MEMORIE VAN TOELICHTING

I. Algemeen deel

1. Inleiding

Nederland en Nederlandse belangen worden in toenemende mate geconfronteerd met massieve dreigingen in het digitale domein, ook wel het cyberdomein.[1] Het gaat hierbij om dreigingen vanuit diverse landen met een offensief cyberprogramma. Voorbeelden van dergelijke landen zijn met name Rusland en China. Een offensief cyberprogramma is er onder meer op gericht om langs digitale weg op heimelijke wijze de beschikking te verkrijgen over vertrouwelijke informatie, economische en technologische kennis of andere informatie van burgers of organisaties waarmee zij hun voordeel doen. Ook kan de hoogwaardige Nederlandse cyberinfrastructuur worden misbruikt bij het uitvoeren van cyberaanvallen op andere landen. Nederland is hierbij bij uitstek in het vizier vanwege het feit dat Nederland in het wereldwijde communicatienetwerk een belangrijk knooppunt is. Daarnaast wordt het cyberdomein door landen ook gebruikt voor het verspreiden van desinformatie en voor het verstoren en vernielen van technische infrastructuur, onder meer bij vitale sectoren. De hier bedoelde acties van landen moeten los gezien worden van de eveneens schadelijke, maar meer met een crimineel oogmerk verrichte digitale aanvallen, die bijvoorbeeld gericht zijn op het verkrijgen van losgeld (aanvallen met ransom-ware).

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. Dergelijke operaties vormen ook onderdeel van een militaire strategie. Dit wordt onderschreven door de recente cyberaanvallen op de overheidssystemen in Oekraïne. Deze aanvallen raken de burger, de bedrijven en instellingen en ook onze nationale veiligheid.

Het is evident dat de uitvoering van dergelijke offensieve cyberprogramma's veel schade kunnen toebrengen Nederland of Nederlandse belangen. Ter illustratie daarvan dienen de volgende voorbeelden.

> *De afgelopen jaren hebben zich in of in relatie tot Nederland talloze cyberincidenten voorgedaan, met zowel een moedwillige als een niet-moedwillige oorzaak. Zo werd in december 2020 het Europees Geneesmiddelenbureau (EMA) doelwit van een hack&leak aanval. Het bureau werkte op dat moment aan de goedkeuring van twee COVID-19 vaccins. Eind december 2020 verschenen delen van EMA-documenten op webfora. De gelekte bestanden waren deels gewijzigd en voorzien van commentaar en context waardoor het moest lijken alsof er sprake was van frauduleus onderzoek door het EMA. Ook was e-mailconversatie aangepast waarbij de indruk werd gewekt dat EU-autoriteiten het EMA onder druk hebben willen zetten om vaccins versneld goed te keuren. Op deze manier kunnen door hacks niet alleen inlichtingen*

[1] Jaarverslag Algemene Inlichtingen en Veiligheidsdienst 2020, Hoofdstuk 2 Internationale dreigingen en politieke veiligheidsbelangen, pagina 8 – 10, Jaarverslag Militaire Inlichtingen en Veiligheidsdienst 2020, Hoofdstuk 1 Inlichtingen en Veiligheid voor Nederland, pagina 7 – 11 en Cybersecuritybeeld Nederland 2021.

ingewonnen worden, maar wordt er ook desinformatie gedeeld. Het delen van desinformatie, oftewel nepnieuws, kan leiden tot ontwrichtingen binnen de maatschappij.

In december 2020 werd bekend dat aanvallers een kwetsbaarheid hadden aangebracht in een update van Orion-software van SolarWinds. Dit bedrijf maakt softwareprogramma's voor overheidsinstanties en grote bedrijven om ICT-omgevingen te monitoren en beheren. Doordat gebruikers van Orion-software onbewust een kwetsbare update uitvoerden kregen de aanvallers stilletjes toegang tot vele bedrijven en overheidsinstanties. Deze toegang kunnen aanvallers misbruiken om vervolgens digitale spionage bij de kwetsbare organisaties uit te voeren. Ook in Nederland werd de kwetsbare update van Orion-software geïnstalleerd, onder andere binnen de overheid en vitale processen. In april 2021 werd de SolarWinds campagne door de VS geattribueerd aan de Russische inlichtingendienst SVR (APT29). Deze attributie werd ondersteund door de EU en de Nederlandse regering.
Nederland hoort bij de meest ontwikkelde landen ter wereld op het gebied van economie, wetenschap en techniek en is daarmee een doelwit voor andere staten. China is op dat vlak de grootste bedreiging. De meeste (digitale) spionage door China is erop gericht de eigen economie te laten groeien en het verkrijgen van kennis en technologie in onder andere de semiconductorindustrie (bijvoorbeeld de productie van microchips), militaire- en dual-use technologie, de telecomsector, bio-farmaceutica en biotechnologie.

Ook blijkt uit onderzoek van de diensten dat Iraanse hackers probeerden intellectueel eigendom te stelen van Nederlandse universiteiten. Als de exclusiviteit van intellectueel eigendom verloren gaat en hierdoor bepaalde investeringen of overnames niet doorgaan, kan dit de Nederlandse economie bedreigen.

De mogelijkheden voor digitale spionage door statelijke actoren zijn dankzij sterke afhankelijkheid van thuiswerken aanzienlijk toegenomen. Omdat veel mensen thuiswerken, zijn veel bedrijven afhankelijker van software waarmee werknemers op afstand kunnen inloggen op het bedrijfsnetwerk. Diverse statelijke actoren misbruiken de coronacrisis om (spear)phishingmails te versturen. Dit zijn e-mails die onjuiste informatie bevatten over het coronavirus en het slachtoffer proberen te verleiden de mail te openen of op een link te klikken. Hierdoor kan de actor toegang krijgen tot het netwerk van het slachtoffer en zo data stelen of malware installeren.

Een onderdeel van een offensief cyberprogramma kan het inwinnen van politieke inlichtingen zijn om zo de democratische rechtsorde in andere landen te ondermijnen en politieke processen te beïnvloeden. Zo heeft de Russische militaire inlichtingendienst (GRU) op online mediaplatforms desinformatie verspreid over het neerhalen van vlucht MH17 en hebben ze hiermee het beeld proberen te kleuren dat mensen hebben van het neerhalen van vlucht MH17 boven Oekraïne in 2014. Zo wordt geprobeerd het beeld te laten ontstaan dat Oekraïne meer blaam treft dan het krijgt en dat het land het luchtruim volledig had moeten sluiten. Zo kan heimelijke beïnvloeding soms gepaard gaan met openlijke propaganda. De diensten spelen een

rol in het kunnen attribueren van de herkomst van dergelijke desinformatie en de duiding ervan.

China probeerde in Nederland en elders beeldvorming te beïnvloeden rond het coronavirus. Dat deed het land met propagenda, die in de loop van het jaar offensief werd: uitingen prezen de Chinese aanpak, en zaaiden twijfel over de oorsprong van het virus en de aanpak van Europese landen.

Ook binnen geopolitieke en militaire conflicten krijgen digitale spionage, sabotage en beïnvloedingscampagnes een steeds belangrijkere rol. Zo heeft de Russische krijgsmacht gedurende het conflict met Georgië in augustus 2008 verschillende maatschappij ontwrichtende digitale aanvallen uitgevoerd tegen de Georgische overheid ter ondersteuning van haar militaire invasie. Bovendien is Oekraïne sinds de annexatie van de Krim door Rusland in 2014 veelvuldig slachtoffer geweest van digitale spionage en sabotagecampagnes. Hierbij heeft de digitale sabotage campagne met NotPetya malware in juni 2017 zelfs verstrekkende gevolgen voor Nederland en Europa. Ook rondom het interstatelijke conflict tussen Rusland en Oekraïne worden verschillende digitale spionage en sabotage campagnes waargenomen. Verder wordt er middels verschillende digitale beïnvloedingscampagnes geprobeerd de beeldvorming omtrent militaire samenwerkingsverbanden te beïnvloeden. Zo zijn in 2021 verschillende digitale beïnvloedingscampagnes uitgevoerd die gericht waren op het in een kwaad daglicht stellen van de NAVO in de Baltische en Oost-Europese staten.

Op grond van de Wiv 2017 hebben de twee Nederlandse inlichtingen- en veiligheidsdiensten, te weten de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), de taak om, waar de nationale veiligheid in het geding is, daar onderzoek naar te doen en waar nodig daar actie op te ondernemen. Vanzelfsprekend gebeurt dit uitsluitend op basis van de wet en voorzien van gepaste waarborgen. Het verrichten van onderzoek naar landen met een offensief cyberprogramma is in de Geïntegreerde Aanwijzing (GA) nadrukkelijk als een onderzoeksopdracht voor beide diensten geformuleerd. Op grond van de Wiv 2017 komt beide diensten bij het verrichten van onderzoeken een ruim scala aan bevoegdheden toe, ook waar het gaat om onderzoeken als hier bedoeld. Met name de bijzondere bevoegdheden tot onderzoeksopdrachtgerichte interceptie (bulkinterceptie) en het verkennen en binnendringen van geautomatiseerde werken (hacken) zijn van onmisbare betekenis bij onderzoeken in het digitale domein. Echter: zonder een adequate inzet van deze bevoegdheden is het voor beide diensten moeilijk, en soms onmogelijk, om dergelijk onderzoek op effectieve wijze uit te voeren en daarmee zicht te krijgen op de intenties, capaciteiten en bewegingen van dergelijke landen. Dat levert evidente risico's op voor de nationale veiligheid. Dergelijke onderzoeken vragen namelijk het combineren van resultaten die zijn verkregen uit de inzet van verschillende bevoegdheden.

In de afgelopen periode, met name sinds de inwerkingtreding van de Wiv 2017, is gebleken dat om uiteenlopende redenen een adequate inzet van genoemde bevoegdheden, waarbij met name de onderzoeksopdrachtgerichte interceptie op de kabelgebonden infrastructuur van cruciale betekenis is, niet kan worden gerealiseerd. Deels leidt dit ertoe dat onderzoeken

niet kunnen worden gestart of worden voortgezet, deels dat de voor dergelijke onderzoeken noodzakelijke wendbaarheid en snelheid niet kan worden bewerkstelligd. In het onderstaande zal daar nader op in gegaan worden. Daaraan voorafgaand is echter in meer algemene zin het volgende op te merken.

Onderzoeken van inlichtingen- en veiligheidsdiensten hebben, in ieder geval voor wat betreft de veiligheidstaak, van oudsher voornamelijk in het teken gestaan van het onderkennen van dreigingen met de focus op concrete targets (personen en organisaties). De zogeheten a-taak van de AIVD is daarvan een goede uitdrukking.[2] Al wat langer is echter die onderzoekstaak (ook) meer in het teken komen te staan van het onderkennen van verborgen dreigingen: je weet dat ze er moeten zijn, maar ze moeten nog aan het licht worden gebracht. Het is ook dit soort onderzoek – namelijk naar verborgen dreigingen – dat bij onderzoek in het cyberdomein van grote betekenis is. Onvoldoende is onderkend, ook bij de voorbereiding en totstandbrenging van de Wiv 2017, wat dit betekent voor de inzet van bijzondere bevoegdheden. Bij de Wiv 2017 is de targetgerichte benadering, ook waar het gaat om de toepassing van bijzondere bevoegdheden, de dominante benadering geweest. De gevolgen daarvan worden in de dagelijkse toepassingspraktijk gereflecteerd in de wijze waarop de wettelijk vastgelegde criteria, waaronder gerichtheid, worden ingevuld en worden getoetst. Onderzoek in het cyberdomein vergt echter een grotendeels andersoortige onderzoeksmethodiek, waar – bij de inzet van bijzondere bevoegdheden - ook een daarop afgestemde vorm van invulling van de hiervoor genoemde criteria aan de orde is. Een goed voorbeeld waarbij dit aan de orde is, betreft de toepassing van het gerichtheidscriterium bij de verwerving van gegevens via onderzoeksopdrachtgerichte interceptie (OOG-interceptie) op de kabelgebonden infrastructuur, waarbij gegevens in bulk worden verzameld. De hier bedoelde bevoegdheid is tot op heden slechts beperkt 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 Toetsingscommissie inzet bevoegdheden (TIB) nog niet tot een oplossing heeft geleid. Daardoor kunnen bepaalde onderzoeken in het cyberdomein nog niet worden opgestart.

