dat over interpretatieverschillen over de uitleg van de wet gaat of ook over geschillenbeslechting. De verschillen van inzicht zoals die de afgelopen jaren zijn voorgekomen, betroffen vooral de uitleg en reikwijdte van wettelijke begrippen, de wijze waarop de vereisten van noodzaak, proportionaliteit, subsidiariteit en

gerichtheid in de aanvragen moeten worden beschreven en de intensiteit van de toetsing. De Afdeling krijgt dus de rol van geschillenbeslechter ten aanzien van de deze aspecten.

De leden van de ChristenUnie-fractie constateren een onderscheid tussen de TIB en de CTIVD waarbij de TIB een rechterlijke autoriteit is en de CTIVD meer vergelijkbaar is met een inspectiedienst, die nu een bindende bevoegdheid krijgt. Zij vragen of het voor de interpretatie en uitleg van de wet na een uitspraak van de TIB een prejudiciële procedure niet veel wenselijker, effectiever en sneller zou zijn. Allereerst zouden wij willen opmerken dat de door deze leden gegeven kwalificatie van zowel TIB als CTIVD onjuist is. De TIB is geen rechterlijke instantie en haar taak is dan ook niet het verlenen van rechterlijke autorisatie. Wat de TIB doet is, zoals ook de ECW aangeeft, vergelijkbaar met de rechtsfiguur van goedkeuring[53]. De CTIVD is voorts niet aan te merken of te vergelijken met een inspectiedienst. De CTIVD is een onafhankelijke toezichthouder en niet aan te merken als een inspectiedienst; dergelijke diensten werken immers veelal onder ministeriele verantwoordelijkheid hetgeen bij de CTIVD niet het geval is. Waar het gaat om de vraag van deze leden inzake de prejudiciële procedure verwijzen wij hen naar hetgeen hiervoor in antwoord op een vergelijkbare vraag van de leden van de D66-fractie is gesteld.

Deze leden vragen of de beroepsgang niet beperkt moet worden voor zaken in relatie tot de CTIVD. Zij vragen de regering of er momenteel interpretatiekwesties bestaan en om een reflectie hierop. Sinds de inwerkingtreding van de Wiv 2017 zijn er verscheidene kwesties geweest waarbij er een verschil van inzicht was met de toezichthouders over de invulling van wettelijke begrippen. Zo heeft een langdurig verschil van inzicht met de afdeling toezicht van de CTIVD over de relevantiebeoordeling van verworven gegevens geleid tot het vernietigen van vijf door de diensten verworven bulkdatasets naar aanleiding van en beslissing van de afdeling klachtbehandeling van de CTIVD. Daarnaast bestaat er een verschil van inzicht met de TIB over het detailniveau waaraan de omschrijving van de technische risico's bij een verzoek tot inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk moet voldoen. Ten aanzien van de inzet van de bevoegdheid tot OOG interceptie op de kabel hebben wij een andere opvatting van de wijze waarop het gerichtheidsvereiste zou moeten worden toegepast dan de TIB, waardoor de inzet van deze bijzondere bevoegdheid sinds de inwerkingtreding van de Wiv 2017 nog nauwelijks heeft plaatsgevonden. Tot slot zijn er meerdere interpretatieverschillen van kleinere aard waarover de diensten in dialoog staan met de toezichthouders. Soms leidt dit tot een voor alle partijen aanvaardbare uitkomst, in andere gevallen blijkt het niet mogelijk om tot overeenstemming te komen. De TIB oordeelt bindend en bij een onrechtmatigheidsoordeel van de TIB vervalt de toestemming van de Minister van rechtswege en kan de bevoegdheid niet worden uitgeoefend zonder dat thans hierover een rechterlijk oordeel kan worden gevraagd. De ECW heeft dit als «weeffout» aangemerkt. Nu ook de afdeling toezicht van de CTIVD met dit wetsvoorstel een bindende oordeelsbevoegdheid krijgt, kan zich daar dezelfde situatie voordoen. De beroepsmogelijkheid geldt derhalve niet alleen voor de bindende oordelen van de TIB, maar ook van de afdeling toezicht van de CTIVD. Met

[53] Zoals de ECW aangeeft is hetgeen de TIB doet materieel gezien als goedkeuring te beschouwen; zij verwijst daarbij naar artikel 10:25 Awb (de voor de inwerkingtreding van een besluit van een bestuursorgaan vereiste toestemming van een ander bestuursorgaan). Bij de procedure van de TIB gaat het aldus de ECW formeel niet om goedkeuring in de zin van deze bepaling, maar alleen omdat de TIB ingevolge artikel 1:1, tweede lid, Awb geen bestuursorgaan is. (p. 127 rapport ECW; voetnoot 265).

een beroep op de Afdeling bestuursrechtspraak kan aldus een gezaghebbend, bindend rechterlijk oordeel over de uitleg van de wet worden verkregen.

De leden van de Volt-fractie vragen hoe de regering oordeelt over de mogelijkheden voor burgers om bezwaar en beroep te maken met betrekking tot de maatregelen waar zij in dit wetsvoorstel mogelijk mee te maken krijgen. De rechtsbescherming die de Wiv 2017 reeds biedt, geldt onverkort bij toepassing van de Tijdelijke wet. De toepasselijkheid van de Algemene wet bestuursrecht is buiten toepassing verklaard waar het gaat om de voorbereiding, totstandkoming en tenuitvoerlegging van de operationele besluiten, met inbegrip van de mogelijkheid tot bezwaar en beroep (zie artikel 145 Wiv 2017). Wel bestaat op grond van de Wiv 2017 de mogelijkheid om een klacht in te dienen bij de afdeling klachtbehandeling van de CTIVD die is belast met het onderzoeken en beoordelen van klachten en van meldingen van vermoedens van misstanden. De afdeling klachtbehandeling is een onafhankelijke en zelfstandige klachtinstantie die diepgaand onderzoek kan doen en bindende oordelen kan geven.

5. Grondrechtelijke en mensenrechtelijke aspecten

De leden van de D66-fractie merken op dat in het voorliggende voorstel de bepaling over de beoordeling van de relevantie van bulkdata is geschrapt. Voorgesteld was om die relevantiebeoordeling jaarlijks opnieuw uit te kunnen voeren, zonder maximum aan de hoeveelheid van die beoordelingen. Hierdoor zou de data, in theorie, tot in het oneindige bewaard kunnen worden. Vooruitlopend op de nota van wijziging, waarin de regering een nieuw voorstel over deze materie zal doen, willen deze leden de regering vragen hoe zij naar die relevantiebeoordeling kijkt. Deze leden vragen of de regering het met de Afdeling advisering eens is dat het niet maximeren van die hoeveelheid beoordelingen kan leiden tot het oneindig verlengen van de beoordelingstermijn. Ook vragen zij of de regering een oplossing voor zich ziet waar tegemoet gekomen kan worden aan de kritiek van de Afdeling advisering en de bulkdatasets niet gemakshalve maar relevant verklaard worden om geen (mogelijk belangrijke) gegevens te verliezen en daarbij tegelijkertijd aan de eisen van het EHRM te voldoen omtrent zo kort mogelijke bewaartermijnen. In reactie op de vragen van deze leden willen we als volgt reageren. Gelijktijdig met deze nota naar aanleiding van het verslag is bij de Tweede Kamer een nota van wijziging ingediend, waarin een aangepaste regeling voor een – belangrijk – onderdeel van de problematiek inzake bulkdatasets is opgenomen. Wij willen deze leden verwijzen naar hetgeen daarop ter toelichting is gesteld alsmede naar onze reactie op het advies van de Afdeling advisering ter zake in het aan de Koning uitgebrachte nader rapport.

De leden van de D66-fractie vragen met betrekking tot voorliggend wetsvoorstel hoe de regering deze in overeenstemming acht met de wens tot toetsing vooraf met het oog op bescherming van mensenrechten en privacy conform de huidige jurisprudentie van het EHRM en het HvJEU. Zowel het EHRM als het Hof van Justitie van de EU hebben in hun jurisprudentie slechts voor een beperkt aantal situaties *de eis* van een voorafgaande bindende toets gesteld. Waar die zijn gesteld, zoals bij de interceptie van communicatie (gericht als in bulk), de selectie van bulkdata verkregen via interceptie als bij de inzet van bevoegdheden jegens journalisten in relatie tot bronbescherming, voldoet de Wiv 2017 alsmede de in onderhavig wetsvoorstel opgenomen voorstellen aan deze eisen. Zoals we ook in de memorie van toelichting hebben aangegeven, wordt de eis van een bindende ex ante toets in de Wiv 2017 in meer gevallen

gesteld dan uit het Europese recht voortvloeit. Er is dus sprake van conformiteit met de huidige jurisprudentie.

De leden van de CDA-fractie nemen aan dat ondanks de fantastische cyberinfrastructuur, ligging en de aanwezige hoogwaardige technologische kennis Nederland niet het enige land is dat bedreigd wordt. Zij vragen of de regering een beeld kan schetsen hoe andere landen hun toezichtregime hebben georganiseerd, bijvoorbeeld Frankrijk, Duitsland en het Verenigd Koninkrijk. Ook vragen zij wat voor gevolgen de inrichting van dat toezichtregime heeft op de effectiviteit van het uitvoeren van onderzoeken voor hun veiligheidsdiensten en of, wanneer dat toezichtregime sneller en adequater kan reageren dan de Nederlandse diensten, Nederland dat toezichtregime dan niet over kan nemen aangezien deze landen zich ook hebben gecommitteerd aan het EVRM.

Vooropgesteld wordt dat de bij het EVRM aangesloten staten in hoge mate zelf kunnen bepalen op welke wijze zij binnen de eigen rechtsorde invulling geven aan de waarborgen die tegenover een beperking van de in het EVRM vastgelegde mensenrechten dienen te staan, zoals het vereiste van onafhankelijk en effectief toezicht. Deze flexibiliteit is ook nodig vanwege het feit dat bij de verdragspartijen grote diversiteit bestaat waar het gaat om de verwerking van persoonsgegevens door inlichtingen- en veiligheidsdiensten en (in het bijzonder) het toezicht daarop. Het is uiteindelijk aan het EHRM om te bepalen of het betreffende rechtstelsel, daaronder begrepen het toezichtregime voor inlichtingen- en veiligheidsdiensten, voldoet aan de vereisten uit het EVRM. Daarbij beoordeelt het EHRM het wettelijk kader waarbinnen door de (instanties van de) staten is geopereerd aan de hand van het voorgelegde feitencomplex in het licht van het EVRM en de jurisprudentie van het EHRM. Het EHRM kijkt daarbij altijd naar het stelsel als geheel waarbij de afwezigheid van de ene waarborg kan worden gecompenseerd door de aanwezigheid van een andere waarborg. Vanwege de verschillen in taken, bevoegdheden en positionering van de betrokken instanties in de genoemde landen, kunnen in algemene zin geen uitspraken worden gedaan over effectiviteit van buitenlandse toezichtregimes, evenmin over de bruikbaarheid daarvan in het Nederlandse stelsel.

Op verzoek van de leden van de CDA-fractie schetsen wij in het onderstaande het beeld met betrekking tot de door deze leden genoemde landen.

Duitsland kent drie federale inlichtingen- en veiligheidsdiensten, te weten het Bundesamt für Verfassungsschutz (hierna: BfV), de Bundesnachrichtendienst (BND) en de Militärischen Abschirmdienst (MAD). Het toezicht op deze diensten is belegd bij het Parlamentarische Kontrollgremium (PKGr), de G10-commissie, de federale commissaris voor gegevensbescherming en vrijheid van informatie en de Onafhankelijke Raad van Toezicht.

De PKGr is onderdeel van de Bondsdag en heeft tot taak toezicht te houden op het BfV, de BND en de MAD.[54] De PKGr heeft in het kader van deze toezichthoudende taak recht op inzage in de dossiers van de diensten, het recht om de kantoren van de diensten te betreden en het recht om het personeel van de diensten te ondervragen.[55] De federale regering kan indien nodig echter gemotiveerd weigeren bepaalde informatie met de PKGr te delen.[56] Daarnaast vindt jaarlijks een openbare

[54] Artikel 1, lid 1, Kontrollgremiumgesetz
[55] Artikel 5 Kontrollgremiumgesetz
[56] Artikel 6, lid 2 Kontrollgremiumgesetz

hoorzitting plaats met de hoofden van de diensten[57] en is een permanente vertegenwoordiger van de PKGr benoemd die de PKGr ondersteunt en zowel reguliere onderzoeken als onderzoeken naar individuele gevallen uitvoert.[58] De PKGr brengt in elk geval halverwege de zittingsperiode en aan het einde daarvan verslag uit aan de Bondsdag over zijn toezichtactiviteiten.[59] Hiernaast brengt de PKGr jaarlijks verslag uit aan de Bondsdag over de aard en omvang van de inzet van inlichtingenmiddelen die inbreuk maken op het brief-, post- en telecommunicatiegeheim.[60]

De G10-commissie oefent toezicht vooraf uit op de inzet van inlichtingenmiddelen die inbreuk maken op artikel 10, eerste lid, van de Duitse Grondwet (brief-, post- en telecommunicatiegeheim).[61] De toezichtbevoegdheden van de commissie strekken zich uit over het gehele proces van verzamelen, verwerken en gebruiken van de persoonsgegevens die via voornoemde inlichtingenmiddelen zijn verkregen, waaronder de beslissing om de betrokkenen al dan niet te notificeren. In dat kader heeft de commissie uitgebreide rechten om informatie op te vragen, dossiers in te zien en toegang te krijgen tot alle kantoren.[62] Verzoeken voor het intercepteren en onderzoeken van telecommunicatie worden schriftelijk gedaan door het diensthoofd of zijn plaatsvervanger bij de Minister van Binnenlandse Zaken.[63] Na instemming beoordeelt de G-10 commissie de rechtmatigheid van de voorgenomen bevoegdheid. De bevoegdheid wordt niet uitgeoefend voordat de G-10 commissie de rechtmatigheid positief heeft beoordeeld.[64]

De PKGr benoemt de G10-commissie, bestaande uit vijf leden en vijf plaatsvervangende leden, voor de duur van één zittingsperiode van de Bondsdag. De Bondsregering adviseert over de benoeming. Minimaal drie leden en drie plaatsvervangend leden moeten voldoen aan de eisen voor benoembaarheid tot rechter. Zij zijn bij de uitvoering van hun taken onafhankelijk en aan geen enkele instructie onderworpen. De commissie komt minstens eenmaal per maand bijeen en haar beraadslagingen zijn geheim.[65] Aan deze beraadslagingen kan worden deelgenomen door de permanente vertegenwoordiger van de PKGr.[66]

De federale commissaris voor gegevensbescherming en vrijheid van informatie is een onafhankelijke toezichthoudende autoriteit als bedoeld in de artikelen 51 en 59 van de AVG en houdt in die hoedanigheid ook toezicht op de uitvoering van regelgeving inzake gegevensbescherming, daaronder ook begrepen uitvoering door de diensten. Op dit punt bestaat overlap met de toezichtbevoegdheid van de G10-commissie, maar alleen de G10-commissie heeft de bevoegdheid om te oordelen over een beperking van de in artikel 10 van de Duitse Grondwet genoemde grondrechten.

De Onafhankelijke Raad van Toezicht[67] houdt toezicht op de BND op het gebied van technische verkenning, in het bijzonder de zogenaamde strategische monitoring van telecommunicatie in het buitenland, maar ook wanneer het vertrouwelijke relaties van bijvoorbeeld journalisten en

---

[57] Artikel 10, lid 3, Kontrollgremiumgesetz
[58] Artikel 5a Kontrollgremiumgesetz
[59] Artikel 13 Kontrollgremiumgesetz
[60] Artikel 14, lid 1 Artikel 10-Gesetz
[61] Artikel 1, lid 2, Artikel 10-Gesetz
[62] Artikel 15, lid 5, Artikel 10-Gesetz
[63] Artikel 9 Artikel 10-Gesetz
[64] Artikel 15, lid 5 en 6, Artikel 10-Gesetz
[65] Artikel 15 Artikel 10-Gesetz
[66] Artikel 15, lid 1 Artikel 10-Gesetz
[67] Artikel 41 BND-Gesetz

advocaten betreft. Het toezicht door de Onafhankelijke Raad van toezicht laat de bevoegdheden van de G10-commissie en de federale commissaris voor gegevensbescherming en vrijheid van informatie onverlet.

Het **Verenigd Koninkrijk** kent een aantal inlichtingen- en veiligheidsdiensten waarvan de Security Service, Secret Intelligence Service, Defence Intelligence en de Government Communications Headquarters het meest relevant zijn.

De bijzondere bevoegdheden zijn geregeld in de Investigatory Powers Act 2016 die samen met de Regulation of Investigatory Powers Act 2000 voorziet in de rechtsgrondslag en de toepasselijke beperkingen en waarborgen voor het gebruik van dergelijke bevoegdheden vastlegt. De IPA 2016 voorziet ook in de regeling voor het gebruik van onderzoeksbevoegdheden voor bulksgewijze verzameling (alleen voor inlichtingendiensten). Om deze bevoegdheden te kunnen uitoefenen, moeten de autoriteiten beschikken over een bevel dat is uitgevaardigd door een bevoegde autoriteit (in de meeste gevallen de Secretary of State). Het bevel moet bevestigd worden door een onafhankelijke Judicial Commissioner (de zogenaamde «double-lockprocedure»).[68]

Het toezicht op deze diensten is belegd bij de Investigatory Powers Commissioner, een onafhankelijke toezichthouder die toeziet op het gebruik van bijzondere bevoegdheden door de Britse inlichtingendiensten (alsmede de inzet van bijzondere bevoegdheden door veel andere overheidsinstanties) die een inbreuk maken op de persoonlijke levenssfeer.[69] De Investigatory Powers Commissioner is uitsluitend belast met het houden van toezicht en het rapporteren aan de prime Minister en kan dus niet zelf ingrijpen. Indien de diensten ernstige fouten maken ten aanzien van een persoon kan de Investigatory Powers Commissioner wel zelfstandig besluiten de betrokken persoon daarover te informeren. Daarnaast is er het Investigatory Powers Tribunal (IPT). Dit is een rechterlijke instantie die klachten onderzoekt inzake vermeend onrechtmatig handelen van de diensten.[70]

Het Intelligence and Security Committee (ISC) is een parlementaire commissie en heeft tot taak de uitgaven, bedrijfsvoering, beleid en operaties te controleren van de Security Service, de Intelligence service, GCHQ en inlichtingenactiviteiten van enkele andere overheidsinstanties.[71] De controle door de ISC vindt achteraf plaats. De diensten hoeven de ISC niet vooraf te informeren over operaties of programma's. Ter uitvoering van haar controletaken heeft de ISC de mogelijkheid om de hoofden van de Security Service, de Intelligence Service en de GCHQ te vragen om toegang tot informatie.[72] De prime Minister kan informatie aan de ISC weigeren indien de gevraagde informatie lopende operaties betreft.

Frankrijk kent meerdere inlichtingen- of veiligheidsdiensten. De Direction Génerale de la Securité Exterieure (DGSE), de Direction Générale de la Sécurité Intérieure (DGSI), de Direction du Renseignement et de la Sécurité de la Défense (DRSD) en de Direction du Reseignement Militaire (DRM) zijn het meest relevant.

---

[68] Artikelen 102–105 IPA 2016
[69] Artikelen 227–237 IPA 2016
[70] Artikel 65 e.v. Regulation of Investigatory Powers Act 2000
[71] Artikel 2 e.v. Justice and Security Act
[72] Schedule 1 Justice and Security Act

De Délégation parlementaire au renseignement (**DPR**) oefent parlementaire controle uit op het optreden van de regering op het gebied van inlichtingen, zij beoordeelt het overheidsbeleid op dit gebied en houdt toezicht op actuele kwesties en toekomstige uitdagingen die daarmee verband houden.[73]

Het juridisch kader voor de diensten is neergelegd in de Code de la Sécurité intérieure (**CSI**). De Commission Nationale de Contrôle des Techniques de Renseignement (**CNCTR**) houdt toezicht op het gebruik van inlichtingentechnieken.[74] De CNCTR bestaat uit negen leden (twee afgevaardigden, twee senatoren, twee leden van de Conseil d»État, twee rechters van het Cour de Cassation en een vertegenwoordiger van ARCEP (Autorité de régulation des Communications et des Postes).[75] De CNCTR is een onafhankelijke commissie en de leden hebben toegang tot alle plaatsen, inlichtingen en documenten die nuttig zijn voor de vervulling van hun taak.[76] De premier geeft toestemming voor de inzet van een bevoegdheid na ontvangst van het advies van de CNCTR.[77] De premier kan gemotiveerd van het advies van de CNCTR afwijken.[78]

De CNCTR heeft permanent toegang tot alle informatie en ontvangt alle informatie met betrekking tot alle verleende toestemmingen voorafgaand aan de uitvoering en ontvangt voor het overige alle informatie waarom zij verzoekt.[79] Zij kan zich op elk moment met een aanbeveling over onderbreking of stopzetting van een bijzondere bevoegdheid en/of vernietiging van verzamelde gegevens wenden tot de bij de uitvoering betrokken instanties, inclusief de premier en de betrokken Minister. Zodra een aanbeveling wordt ontvangen, informeert de premier de CNCTR onmiddellijk over de wijze waarop uitvoering wordt gegeven aan de aanbeveling. Wanneer de premier geen of onvoldoende gevolg geeft aan de aanbevelingen van de commissie, kan de voorzitter dan wel drie leden van de CNCTR de Conseil d»État informeren.[80] Jaarlijks brengt de CNCTR een openbaar rapport uit over haar werkzaamheden.[81]

Een ieder kan zich tot de CNCTR wenden met het verzoek te controleren of tegen hem op legitieme wijze middelen worden of zijn ingezet.[82] Een klacht kan worden ingediend bij de Conseil d»État.[83]

Daarnaast houdt de Commission nationale de l'informatique et des libertés (**CNIL**) toezicht op de DGSI. Deze commissie is een onafhankelijke toezichthouder op grond van de AVG[84] en ziet ook toe op de bescherming van persoonsgegevens in het kader van inlichtingenactiviteiten.