Wendbaarheid en snelheid zijn essentieel bij onderzoeken in het cyberdomein. In het cyberdomein is het immers, in tegenstelling tot het fysieke domein, zeer eenvoudig om snel en vaak te wisselen van locatie, wereldwijd. Bij cyberaanvallen gebeurt dit bewust met als doel beveiligingsmaatregelen te doorbreken en om te verhullen waar de aanval vandaan komt. Het ene moment kan een computer of server in Nederland gebruikt worden en het andere moment kan voor hetzelfde doel een computer of server in Zuid-Amerika gebruikt worden. Het is van belang mee te kunnen bewegen met dergelijke veranderingen. De gewenste wendbaarheid en snelheid kan op dit moment echter niet worden gerealiseerd doordat bijvoorbeeld de mogelijkheden om bij de toepassing van bepaalde bevoegdheden

[2] Artikel 8, tweede lid, aanhef en onder a, Wiv 2017 luidt als volgt: De Algemene Inlichtingen- en Veiligheidsdienst heeft in het belang van de nationale veiligheid tot taak (a) het verrichten van onderzoek met betrekking tot organisaties en personen die door de doelen die zij nastreven, dan wel door hun activiteiten aanleiding geven tot het ernstig 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.

over te kunnen gaan tot “bijschrijving” onvoldoende helder in de wetgeving zijn neergelegd dan wel beperkend wordt uitgelegd.

Tegen deze achtergrond wordt het wenselijk geacht om in onderhavig wetsvoorstel, waar het gaat om onderzoeken naar landen met een offensief programma tegen Nederland of Nederlandse belangen, enkele wettelijke voorzieningen te treffen die de mogelijkheden tot effectieve inzet van de bijzondere bevoegdheden die voor dit soort onderzoek van cruciale betekenis zijn, te vergroten, waarbij tegelijkertijd de waarborgen waarmee die inzet moet zijn omgeven op een hoog niveau blijven.

Er is voor gekozen om een en ander in een afzonderlijk, op zichzelf staand wetsvoorstel neer te leggen in plaats van een voorstel tot wijziging van de Wiv 2017. Het doel van het onderhavige wetsvoorstel is het op korte termijn treffen van een tijdelijke voorziening om een beter antwoord te kunnen geven op bovengenoemd veiligheidsprobleem. Een definitieve regeling zal onderdeel uitmaken van het wetsvoorstel dat wordt voorbereid na het uitbrengen van de aan de Tweede Kamer toegezegde hoofdlijnennotitie ter zake van het door de ECW uitgebrachte rapport met betrekking tot de evaluatie van de Wiv 2017.

2. Inhoud van het wetsvoorstel op hoofdlijnen

2.1 Inleiding

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. Het gaat daarbij om maatregelen die ertoe bijdragen dat bepaalde in de Wiv 2017 neergelegde bijzondere bevoegdheden ook daadwerkelijk kunnen worden ingezet (zoals OOG-interceptie op de kabelgebonden infrastructuur) dan wel de inzet ervan op een effectievere wijze kan plaatsvinden (zoals het verkennen en binnendringen van geautomatiseerde werken). Daarnaast worden in het wetsvoorstel bestaande bijschrijfmogelijkheden aangevuld en bij een enkele bevoegdheid toegevoegd. Bij alle voorgestelde maatregelen geldt dat de thans geldende waarborgen voor de toepassing daarvan in totaliteit bezien dienen te worden gehandhaafd, maar dat er een betere aansluiting van de aard van het toezicht (ex ante of ex durante) bij de fase waarin de (voorgenomen) uitvoering van een bijzondere bevoegdheid zich bevindt wordt bewerkstelligd met als resultaat dat deze meer dan nu recht doet aan de dynamische praktijk van het cyberdomein. Dit geheel moet ertoe leiden dat de AIVD en de MIVD op een integrale wijze hun wettelijke taakopdracht met betrekking tot de dreigingen in het cyberdomein kunnen uitvoeren. Alvorens de verschillende voorgestelde wettelijke maatregelen te benoemen, zal eerst uiteengezet worden wat met een integrale werkwijze wordt bedoeld, teneinde de voorgestelde maatregelen van een operationele context te voorzien.

2.2 Integrale wijze van onderzoek in het cyberdomein en gegevensverwerking

2.2.1 De inzet van bijzondere bevoegdheden

De diensten doen onderzoek naar de doelwitten, intenties, capaciteiten en wijze van aansturing van landen met een offensief cyberprogramma. Om deze vragen te kunnen beantwoorden is het nodig om naar meer dan alleen de specifieke aanval 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 en politieke intenties van cyberaanvallen, maar ook op hun doelwitten en slachtoffers. De verschillende onderzoeken van de diensten naar de dreiging die uitgaat van landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen kenmerken zich dan ook door een grote onderlinge verwevenheid en afhankelijkheid. Kennis die wordt verkregen uit het ene onderzoek kan een onmisbare bouwsteen zijn in een ander onderzoek. Dit geldt niet alleen voor de verschillende onderdelen van de aanvalsinfrastructuur, maar ook voor verschillende bijzondere bevoegdheden die kunnen worden ingezet om zicht te verkrijgen op de bewegingen en intenties van tegenstanders.

Bij onderzoeken naar landen met een offensief cyberprogramma kan de weg die moet worden bewandeld op voorhand niet in detail worden beschreven. De oorzaak hiervan is onder meer dat de wijze van opereren door de betreffende landen steeds geavanceerder wordt en de technische omgeving constant wijzigt. Landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen maken gebruik van een grote hoeveelheid verschillende infrastructurele elementen, verdeeld in verschillende soorten, verspreid over de gehele wereld. Elk stuk infrastructuur ondersteunt een klein gedeelte van de aanval. Dit maakt dat zicht op slechts een klein deel van de infrastructuur onvoldoende is voor de taakuitvoering van de diensten. Bovendien wisselen betreffende landen voortdurend van infrastructuur, waardoor het steeds meer moeite kost hun activiteiten te volgen. Daarnaast wordt het ook steeds lastiger om de geautomatiseerde werken waar deze landen in het kader van hun offensieve cyberprogramma's gebruik van maken binnen te dringen aangezien zij hun beveiliging steeds verhogen. Dit bemoeilijkt het doen van zogenaamd "upstream onderzoek", waarbij de diensten het spoor naar de achterliggende cyberactor proberen te volgen tot de bron. Door dicht tot de bron te naderen, krijgen de diensten inzicht in de intenties, capaciteiten, doelwitkeuze, capaciteiten en activiteiten van de cyberactor.

De diensten zijn derhalve genoodzaakt hun onderzoeksmethoden hierop aan te passen en vanuit een brede basis geïntegreerd onderzoek uit te voeren om deze ook effectief te doen zijn. Daarbij moeten gelijktijdig verschillende soorten operaties gericht op verschillende onderdelen van de aanvalsinfrastructuur van de actor worden uitgevoerd, omdat alleen op deze wijze succesvol zicht kan worden verkregen op de betreffende landen. Dit geldt zowel voor de inzet van de hackbevoegdheid, kabelinterceptie als voor geautomatiseerde data-analyse. Door kabelinterceptie worden zogeheten "leads" onderkend, zoals technische kenmerken van geautomatiseerde werken, waarmee nieuwe aanvalsinfrastructuur inzichtelijk kan worden gemaakt. De hackbevoegdheid en de bevoegdheid tot kabelinterceptie zijn bij de hier bedoelde onderzoeken complementair aan elkaar.

Gelet op de modus operandi van landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen, zijn de diensten genoodzaakt om ook actief in te zetten op het onderdeel van de aanvalsinfrastructuur waarbij de actor gebruik maakt van legaal en illegaal verworven openbare en/of commerciële internetinfrastructuur. Hier zijn ook (veel) andere gebruikers actief. Bij inzet op dit soort onderdelen is het onvermijdelijk dat er een inbreuk op de privacy van andere gebruikers wordt gemaakt. In dat kader is bij de inzet de daadwerkelijke privacy-inbreuk die zal plaatsvinden leidend en de waarborgen die vervolgens van toepassing worden geacht om betreffende inbreuk te rechtvaardigen. Deze infrastructuur bevindt zich bij derden en non-targets, mogelijk bij hen die een functie als dienstverlener vervullen. Zicht op onderdelen van de infrastructuur van de actor is belangrijk, aangezien dit doorgaans tussenstations betreft van het aansturen van een digitale aanval en het daadwerkelijk uitvoeren van de aanval. Vaak is het vanwege technische of operationele redenen niet mogelijk om handelingen op de systemen van de aanbieders van deze infrastructuur uit te voeren. In die gevallen kan het noodzakelijk zijn om bij betreffende partijen (bulk)gegevens te verwerven. Dit om onder andere de beweging van de cyberactor tussen betreffende partijen inzichtelijk te maken. Op deze manier kan, voordat een aanval plaatsvindt, nieuw in gebruik genomen aanvalsinfrastructuur worden onderkend.

2.2.2 Strategische operaties

Het is noodzakelijk dat de diensten niet alleen middelen in kunnen zetten als reactie op een aanval of om specifieke informatie voor een onderzoek te verkrijgen, maar ook om zicht te krijgen op toekomstige aanvallen van landen en de daaraan verbonden technologie. Daarnaast moeten de diensten de mogelijkheid hebben technische kennis op te doen over de werking van systemen waar actoren gebruik van maken.

Bovenstaande vergt een strategische inzet van middelen, gericht op het vergaren van kennis en het ontwikkelen van mogelijkheden ten behoeve van toekomstige inzet van middelen waarbij de inzet ook gericht kan zijn op non-targets. Deze manier van werken is van cruciaal belang in het onderzoek naar landen met een offensief cyberprogramma omdat door de strategische inzet van de hackbevoegdheid en de bevoegdheid tot OOG-interceptie zicht ontwikkeld kan worden op het huidig en toekomstig offensief potentieel, zowel in termen van technische capaciteiten als intenties.

2.2.3 De wijze van verwerking van gegevens

De kernactiviteit van de AIVD en de MIVD is de verwerking van gegevens, waarvoor de Wiv 2017 een uitputtende regeling geeft. Een belangrijk element daarvan betreft de wettelijk vastgelegde zorgplicht voor de kwaliteit van gegevensverwerking. Ook bij onderzoeken als hier bedoeld gaat het om verwerving en de verdere verwerking van gegevens. Zoals hiervoor al kort is aangestipt kenmerken dit soort onderzoeken zich (grotendeels) door een andere onderzoeksmethodiek, waarbij met name het doel om verborgen dreigingen tijdig te onderkennen en te kunnen attribueren aan landen, het noodzakelijk maakt om gegevens in bulk te verwerven. Alleen daardoor wordt het mogelijk om de (nieuwe) aanvalsinfrastructuur van een actor in beeld te krijgen en een nog ongekende cyberdreiging in beeld te krijgen. De diensten verwerven slechts die bulkdatasets waarvan zij de operationele inschatting maken dat deze een grote meerwaarde hebben voor onderzoeken als hier bedoeld. De verwerving

en verdere verwerking, met name via methodieken van geautomatiseerde data-analyse, van dergelijke bulkdatasets, leveren in een vrijwel continu proces nieuwe gegevens en inzichten op voor verder onderzoek en voor de afweging of en, zo ja, welke bijzondere bevoegdheid op welke wijze moet worden ingezet. Gegevens die door inzet van combinaties van bijzondere bevoegdheden worden verworven moeten in samenhang kunnen worden verwerkt en de resultaten daarvan moeten onder meer gebruikt kunnen worden om sturing te geven aan de inzet van (combinaties van) bijzondere bevoegdheden (de zogeheten intelligente mix van inlichtingenmiddelen). Dat is een dynamisch proces waarbij ook het toezicht dynamisch van karakter dient te zijn om ook effectief te kunnen zijn en deze als het ware mee kan bewegen met de wijze waarop een onderzoek wordt uitgevoerd. Op deze wijze kan niet alleen een (voortdurende) rechtmatige uitvoering van de wet worden gemonitord, maar ook de mede daarmee beoogde toepassing van de in de wet voorziene waarborgen in verband met de bescherming van de persoonlijke levenssfeer adequate invulling krijgen. Een statische toets aan de voorkant (bij de vraag of de voorgenomen inzet van een specifieke bijzondere bevoegdheid rechtmatig is) is naar zijn aard ongeschikt om deze – vaak op voorhand ook niet te voorspellen – dynamiek van uitvoering te kunnen omvatten en te normeren. Dat is inmiddels een bij de toepassing van de Wiv 2017 gerijpt inzicht. Zowel in de Wiv 2017 als in het kader van deze wet zal het stelsel van toetsing en toezicht niet alleen passend dienen te zijn bij de aard van en de fase waarin een (verwerkings)activiteit van de diensten plaats vindt, maar ook sluitend. Overigens zal een integrale heroverweging van het stelsel van toets en toezicht, zoals dat in de Wiv 2017 is neergelegd, mede in het licht van de bevindingen van de Evaluatiecommissie Wiv 2017, pas bij de voorgenomen herziening van de Wiv 2017 aan de orde komen. In dat kader zal ook acht worden geslagen op de inzichten verkregen uit de BZK-interne alsmede de externe analyse inzake de recente jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) met betrekking tot bulkinterceptie en de verwerking van bulkdatasets.

2.3 Overzicht van de voorgestelde maatregelen

Teneinde de dreiging afkomstig van landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen effectief te ondervangen is geïnventariseerd op welke aspecten van de Wiv 2017 dat betrekking heeft. Die zien deels op het scheppen van de voorwaarden waardoor een effectieve inzet van de bijzondere bevoegdheden tot het verkennen en binnendringen van geautomatiseerde werken (hacken; artikel 45 Wiv 2017) en de verdere verwerking van via hacks verworven bulkdatasets, de onderzoeksopdrachtgerichte interceptie van communicatie (artikel 48) en de toepassing van geautomatiseerde data-analyse op metadata verworven door de inzet van de bevoegdheid ex artikel 48 (GDA op OOG-metadata) in het cyberdomein wordt bewerkstelligd. Deels door maatregelen te treffen waarbij de aard van het toezicht, uitgevoerd door de TIB en door de afdeling toezicht van de CTIVD, beter aansluit bij de fase en de dynamiek van het onderzoek. Zoals hiervoor al is aangegeven zal het stelsel van toetsing en toezicht niet alleen passend dienen te zijn bij de aard van en de fase waarin een (verwerkings)activiteit van de diensten plaats vindt, maar ook sluitend. In het kader van dit wetsvoorstel is daar aldus invulling aan gegeven, dat daar waar de bindende ex ante toets van de TIB komt te vervallen deze wordt vervangen door een bindende toets ex durante door de afdeling toezicht van de CTIVD. Tot

slot is voorzien in de mogelijkheid van beroep bij de Afdeling bestuursrechtspraak tegen de bindende oordelen van zowel de TIB als de CTIVD die onder toepassing van deze wet worden genomen.

De opbouw van het wetsvoorstel en de daarin opgenomen maatregelen (overzicht)

Artikel 1	*Definitiebepaling*
Artikel 2	*Reikwijdte van de wet en toepasselijkheid*
Artikel 3	*TIB-oordeel inzake toepasselijkheid wet*
Artikel 4	*Voorziening inzake de bevoegdheid tot het verkennen van geautomatiseerde werken*
Artikel 5	*Voorziening inzake de toepassing van de bevoegdheid tot het binnendringen van een geautomatiseerd werk (geen vermelding technisch risico en aanvulling bijschrijfmogelijkheid)*
Artikel 6	*Voorzieningen inzake de verdere verwerking van bulkdatasets verworven met de hackbevoegdheid (termijn voor relevantietoets en verlengingsmogelijkheid)*
Artikel 7	*Voorziening inzake de bevoegdheid tot het verkennen van communicatie-infrastructuur ter vaststelling gegevensstromen met het oog op inzet bevoegdheid van onderzoeksopdrachtgerichte interceptie*
Artikel 8	*Precisering afwegingscriteria ex artikel 26, tweede en vijfde lid, Wiv 2017*
Artikel 9	*Laten vervallen verplichting om toestemming voor GDA op OOG-metadata voor ex ante toets voor te leggen aan TIB*
Artikel 10	*Aanvulling bijschrijfmogelijkheid in artikel 47 Wiv 2017*
Artikel 11	*Aanvulling bijschrijfmogelijkheid in artikel 54 Wiv 2017*
Artikel 12	*Informatie-uitwisseling TIB en afdeling toezicht van de CTIVD*
Artikel 13	*Regeling bindende toezicht door de afdeling toezicht van de CTIVD*
Artikel 14	*Beroepsmogelijkheid bij de Afdeling bestuursrechtspraak van de Raad van State*
Artikel 15	*Mogelijkheid van een voorlopige voorziening bij bindende oordelen van de afdeling toezicht*

Artikel 16	*Overgangsbepaling inzake bij de TIB aanhangige toetsverzoeken*
Artikel 17	*Inwerkingtredingsbepaling en vervaltermijn wet*
Artikel 18	*Citeertitel*

In hoofdstuk 3 zullen de verschillende onderdelen nader worden toegelicht.

2.4 De verhouding van de tijdelijke wet tot de Wiv 2017

In artikel 2, tweede lid, van het wetsvoorstel is bepaald dat op de in het eerste lid bedoelde taak de Wiv 2017 van toepassing is met inachtneming van het bepaalde in deze wet. Concreet betekent dat allereerst dat de Wiv 2017 gewoon van toepassing is en blijft op de in artikel 2, eerste lid, geformuleerde taak. Het is dus niet zo dat met de tijdelijke wet hetgeen in de Wiv 2017 is bepaald met betrekking tot de verschillende aspecten verbonden aan de taakuitvoering van de diensten, waaronder dus het bepaalde in hoofdstuk 3 van de wet (de verwerking van gegevens), waar het gaat om de taak om onderzoek te verrichten naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen, buiten toepassing wordt verklaard. De in dit wetsvoorstel voorgestelde maatregelen hebben ten opzichte van het bepaalde in de Wiv 2017 deels een aanvullend en deels een afwijkend karakter met betrekking tot een beperkt aantal onderdelen van de Wiv 2017, te weten de uitoefening van bijzondere bevoegdheden inzake het verkennen van en binnendringen in geautomatiseerde werken en de verdere verwerking van daarmee verworven bulkdatasets (in het bijzonder de het regime voor relevantie-beoordeling), de uitoefening van de bevoegdheid tot onderzoeksopdrachtgerichte interceptie (introductie van de bevoegdheid tot verkennen) alsmede de geautomatiseerde data-analyse op langs deze weg verworven metadata (GDA op OOG-metadata); daarnaast wordt op onderdelen de bijschrijfmogelijkheid uitgebreid.

Bij het uitwerken van de in dit wetsvoorstel neergelegde maatregelen is nadrukkelijk bezien in hoeverre het stelsel van waarborgen zoals in de Wiv 2017 is neergelegd – bijvoorbeeld waar het gaat om de toetsbevoegdheid van de TIB – wordt geraakt en hoe aan het totaal aan waarborgen kwalitatief bezien geen afbreuk wordt gedaan. Dat heeft er bijvoorbeeld toe geleid dat daar waar de bindende TIB-toets (ex ante) vervalt dit in het kader van dit wetsvoorstel wordt gecompenseerd door een bindende oordeelsbevoegdheid (ex durante en ex post) van de afdeling toezicht van de CTIVD. Daarbij speelde in belangrijke mate ook de overweging een rol in welke fase bij de inzet van bijzondere bevoegdheden (ex ante of ex durante) de aan de TIB dan wel afdeling toezicht opgedragen taak het meest effectief kan worden ingezet. De thans geïntroduceerde bindende oordeelsbevoegdheid van de afdeling toezicht heeft waar het gaat om de toepassing van de tijdelijke wet een aanvullend karakter ten opzichte van reguliere in de Wiv 2017 geregelde toezichtstaak van de afdeling toezicht.

De toepassing van de tijdelijke wet zal in de praktijk de vraag op kunnen roepen op welke wijze de onder toepassing deze wet verworven gegevens (verder) mogen worden verwerkt. Het in de Wiv 2017 neergelegde stelsel kent weliswaar het wettelijk vastgelegde – en ook hier van toepassing zijnde – uitgangspunt dat bepaalde gegevens slechts voor een bepaald doel mogen worden verworven, maar zodra deze rechtmatig zijn verworven kunnen die ook

– mits relevant – voor andere onderzoeken van de dienst (als bijvangst) beschikbaar komen. Dat is met de gegevens te verwerven of verworven onder toepassing van de tijdelijke wet niet anders. Bij de beoordeling of met betrekking tot een bijzondere bevoegdheid al dan niet terecht de toepasselijkheid van de tijdelijke wet wordt ingeroepen, is een belangrijke rol voor de TIB weggelegd; zie daartoe artikel 3, eerste lid. Langs deze weg kan er ook op worden toegezien dat de tijdelijke wet niet wordt ingezet voor andersoortige onderzoeken. Het kan natuurlijk altijd voor komen dat met betrekking tot een bepaald target vanuit verschillende lopende onderzoeken van de dienst aandacht is. In die gevallen kan een bevoegdheid alleen onder toepassing van de tijdelijke wet worden ingezet als het zwaartepunt van de inzet op onderzoeksopdrachten binnen de reikwijdte van deze wet valt. Op grond van artikel 3, eerste lid, van het wetsvoorstel kan de TIB beoordelen of dit terecht zo is.

Voor alle maatregelen in onderhavig wetsvoorstel, dus ook waar het gaat om de hiervoor bedoelde bindende oordeelsbevoegdheid van de afdeling toezicht, geldt dat die een nadrukkelijk een tijdelijk karakter hebben. In artikel 17 van het wetsvoorstel is bepaald dat de tijdelijke wet na vier jaar vervalt. De reden daarvoor is dat ter opvolging van de aanbevelingen van de Evaluatiecommissie Wiv 2017 (ECW), na het uitbrengen van een hoofdlijnennotitie waarbij ingegaan wordt op de door de ECW gedane aanbevelingen, een traject tot herziening van de Wiv 2017 als zodanig zal worden ingezet, waarvan de verwachting is dat die 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.

In de brede wetswijziging zal de ervaring opgedaan met de maatregelen in de tijdelijke wet een belangrijke rol kunnen spelen. Dat geldt niet alleen voor hetgeen met betrekking tot enkele bijzondere bevoegdheden is geregeld, maar ook waar het gaat om het stelsel van toets en toezicht. Dat kan betekenen dat bepaalde arrangementen niet – zoals nu – een tijdelijk maar een structureel karakter kunnen krijgen. Echter dat zal moeten worden bezien in het licht van de totaliteit aan aanbevelingen die de ECW heeft gedaan, waarbij men – ook op het vlak van toets en toezicht – ook oog heeft gehad voor de samenhang tussen de gedane voorstellen. Bij de uitwerking van die voorstellen zullen ook nieuwe inzichten, opgedaan na het verschijnen van het rapport van de ECW, een rol moeten en kunnen spelen.

3. De maatregelen nader beschouwd

3.1 De reikwijdte van de wet

In artikel 2, eerste juncto tweede lid, van het wetsvoorstel is – in verband met de aanduiding van het toepassingsbereik van hetgeen in dit wetsvoorstel bepaald – aangegeven dat de AIVD en de MIVD in het kader van de aan hen in artikel 8, tweede lid, onder a en d, onderscheidenlijk 10, tweede lid, onder a, c en e, van de WIV 2017 opgedragen taak in het belang van de nationale veiligheid, belast zijn met het verrichten van onderzoek naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen en dat op de uitvoering van die taak de Wiv 2017 met inachtneming van het bepaalde in onderhavige wet van toepassing is. Onderhavig wetsvoorstel geeft dan ook een regeling die niet geldt in de plaats van de Wiv 2017, maar – voor zover het de hier bedoelde taakuitvoering betreft – daarvoor deels in aanvulling op of in afwijking van de in de Wiv 2017 opgenomen regels

specifieke voorzieningen treft. De toepasselijkheid van de tijdelijke wet in concrete onderzoeken en wel bij de (voorgenomen) toepassing van bijzondere bevoegdheden, zal voor zover het gaat om bijzondere bevoegdheden als bedoeld in paragraaf 3.2.5 van de Wiv 2017 in de aanvraag voor toestemming voor de inzet van die bevoegdheid moeten worden aangegeven (artikel 2, derde lid). Het wetsvoorstel kent hierop slechts een enkele uitzondering, namelijk waar het gaat om de als afzonderlijk opgenomen bevoegdheid tot verkennen als bedoeld in artikel 7 van het wetsvoorstel, met het oog op de toepassing van artikel 48 Wiv 2017. Deze bevoegdheid kan immers slechts in het kader van de hier bedoelde onderzoeken worden ingezet. Kenbaarheid van de wel of niet toepasselijkheid van hetgeen in onderhavig wetsvoorstel is bepaald, is van belang voor de uitvoering van de toetstaak door de TIB en de toezichtstaak door de afdeling toezicht van de CTIVD.

De reikwijdte van deze tijdelijke wet is beperkt tot onderzoeken van de diensten naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen. Dat betekent dat het onderwerp van onderzoek bepaalt of de inzet van een bevoegdheid kan plaatsvinden onder deze wet. Het is de taak van de diensten om te achterhalen of, hoe en waarom landen een offensief cyberprogramma uitvoeren.[3] Daarom doen de diensten onderzoek naar hun doelwitten, capaciteiten, intenties en wijze van aansturing. Hiervoor is het nodig verder te kijken dan alleen naar een specifieke aanval. Cyberaanvallen worden door landen immers niet uitgevoerd als doel op zich, maar, naast andere meer klassieke inlichtingenmiddelen, als onderdeel van een integrale strategie gericht op het realiseren van geopolitieke doeleinden. Daarbij vinden aanvallen niet uitsluitend plaats vanuit een inlichtingendienst of krijgsmacht, maar ook door of via bedrijven of instellingen of meer diffuse proxy-organisaties. Dit betekent dat het onderzoek van de diensten hier dus ook op gericht dient te zijn. Dit gegeven maakt dat ook de AIVD en de MIVD in het kader van hun onderzoek zich niet dienen te beperken tot een concrete aanval maar ook naar de plaats van die aanval in de bredere context van het land dat achter die cyberaanval zit. De diensten moeten dan ook integraal onderzoek doen naar het land achter de aanval zodat zij zicht krijgen op de herkomst, aansturing en politieke intenties en nieuwe aanvallen voorkomen kunnen worden.