Daarnaast is voorzien in toezicht door andere instanties op diverse niveaus, zoals de Contrôle de l'inspection des services de renseignement **(ISR)** die als inspectiedienst op verzoek van de Minister-President inspectiemaatregelen kan treffen ten aanzien van de inlichtingendiensten.[85]

---

[73] LOI n° 2007–1443 du 9 octobre 2007
[74] Artikel L831–1 e.v. Code de la sécurité intérieure
[75] Artikel L831–1 Code de la sécurité intérieure
[76] Artikel L833–2 Code de la sécurité intérieure
[77] L821–1 Code de la sécurité intérieure
[78] L821–4 Code de la sécurité intérieure
[79] L833–2 Code de la sécurité intérieure
[80] L833–6 t/m L833–8 Code de la sécurité intérieure
[81] L833–9 Code de la sécurité intérieure
[82] L833–4 Code de la sécurité intérieure
[83] L841–1 Code de la sécurité intérieure
[84] Artikel 8 Loi n° 78–17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[85] Décret n° 2014–833 du 24 juillet 2014 relatif à l'inspection des services de renseignement

De leden van de SP-fractie hebben grote zorgen over de grondrechtelijke en mensenrechtelijke aspecten bij deze wet. De consultatietijd voor maatschappelijke organisaties was zeer krap – twee weken – en de inzendingen zijn toch ongemeen kritisch. Het wetsvoorstel redeneert geheel vanuit de werkwijze en wens te opereren van de geheime diensten. Hun wens is bekend en ook begrijpelijk. Maar juist een wetsvoorstel dat bevoegdheden om te tappen, te hacken, data te onderzoeken, data te delen en data te bewaren, verruimt, moet de balans tussen de impact van onderzoek van de diensten op mensenrechtenaspecten bewaren. Deze leden zien die balans niet terug. Zij vragen of de regering hierop een reflectie geven. Allereerst willen we opmerken dat de Wiv 2017, dus inclusief de daarin vervatte waarborgen, gewoon van toepassing is op de uitoefening van de taak van de diensten zoals omschreven in artikel 2, eerste lid, maar dat op een beperkt aantal onderdelen in het wetsvoorstel sprake is van een aanvulling dan wel een afwijking van enkele bepalingen in de Wiv 2017. Bij de uitwerking daarvan in het wetsvoorstel hebben we ons wel degelijk rekenschap gegeven van wat een en ander zou moeten betekenen voor de balans tussen enerzijds de voor de diensten benodigde bevoegdheden om onderzoek te kunnen doen naar cyberdreigingen en anderzijds hoe de daaruit voortvloeiende beperkingen op met name de privacy van burgers kunnen worden geminimaliseerd en van adequate waarborgen kunnen worden voorzien. Dat heeft ertoe geleid dat in de gevallen waar ex ante toets door de TIB is beperkt, de afdeling toezicht de bevoegdheid tot bindend toezicht heeft gekregen, en dat voorts ook bindend toezicht is geïntroduceerd met betrekking tot bijvoorbeeld de in het wetvoorstel opgenomen voorzieningen inzake bijschrijfbevoegdheden. Op die wijze is naar ons oordeel een goede balans tussen beide belangen gevonden. Voorts vragen zij of de regering zich een faciliteerder van het oprekken van de mogelijkheden van de geheime diensten of een hoeder van het algemeen belang, waarbij belangen van burgers en hun privacy zorgvuldig moeten meetellen, vindt. Wij merken op dat naar ons oordeel deze leden hier een valse tegenstelling creëren. Bij de regering staat het algemeen belang voorop. Daartoe behoort ervoor zorgen dat burgers, bedrijven en anderen gevrijwaard worden van dreigingen en hun belangen en grondrechten worden beschermd. Het is de taak van de diensten om deze belangen en grondrechten te beschermen en daarom zijn in de Wiv 2017 en de Tijdelijke wet hun bevoegdheden en waarborgen bij de uitoefening daarvan vastgelegd. Het beschermen van burgerrechten en het beschermen van de nationale veiligheid zijn geen tegengestelde doelstellingen. De AIVD en de MIVD spelen een cruciale rol bij het beschermen van de persoonlijke levenssfeer van Nederlandse burgers, bijvoorbeeld tegen landen die actief cyberprogramma's voeren gericht tegen Nederland. Hierbij zetten zij zich in om met rechtsstatelijke middelen en robuuste waarborgen onder parlementaire verantwoording de strijd aan te gaan met veelal niet-rechtsstatelijke tegenstanders. De Nederlandse diensten onderscheiden zich in hun handelen door een cultuur van rechtmatigheid hoog in het vaandel te dragen. Hun medewerkers worden gedreven door een intrinsiek besef van het belang daarvan en door de wens onze open en vrije samenleving, waar zij zelf als burger ook onderdeel van zijn, te beschermen. Dit besef is diep verankerd in hun dagelijkse handelen. Andersom is het zo dat de bescherming van burgerrechten via toezicht op de diensten en andere waarborgen niet tegengesteld is aan het belang de democratische rechtsorde te beschermen. Onafhankelijk en effectief intern en extern toezicht draagt bij aan het vertrouwen bij de burger dat de diensten zich (enkel) bedienen van rechtmatige middelen. Kortom, veiligheidsbelangen en het beschermen van de grondrechten van burgers zijn onlosmakelijk met elkaar verbonden en kunnen elkaar zelfs versterken. Burgers moeten er immers zeker van kunnen zijn dat de overheid hen zowel beschermt tegen uiteenlopende dreigingen als zorgt voor een wettelijk kader met stevige

waarborgen en onafhankelijk toezicht ter bescherming van de persoonlijke levenssfeer.

De leden van de SP-fractie vragen de regering uit te leggen hoe de «notificatie» van inzet van artikelen 5, 10 en 11, die de CTIVD niet verplicht om tot onderzoek over te gaan, voldoende is om aan de criteria van «end-to-end safeguards» en «sufficient guarantees against abuse» van Europees Hof voor de Rechten van de Mens te voldoen. Het concept van «end-to-end safeguards» waar deze leden naar verwijzen, is door het Hof in de zaak Big Brother Watch e.a. tegen het Verenigd Koninkrijk geïntroduceerd in het kader van bulkinterceptieregimes en geeft uitdrukking aan de gedachte dat naarmate men verder komt in de keten van verwerking van gegevens verkregen door bulkinterceptie ook het inbreukmakende karakter van die verwerking toeneemt. Dit concept heeft dus een beperkte reikwijdte en kan aldus niet op de toepassing van de andere bijzondere bevoegdheden door de diensten worden getransponeerd. De door deze leden aangehaalde notificaties hebben geen betrekking op bulkinterceptie en daarop zijn de criteria van «end-to-end safeguards» niet van toepassing. Waar het gaat om het criterium dat er voorzien dient te zijn in «sufficient guarantees against abuse» oftewel voldoende waarborgen tegen misbruik, betreft het een eis die door het EHRM in algemene zin wordt gesteld bij de regulering van beperkingen van – in casu – het door artikel 8 EVRM beschermde recht op privacy. Zowel de Wiv 2017 als onderhavig wetsvoorstel gezamenlijk genomen voorziet in die adequate waarborgen. De notificaties waar deze leden op wijzen, namelijk dat de afdeling toezicht van de toepassing van een bepaalde bevoegdheid terstond op de hoogte wordt gesteld, dragen er aan bij dat het toezicht op die bevoegdheidsuitoefening adequaat kan worden uitgeoefend en vormen aldus een (aanvullende) waarborg tegen misbruik.

Deze leden hebben nog een aantal specifieke vragen over de verhouding van artikelen in het wetsvoorstel als het gaat om uitspraken van het Europees Hof van de Rechten van de Mens, bijvoorbeeld de verhouding van het nieuwe artikel 6 (verkennen tot een jaar en data opslaan tot 6 maanden) met randnummers 350 en 360 van de zaak van Big Brother Watch en others vs het Verenigd Koninkrijk. Hoe is er, zo vragen deze leden, volgens de regering, sprake van «end-to-end safeguards» en «sufficient guarantees against abuse» als beide toezichthouders beperkt zijn in de criteria waarop ze kunnen toetsen en het bindend toezicht van de CTIVD op dit artikel ontbreekt. Alvorens concreet op deze vragen in te gaan achten wij het voor de goede orde wenselijk om hetgeen in de desbetreffende randnummers wordt gesteld hier integraal weer te geven:

«350. Therefore, in order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to «end-to-end safeguards», meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review. In the Court's view, these are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime (see also the report of the Venice Commission, at paragraph 197 above, which similarly found that two of the most significant safeguards in a bulk interception regime were the authorisation and oversight of the process).»
En

«*360. In the light of the above, the Court will determine whether a bulk interception regime is Convention compliant by conducting a global assessment of the operation of the regime. Such assessment will focus primarily on whether the domestic legal framework contains sufficient guarantees against abuse, and whether the process is subject to «end-to-end safeguards» (see paragraph 350 above). In doing so, it will have regard to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse (see Association for European Integration and*

Human Rights and Ekimdzhiev, cited above, § 92).»