Welke landen dat zijn wordt bepaald aan de hand van de geïntegreerde aanwijzing (GA).[4] Het is voor de diensten echter niet altijd (direct) mogelijk om een digitale aanval te attribueren aan een land. Landen zijn wereldwijd met elkaar verbonden door middel van communicatienetwerken, zoals het internet. Bij het uitvoeren van een cyberaanval wordt gebruik gemaakt van deze communicatienetwerken waarbij het voor de aanvaller van belang is anoniem en heimelijk te werk te gaan. Daarom zal een aanval nooit direct van de aanvaller naar het slachtoffer plaatsvinden, maar wordt deze uitgevoerd met behulp van een groot aantal verschillende tussenstappen. Wel kan een veronderstelling zijn dat een bepaald land achter de aanval zit. Daarom is deze wet ook van toepassing op onderzoeken naar een cyberdreiging en cyberaanvallen tegen Nederland of Nederlandse belangen, waarnaar de

[3] In hoofdstuk 1 van deze toelichting zijn enkele voorbeelden daarvan gegeven.
[4] De specifieke onderzoeken, dus ook die welke plaatsvinden naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen, zijn nader uitgewerkt in de als staatsgeheim gerubriceerde bijlage bij de GA. De inhoud daarvan is bekend bij zowel de TIB als de afdeling toezicht van de CTIVD in verband met de uitvoering van hun taken. Ook de Commissie voor de Inlichtingen- en Veiligheidsdiensten van de Tweede Kamer wordt vertrouwelijk op de hoogte gesteld van de inhoud van de GA, inclusief bijlage.

diensten op grond van de GA onderzoek kunnen doen, ook als die (nog) niet geattribueerd kunnen worden aan een specifiek land.

3.2 Verkennen van en binnendringen in een geautomatiseerd werk

3.2.1 Algemeen

In de artikelen 4 en 5 wordt in afwijking van en in aanvulling op het bepaalde in artikel 45 van de Wiv 2017 voor een aantal onderdelen een regeling voorgesteld ten aanzien van de inzet van de bijzondere bevoegdheid tot het verkennen en binnendringen van een geautomatiseerd werk (hacken) met als doel de hackbevoegdheid in de praktijk beter te laten aansluiten bij onderzoeken naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen. De hackbevoegdheid is van groot belang om zicht te krijgen op de activiteiten, intenties en capaciteiten van deze landen. De voorgestelde wijzigingen beogen zowel het (tijdig) opstarten van operaties mogelijk te maken als operaties ononderbroken te kunnen voortzetten. Daarbij wordt ook het toets- en toezichtstelsel op de hackbevoegdheid betrokken. In de toepassingspraktijk van de Wiv 2017 is bij de toepassing van de hackbevoegdheid namelijk gebleken dat de statische ex-ante toets van de TIB minder goed past bij bepaalde aspecten van de uitvoering van de hackbevoegdheid. Daarom wordt in dit wetsvoorstel op die aspecten een verschuiving voorgesteld van een bindende ex-ante toets door de TIB naar bindend toezicht op de uitvoering door de afdeling toezicht van de CTIVD. Bij deze vorm van toezicht is de afdeling toezicht van de CTIVD in staat in te spelen op ontwikkelingen die zich tijdens de uitvoering voordoen. Deze verschuiving zal ook gevolgen hebben voor concrete casuïstiek, bijvoorbeeld waar het gaat om de invulling van open normen zoals die van de proportionaliteitstoets.

3.2.2 Verkennen van een geautomatiseerd werk

Op grond van artikel 45, eerste lid, onder a, van de Wiv 2017 zijn de diensten bevoegd tot het verkennen van de technische kenmerken van geautomatiseerde werken die op een communicatienetwerk zijn aangesloten. Daarbij wordt nog niet binnengedrongen in het geautomatiseerde werk (het daadwerkelijke hacken). De inzet van deze bevoegdheid heeft tot doel het verkrijgen van een beeld van de eigenschappen van een geautomatiseerd werk, zoals geïnstalleerde software, aanwezige netwerkverbindingen en hardware. 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. Het verkennen dient dus ter ondersteuning van het uiteindelijke binnendringen in een geautomatiseerd werk. Daarnaast dient verkennen ertoe een up-to-date beeld te krijgen van de voor de diensten relevante delen van het digitale landschap.

De huidige wet biedt de diensten op dit moment echter onvoldoende handvatten om de bevoegdheid tot verkennen effectief in te zetten. De veranderlijkheid van de huidige cyberdreiging vereist dat de diensten de bevoegdheid tot verkennen snel en flexibel kunnen inzetten zodat zij in staat zijn te onderzoeken op welke wijze de uiteindelijke

hackbevoegdheid kan worden ingezet. Met de bevoegdheid tot verkennen kunnen verschillende wijzen van binnendringen op potentie worden onderzocht. Hiermee wordt de snelheid en de gerichtheid van de uiteindelijke inzet van de hackbevoegdheid door de diensten vergroot en kan beter worden ingeschat wanneer binnendringen een reële kans van slagen heeft. Met de bevoegdheid tot verkennen wordt geen toegang verkregen tot het geautomatiseerde werk of een deel daarvan tegen de wil van de rechthebbende (er is nog geen sprake van binnendringen). Bij het verkennen wordt in vergelijking met het daadwerkelijk binnendringen slechts een beperkte inbreuk op de privacy gemaakt, maar het toestemmingsniveau is voor beide bevoegdheden belegd op het niveau van de minister. Geconstateerd wordt dat het thans in de wet neergelegde toestemmingsniveau voor verkennen in vergelijking met de toestemming voor het daadwerkelijk binnendringen gelet op de daarmee gepaard gaande privacy-inbreuk als te hoog moet worden beoordeeld. In artikel 4, eerste lid, wordt daarom voorgesteld het verlenen van toestemming tot verkennen te beleggen bij het hoofd van de betrokken dienst en de TIB-toets te laten vervallen. Het laten vervallen van de TIB-toets is ook overeenkomstig aanbeveling 23 van de ECW. De ECW constateerde in haar rapport dat ook de TIB en CTIVD van oordeel zijn dat het huidige toestemmingsniveau wel erg hoog is voor een relatief licht instrument met een zeer beperkte inbreuk op de privacy[5]. In plaats van de bindende TIB-toets krijgt de afdeling toezicht van de CTIVD in deze wet de bevoegdheid tot bindend toezicht op de uitvoering van de verkenningsbevoegdheid (zie artikel 13). Dat zorgt ervoor dat het niveau van waarborgen als geheel gelijk blijft. Voorts draagt deze wijziging bij aan de snelheid die vereist is bij onderzoeken door de diensten naar cyberdreigingen.

3.2.3 Meldplicht aan de afdeling toezicht van een verleende toestemming voor verkennen

In artikel 4, tweede lid, van het wetsvoorstel wordt een meldplicht ingesteld voor de diensten bij de afdeling toezicht van de CTIVD wanneer het hoofd van de dienst toestemming verleent voor het verkennen van technische kenmerken van geautomatiseerde werken. Deze meldplicht hangt samen met het laten vervallen van de ex ante toets door de TIB. De door de diensten te verrichten melding omvat niet meer dan de operatienaam, de datum van toestemming van het hoofd van de dienst en het unieke nummer van de betreffende toestemming. De afdeling toezicht van de CTIVD wordt met de voorgestelde meldplicht in staat gesteld effectief toezicht te houden op de uitvoering door de diensten van deze bevoegdheid. Zij kunnen hiermee vanaf de start van de inzet van de bevoegdheid meekijken en bindend oordelen zodra er volgens de afdeling toezicht van de CTIVD sprake is van een onrechtmatigheid. Deze accentverschuiving in het toezicht zorgt voor effectiever toezicht tijdens de uitvoering van de bevoegdheid.

3.2.4 De omgang met technische risico’s en onbekende kwetsbaarheden bij hacken

3.2.4.1 Technische risico's

In artikel 45, vierde lid, onder a, van de Wiv 2017 is bepaald dat in het verzoek om toestemming voor de inzet van de bevoegdheid tot binnendringen in een geautomatiseerd

[5] Evaluatie 2020 Wet op de Inlichtingen- en Veiligheidsdiensten 2017, p. 91.

werk, in aanvulling op het bepaalde in artikel 29, tweede lid, Wiv 2017, een omschrijving van de technische risico's die zijn verbonden aan de uitoefening van die bevoegdheid dient te bevatten. De omschrijving van de technische risico's dient ertoe dat een afweging kan worden gemaakt tussen het belang van de nationale veiligheid enerzijds, en de technische risico's die verbonden zijn aan de inzet van de hackbevoegdheid, zoals de kans dat het geautomatiseerd werk onbedoeld schade ondervindt van de hack, anderzijds.

Vooropgesteld dient te worden dat het minimaliseren van technische risico's voor de diensten van groot belang is. Niet alleen omdat de diensten zorgvuldig werken en de met de inzet gepaard gaande technische neveneffecten zo klein mogelijk willen houden, maar ook omdat het voor de diensten essentieel is om bij de uitvoering van de hackbevoegdheid niet onderkend te worden. Daarom zullen de diensten bij de uitvoering van de hackbevoegdheid ervoor zorgen dat de technische risico's zo klein mogelijk zijn en in evenredige verhouding staan tot het belang van de bescherming van de nationale veiligheid. Daaronder vallen ook de risico's die voortvloeien uit onderkenning en de risico's ten aanzien van het misbruik door derden.

Er is een spanningsveld ontstaan tussen de dynamiek van de uitvoering van de hackbevoegdheid en de statische ex ante toetsing van de TIB voorafgaand aan de inzet van deze bevoegdheid. Het is namelijk niet mogelijk voorafgaand aan een toestemmingsperiode van drie maanden te voorspellen welke handelingen precies nodig zullen zijn om gedurende die periode het met de inzet van de hackbevoegdheid beoogde doel te bereiken. De eventuele technische risico's die gekoppeld zijn aan deze handelingen zijn daarom van tevoren ook niet te voorzien.
De praktijk wijst uit dat de manier van ex-ante toetsing, zoals is beschreven in de Wiv 2017, niet passend is voor operaties binnen het cyberdomein gezien de technische complexiteit, dynamiek en snelheid van ontwikkelingen binnen de onderzoeken, en heeft geleid tot het verlies van zicht en snelheid in het onderzoek. Om deze reden wordt in onderhavig wetsvoorstel het toezicht op technische risico's bij inzet van de hackbevoegheid ex durante belegd bij de CTIVD.

Ook wanneer toestemming wordt gevraagd voor de inzet van de hackbevoegdheid in de situatie dat de diensten eerder ervaring hebben opgedaan met het binnendringen in vergelijkbare systemen of bij vergelijkbare targets, betekent dit niet automatisch dat een meer gedetailleerde beschrijving van de technische risico's kan worden gegeven. De technische risico's zijn namelijk altijd afhankelijk van veel verschillende factoren, zoals de gebruikte hard- en software, de samenstelling van het (eventuele) netwerk, de beveiliging daarvan, en de gebruiker(s) en/of beheerders. Het is voor de inzet vaak niet duidelijk hoe een geautomatiseerd werk technisch in elkaar zit, hoe een netwerk er precies uitziet, en hoe daarvan en door wie gebruik wordt gemaakt. Zelfs als dit wel (deels) bekend is, kunnen deze factoren snel wisselen.

De CTIVD heeft verschillende onderzoeken verricht naar de uitvoering van de hackbevoegdheid, resulterend in rapporten 53[6] en 70[7]. De CTIVD heeft in rapport 70 onder meer gekeken naar de wijze waarop de afdeling van de Joint SIGINT Cyber Unit (JSCU) van de beide diensten die zich specifiek bezighoudt met Computer Network Exploitation (CNE) omgaat met technische risico's en de afweging daarvan. In rapport 70 heeft de CTIVD vastgesteld dat de werkwijze die deze afdeling intern met betrekking tot het nemen en inschatten van risico's toepast, (met inachtneming van de aanbevelingen) in voldoende mate een afweging van risico's waarborgt.

Gelet op het voorgaande leent de weging van de technische risico's (in het kader van artikel 45, vierde lid, onder a, Wiv 2017 of de generieke proportionaliteitstoets) zich niet goed voor de statische toetsing vooraf door de TIB. Daarom wordt voorgesteld de wettelijke verplichting tot het geven van een omschrijving van technische risico's (artikel 45, vierde lid, aanhef en onder a, Wiv 2017) in toestemmings- of verlengingsaanvragen voor de hackbevoegdheid die vallen binnen de reikwijdte van deze wet te laten vervallen (artikel 5, eerste lid). Met de in dit wetsvoorstel voorgestelde regeling verschuift de ex ante toets van (onbekende) technische risico's van de TIB aldus naar de fase van het dynamisch toezicht door de afdeling toezicht van de CTIVD. Dat neemt niet weg dat de TIB in het kader van haar proportionaliteitstoets wel de op het moment van het verzoek om toestemming voor inzet van de bevoegdheid redelijkerwijs voorzienbare risico's kan betrekken. Gezien de dynamische en onvoorzienbare aard van deze operaties zal dat, zoals hier boven beschreven een beperkt en daarmee een hoger abstractieniveau hebben. In het geval zich gedurende de uitvoering andere risico's voordoen dan voorzien, valt dit onder het bindend toezicht van de CTIVD.

De handelingen die tijdens de uitvoering van de hackbevoegdheid worden verricht worden vastgelegd in logging waarmee de CTIVD tijdens en achteraf bindend toezicht kan houden, hetgeen een stevige waarborg is voor de rechtmatige toepassing van deze wet. De CTIVD kan, doordat zij toegang heeft tot de systemen van de diensten, effectief toezicht houden op de gekozen werkwijze van de diensten en daarmee op de technische risico's. Omdat hiermee wordt voorzien in bindend toezicht op technische risico's vanaf het moment dat de hackbevoegdheid wordt ingezet laat dat geen ruimte voor extra toetsing vooraf op technische risico's.

3.2.4.2 Onbekende kwetsbaarheden

Bij het programmeren en configureren van geautomatiseerde werken worden fouten gemaakt. Dergelijke fouten worden aangeduid als onbekende kwetsbaarheden en zijn daardoor onlosmakelijk verbonden aan het bestaan en gebruik van geautomatiseerde werken. Vanuit het uitgangspunt van heimelijk optreden en het voorkomen dat de diensten worden onderkend, maken de diensten ten behoeve van het binnendringen veelal gebruik van bestaande functionaliteiten van geautomatiseerde werken. Soms is het ook noodzakelijk

[6] Toezichtsrapport nr. 53 van de CTIVD: 'Over de inzet van de hackbevoegdheid door de AIVD en de MIVD in 2015'.
[7] Toezichtsrapport nr. 70 van de CTIVD: 'over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD' 2020(paragraaf 2.4).

om gebruik te maken van een kwetsbaarheid om een geautomatiseerd werk binnen te dringen. Daarbij kan het voorkomen dat een gevonden kwetsbaarheid onbekend is.

Er bestaat een grote verscheidenheid aan onbekende kwetsbaarheden. Deze verscheidenheid is te illustreren aan de hand van een aantal niet limitatieve voorbeelden: het gaat van onbekende kwetsbaarheden die rechtstreeks door iedereen via het internet te gebruiken zijn, tot aan onbekende kwetsbaarheden waar eerst al een bepaalde mate van controle over een netwerk verkregen moet zijn en waarmee dieper in een geautomatiseerd werk of netwerk binnengedrongen kan worden. En verder ook van onbekende kwetsbaarheden die moeilijk te vinden zijn, pas na een ruime voorbereidingstijd gebruikt kunnen worden of veel specifieke expertise vereisen, tot aan relatief eenvoudige, snel inzetbare onbekende kwetsbaarheden. En tevens van onbekende kwetsbaarheden in een geautomatiseerd werk dat breed gebruikt worden, tot onbekende kwetsbaarheden in een systeem dat slechts op één plek in de wereld gebruikt wordt. Afhankelijk van deze verschillende aspecten, kan het bestaan van die onbekende kwetsbaarheid een cybersecurityrisico met zich meebrengen.

Het gebruik maken van een onbekende kwetsbaarheid is een keuze die na zorgvuldige afweging in aanloop naar en tijdens de uitvoering van de hackbevoegdheid gemaakt wordt.

Het gebruik van onbekende kwetsbaarheden is één van de onderdelen die mee worden genomen bij het inschatten van technische risico's. Zoals in paragraaf 3.2.4.1 reeds is toegelicht wordt het bindend toezicht op het gebruik van de technische risico's bij de uitvoering van de hackbevoegdheid bij de CTIVD belegd, hetgeen dus ook zal gelden voor het gebruik van onbekende kwetsbaarheden. Voor het gebruik van onbekende kwetsbaarheden geldt eveneens dat het voorafgaand aan de uitvoering van de bevoegdheid veelal niet te voorzien is of het daadwerkelijk noodzakelijk is een onbekende kwetsbaarheid in te zetten. Ook bij de inzet van onbekende kwetsbaarheden is vaak enige spoed geboden om gebruik te kunnen maken van een operationele kans en/of snel sporen uit te wissen. De CTIVD kan met bindend toezicht gedurende de gehele uitvoering effectief toezicht houden, aangezien dit toezicht niet gebonden is aan een specifiek moment en doorlopend is. Het gebruik van onbekende kwetsbaarheden hoeft derhalve niet meer te worden beschreven bij toestemmings- of verlengingsaanvragen.

3.2.5 Verduidelijking bijschrijfmogelijkheid

In artikel 45, achtste lid, van de Wiv 2017 is bepaald dat een verleende toestemming tot het binnendringen van een geautomatiseerd werk van een persoon of organisatie voor de duur van de toestemming ook de bevoegdheid omvat om binnen te dringen in een ander geautomatiseerd werk van die persoon of organisatie, voor zover dat in de plaats treedt van of een aanvulling is op het geautomatiseerde werk waar oorspronkelijk de toestemming voor is verleend. Deze bevoegdheid staat bekend als de bijschrijfmogelijkheid.

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.

In de praktijk is gebleken dat de TIB, in het kader van de uitvoering van haar rechtmatigheidstoets op de door de minister verleende toestemming, het feit dat in het artikellid gesproken wordt van een geautomatiseerd werk *van* een persoon of organisatie, zodanig uitlegt dat het hier dient te gaan om een geautomatiseerd werk dat *exclusief* aan die persoon of organisatie toebehoort. De TIB maakt 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. Ter illustratie van deze problematiek dient het volgende praktijkvoorbeeld.

In april 2020 komt de AIVD een nieuwe digitale spionagecampagne op het spoor. Deze campagne richt zich maandenlang op westerse overheden, waaronder de Nederlandse overheid en diverse Nederlandse ministeries. De AIVD constateert al snel dat sprake is van een grootscheepse digitale spionagecampagne van een statelijke actor en besluit verder onderzoek te doen naar deze aanvaller. Deze spionagecampagne staat in open bronnen bekend als Advanced Persistent Threat (APT) 31 en wordt door diverse bronnen gerelateerd aan China. Dit soort aanvallen komen zeer regelmatig voor. De AIVD wil bij dit soort aanvallen de aanvaller identificeren, de modus operandi vastleggen en de slachtoffers waarschuwen.

Uit het onderzoek blijkt dat de aanvallers systemen van Europese burgers (ook Nederlanders) hacken om zo een groot netwerk van aanvalssystemen te creëren. Hierbij wisselen de aanvallers in hoog tempo van gehackte systemen om onderkenning en onderbreking van hun spionageactiviteiten te voorkomen. Aanvallers weten dat inlichtingendiensten onderzoek doen naar aanvalsinfrastructuur en wisselen daarom snel en regelmatig van aanvalsinfrastructuur.

Het snelle wisselen van aanvalsinfrastructuur vraagt om snelheid en flexibiliteit in het handelen van de AIVD om deze spionagecampagne te kunnen blijven volgen. Zo vraagt de AIVD telkens toestemming om door de aanvaller gehackte infrastructuur te mogen onderzoeken.

Echter, omdat de infrastructuur niet exclusief in gebruik is bij de aanvaller (het betreffen onder andere gehackte systemen van burgers) moet de AIVD telkens een volledig nieuw en tijdrovend verzoek tot toestemming indienen om deze te mogen onderzoeken. Als de aanvaller een infrastructuur had gehuurd in plaats van gehackt had de AIVD deze infrastructuur mogen bijschrijven. Bijschrijven stelt de AIVD in staat sneller te reageren. Maar, omdat het gehackte systemen betreft moet de AIVD telkens een nieuw verzoek tot

toestemming indienen. In sommige gevallen wordt de toestemming pas verkregen nadat de aanvaller alweer een nieuw systeem heeft gehackt.

Deze vertraging in het onderzoek belemmert het actuele zicht van de AIVD op de aanvalsinfrastructuur van de aanvaller omdat in de periode dat toestemming moet worden verkregen informatie wordt gemist. Ook wordt het voor de AIVD moeilijker om nieuwe slachtoffers te notificeren en onderzoek te doen naar de achterliggende daders.

Deze vertraging kan worden verholpen door het loslaten van het criterium van exclusiviteit waardoor de AIVD de juiste infrastructuur binnen één onderzoek kan bijschrijven en sneller een aanvaller kan volgen. Hierdoor is de AIVD beter in staat onderzoek te doen naar digitale aanvalscampagnes gericht tegen Nederland of Nederlandse belangen.

Om deze reden wordt in deze tijdelijke wet geregeld dat het niet langer vereist is dat er sprake is van exclusief gebruik om te kunnen bijschrijven. Dit geldt zowel voor artikel 45 Wiv 2017 als voor artikel 47 en 54 Wiv 2017.

Met het voorgestelde artikel 5, tweede lid, wordt verduidelijkt dat niet is vereist dat er sprake is van exclusief gebruik om te kunnen bijschrijven. Gedurende de toestemmingsperiode kunnen dus ook geautomatiseerde werken die behalve door de actor zelf ook door anderen worden gebruikt, worden bijgeschreven voor zover dat noodzakelijk is voor het doel waarvoor de oorspronkelijke toestemming is gevraagd. Hiervoor geldt onverkort dat er sprake moet zijn van een interne toestemming en er voldaan moet zijn aan de eisen van noodzakelijkheid, gerichtheid, proportionaliteit en subsidiariteit als in de oorspronkelijke toestemmingaanvraag is opgenomen.

De afdeling toezicht van de CTIVD houdt bindend toezicht op de bijschrijvingen. Daarnaast kan de TIB oordelen over de bijgeschreven geautomatiseerde werken die in de verzoeken tot verlenging van de toestemming door de ministers zijn opgenomen en na akkoord van de minister aan de TIB ter toetsing worden voorgelegd. Dit waarborgt dat in elke fase van de inzet van de hackbevoegdheid de juiste waarborgen aanwezig zijn: vooraf onafhankelijk getoetst door de TIB en tijdens en na afloop bindend toezicht door CTIVD.

3.2.6 Beoordelingstermijn bulkdatasets verkregen via de hackbevoegdheid

Een bulkdataset is een omvangrijke gegevensverzameling waarbij het merendeel van de gegevens betrekking heeft op personen of organisaties die geen onderwerp van onderzoek zijn van een dienst en dat ook nooit zullen worden (artikel 1, onder d). Bulkdatasets vervullen een belangrijke functie bij de onderzoeken van de diensten in zowel de analyse van bekende dreigingen, als bij de analyse van het onderkennen en identificeren van verborgen dreigingen. Deze sets hebben over het algemeen een langdurige operationele waarde, zoals de ECW in haar evaluatierapport onderschrijft.[8] Bij onderzoek naar dreigingen in het digitale domein vervullen bulkdatasets een belangrijke rol bij het achterhalen welke infrastructuur gebruikt wordt door cyberactoren bij hun digitale aanvallen.

[8] Rapport Evaluatiecommissie Wiv 2017 (ECW), p. 65 e.v.

De Wiv 2017 biedt geen aparte regeling voor de verwerving of verdere verwerking van bulkdatasets. Wel gelden voor alle gegevens die door de diensten worden verwerkt de algemene beginselen voor behoorlijke gegevensverwerking als genoemd in paragraaf 3.1 van de Wiv 2017. Na inwerkingtreding van de Wiv 2017 was er, naast deze algemene beginselen, behoefte aan meer duidelijkheid over specifiek de omgang met bulkdatasets. Gelet op het belang van een zorgvuldige verwerking van bulkdatasets, was het passend aanvullende regels te stellen met betrekking tot de omgang met dergelijke datasets. Dit heeft geresulteerd tot de Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017[9]. Deze Tijdelijke regeling betreft aldus aanvullende waarborgen ten opzichte van de Wiv 2017.