Uit de eerste geciteerde overweging blijkt dat – waar het gaat om het bulkinterceptie-regime – er in elke fase van het proces van verwerking – waarbij het EHMR een viertal fasen onderscheidt, te weten (1) de verzameling en opslag, (2) het doorzoeken van de verworven gegevens (via toepassing van selectoren of complexe query's), (3) het onderzoeken van de geselecteerde gegevens en (4) het gebruik van de gegevens – de noodzakelijkheid en proportionaliteit van de handelingen die worden verricht moet worden beoordeeld. In artikel 18 e.v. van de Wiv 2017 zijn aan de verwerking van gegevens in algemene zin eisen gesteld en waar het gaat om de verzameling van gegevens in de artikelen 25 e.v. Wiv 2017 meer specifieke eisen; de eisen van noodzakelijkheid en proportionaliteit zijn in de Wiv 2017 wettelijk verankerd. Die eisen gelden dus ook bij de toepassing van de bijzondere bevoegdheid in artikel 6 van het wetsvoorstel. Voor de toepassing van deze bevoegdheid is toestemming van de Minister vereist, die vervolgens onderworpen is aan de voorafgaande bindende toets door de TIB; zoals door het EHRM wordt geëist. Het verzoek om toestemming moet voldoen aan de eisen van artikel 29, tweede lid, Wiv 2017, waarbij dus ook het doel en de reikwijdte van de bevoegdheidsuitoefening moeten worden gemotiveerd. Op het gehele verwerkingsproces is vervolgens toezicht mogelijk door de afdeling toezicht van de CTIVD; voor het effectief kunnen zijn van dit toezicht is het niet vereist dat deze bindend is. Waar het gaat om het ex post facto review – te weten de beoordeling van klachten van burgers over de (vermeende) toepassing van de bevoegdheid – biedt de afdeling klachtbehandeling van de CTIVD die bindend kan oordelen de betreffende geëiste remedie. Ook waar het dus gaat om de toepassing van artikel 6. De TIB en de afdeling toezicht van de CTIVD kunnen op de toepassing van dit artikel conform het bepaalde in de Wiv 2017 hun rechtmatigheidstoets onderscheidenlijk rechtmatigheidstoezicht toepassen; waar het gaat om de proportionaliteitstoetsing door de TIB verwijzen wij in dit verband naar de door ons aan de Kamer gezonden afschrift van de brief aan de voorzitter van de TIB ter zake.[86] Overweging 360 geeft uitdrukking aan wat ook wel aangeduid wordt als de holistische benadering van het EHRM waar het gaat om de vraag of een bepaalde wettelijk stelsel voldoet aan de eisen van het EVRM. Naar ons oordeel kan zowel de Wiv 2017 en de in het wetsvoorstel voorziene bepalingen (deels in aanvulling, deels in afwijking van de Wiv 2017) in totaliteit bezien in overeenstemming met de eisen van het EVRM worden beschouwd.

Deze leden vragen voorts of de regering ook kan uitleggen hoe het nieuwe artikel 7, dat de criteria voor toetsen van bulkinterceptie verzwakt, zich verhoudt tot de eerder genoemde randnummers van de zaak. Wij delen niet de opvatting van de leden van de SP-fractie dat met artikel 7 de criteria voor toetsen van verleende toestemming voor bulkinterceptie wordt verzwakt. Zoals in de memorie van toelichting is aangegeven strekt

[86] Kamerstukken II 2022/2023, 36 263, nr. 6.

artikel 7 ertoe om de eisen van proportionaliteit (artikel 26, tweede lid) en gerichtheid (artikel 26, vijfde lid) in relatie tot de bevoegdheid van OOG-interceptie ex artikel 48 Wiv 2017 te verduidelijken en aan te geven waar naar ons oordeel met name het accent dient te liggen. OOG-interceptie is immers een bulkbevoegdheid en met deze karakteristiek moet bij de invulling van de genoemde criteria nadrukkelijk rekenschap worden gegeven. Met het voorgestelde artikel 7 in combinatie met de daarbij gegeven uitleg wordt – mits het wetsvoorstel de instemming van beide Kamers der Staten-Generaal verkrijgt – door de wetgever ter zake een duidelijke, richtinggevende uitspraak gedaan. Daarmee wordt voor de toepassingsprakrijk de gewenste helderheid geschapen. Nu de waarborgen die de Wiv 2017 – aangevuld met artikel 7 van het wetsvoorstel – niet worden gewijzigd, lijkt ons dat een toets aan hetgeen in de randnummers wordt gesteld niet aan de orde. Zie ook hetgeen we hiervoor al daarover hebben opgemerkt.

De leden van de SP-fractie vragen of een niet-bindende «indicatie van verkeersstromen en datareductie» een voldoende stevig criterium is volgens Europees recht. Deze leden vragen of de regering erkent dat dit relevant is, omdat de nieuwe wet toezichthouders opdraagt «met name» en «daarmee het zwaarwegendst» te toetsen op alleen deze twee niet-bindende indicaties. Zij vragen of de regering kan uitleggen waarom zij heeft gekozen voor deze indicatoren voor OOG-interceptie.
OOG-interceptie is een bulkbevoegdheid. Dit heeft een wezenlijk effect op de invulling van het gerichtheidscriterium en de proportionaliteitstoets. Artikel 7 van het wetsvoorstel geeft meer richting aan de wijze waarop aan deze beginselen dient te worden getoetst, gelet op de bijzondere aard van de bevoegdheid. Er is voor deze criteria gekozen aangezien hiermee inzage kan worden gegeven in de mate van gerichtheid van de verwerving en de (direct daaropvolgende) verwerking (en dus reductie) van de gegevens, en daarmee ook de proportionaliteit van de inzet zorgvuldig kan worden getoetst. Gelet op het feit dat de diensten voor aanvang van de inzet van de bevoegdheid slechts tot op zekere hoogte kennis hebben van de exacte klantkanalen waarop zal worden geïntercepteerd en de gegevens die vervolgens worden verworven, stelt artikel 7 expliciet dat de toets op gerichtheid en proportionaliteit dient plaats te vinden aan de hand van een indicatie hiervan. Deze twee aspecten zijn gerelateerd aan uitspraken van het EHRM. Het Hof spreekt voornamelijk over de keuze van gegevensstromen, omdat de keuze voor de interceptie van gegevensstromen gericht moet zijn op internationaal verkeer waarvan het waarschijnlijk is dat deze gegevens en meerwaarde kunnen hebben voor het inlichtingenonderzoek en de beantwoording van onderzoeksvragen. De verdere reductie van gegevens in de keten van OOG-interceptie bestaat uit verschillende stappen, ook wel: de keten van verwerving genoemd. Het eindresultaat van dit proces leidt tot de gegevens die voor de diensten toegankelijk zijn bij het beantwoorden van onderzoeksvragen. Deze gehele keten van verwerven moet dus gezien worden als een proces van datareductie inclusief effectieve en robuuste waarborgen. Er is namelijk sprake van diverse stappen voordat geïntercepteerde en opgeslagen gegevens daadwerkelijk in een inlichtingenonderzoek kunnen worden betrokken. Per stap in het proces nemen de waarborgen ook toe. Gegevensstromen zijn daarnaast dynamisch en wijzigen voortdurend. De filters moeten daarop worden aangepast. Daarom kan bij de aanvraag voor het inzetten van het middel slechts een indicatie worden gegeven voor de wijze waarop de diensten van plan zijn om de gegevens te reduceren. Op de uitvoering van dit gehele proces houdt de afdeling toezicht van de CTIVD toezicht. Bij het inzetten van kabelinterceptie ten behoeve van een onderzoek moet een indicatie gegeven worden van de reductie van gegevens. Gelet op de hiervoor beschreven veranderlijke methode, is het niet mogelijk om op voorhand en categorisch gegevens-

stromen uit te sluiten van interceptie. Het wetsvoorstel biedt helderheid over welke aspecten vooraf te toetsen zijn door de TIB en op welke wijze de afdeling toezicht van de CTIVD toezicht kan houden op rechtmatige uitvoering van deze bevoegdheid.

Het is voor de leden van de GroenLinks-fractie van groot belang dat de inrichting van het wettelijk stelsel voor het werk van de inlichtingen- en veiligheidsdiensten adequaat is ingebed binnen onze Grondwet en binnen internationale verdragen die de mensenrechten beschermen. Een belangrijk ijkpunt hierbij is voor deze leden het feit dat het EHRM in haar rechtspraak als uitgangspunt heeft genomen dat toetsing van noodzakelijkheid en proportionaliteit vooraf door een onafhankelijke rechterlijke instantie de voorkeur geniet. Omdat burgers doorgaans geen weet hebben van het precieze werk van inlichtingendiensten is het van belang dat de inzet van bijzondere bevoegdheden vooraf door een onafhankelijke instantie (de TIB) wordt getoetst. Zij vragen of de regering kan toelichten op welke wijze dit uitgangspunt van het EHRM in de voorliggende wet is verankerd. Voorts vragen zij of de regering helder kan toezeggen dat het voorliggende wetsvoorstel EHRM-proof is. Met deze leden zijn wij het eens dat het wettelijk stelsel adequaat dient te zijn ingebed binnen onze Grondwet en binnen internationale verdragen die de mensenrechten beschermen. Dat geldt niet alleen voor de Wiv 2017, maar ook voor onderhavig wetsvoorstel. Naar ons oordeel is daarvan ook sprake. Er kan natuurlijk altijd discussie zijn over een bepaalde keuze die is gemaakt in wetgeving en die anderen wellicht anders hadden willen zien, maar wij zijn van oordeel dat de wetgeving EVRM-proof is. Waar het gaat om het door deze leden gememoreerde ijkpunt over de toetsing vooraf door een onafhankelijke rechterlijke instantie, merken we op dat zowel het EHRM als het Hof van Justitie van de EU hebben in hun jurisprudentie slechts voor een beperkt aantal situaties *de eis* van een voorafgaande bindende toets hebben gesteld. Waar die zijn gesteld, zoals bij de interceptie van communicatie (gericht als in bulk), de selectie van bulkdata verkregen via interceptie als bij de inzet van bevoegdheden jegens journalisten in relatie tot bronbescherming, voldoet de Wiv 2017 alsmede de in onderhavig wetsvoorstel opgenomen voorstellen aan deze eisen. Zoals we ook in de memorie van toelichting hebben aangegeven, wordt de eis van een bindende ex ante toets in de Wiv 2017 in meer gevallen gesteld dan uit het Europese recht voortvloeit. Er is dus sprake van conformiteit met de huidige jurisprudentie. In aanvulling daarop merken we op dat het EHRM inderdaad consistent haar voorkeur heeft uitgesproken voor een toets (of toestemming) door een onafhankelijke rechterlijke instantie. Maar in plaats daarvan kan ook een – qua onafhankelijkheid daarmee vergelijkbare – niet-rechterlijke autoriteit daarmee worden belast.[87] In het kader van de uitvoering van de Wiv 2017 kennen we beide situaties. Zo is voor het openen van brieven en andere geadresseerde zendingen, de inzet van bijzondere bevoegdheden jegens journalisten gericht op het achterhalen van hun bronnen alsmede de inzet van bijzondere bevoegdheden jegens advocaten waarbij kennis kan worden genomen van de vertrouwelijke communicatie tussen de advocaat en diens client de toestemming vereist van de rechtbank Den Haag. In de andere gevallen waarbij de wet een bindende toets vooraf eist, is die in handen gelegd van de TIB.