Bulkdatasets die verworven zijn door middel van de inzet van bijzondere bevoegdheden, waaronder de hackbevoegdheid, moeten op grond van artikel 27, eerste lid, Wiv 2017 binnen een jaar (met een mogelijke eenmalige verlenging van een half jaar) worden beoordeeld op relevantie.[10] Deze termijn is in de praktijk problematisch, omdat de gegevens in bulkdatasets vaak langer van waarde zijn voor de onderzoeken van de diensten. Het is voor de diensten daarom noodzakelijk om bulkdatasets langer te kunnen gebruiken dan anderhalf jaar, omdat de gegevens in deze bulkdatasets ook na verloop van deze termijn nog van grote waarde kunnen zijn voor de beantwoording van onderzoeksvragen. Ommekomst van de beoordelingstermijn kan er echter toe leiden dat mogelijk waardevolle gegevens moeten worden vernietigd.

De ECW heeft een groot aantal aanbevelingen gedaan met betrekking tot bulkdatasets. Deze zien onder andere op de beoordelingstermijn, maar ook op de manier van relevant verklaren. Deze aanbevelingen worden meegenomen bij de herziening van de Wiv 2017. De in dit wetsvoorstel opgenomen verlengbare beoordelingstermijn op relevantie is nadrukkelijk een tijdelijke oplossing, zodat gedurende de looptijd van de tijdelijke wet een belangrijk operationeel knelpunt voor de onderzoeken waarop dit wetsvoorstel betrekking heeft wordt opgelost.

In artikel 6, eerste en tweede lid, van dit wetsvoorstel wordt de mogelijkheid geboden om de beoordelingstermijn voor bulkdatasets die met de hackbevoegdheid zijn verworven te verlengen met steeds één jaar. Bovendien geldt dat – in afwijking van artikel 27, eerste lid, Wiv 2017 – de gegevens niet zo spoedig mogelijk op relevantie dienen te worden onderzocht. Binnen de strekking van dit wetsvoorstel vallen die bulkdatasets die gegevens bevatten die verworven zijn in onderzoeken naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen.

Voor verlenging van de termijn dienen de diensten telkens de toestemming van de verantwoordelijke minister te verkrijgen. Daarbij onderbouwen de diensten waarom het noodzakelijk is om de betreffende bulkdataset een jaar langer te bewaren. Die onderbouwing kan zich ook richten op noodzaak voor onderzoeksopdrachten die niet binnen de reikwijdte van deze wet vallen. De set wordt immers verworven binnen de reikwijdte van de wet, maar kan in de praktijk ook gegevens bevatten die voor andere onderzoeksopdrachten relevant zijn. Wordt de toestemming geweigerd dan dient de bulkdataset terstond te worden

[9] Stcrt. 2020, 56482.
[10] Voor bulkdata verworven met de bijzondere bevoegdheid van onderzoeksopdrachtgerichte interceptie, geldt op grond van artikel 48, vijfde lid, Wiv 2017 een andere regeling met een termijn van drie jaar.

vernietigd. Dat geldt ook indien geen toestemming voor verdere verlenging wordt gevraagd. De CTIVD houdt op dit proces bindend toezicht en dient over zowel de verleende toestemming voor een langere bewaartermijn als de vernietiging van een bulkdataset te worden geïnformeerd.

Voor regels omtrent toegang tot (relevant verklaarde) bulkdatasets is de Tijdelijke regeling verdere verwerking bulkdatasets onverkort van toepassing.

3.3 Onderzoeksopdrachtgerichte (OOG) interceptie en GDA

3.3.1 Inleiding

De bevoegdheid voor de diensten om OOG-interceptie op de kabel te verrichten was één van de belangrijkste moderniseringen in de Wiv 2017. De introductie van kabelinterceptie vloeide voort uit aanbevelingen van de commissie Dessens, die de Wiv 2002 heeft geëvalueerd.[11] Deze commissie concludeerde dat de interceptiebepalingen in de Wiv 2002 vanwege de voortschrijdende technologische ontwikkelingen te weinig recht deden aan de noodzakelijke bevoegdheden in het kader van de nationale veiligheid.

De diensten hebben deze bevoegdheid tot op heden nog slechts beperkt kunnen inzetten voor inlichtingendoeleinden. Deze noodzakelijke uitbreiding van de Wiv 2002 is daarom tot op heden beperkt benut.

Zoals eerder toegelicht vinden cyberdreigingen vooral plaats via het wereldwijde communicatienetwerk. Dit netwerk bestaat uit kabels. Om inzicht te krijgen op de cyberdreiging is het daarom cruciaal om gegevensstromen van deze kabels te intercepteren. Een vergelijkbaar alternatief is niet beschikbaar.

Benadrukt dient te worden dat de gerichtheid bij OOG-interceptie ziet op de onderzoeksopdracht en niet op personen of organisaties: het is immers *onderzoeksopdrachtgerichte* interceptie. Het middel moet dan ook bij uitstek niet gezien worden als een stapeling van gerichte intercepties.[12] De invulling van het gerichtheidsvereiste moet afgestemd worden op de aard van de bevoegdheid en de context waarin deze toepassing vindt, mede in het licht van het daarmee te bereiken doel. Die is bij OOG-interceptie anders dan bij gerichte interceptie. De verzameling van gegevens (bulkdatasets) verkregen uit OOG-interceptie dragen in hun geheel en in samenhang met andere gegevens bij aan het beantwoorden van de onderzoeksvragen van de diensten. Kabelinterceptie is per definitie een bulkbevoegdheid met een grote mate van inherente ongerichtheid bij het verzamelen van gegevens. Het merendeel van de gegevens die worden geïntercepteerd zal altijd zien op personen en/of organisaties die niet in onderzoek bij de diensten zijn en dat ook nooit zullen zijn. De noodzaak van kabelinterceptie ligt volgens de wetgever met name in het onderkennen van ongekende dreigingen. Juist het feit dat het gaat om het blootleggen van ongekende (cyber)dreigingen maakt dat dit middel alleen effectief is als sprake is van een bepaalde mate van ongerichtheid bij het verzamelen van gegevens. De

[11] Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen. (2013)
[12] Gerichte intercepties zijn gericht op een daarbij aangeduide persoon of organisatie, waarvoor artikel 47 Wiv 2017 de grondslag biedt.

gegevens die uiteindelijk door de diensten worden opgeslagen, zijn gerelateerd aan de onderzoeksopdrachten van de diensten.[13]

Na de invoering van de Wiv 2017 zijn zowel technisch als juridisch veel voorbereidingen getroffen om kabelinterceptie mogelijk te maken. Bij deze voorbereidingen is gebleken dat enkele elementen van de Wiv 2017 achteraf minder goed aansloten bij de operationele praktijk. Deze elementen vormen de basis voor de specifieke voorzieningen die in deze wet worden voorgesteld ten aanzien van OOG-interceptie. Het betreft de volgende voorzieningen:

- Het opnemen van een zelfstandige juridische grondslag voor OOG-interceptie ten behoeve van verkennen.
- Het benoemen van aspecten die met name moeten worden betrokken bij de invulling van de eisen van gerichtheid en proportionaliteit bij de aanvraag van een toestemming voor OOG-interceptie.
- De introductie van bindend toezicht door de afdeling toezicht van de CTIVD op het uitvoeren van GDA waarbij OOG-metadata wordt betrokken ter vervanging van de voorafgaande toets door de TIB.

De getroffen voorzieningen met betrekking tot OOG-interceptie gelden – vanuit de optiek van techniekonafhankelijkheid - voor zowel de interceptie van communicatie in de ether als op de kabel. Gelet op bovengeschetste problematiek spitst onderstaande toelichting zich echter toe op kabelinterceptie.

3.3.2 Het verkennen ten behoeve van OOG-interceptie

Bij de aanvraag van toestemming om tot OOG-interceptie over te kunnen gaan dient zo duidelijk mogelijk te worden omschreven welke gegevensstromen worden geïntercepteerd. Om die duidelijkheid te kunnen geven is het noodzakelijk inzicht te hebben in 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. Dit is alleen mogelijk door gegevensstromen van een kabel te intercepteren en daarvan vervolgens door middel van technisch onderzoek te bepalen of en op welke wijze een gegevensstroom mogelijk een bijdrage levert aan de beantwoording van onderzoeksvragen. Interceptie met dit doel wordt ‘het intercepteren ten behoeve van verkennen' genoemd. In het wetsvoorstel wordt daarvoor een zelfstandige juridische grondslag vastgelegd. Het is van belang op te merken dat de geïntercepteerde gegevens enkel en alleen met dit doel mogen worden onderzocht. Het doel is namelijk om met deze kennis de uiteindelijke toestemmingsaanvraag voor kabelinterceptie ex artikel 48 Wiv 2017 zo goed mogelijk te kunnen onderbouwen. Indien de minister daarvoor de gevraagde toestemming verleent en de TIB deze goedkeurt, kan de bijzondere bevoegdheid tot het doen van kabelinterceptie worden ingezet ter verkrijging van gegevens die gebruikt mogen worden in het inlichtingenproces. Het introduceren van de wettelijke grondslag voor verkennen ten behoeve van interceptie zorgt er voor dat er een betere, technische onderbouwing gegeven kan worden bij de inzet van

13 Toezichtsrapport nr. 75 van de CTIVD, over de inzet van kabelinterceptie ten behoeve van snapshotten door de AIVD en de MIVD, gepubliceerd op 15 maart 2022.

kabelinterceptie ex artikel 48 Wiv 2017. Het is belangrijk om op te merken dat dit dus niet betekent dat de inzet van kabelinterceptie daardoor per definitie in kwantitatieve zin kleiner of beperkter zal worden, maar enkel dat de aanvraag in technische zin beter kan worden onderbouwd. Bij het uitoefenen van de bevoegdheid tot OOG-interceptie ten behoeve van verkennen is ook sprake van bulkinterceptie.

Voor de uitoefening van de bevoegdheid tot verkennen is toestemming van de minister nodig, waarna de TIB deze toestemming op rechtmatigheid beoordeelt. Aanvragen voor de inzet van bevoegdheden worden onderbouwd met de eisen van noodzaak, subsidiariteit, doelmatigheid, proportionaliteit en gerichtheid. Deze eisen zijn neergelegd in artikel 26 Wiv 2017. Omdat de toepassing van de bevoegdheid tot OOG-interceptie *ten behoeve van verkennen* juist dient om vast te stellen waarop de toepassing van artikel 48 Wiv 2017, waarbij sprake is van verwerving van gegevens ten behoeve van het inlichtingenproces, zich dient te richten, is de in artikel 26, vijfde lid, Wiv 2017 neergelegd eis van gerichtheid bij de uitoefening van de verkenningsbevoegdheid naar zijn aard niet toepasbaar. De bevoegdheid tot verkennen is immers per definitie ongericht. Daarom is in artikel 7, vierde lid, van het wetsvoorstel het gerichtheidsvereiste buiten toepassing verklaard.

De toestemming wordt verleend voor een periode van ten hoogste twaalf maanden. Ingeval de TIB een verleende toestemming rechtmatig beoordeeld, doet zij daarvan mededeling aan de afdeling toezicht van de CTIVD die vervolgens op de uitvoering daarvan toezicht kan uitoefenen (artikel 7, derde lid). De toestemming tot verlengen van de bevoegdheid geldt ook voor (ten hoogste) twaalf maanden, evenals het bewaren van de gegevens die zijn verkregen uit het intercepteren ten behoeve van verkenning.

Voor de uitvoering van deze bevoegdheid is de medewerking van aanbieders van communicatiediensten vereist. Deze medewerkingsverplichting is geregeld in artikel 53 van de Wiv 2017. In artikel 7, vijfde lid, van het wetsvoorstel is in verband daarmee artikel 53 van de Wiv 2017 van overeenkomstige toepassing verklaard. Een separate toestemming van de minister voor de uitoefening van de bevoegdheid als bedoeld in artikel 53, tweede lid, Wiv 2017 blijft vereist.

Artikel 7, zesde lid, van het wetsvoorstel regelt de volgende aspecten. Gegevens die worden verkregen bij het uitoefenen van de bevoegdheid tot verkennen zijn enkel toegankelijk voor daartoe aangewezen functionarissen binnen de diensten. Zij hebben uitsluitend toegang tot deze gegevens om te onderzoeken op welke gegevensstromen een verzoek als bedoeld in artikel 48, eerste lid, Wiv 2017 betrekking dient te hebben. Hiervan zal aantekening worden gehouden. Deze gegevens mogen ten hoogste voor 12 maanden worden bewaard en dienen voor zover niet relevant zijn voor het doel van de verwerking te worden vernietigd.

3.3.3 Aspecten te betrekken bij invulling van de eisen proportionaliteit en gerichtheid bij OOG-interceptie

In artikel 8 van het wetsvoorstel worden twee aspecten verduidelijkt die de eisen invullen inzake gerichtheid en proportionaliteit, zoals neergelegd in artikel 26, tweede en vijfde lid, van de Wiv 2017, bij de aanvraag van toestemming voor OOG-interceptie ex artikel 48 Wiv 2017, waarbij de gegevens die daarmee worden verworven wél mogen worden gebruikt in het inlichtingenproces. De diensten hebben als taak onderzoek te doen naar zowel bekende

als verborgen dreigingen. Bij een bekende dreiging hebben de diensten een redelijk goed beeld van de oorsprong van de dreiging en hoe deze dreiging eruitziet. Bij verborgen dreigingen weten de diensten dat er een dreiging is, maar is nog niet bekend hoe deze dreiging eruitziet en hoe deze zich precies technisch manifesteert. Het inzetten van kabelinterceptie is bij uitstek een middel om zicht te krijgen op zowel de bekende als de verborgen dreiging.

De inzet van het middel wordt gerechtvaardigd door de ernst van de dreiging die van offensieve cyberprogramma's uitgaat. Daarbij is het van belang dat de invulling van de proportionaliteit en de gerichtheid niet beperkt is tot (technische) kenmerken die zijn gerelateerd aan gekende targets, maar dat kabelinterceptie ook kan worden ingezet voor *target discovery*. Voor dat doel is het van belang dat het voor de diensten mogelijk is om gegevens in bulk te intercepteren. Want juist op die manier is kabelinterceptie van operationele meerwaarde voor de diensten. De inzet van deze bevoegdheid op bovengenoemde wijze kan dus, gelet op de aard en de ernst van de cyberdreiging, als proportioneel en zo gericht mogelijk worden beschouwd.

De twee aspecten die bij de invulling van de eisen van gerichtheid en proportionaliteit bij een aanvraag tot OOG-interceptie moeten worden betrokken zullen hieronder nader worden toegelicht.

Sub a: indicatie gegevensstromen

Bij de invulling van het gerichtheids- en proportionaliteitsvereiste moet ook een indicatie van de te intercepteren gegevensstromen worden betrokken. Bij het geven van deze indicatie leveren de resultaten van de OOG-interceptie bevoegdheid ten behoeve van verkenning daarvoor de onderbouwing. Met deze indicatie wordt bedoeld de feitelijke, technische aanduiding van de te intercepteren gegevensstromen, zoals die op het moment van de aanvraag te geven zijn. Een voorbeeld van de feitelijke, technische aanduiding zijn bij kabelinterceptie klantkanalen, waarmee de te intercepteren gegevensstromen aan worden geduid.

Sub b: indicatie reductie gegevens

Kabelinterceptie bestaat uit verschillende stappen: de keten van verwerving. Het begint met het overnemen (kopiëren) van de in de toestemming aangeduide gegevensstromen. Deze gegevensstromen worden vervolgens gefilterd. Door de toepassing van filters worden alleen voor het onderzoek bruikbare gegevens uit de gegevensstromen doorgelaten; overige gegevens dus niet. 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.

Gegevensstromen zijn 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. De diensten beschrijven dit plan van datareductie in hun toestemmingsaanvraag, zodat de TIB dit aspect kan betrekken in haar toets van een verleende toestemming. Op de

daadwerkelijke uitvoering van het proces van datareductie houdt de CTIVD toezicht.

Streamingsdiensten

Het categorisch op voorhand aanmerken van bepaalde gegevensstromen zoals streamingdiensten of gegevenstypen als niet-relevant levert voor de diensten een risico op bij het voldoende zicht kunnen houden op de dreiging. De verplichting tot het filteren op streamingsdiensten en niet-grensoverschrijdende communicatie buiten *cyber-defence*, bergt het risico van misbruik door actoren in zich. Daardoor is het van belang dat de diensten per geval een afweging kunnen maken welke gegevens gefilterd moeten worden en welke gegevens doorgelaten kunnen worden.

3.3.4 Geautomatiseerde data-analyse (GDA) op OOG-metadata

3.3.4.1 Geautomatiseerde data-analyse (GDA)

Gegevensverwerking is een kernactiviteit van de diensten. Eén van de verwerkingsmethoden is geautomatiseerde data-analyse (GDA). Zonder toepassing van vormen van GDA zijn grote gegevensbestanden – zoals bulkdatabestanden - vrijwel niet te ontsluiten. De juridische grondslag voor deze verwerkingsmethode is neergelegd is artikel 60 van de Wiv 2017. In het tweede lid van dat artikel wordt een drietal voorbeelden gegeven van GDA, namelijk het op geautomatiseerde wijze onderling vergelijken van gegevens, het doorzoeken van gegevens aan de hand van profielen en het vergelijken van gegevens met het oog op het opsporen van bepaalden patronen. Andere – niet in artikel 60 benoemde - voorbeelden betreffen de enkelvoudige (komt een bepaalde term voor in een bestand) of meervoudige naslag (komt een bepaalde term voor in een combinatie van bestanden). Op grond van het derde lid van artikel 60 is het de diensten niet toegestaan om maatregelen jegens een persoon te bevorderen of te treffen uitsluitend gebaseerd op de resultaten van GDA. Deze norm behelst dus dat in deze gevallen altijd sprake zal dienen te zijn van menselijke tussenkomst.[14]

3.3.4.2 Toestemming voor GDA op OOG-metadata

De diensten zijn bevoegd om GDA toe te passen op alle gegevens die de diensten verwerven. Hiervoor is geen toestemming nodig, met uitzondering van de toepassing van GDA op OOG-metadata. Dat zijn dus metadata verkregen uit OOG-interceptie ex artikel 48 Wiv 2017. In algemene zin kan gesteld worden dat metadata die gegevens zijn die niet de inhoud betreffen. Bij e-mail zijn dit bijvoorbeeld het tijdstip van verzenden, de verzender en de ontvanger. Voor GDA als hier bedoeld is ingevolge artikel 50, eerste lid onder b, van de Wiv 2017 toestemming van de verantwoordelijke minister nodig gevolgd door een rechtmatigheidstoets van de TIB op de verleende toestemming.

In artikel 9 van het wetsvoorstel wordt voorgesteld de ex ante toets van de TIB op de door de minister verleende toestemming voor GDA op OOG te laten vervallen. De reden hiervoor is dat de aard van die toets zich niet goed verhoudt tot het dynamische proces van gegevensverwerking. Omdat bij het analyseren van gegevens voortdurend nieuwe inzichten worden verkregen en aan nieuwe hypotheses worden getoetst, is niet op voorhand te

[14] Zie ook artikel 22, eerste lid, van de Algemene Verordening Gegevensbescherming (AVG) en de nadere invulling daarvan in artikel 40 Uitvoeringswet AVG.

voorspellen op welke exacte wijze GDA (en in welke vorm) wordt ingezet bij de uitvoering van onderzoeken van de diensten.

Het is de taak van de CTIVD om toe te zien op het rechtmatig handelen van de diensten. De CTIVD ziet op dit moment dus al toe op de uitvoering van GDA. Omdat de bindende ex ante toets van de TIB bij GDA op OOG-metadata vervalt, krijgt de CTIVD in de plaats daarvan de bevoegdheid om bindend te kunnen oordelen over de wijze waarop de diensten GDA als hier bedoeld toepassen.

3.4 Bijschrijfmogelijkheid artikel 47 Wiv 2017

Op basis van artikel 47 van de Wiv 2017 hebben de diensten de bevoegdheid tot gerichte interceptie van communicatie (ook wel: tappen). Het zevende lid van artikel 47 van de Wiv 2017 bepaalt dat een verleende toestemming voor de inzet van deze bevoegdheid ook, voor de duur van de verleende toestemming, na de toestemmingsverlening bekend geworden andere nummers of technische kenmerken van de desbetreffende persoon of organisatie omvat. Dit wordt de bijschrijfmogelijkheid genoemd.

In artikel 10 van het wetsvoorstel wordt bepaald dat in aanvulling op het bepaalde in artikel 47, zevende lid, Wiv 2017 de verleende toestemming tot interceptie tevens de bevoegdheid omvat om, voor de duur van de verleende toestemming, de in verband met de in deze wet aan de toetsingscommissie en afdeling toezicht toegekende taak bevoegd en telecommunicatie te ontvangen of op te nemen aan de hand van na de toestemmingverlening bekend geworden andere nummers of technische kenmerken *die in gebruik worden genomen* door de desbetreffende persoon of organisatie. Daarmee wordt ook bij toepassing van deze bevoegdheid niet vereist dat er sprake is van het exclusieve gebruik door de persoon of organisatie van het desbetreffende nummer of technisch kenmerk jegens wie de bevoegdheid wordt ingezet, hetgeen door de zinsnede “nummers of technische kenmerken *van* de desbetreffende persoon of organisatie” in die zin wordt uitgelegd.

Gedurende de toestemmingsperiode kunnen nummers dan wel technische kenmerken worden bijgeschreven voor zover dat noodzakelijk is voor het doel waarvoor de oorspronkelijke toestemming is gevraagd. Hiervoor geldt onverkort dat er – naast de wettelijk vereiste toestemming voor de uitoefening van de tapbevoegdheid - sprake moet zijn van een geldige *interne* toestemming en er ook voldaan moet zijn aan de eisen van noodzakelijkheid, gerichtheid, proportionaliteit en subsidiariteit. Indien dit niet het geval is, zullen de diensten een nieuw toestemmingsverzoek indienen.

Er is voor gekozen om de uitoefening van de bevoegdheid tot bijschrijving onder de werking van de regeling inzake bindend toezicht door de afdeling toezicht van de CTIVD te brengen. Aldus kan er op een rechtmatige uitoefening van deze bevoegdheid adequaat worden toegezien.

3.5 Bijschrijfmogelijkheid artikel 54 Wiv 2017

Op basis van artikel 54 kunnen de diensten gegevens opvragen bij aanbieders van telecommunicatie- en opslagdiensten. De binnen het cyberonderzoek meest voorkomende

inzet van artikel 54 is het opvragen van disk-images van servers. Op basis van dit artikel is het ook mogelijk andere vormen van in Nederland opgeslagen gegevens op te vragen.

Artikel 54 kent, anders dan de artikelen 45 en 47, geen mogelijkheid tot bijschrijven. Als na ontvangst van de opgevraagde gegevens blijkt dat een cyberactor inmiddels gebruikmaakt van een ander technisch kenmerk moet hiervoor opnieuw toestemming worden gevraagd aan de minister en dient de verleende toestemming te worden getoetst door de TIB. Bovendien kan een cyberactor overstappen naar een nieuwe aanbieder, zoals een andere hostingprovider. Ook in dit geval moet opnieuw toestemming worden gevraagd om het target te kunnen volgen. Deze procedure staat de benodigde snelheid in het cyberdomein in de weg. Als een nieuwe toestemming op basis van artikel 54 Wiv 2017 eenmaal is verleend door minister en goedgekeurd door de TIB, dan kan de cyberactor in de praktijk alweer gewisseld zijn van aanbieder en/of kenmerk en verdwijnt deze uit beeld. Zowel de diensten als de TIB zien het ontbreken van de bijschrijfmogelijkheid bij artikel 54 als een hiaat in de wet. Het ontbreken van de mogelijkheid tot bijschrijven van aanbieders en kenmerken draagt bij aan het verminderen van het zicht op de dreiging waar dit wetsvoorstel op ziet.

Met de in artikel 11 voorgestelde regeling wordt aldus mogelijk gemaakt dat een verleende toestemming voor het opvragen van gegevens ook, voor de duur van de verleende toestemming, de bevoegdheid omvat om aan de hand van een na de toestemmingsverlening van de desbetreffende persoon of organisatie bekend geworden ander nummer of technisch kenmerk gegevens op te vragen en dit een aanvulling is op of in de plaats treedt van een eerder nummer of technisch kenmerk waarvan al toestemming is verkregen. Hierbij geldt eveneens dat de inzet ten aanzien van een nieuw nummer of technisch kenmerk een gelijkwaardige afweging ten aanzien van de noodzakelijkheid, proportionaliteit, subsidiariteit en gerichtheid kent. Ook wordt geregeld dat de diensten zich voor het opvragen van gegevens kunnen wenden tot een andere aanbieder, ingeval gebleken is dat deze in de plaats van de oorspronkelijke aanbieder is getreden of naast de oorspronkelijke aanbieder door de gebruiker wordt ingeschakeld.

Conform hetgeen ten aanzien van de bevoegdheid ex artikel 45 en 47 Wiv 2017 is overwogen geldt bij deze bevoegdheid ook dat er ten behoeve van het kunnen bijschrijven niet is vereist dat er sprake is van exclusief gebruik. Gedurende de toestemmingsperiode kunnen nummers dan wel technische kenmerken worden bijgeschreven voor zover dat noodzakelijk is voor het doel waarvoor de oorspronkelijke toestemming is gevraagd. Hiervoor geldt onverkort dat er sprake moet zijn van een geldige interne toestemming voor bijschrijving en er voldaan moet zijn aan een gelijkstrekkende motivering van de eisen van noodzakelijkheid, gerichtheid, proportionaliteit en subsidiariteit als in de oorspronkelijke toestemmingaanvraag is opgenomen. Indien dit niet het geval is, zullen de diensten een nieuw toestemmingsverzoek indienen.