De leden van de Volt-fractie merken op dat om een goede afweging te kunnen maken tussen het inbreuk maken op fundamentele rechten en vrijheden van mensen voor nationale veiligheid en het beschermen van fundamentele rechten en vrijheden voor individuen en groepen mensen, het belangrijk is dat duidelijk is wat de dreiging inhoudt. De inbreuk moet

[87] Zie o.m. de uitspraken van het EHRM in de zaken Roman Zakharov tegen Rusland, par. 275, en Klass and Others, par. 56.

immers noodzakelijk zijn in een democratische samenleving. Hoewel de leden van Volt-fractie begrijpen dat de regering niet exact kan duiden wat de dreiging inhoudt, vragen deze leden wel om toe te lichten aan de hand van een concreet (fictief) voorbeeld welke gevolgen het niet nemen van deze maatregelen heeft voor mensen die zich in Nederland bevinden. Gaat het, aldus deze leden, bijvoorbeeld om economische schade of ook om schade aan (groepen) burgers, en wat gebeurt er als de maatregelen niet worden getroffen. Ook vragen zij aan welke potentiële risico's mensen die zich in Nederland bevinden dan worden blootgesteld en in welke mate. Waarom rechtvaardigt die dreiging de inbreuk op de fundamentele rechten en vrijheden? Wij antwoorden deze leden graag als volgt. Landen als China, Rusland, Iran en Noord-Korea zetten op grote schaal digitale aanvallen in. Doelwitten daarbij zijn persoonsgegevens, belangrijke hightech innovaties, politieke standpunten, militaire geheimen, kwetsbaarheden van onze vitale infrastructuur, informatie over dissidenten en nog veel meer. Het gaat dus om economische schade, militaire schade, fysieke schade en/of geopolitieke schade veroorzaakt bij zowel Nederlandse organisaties als ook individuele Nederlanders. Bijvoorbeeld doordat routers van Nederlanders worden gebruikt vanuit Rusland door hackers van de GRU. Of doordat persoonsgegevens van Nederlandse burgers worden buitgemaakt. De AIVD zag dit in 2022 gebeuren toen verschillende landen met offensieve cyberprogramma's probeerden data te stelen in de (Europese) reis- en luchtvaartsector (Jaarverslag 2022). Ook hebben de diensten in het afgelopen jaar gezien dat Russische staatshackers een cyberoperatie aan het voorbereiden waren waarbij de website van een Nederlandse overheidsinstelling zou worden misbruikt. De hackers maakten een kopie van deze overheidswebsite om bezoekers daarvan te kunnen infecteren met malware om ze hiermee te kunnen bespioneren. In potentie kunnen de gegevens van Nederlandse burgers die hackers buitmaken gebruikt worden voor allerlei doeleinden. Denk aan desinformatiecampagnes rond MH17. Voor landen met een offensief cyberprogramma kunnen Nederlandse burgers een middel zijn om bepaalde doelen (beïnvloeding, spionage, sabotage) te bereiken. Nederland is een aantrekkelijk doelwit. We zijn een technologisch geavanceerd digitaal knooppunt van het wereldwijde internet. Andere landen maken hier misbruik van. De AIVD en MIVD zien een steeds grotere kloof ontstaan tussen de ontwikkeling van de dreigingen en onze weerbaarheid daartegen. Cruciaal voor die weerbaarheid is dat je weet wie je aanvalt, hoe ze dat doen, wie we moeten waarschuwen en wat je er aan kunt doen om dit te voorkomen. Maar ook dat we tijdig de cyberaanvallen tegen kunnen gaan.

Deze leden vragen tot slot of de regering kan toelichten welke impact de afzonderlijke maatregelen hebben op de bescherming van relevante fundamentele rechten en vrijheden en in hoeverre de maatregelen in lijn zijn met geldende Europese en nationale rechtspraak over fundamentele rechten en vrijheden. Zij vragen of daarbij de analyse van de heer Bovend'Eert kan worden betrokken, zoals gegeven in zijn position paper ten behoeve van het rondetafelgesprek over de Tijdelijke wet cyberoperaties d.d. 5 april 2023. Wij reageren hierop graag als volgt. De in de Tijdelijke wet opgenomen maatregelen betreffen deels aanvullingen en deels afwijkingen van een beperkt aantal in de Wiv 2017 geregelde bijzondere bevoegdheden voor de diensten, waarbij – met inachtneming van die aanvullingen en afwijkingen – de Wiv 2017 als zodanig gewoon van toepassing blijft. Voorts komt in een tweetal gevallen de thans bestaande bindende ex ante toets door de TIB te vervallen en wordt deze vervangen door bindend toezicht door de afdeling toezicht van de CTIVD ex durante (tijdens de uitvoering van de bevoegdheid) en ex post (na afloop). Daarnaast wordt met betrekking tot de aanvullingen in de sfeer van bijschrijfbevoegdheden voor de diensten voorzien in bindend toezicht

ex durante en ex post door genoemde afdeling toezicht. Waar het gaat om de impact waarnaar deze leden vragen, merken wij op dat voor alle maatregelen die betrekking hebben op de bevoegdheden van de diensten geldt dat bij toepassing daarvan deze een beperking op kunnen leveren van de in de artikelen 10 (recht op bescherming van de persoonlijke levenssfeer) en 13 (recht op brief- en telecommunicatiegeheim) Grondwet alsmede artikel 8 EVRM (recht op privacy) gegarandeerde grondrespectievelijk mensenrechten. Dergelijke beperkingen zijn geoorloofd, indien aan een aantal eisen wordt voldaan. Naast de grondwettelijke eis dat een dergelijke beperking een formeel wettelijke grondslag dient te hebben (waaraan zonder meer wordt voldaan), vloeien uit artikel 8 EVRM en de jurisprudentie van het EHRM meer materiële eisen voort. Het gaat dan om de eisen dat de beperking een legitiem doel moet dienen, bij wet voorzien moet zijn en noodzakelijk moet zijn in een democratische samenleving en die door de jurisprudentie van het EHRM in de loop der jaren nadere invulling en precisering hebben gekregen. Waar het gaat om bulkinterceptie heeft het EHRM nog vrij recent in de uitspraken van het EHRM in de zaken Big Brother Watch e.a. tegen het VK en Centrum för Rätvissa tegen Zweden een aangepast toetsingskader vastgesteld, waaraan wetgeving en praktijk ter zake dient te voldoen. De door de directie CZW van het Ministerie van BZK opgestelde interne analyse van deze uitspraken en wat deze betekenen voor de regeling in de Wiv 2017 is aan de beide kamers der Staten-Generaal is gezonden. Daarnaast is door het Hof van Justitie van de EU in de gevoegde zaken C-511/18, C-512/18 en C-520/18 (Quadrature du Net e.a.) uitgesproken dat real time verzameling van verkeers- en locatiegegevens («stomme tap») uitsluitend geoorloofd is indien dit is onderworpen aan een voorafgaand bindend toezicht door een onafhankelijke instantie (bij voorkeur een rechter of een qua onafhankelijkheid daarmee vergelijkbare instantie). In de nota van wijziging wordt voor de stomme tap voorzien in de door het Hof van Justitie van de EU vereiste toets ex ante. In hoofdstuk 9 van de memorie van toelichting bij het wetsvoorstel dat tot de Wiv 2017 heeft geleid is uitvoerig op de betekenis van genoemde Grondwets- en verdragsartikelen en de daaromtrent gevormde jurisprudentie ingegaan waar het gaat om de in de Wiv 2017 en met name de daarin opgenomen bevoegdheden van de diensten en de waarborgen die daarbij moeten zijn voorzien. De daar gegeven uiteenzettingen voor de bijzondere bevoegdheden waarop onderhavig wetsvoorstel aanvullingen dan wel afwijkingen aanbrengt, zijn evenzeer van toepassing op de maatregelen in dit wetsvoorstel. Kortheidshalve wordt daarnaar verwezen. Ten opzichte van de regeling van het stelsel van toetsing en toezicht in de Wiv 2017 wordt naar ons oordeel met de in onderhavig wetsvoorstel opgenomen maatregelen inzake de toets door de TIB en de introductie van bindend toezicht door de afdeling toezicht van de CTIVD per saldo voorzien in een versterking van de reeds bestaande waarborgen waarmee de uitoefening van de bijzondere bevoegdheden van de diensten wordt omgeven. Daarmee kan door beide instanties corrigerend worden opgetreden indien de impact van de door de diensten ingezette bevoegdheden op met name het recht op bescherming van de persoonlijke levenssfeer zodanig is dat deze onrechtmatig moet worden beschouwd. Tegen die bindende oordelen wordt de mogelijkheid van beroep bij de Afdeling bestuursrechtspraak geïntroduceerd. In het door de heer Bovend'Eert uitgebrachte position paper, dat aansluit op het eerder door hem en twee collega hoogleraren uitgebrachte advies «Naar een duurzaam en effectief stelsel van toezicht door inlichtingen- en veiligheidsdiensten, staan niet zozeer de maatregelen centraal die erop gericht zijn de diensten in staat te stellen om beter op te kunnen treden tegen dreigingen in het cyberdomein, maar het stelsel van toetsing en toezicht («de verschuiving van bevoegdheden van TIB naar CTIVD») en de rechtsgang bij de Afdeling bestuursrechtspraak. Hetgeen in het position paper naar voren wordt gebracht zijn grotendeels

noties die bij de voorgenomen herziening van de Wiv 2017 dienen te worden betrokken en waarvoor de heer Bovend'Eert aandacht vraagt. Waar het gaat om onderhavig wetsvoorstel werpt hij de vraag op welke argumenten voor de regering nu precies de doorslag hebben gegeven om een, zij het beperkte, verschuiving van het toezicht door te voeren. Zoals hiervoor is aangegeven is die verschuiving inderdaad zeer beperkt en heeft de TIB aangegeven dat ze zich kan vinden in de verschuiving met betrekking tot het verkennen (in haar woorden: scannen) van geautomatiseerde werken en die met betrekking tot GDA op OOG-metadata verdedigbaar acht. Het gaat hier om gevallen waarvan is vastgesteld – in de praktijk en door de ECW – dat een statische toets ex ante niet past en dat daarbij beter kan worden voorzien in een dynamisch toezicht gedurende de uitvoering van de bevoegdheid. Dat heeft niets met snelheid van besluitvorming te maken of het voorhanden zijn van een spoedprocedure. De spoedprocedure dient een ander doel en biedt geen oplossing voor de geconstateerde problemen in de uitvoeringspraktijk. Waar het gaat om de beroepsgang bij de Afdeling bestuursrechtspraak is naar het oordeel van de heer Bovend'Eert sprake van een fundamentele wijziging van het stelsel van toezicht. Evenals in het eerder genoemde advies van Bovend'Eert c.s. wordt gesteld dat er in feite een procedure in twee instanties wordt ingevoerd, waarbij de TIB als de eerste instantie en de Afdeling bestuursrechtspraak als tweede instanties geldt. Dit vanuit de veronderstelling dat de TIB als een rechterlijke instantie zou moeten worden aangemerkt. Zoals wij al eerder hebben aangegeven beschouwen wij – in navolging van hetgeen de ECW ter zake stelt – de activiteit van de TIB niet als rechterlijk, maar als een activiteit welke te vergelijking is met de figuur van goedkeuring als bedoeld in hoofdstuk 10 Awb. Een karakterisering van een en ander als een procedure in twee instanties is dan ook in dat licht bezien onjuist. De opmerking dat de introductie van een rechtsgang bij de Afdeling bestuursrechtspraak niet goed te rijmen zou zijn met de positieve recensie van het functioneren van de TIB, doet niet af aan de conclusie van de ECW – die wij delen – dat het bestaande stelsel een weeffout bevat en die door de beroepsgang wordt hersteld. Ook daar zijn wij reeds uitvoerig op ingegaan. Voor het overige verwijzen wij deze leden graag naar de uitgebrachte Hoofdlijnennotitie.

6. Gevolgen verbonden aan de uitvoering van de wet

6.1 Algemeen

De leden van de Volt-fractie vragen wat de geschatte kosten zijn voor de uitvoering van de Tijdelijke wet en of er voldoende kosten zijn begroot om deze wet uit te voeren. Het is moeilijk in te schatten wat de kosten aangaande de uitvoering van de implementatie van de Tijdelijke wet zullen zijn. Zo hebben de diensten inmiddels de capaciteit vergroot. De Algemene Rekenkamer concludeerde dat dit bij aanvang van de implementatie van de Wiv 2017 niet het geval was. Deze situatie is nu anders en de diensten zijn daardoor beter voorbereid op de implementatie. De Tijdelijke wet heeft bovendien prioriteit bij de diensten waardoor hiervoor middelen vrijgemaakt zullen worden. Gezien de geleerde lessen van de implementatie van de Wiv 2017 en de daarop genomen acties zijn de diensten financieel voldoende voorbereid op de implementatie van de Tijdelijk wet.

6.2 De uitvoeringsconsequenties voor de TIB, de CTIVD en de Afdeling bestuursrechtspraak van de Raad van State

De leden van de D66-fractie merken op dat doordat een deel van het toezicht verschuift meer inspanning wordt gevraagd van de CTIVD. Zij vragen of de regering aan kan geven of de verwachte toename in

werkdruk bij de CTIVD niet tot problemen bij de implementatie van onderliggend wetsvoorstel zal leiden. Ook vragen zij of de CTIVD voldoende capaciteiten heeft en of hier op voorhand rekening mee is gehouden en, zo ja, in welke mate wordt verwacht dat de capaciteit toe zal nemen in vergelijking met voorgaande jaren onder de Wiv 2017. In overleg met de voorzitter van de CTIVD is besloten om vooruitlopend op de inwerkingtreding van de Tijdelijke wet de formatie van het secretariaat van de CTIVD met 10 FTE uit te breiden van 16,89 FTE naar 26,89 FTE. De CTIVD heeft hierover in haar reactie op de nota van wijziging op de Tijdelijk wet het volgende geschreven: «De CTIVD gaat er vanuit dat de uitbreiding van haar taken zoals geregeld in de ontwerpnota van wijziging kan worden gerealiseerd met de extra formatie waarvoor de CTIVD nu de vacatures aan het invullen is (10 fte).»

De leden van de SP-fractie willen de regering vragen om een oordeel over de werkwijze van de TIB. Zij stellen in dat verband de vraag of de regering die als zorgvuldig en integer beoordeelt. Vervolgens stellen deze leden diverse vragen omtrent het feit dat er in het jaarverslag van de TIB is gelakt. Allereerst willen wij opmerken dat wij er geen twijfel over hebben dat de TIB op een zorgvuldige en integere wijze werkt. Dat is ook bij de kwestie rond het jaarverslag van de TIB niet aan de orde. Het is zowel voor de diensten als de TIB en de CTIVD een wettelijke verplichting om jaarlijks een openbaar verslag uit te brengen over de wijze waarop de respectievelijke organisaties hun taken in het voorafgaande jaar hebben verricht. Hiermee kan de maatschappij kennis nemen van het werk van de diensten en van de wijze waarop de TIB en CTIVD de aan hen bij de wet opgedragen taken in het verslagjaar hebben vervuld. Ook de diensten maken ieder jaar een jaarverslag. Zo ontstaat er een breed en openbaar beeld van het functioneren van het stelsel van inlichtingen- en veiligheidsdiensten in Nederland en het toezicht daarop. Er zijn door de wetgever wel enkele beperkingen opgelegd aan deze openbare verslaglegging in het belang van de nationale veiligheid. Zo moeten de gegevens die zicht geven op de door de diensten aangewende midden in concrete aangelegenheden, de door de diensten gebruikte geheime bronnen en het actuele kennisniveau van de diensten achterwege blijven. Om parlementaire controle ook op deze – niet openbare – aspecten van het werk van de diensten mogelijk te maken, zijn deze gegevens wel vertrouwelijk met de Kamer gedeeld via de daartoe geëigende kanalen. Het openbaar verslag doen van het werk van de diensten en het toezicht daarop is een groot goed. In het jaarverslag van de TIB over het kalenderjaar 2021 en 2022 zijn enkele zinsneden door de TIB zwartgelakt omdat deze teveel zicht geven op de gegevens zoals hierboven genoemd. Dat het zwartlakken van deze passages door de regering zou zijn gebeurd, lijkt te berusten op een misverstand. De TIB is onafhankelijk en bepaalt zelf wat zij middels haar jaarverslag wel of niet openbaar maakt, maar dient daarbij uiteraard wel de hiervoor aangegeven wettelijke beperkingen in acht te nemen. Het ontwerpjaarverslag is – hoewel niet wettelijk verplicht – voor een zogeheten check op mogelijke staatsgeheime informatie aan de verantwoordelijke Ministers voorgelegd. De diensthoofden worden aldus in de gelegenheid gesteld om – vanuit de op hen berustende zorgplicht ex artikel 23 en 24 Wiv 2017 – aan te geven of het jaarverslag gerubriceerde gegevens bevat. Naar aanleiding daarvan is gewezen op enkele passages die naar ons oordeel staatsgeheime informatie bevatten. Het betreffen hier passages die zicht geven op de door de diensten aangewende middelen in concrete aangelegenheden, de door de diensten gebruikte geheime bronnen en het actuele kennisniveau van de diensten. De TIB heeft dan een aantal mogelijkheden. Zij kan ervoor kiezen om – nu zij meent dat het geen staatsgeheime informatie betreft – deze toch openbaar te maken. Dat zou naar ons oordeel schade voor de nationale veiligheid hebben opgeleverd met alle gevolgen van dien en wij zijn de

TIB dan ook erkentelijk voor het feit dat dit niet heeft plaatsgevonden. Het stond en staat de TIB echter vrij om de desbetreffende passages zodanig te formuleren dat de nationale veiligheid niet wordt geraakt. Daar heeft zij om haar moverende redenen echter niet voor gekozen en heeft deze passages zwart gelakt. Dat is een beslissing die bij de TIB rust.

De leden van de SP-fractie geven aan geschrokken te zijn van het feit dat de TIB zowel in het jaarverslag als in de technische briefing geen inzicht mag geven over de schaal van gegevens verzameling door de diensten. Zij vragen hoe Kamerleden de proportionaliteit van dit wetsvoorstel kunnen toetsen als zij niet kunnen vergelijken wat de situatie mét en zonder dit wetsvoorstel precies oplevert.

De situatie mét en zonder wetsvoorstel is wel met elkaar te vergelijken. Het ECW rapport en het rapport van de Algemene Rekenkamer laten zien wat de huidige situatie onder de Wiv 2017 is. De reikwijdte van dit wetsvoorstel is in volle omvang te bespreken en te toetsen zonder de nationale veiligheid te raken. Maar vanwege de nationale veiligheid zijn er enkele wettelijke randvoorwaarden die zowel voor de diensten als de TIB en CTIVD gelden. Voorbeelden uit de praktijk zijn bijvoorbeeld vaak staatsgeheime informatie en kan er van lopende operaties in het openbaar niet veel naar buiten gebracht worden.

De leden van de SP-fractie stellen vast dat de diensten geen blad voor de mond nemen en geen argument schuwen – ook onjuiste argumenten – om de Kamerleden en de samenleving te imponeren voor dit wetsvoorstel te zijn en deze leden vinden het de mond snoeren van de toetsingscommissie daarmee in bitter schril contrast staan. Zij vragen of de regering kan aangeven waarom zij dit wenselijk vindt en waarom men deze informatie-onbalans acceptabel vindt. Wij herkennen ons volstrekt niet in het beeld dat deze leden schetsen. Voor zover het gaat om de TIB en de kwestie van het lakken, zijn wij hiervoor in antwoord op vragen van deze leden uitvoering ingegaan. Het lakken is een autonome keuze van de TIB geweest. Voor het overige staat het eenieder vrij om zich in het openbaar uit te spreken over de werkwijze van de diensten, waarbij wel voorkomen moet worden dat zeker degenen die vanuit hun functie kennis dragen van staatsgeheime informatie ervoor zorgen dat deze niet wordt geopenbaard. Dat onze argumenten door sommigen niet worden gedeeld, en dat men daar andere argumenten tegenover stelt, is in onze democratie gelukkig mogelijk. Dat bevordert een open debat. Voor het overige zien we niet in waar de informatie-onbalans waar deze leden op doelen, uit zou bestaan.

De leden van de SP-fractie vinden de route voor geschilbeslechting bij de Raad van State ongewenst omdat hiermee de uitleg van de wet niet democratisch maar juridisch (bestuursrechtelijk) wordt ingevuld. Een geschil tussen de diensten en de toezichthouders hoeft geenszins een bestuurlijke aangelegenheid te zijn maar kan een fundamentele mensenrechtenkwestie behelzen. Als dit dan achter gesloten deuren bedisseld wordt door de bestuursrechter, met hooguit een geheime notificatie aan de commissie stiekem, dan zijn de democratische waarborgen van toezicht op de diensten – waar het kan zo transparant mogelijk – totaal ondermijnd. Hiermee kunnen de diensten namelijk aan grensverkenning doen (onderzoeken wat de grenzen van de wet zijn) zonder dat het parlement, of de samenleving, daar enige kennis van heeft. Gegeven het feit dat de diensten logischerwijs vaker dan andere uitvoeringsdiensten in vertrouwen handelen, hoort niet te betekenen dat het toezicht en democratische controle moet worden ondermijnd. Zij vragen hoe de regering dit ziet. Wij beantwoorden deze vraag als volgt. In de memorie van toelichting is uitvoerig uiteengezet waarom in het wetsvoorstel – in navolging van hetgeen de ECW heeft aanbevolen – een beroepsprocedure

bij de Afdeling bestuursrechtspraak wordt opengesteld tegen specifiek aangewezen oordelen van de TIB als van de afdeling toezicht van de CTIVD. Dat zijn geen geschillen omtrent bestuurlijke aangelegenheden maar om rechtsgeschillen, immers zowel TIB als de afdeling toezicht van de CTIVD beoordelen de rechtmatigheid van de (besluiten en handelingen ter) uitvoering van de wet. En daar kunnen fundamentele mensenrechtenkwesties aan de orde zijn. De ECW heeft geconstateerd dat de uitleg van wettelijke begrippen, de invulling van de toetsingsnormen en de intensiteit van de toetsing bij uitstek een rechterlijke taak is, waarbij de toezichthouders (TIB en CTIVD), gegeven de rechterlijke overwegingen, gaan over de toepassing in concrete gevallen. [88] Het is in een rechtstaat als de onze volstrekt normaal dat geschillen omtrent de uitleg van wettelijke bepalingen aan een rechter worden voorgelegd en voor de geschillen waarop de in het wetsvoorstel opgenomen beroepsregeling betrekking heeft ligt het voor de hand daarvoor de Afdeling bestuursrechtspraak (in eerste en enige instantie) als beroepsinstantie aan te wijzen. De Wiv 2017 en ook hetgeen in onderhavig wetsvoorstel wordt geregeld is immers (bijzonder) bestuursrecht en dan ligt een gang naar de bestuursrechter in de rede. De aan de Afdeling bestuursrechtspraak voor te leggen geschillen zijn naar hun aard vertrouwelijk van aard, immers het gaat om kwesties inzake de nationale veiligheid, waarin staatsgeheime informatie aan de orde komt, hetgeen grenzen stelt aan de openbaarheid van de procedure en aan de openbaarheid van de uitspraak. Dat is niet wezenlijk anders bij de uitoefening van de taak door de TIB en door de CTIVD: ook daar gaat het om kwesties inzake de nationale veiligheid, is staatsgeheime informatie aan de orde, hetgeen grenzen stelt aan de openbaarheid van hun taakuitvoering en de mate waarin zij van hun werkzaamheden in het openbaar verslag kunnen uitbrengen. Parlementaire controle is en blijft in alle gevallen mogelijk: openbaar waar dat kan, gesloten waar dat moet.

De leden van de SP-fractie willen ten slotte graag van de regering weten of de TIB en de CTIVD voldoende capaciteit en werkplekken hebben, en hoeveel meer zij hebben voor hun toezichtstaken. Zij werken met staatsgeheime gegevens en houden live toezicht op de netwerken van de AIVD/MIVD. Hebben de toezichthouders, zo vragen deze leden, de (fysieke) mogelijkheid om dit werk goed uit te voeren. In overleg met de voorzitter van de CTIVD is besloten om vooruitlopend op de inwerkingtreding van de Tijdelijke wet de formatie met 10 FTE uit te breiden (zie ook antwoord 225). Voor de TIB geldt dat de formatie bestond uit 8,17 FTE en dat deze in het kader van de Tijdelijke wet in overleg met de voorzitter van de TIB met 3 FTE wordt uitgebreid. De werving voor deze extra capaciteit is momenteel gaande. Voor de CTIVD geldt dat het aantal werkplekken dient te worden uitgebreid. Hier wordt momenteel aan gewerkt. De TIB beschikt, ook na uitbreiding van het secretariaat, over voldoende werkplekken. Het gaat hierbij om werkplekken die voldoen aan de eisen om te werken met staatsgeheime informatie.

De leden van de GroenLinks-fractie constateren dat met het voorliggende wetsvoorstel zowel het werk als de werkbelasting voor zowel TIB, de CTIVD als voor de Afdeling bestuursrechtspraak van de Raad van State kan wijzigen. Zij vragen of de regering kan aangeven op welke wijze de TIB, de CTIVD en de Afdeling bestuursrechtspraak zich hierop voorbereiden en wat dit concreet betekent voor de personele bezetting bij de drie instanties. Wij verwijzen deze leden naar ons antwoord op een vergelijkbare vraag van de leden van de SP-fractie.

[88] Zie het rapport van de ECW, pag. 136.

De leden van de Volt-fractie vragen of de toezichthouders volgens de regering op dit moment inhoudelijk en qua capaciteit voorbereid zijn op de voorgenomen wijzigingen. Is er, aldus deze leden, voldoende expertise binnen de toezichthouders om effectief toezicht te houden op de voorgenomen maatregelen en zullen de toezichthouders tijdig in staat zijn om de Tijdelijke wet uit te voeren. Wij verwijzen deze leden graag naar de hiervoor door ons gegeven antwoorden op vergelijkbare vragen van de leden van de fracties van D66, SP en GroenLinks.

7. Advies en consultatie

7.1 Algemeen

De TIB is van mening dat omdat onder de voorliggende wet het mogelijk is dat alle verworven gegevens ook worden bekeken door teams met andere onderzoeksopdrachten, dat een forse uitbreiding van de bevoegdheden van de diensten met zich meebrengt. De regering deelt die conclusie niet omdat de waarborgen van de Wiv 2017 hierbij van toepassing blijven. Daarin is immers al bepaald dat rechtmatig verworven gegevens ook voor andere lopende onderzoeken van de diensten mogen worden gebruikt. De leden van de PvdA-fractie zijn echter van mening dat juist omdat de voorliggende wet het toezicht vooraf voor een deel naar achter verschuift en het vereiste van gerichtheid vooraf verdwijnt, dat het brede gebruik van gegevens op basis van de Tijdelijke wet niet een op een vergelijkbaar is met de Wiv 2017. Deze leden vragen of de regering de mening deelt dat het voor het breder gebruiken van gegevens op basis van de Tijdelijke wet verworven extra waarborgen nodig zijn. Allereerst willen we opmerken dat slechts in twee situaties de toets vooraf door de TIB komt te vervallen, namelijk bij de bevoegdheid tot het verkennen van geautomatiseerde werken en bij geautomatiseerde data-analyse op met OOG-interceptie verworven metadata. In beide gevallen gaat de afdeling toezicht van de CTIVD bindend toezicht houden. De TIB heeft in haar reactie op het ontwerpwetsvoorstel aangegeven zich in deze voorstellen te kunnen vinden. Dit staat overigens los van de vraag van deze leden inzake het breder gebruiken van de gegevens die op basis van de Tijdelijke wet zijn verworven en of daarvoor extra waarborgen nodig zijn. Zoals ook uit onze reactie op de opmerking ter zake van de TIB in haar reactie op het ontwerpwetsvoorstel blijkt (zie par. 7.2 van de memorie van toelichting) en door deze leden is aangehaald, zijn wij niet van mening dat er extra waarborgen nodig zijn. We lichten dit graag toe. Bij het onderzoek van de diensten naar landen met een offensief cyberprogramma is de Wiv 2017 van toepassing, zij het dat de Tijdelijke wet deels in aanvullingen op en deels in afwijkingen van een beperkt aantal bepalingen in de Wiv 2017 voorziet. De verwerving en de verdere verwerking van gegevens door de diensten geschiedt gewoon onder toepassing van de regeling in de Wiv 2017. En in lijn met hetgeen onder de Wiv 2017 geldt, komen de gegevens die in het onderzoek naar landen met een offensief cyberprogramma worden verworven ook beschikbaar voor de andere lopende inlichtingenonderzoeken van de diensten. Waar het gaat om de in artikel 6 van het wetsvoorstel opgenomen bevoegdheid tot verkennen met het oog op de toepassing van de bevoegdheid tot OOG-interceptie is bepaald dat de daarmee verkregen gegevens juist niet ter beschikking van de inlichtingenonderzoeken. Dus daar is breder gebruik sowieso niet aan de orde. In het wetsvoorstel is, zoals gezegd, ten opzichte van een beperkt aantal in de Wiv 2017 geregelde bijzondere bevoegdheden voorzien in aanvulling van de – veelal reeds bestaande – bijschrijfmogelijkheden. Deze mogelijkheden zijn alleen aanwezig indien de bijzondere bevoegdheid waarop de aanvulling betrekking heeft, reeds onder toepassing van de Wiv 2017 – en dus met inachtneming van de daaraan in de Wiv 2017 verbonden waarborgen – door de diensten wordt ingezet. Behoudens artikel 6

(verkennen ten behoeve van OOG-interceptie) schept de Tijdelijke wet dus geen nieuwe zelfstandige bijzondere bevoegdheden. Overigens is er wel anderszins sprake van extra waarborgen, omdat – naast de twee genoemde situaties waar de voorafgaande toets door de TIB komt te vervallen – de in het wetsvoorstel voorziene aanvullingen van de bijschrijfmogelijkheid worden onderworpen aan bindend toezicht door de afdeling toezicht van de CTIVD.

7.2 De reactie van de TIB

De leden van de D66-fractie memoreren dat in het rondetafelgesprek met de Kamer de TIB aangaf dat zij de Kamer graag hadden ingelicht over de bevoegdheden die de inlichtingendiensten reeds hebben en dat tot spijt van de TIB de passages daarover niet publiceerbaar waren. De leden van de D66-fractie vragen of de regering de leden van deze commissie op een andere manier vertrouwelijk kan informeren. De bevoegdheden die de diensten hebben staan in de Wiv 2017 en zijn voor een ieder kenbaar. Wat niet openbaar is informatie over deze bevoegdheden voor zover daarmee zicht wordt gegeven op de door de diensten aangewende middelen in concrete aangelegenheden, de door de diensten gebruikte geheime bronnen en het actuele kennisniveau van de diensten. Dat is staatsgeheime informatie. Dergelijke informatie kan vertrouwelijk met de Kamer worden gedeeld, maar uitsluitend met de door de Tweede Kamer daartoe ingestelde Commissie voor de Inlichtingen- en Veiligheidsdiensten.

De leden van de GroenLinks-fractie constateren dat de laatste tijd veel discussie is geweest over de vraag of het toezicht door de TIB in het voorliggende wetsvoorstel wel effectief blijft. In deze discussie hebben zowel de huidige TIB als voormalige leden van de TIB zich gemengd. Deze leden vragen aan de regering hoe zij terugkijkt op deze discussie en op hoe de TIB betrokken is geweest bij de totstandkoming van het voorliggende wetsvoorstel. Wat had de regering terugkijkend anders kunnen doen om te voorkomen dat er onrust zou ontstaan over het uitgeklede toezicht door de TIB, zo vragen deze leden. Allereerst is het goed om te benadrukken dat het toezicht door de TIB niet wordt uitgekleed en effectief blijft. Voor zover in het wetsvoorstel sprake is van beperking van de toetstaak van de TIB wordt dat vervangen door bindend toezicht door de afdeling toezicht van de CTIVD. In de memorie van toelichting is dit naar ons oordeel adequaat toegelicht. Waar het gaat om de gerezen onduidelijkheid inzake de door de TIB uit te voeren proportionaliteitstoetsing hebben wij die zowel mondeling als schriftelijk weggenomen. De brief die we aan de voorzitter van de TIB hebben gezonden is ook in afschrift aan de Kamer toegezonden. Ook wij hebben kennisgenomen van het verschil in perceptie dat bestaat tussen de voormalige technische leden van de TIB. Voor het overige geldt dat zowel de TIB als CTIVD vanaf de start van de voorbereiding van de Tijdelijke wet nauw bij het wetgevingsproces zijn betrokken. Het wetsvoorstel is zowel formeel als informeel ter consultatie aangeboden aan de TIB en CTIVD. Daarnaast hebben meerdere overleggen en ketentesten plaatsgevonden, mét de TIB, CTIVD en de Afdeling bestuursrechtspraak van de Raad van State.

7.3 Overige reacties (burgers en NGO's)

De leden van de GroenLinks-fractie hechten veel waarde aan breed draagvlak in de samenleving voor het werk van de veiligheidsdiensten. Om een stevig draagvlak in stand te houden en zo mogelijk te vergroten vinden deze leden het daarom van belang dat de regering en de diensten zelf zoveel als mogelijk is aan de samenleving communiceren op welke wijze de rechten van burgers zo goed mogelijk worden beschermd. Zij vragen op welke wijze gaat de regering ervoor gaat zorgen dat het

draagvlak voor het werk van de diensten wordt versterkt. Wij zijn het met deze leden eens dat het voor het werk dat de AIVD en MIVD in het kader van onze nationale veiligheid verrichten een breed draagvlak in de samenleving wenselijk is. Een belangrijk instrument om draagvlak te verwerven en te behouden is, zoals deze leden terecht aangeven, communicatie. Hoewel de diensten de laatste jaren al veel meer openheid betrachten over het werk dat ze verrichten, niet allen door optredens van de diensthoofden in de media maar ook door gebruikmaking van sociale mediakanalen en publicaties over uiteenlopende onderwerpen, kan het nuttig zijn om te verkennen of ook anderszins mogelijkheden bestaan om de diverse aspecten van het – veelal geheime – werk van de diensten voor een breder publiek toegankelijk te maken.

II. Artikelsgewijze toelichting

De leden van de GroenLinks-fractie hebben nog enkele specifieke vragen bij enkele artikelen.

Artikel 2

Deze leden vragen wanneer de diensten voldoende aanwijzingen en gronden hebben om van een vermoeden te spreken. Het attribueren van een digitale aanval aan een specifiek land vergt soms veel onderzoek. Dit heeft onder meer te maken met het feit dat er bij cyberaanvallen gebruik wordt gemaakt van een groot aantal verschillende tussenstappen, waarbij diverse partijen verspreidt over verschillende landen betrokken kunnen zijn. Vermoedens over de betrokkenheid van statelijke actoren zijn gebaseerd zijn op een groot aantal verschillende factoren. Denk hierbij aan de gebruikte aanvalsinfrastructuur, de modus operandi en de gekozen slachtoffers. Bij de inzet van bijzondere bevoegdheden worden de vermoedens concreet onderbouwd op basis van inlichtingen. Deze aanvragen voor de inzet van bijzondere bevoegdheden worden op rechtmatigheid getoetst door de TIB.

Voorts vragen deze leden of de regering in het kader van dit artikel ook in kan gaan hoe voorkomen wordt dat meerdere wettelijke regimes tot onduidelijkheid leidt. Wij zijn aan het begin van onderdeel I (algemeen) van deze nota naar aanleiding van het verslag ingegaan op vragen van de leden van de SP-fractie inzake onder meer de wenselijkheid met het werken met twee verschillende toezichtsregimes. Wij zouden deze leden allereerst naar hetgeen wij in reactie op die vragen hebben gesteld willen verwijzen. In aanvulling daarop merken we op dat juist door de regeling dat een verzoek om toestemming voor de inzet van een bijzondere bevoegdheid aangegeven moet worden of de Tijdelijke wet van toepassing is, het van meet af aan duidelijk is dat de in de Tijdelijke wet opgenomen voorzieningen – in aanvulling dan wel in afwijking van de Wiv 2017 – van toepassing is. Indien het gaat om een toestemming die onderworpen is aan de rechtmatigheidstoets van de TIB kan zij ter zake bindend oordelen dat de Tijdelijke wet niet van toepassing is en dient de Minister hiervan terstond op de hoogte te worden gesteld. Op dat moment is duidelijk dat uitsluitend de Wiv 2017 van toepassing is; wel kan tegen het oordeel van de TIB beroep bij de Afdeling bestuursrechtspraak worden ingesteld en indien de Afdeling het beroep gegrond acht staat de Afdeling op grond van artikel 13 diverse mogelijkheden ter beschikking ter effectuering van dat oordeel.

Artikel 4

De regering schrijft dat het verschuiven van het toezicht gevolgen kan hebben voor de proportionaliteitstoets. Kan de regering dit nader toelichten en hierbij concrete (fictieve) voorbeelden geven? In paragraaf 3.2 van deze nota naar aanleiding van het verslag zijn wij aan het slot ingegaan op een vergelijkbare vraag van de leden van de Volt-fractie. Wij verwijzen deze leden graag naar hetgeen we daar hebben gesteld.

Artikel 6

De leden van de GroenLinks-fractie ontvangen graag een nadere toelichting op de stelling dat een bovengrens van de bruikbaarheid zes maanden is. Ook vragen zij ten aanzien van dit artikel op welke wijze de TIB volgens de regering het afgenomen gerichtheidscriterium betrekt bij de toetsing aan proportionaliteit. De diensten moeten (een deel van) de gegevens die zij in het kader van de in artikel 6 geregelde verkenningsbevoegdheid hebben verworven zes maanden kunnen bewaren om de geïntercepteerde gegevensstromen goed te kunnen beoordelen op bruikbaarheid voor het doel waarvoor deze zijn verworven. Dat doel is om te komen tot een zo gericht mogelijk inzet van OOG-interceptie voor inlichtingendoeleinden. Een termijn van zes maanden is, gelet op de praktijkervaring bij de diensten met deze werkwijze, daarvoor voldoende. Omdat, zoals in de memorie van toelichting en in deze nota naar aanleiding van het verslag in reactie op vragen ter zake is uiteengezet, gelet op de aard van de bevoegdheid – verkennen – het gerichtheidscriterium hier niet van toepassing is, betekent dat ook dat dit criterium dus ook niet kan worden betrokken in een proportionaliteitstoets.

Artikel 12

De leden van de GroenLinks-fractie vragen de regering in het kader van dit artikel nader in te gaan op het feit dat dat het toezichtsstelsel complexer wordt. Op welke wijze, aldus deze leden, wordt voorkomen dat een complexer toezichtsstelsel zorgt voor vertraging van de operationele snelheid. Wij antwoorden graag als volgt. Ook de leden van de SGP-fractie hebben eerder gewezen op de constatering van de Afdeling advisering dat het stelsel van toezicht in complexiteit toeneemt. Zoals wij in reactie op hun vragen ter zake hebben aangegeven, hebben wij van die zorgen kennisgenomen, maar ook van het feit dat de Afdeling – gelet op de dreiging die thans uitgaat van landen met een offensief cyberprogramma – het niettemin begrijpelijk acht dat, vooruitlopend op een definitieve wetswijziging, een aangepast regime voor een beperkt deel van de taken en bevoegdheden wordt beproefd. Van belang is daarbij, aldus de Afdeling advisering, dat veel van de in onderhavig wetsvoorstel gekozen oplossingen corresponderen met de aanbevelingen van de ECW. Het bindend toezicht dat door de afdeling toezicht van de CTIVD zal worden uitgeoefend, is overigens niet aanbevolen door de ECW. Niettemin hebben wij ervoor gekozen die wel in het wetsvoorstel op te nemen. Zoals we ook uiteen hebben gezet in de memorie van toelichting, is bij de uitwerking van de maatregelen in het wetsvoorstel bezien in hoeverre het stelsel van waarborgen zoals neergelegd in de Wiv 2017 wordt geraakt en hoe aan het totaal aan waarborgen kwalitatief bezien geen afbreuk wordt gedaan. Deze afweging heeft ertoe geleid dat waar de bindende toets door de TIB komt te vervallen ervoor is gekozen deze te compenseren met een bindende oordeelsbevoegdheid van de afdeling toezicht. Voorts is bezien in welke fase van de inzet van een bijzondere bevoegdheid welke vorm van toezicht (ex ante dan wel ex durante) het meest effectief is. Naast voornoemde compensatie van de ex ante toets door bindend ex durante toezicht is ook de toepassing van de in het

wetsvoorstel voorziene bijschrijfmogelijkheden van de diensten onderworpen aan het bindend toezicht van de afdeling toezicht van de CTIVD. Wij achten het van belang dat er sprake zal zijn van een balans tussen enerzijds de verbetering van de mogelijkheden voor de diensten om onderzoek te doen naar dreigingen vanuit landen met een offensief cyberprogramma en anderzijds te voorzien in adequaat en effectief toezicht daarop. We erkennen dat er tijdelijk twee stelsels, ook waar het gaat om toezicht, naast elkaar bestaan. Maar zoals eerder in deze nota naar aanleiding van het verslag is uiteengezet, is dit vanuit het perspectief van de diensten werkbaar. Voor zover dit tot vertraging leidt van de operationele snelheid is die vertraging naar ons oordeel acceptabel. Overeenkomstig het advies van de Afdeling advisering zullen de ervaringen met de voorgestelde maatregelen worden gemonitord, waarbij uiteraard ook aandacht zal zijn voor de effecten van het bindend toezicht op de taakuitvoering van de diensten, en die zullen vervolgens worden betrokken bij de herziening van de Wiv 2017.

Artikel 17

De leden van de GroenLinks-fractie vragen ten slotte of de regering in het kader van dit artikel kan aangeven wat de concrete planning is voor het algeheel herzien en evalueren van de Wiv 2017. Gelijktijdig met deze nota naar aanleiding van het verslag wordt aan de Tweede Kamer de Hoofdlijnennotitie aangeboden. De Hoofdlijnennotitie geeft richting aan de algehele herziening van de Wiv 2017. Na bespreking van de Hoofdlijnennotitie met de Tweede Kamer zal begonnen worden met het opstellen van het wetsvoorstel tot herziening van de Wiv 2017. Het herzieningstraject zal naar zijn aard omvangrijk zijn en meer voorbereidingstijd vragen dan het traject van de Tijdelijke wet. Niettemin menen wij dat de herziening voor afloop van de voorgestelde werkingsduur van de Tijdelijke wet, te weten vier jaar, kan worden gerealiseerd. De met de toepassing van de Tijdelijke wet opgedane ervaringen zullen waar mogelijk bij de herziening worden betrokken. Bovendien zal er blijvend worden ingespeeld op Europeesrechtelijke en technologische ontwikkelingen (zoals rondom *Artificial Intelligence*). De voortvarendheid van het wetstraject is afhankelijk van verschillende factoren en randvoorwaarden, waarop waar nodig en mogelijk wordt gestuurd.

Deze nota naar aanleiding van het verslag wordt mede-ondertekend door de Minister van Defensie.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
H.G.J. Bruins Slot