In de praktijk zullen de bijgeschreven kenmerken worden opgenomen in een eventueel verzoek tot verlenging van de bevoegdheidsuitoefening. Tot slot is ervoor gekozen om de uitoefening van de bevoegdheid tot bijschrijving onder de werking van de regeling inzake bindend toezicht door de afdeling toezicht te brengen. Aldus kan er op een rechtmatig uitoefening van deze bevoegdheid effectief worden toegezien.

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

4.1 Inleiding

In het onderzoek naar landen met een offensief cyberprogramma gericht tegen Nederland of Nederlandse belangen zetten de diensten bijzondere bevoegdheden in die gepaard kunnen gaan met diepgaand ingrijpen in de persoonlijke levenssfeer van burgers. Daarom is de inzet van bevoegdheden door de diensten aan stevige waarborgen onderworpen. In de Wiv 2017 is daaraan, met inachtneming van de eisen die onder meer voortvloeien uit het Europees Verdrag voor de Rechten van de Mens (EVRM) en de jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM), uitwerking gegeven. Daarbij is, met de geïntroduceerde TIB-toets, verder gegaan dan als minimumnorm op grond van het EVRM en de jurisprudentie van het EHRM geldt.[15] Dit waarborgenstelsel werkt als volgt.

Voorafgaand aan de inzet van een aantal bijzondere bevoegdheden is toestemming van de verantwoordelijke minister vereist. De TIB beoordeelt vervolgens de toestemming die de minister heeft gegeven op rechtmatigheid (niet op doelmatigheid). De TIB-toets is een bindende ex ante toets voorafgaand aan de start of verlenging van de inzet van een bijzondere bevoegdheid. De TIB toetst de toestemming van de minister aan de hand van vier criteria: noodzaak, proportionaliteit, subsidiariteit en gerichtheid. Deze criteria hebben alle zelfstandige betekenis en dienen bij een verzoek om toestemming afzonderlijk te worden onderbouwd. De criteria zijn in de Wiv 2017 als norm open geformuleerd. Een toets op deze criteria gebeurt niet alleen bij de TIB, maar daaraan voorafgaand allereerst door de minister die de toestemming verleent en door de diensten zelf in het kader van de voorbereiding van de aanvraag voor toestemming waarbij het resultaat van die toets in de aanvraag wordt verantwoord. De betrokken minister draagt steeds volledige verantwoordelijkheid voor de inzet van deze bijzondere bevoegdheden en is gehouden daarover parlementaire verantwoording af te leggen. De aard van de dreiging bepaalt mede de noodzaak van de inzet en dit heeft uiteraard ook effect op de weging van de proportionaliteit. Ingevolge artikel 26, vierde lid, van de Wiv 2017 dient de uitoefening van een bevoegdheid evenredig te zijn aan het daarmee beoogde doel. Dit brengt met zich mee dat naarmate de dreiging en de noodzaak om daartegen op te treden groter is, sneller aan deze eis voldaan wordt.

De afdeling toezicht van de CTIVD houdt toezicht op een rechtmatige taakuitvoering door beide diensten. Deze vorm van toezicht kan zowel plaatsvinden tijdens (ex durante) als na de inzet (ex post). De afdeling toezicht van de CTIVD kan haar toezichthoudende taak dus al uitvoeren op het moment dat uitvoering wordt gegeven aan een door de TIB goedgekeurde toestemming voor de inzet van een bijzondere bevoegdheid. Naast de afdeling toezicht van de CTIVD houden de diensten zelf ook intern toezicht op de naleving van de wet- en regelgeving en de daaruit voortvloeiende zorgplicht. De diensten hebben hiervoor een eigen intern compliance stelsel opgezet, waarbij compliance en data adviseurs toezien op een rechtmatige taakuitvoering van de diensten. Op deze manier proberen de diensten hun processen continu te verbeteren. Als er een compliance incident heeft plaatsgevonden bij de diensten wordt dit door middel van een interne procedure gemeld en vastgelegd in een

[15] In die zin dat de TIB-toets als onafhankelijk bindende toets ex ante bij meer bevoegdheden wordt vereist dan uit de jurisprudentie van het EHRM en HvJEU voortvloeit.

register. De afdeling toezicht van de CTIVD wordt actief door de diensten op de hoogte gesteld van de incidenten in de hoogste risico- en impactcategorieën.

Het voorliggende wetsvoorstel brengt ten opzichte van dit stelsel waar het gaat om de uitvoering van de in artikel 2, eerste lid, van het wetsvoorstel bedoelde taak van de diensten enkele veranderingen. De reikwijdte daarvan is beperkt tot de gevallen waarop onderhavig wetsvoorstel betrekking heeft.

In de voorgestelde wettelijke regeling wordt erin voorzien dat de eis van een ex ante rechtmatigheidstoets door de TIB voor bepaalde toestemmingen (bijvoorbeeld het kunnen verkennen van geautomatiseerde werken) niet meer wordt gesteld. In die gevallen wordt deze vervangen door bindend toezicht door de afdeling toezicht van de CTIVD, waarbij – zoals ook eerder in deze memorie is uiteengezet – wordt aangesloten bij een vorm van toezicht die beter past bij de aard en fase waarin de toepassing van de bevoegdheid zich bevindt. Op deze wijze wordt een hoog niveau van waarborgen gehandhaafd. Artikel 13 van het wetsvoorstel voorziet in een regeling voor dit bindende toezicht.

Met de voorgestelde regeling inzake bindend toezicht wordt ten opzichte van het stelsel van toets en toezicht zoals de Wiv 2017 thans kent voor de duur van en beperkt tot de toepassing van de tijdelijke wet, een nieuw toezichtselement geïntroduceerd. Daarmee wordt de kwestie inzake de noodzaak van een vorm van rechterlijke toets, waarvoor de ECW in haar rapport aandacht heeft gevraagd, reeds nu actueel. Naar het oordeel van de regering moet dan ook – vooruitlopend op het wetstraject dat naar aanleiding van het rapport van de ECW zal worden ingezet – reeds nu in een vorm van een rechterlijke toets worden voorzien waar het gaat om de oordelen die in het kader van het bindend toezicht door de afdeling toezicht van de CTIVD tot stand komen, maar evenzeer waar het gaat om enkele oordelen van de TIB. Zoals de ECW terecht heeft aangegeven kent het huidige stelsel van toets en toezicht een weeffout, waarbij de toezichthouders niet alleen in het laatste woord in een concrete casus hebben, maar ook wat betreft de uitleg van begrippen en criteria, en de wijze waarop zij hieraan toetsen. Deze kwestie heeft, zoals de ECW aangeeft, in de afgelopen jaren verschillende malen tot knelpunten geleid. Een deel van de knelpunten waarop de constatering van de ECW betrekking heeft, betreft de inzet van met name de bijzondere bevoegdheden ex artikel 45 (hacken) en 48 (OOG-interceptie) van de Wiv 2017 in de context van onderzoeken naar landen met een offensief cyberprogramma. Dit is eerder in de memorie van toelichting van context en inhoud voorzien. In deze context is het dan ook noodzakelijk om een voorziening te treffen waarmee tot een gezaghebbende en eenduidige wetsuitleg kan worden gekomen, waarin het door TIB en CTIVD gevoerde rechtseenheidsoverleg slechts ten dele in kan voorzien omdat daarbij geen betrokkenheid van de ministers is voorzien. Daarom voorziet dit wetsvoorstel eveneens in een - relatief eenvoudig vormgegeven - beroepsprocedure bij de Afdeling bestuursrechtspraak van de Raad van State (artikel 14). In aanvulling hierop wordt tevens voorzien in een regeling voor een voorlopige voorziening (artikel 15). Dit houdt verband met het feit dat een oordeel van de afdeling toezicht van de CTIVD bindend is en in beginsel binnen 48 uur moet worden uitgevoerd. Met een voorlopige voorziening kunnen onomkeerbare operationele gevolgen worden voorkomen in afwachting van de uitspraak op het beroep.

Deze regeling heeft, evenals die betreffende het bindend toezicht van de afdeling toezicht, een tijdelijk karakter en is beperkt tot de toepassing van hetgeen in dit wetsvoorstel is bepaald. In het kader van het wetstraject naar aanleiding van het rapport van de ECW en – eerder – de daaromtrent uit te brengen hoofdlijnennotitie zal het stelsel van toets en toezicht dat in de Wiv 2017 is neergelegd meer fundamenteel en in zijn geheel op zijn merites worden beoordeeld. Hierbij zullen onder meer ook de door de Tweede Kamer aangenomen moties inzake het stelsel van toetsing en toezicht worden betrokken, alsmede de aan het Parlement toegezonden analyse van de jurisprudentie van het Europese Hof voor de Rechten van de Mens en het rapport van de Algemene Rekenkamer inzake de slagkracht van de AIVD en MIVD.

In het onderstaande zal eerst worden ingegaan op de voorgestelde bindende toezichtsbevoegdheid van de afdeling toezicht en aansluitend de regeling van beroep bij de Afdeling bestuursrechtspraak en tot slot de regeling omtrent de voorlopige voorziening

4.2 Bindend toezicht door de afdeling toezicht van de CTIVD

In artikel 2, tweede lid, van het wetsvoorstel is bepaald dat op de uitvoering van de op de in artikel 2, eerste lid, geformuleerde taak de Wiv 2017 van toepassing is met inachtneming van het bepaalde in deze wet. Hieruit vloeit dan ook voort dat de in de Wiv 2017 geregelde taak van de afdeling toezicht om toe te zien op de rechtmatigheid van de uitvoering van hetgeen bij of krachtens de Wiv 2017 is gesteld onverkort van toepassing is op de uitvoering van de taak van de diensten om onderzoek te verrichten naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen. Het betreft hier overigens een bestaande taak van de diensten waarover het toezicht van de afdeling toezicht zich nu reeds uitstrekt. In artikel 2, tweede lid, wordt bepaald dat het bepaalde bij deze tijdelijke wet in acht genomen dient te worden. Dat betekent concreet dat bij de taak van de afdeling toezicht om toe te zien op de uitvoering van de hier bedoelde onderzoekstaak van de diensten, de in artikel 13 opgenomen regeling inzake bindend toezicht – aanvullend - van toepassing is.

Artikel 12 van het wetsvoorstel biedt de grondslag voor de bindende toezichtsbevoegdheid van de afdeling toezicht en geeft met betrekking tot de uitvoering daarvan enkele procedurele voorschriften. Met die voorschriften wordt beoogd een zorgvuldige toepassing van de toezichtsbevoegdheid te realiseren. De voorgestelde regeling valt uiteen in de volgende onderdelen:

a. een limitatieve opsomming van de bepalingen van het wetsvoorstel waarop de regeling inzake bindend toezicht kan worden toegepast;
b. bij constatering van een onrechtmatigheid kan de afdeling toezicht dit vervolgens als een voorlopig oordeel mededelen aan de verantwoordelijke minister;
c. bij dat voorlopige oordeel kan de afdeling toezicht aangegeven of en, zo ja, welke gevolgen aan dat oordeel worden verbonden;
d. de gevolgen zijn beperkt tot twee – limitatieve – opties: beëindiging van de desbetreffende bevoegdheid en/of de verwijdering en vernietiging van de bij de uitvoering daarvan verwerkte gegevens;

e. een wettelijk vastgelegde termijn waarbij de minister op het voorlopig oordeel en de daaraan verbonden gevolgen kan reageren;
f. de vaststelling van het oordeel en de daaraan te verbinden gevolgen door de afdeling toezicht nadat de reactie van de minister is ontvangen of indien deze binnen de gestelde termijn is uitgebleven. Dit oordeel is vervolgens bindend;
g. indien de minister het oordeel en de daaraan verbonden gevolgen onderschrijft, dient de minister daar binnen 48 uur uitvoering aan te geven, tenzij beroep wordt ingesteld waarbij tevens een verzoek om een voorlopige voorziening wordt gedaan;
h. de plicht om de beide kamers der Staten-Generaal te informeren over het oordeel van de afdeling toezicht, waarbij de regeling inzake vertrouwelijkheid onverkort van toepassing is.

Ad a: de bindend toezichtsbevoegdheid ziet uitsluitend op de toepassing van (1) artikel 45, eerste lid, onder a, van de Wiv 2017, juncto artikel 4, inzake de bevoegdheid tot verkennen van geautomatiseerde werken, (2) artikel 45, eerste lid, onder b, van de Wiv 2017, juncto artikel 5, eerste lid, inzake de bevoegdheid tot hacken voor zover het de daaraan verbonden technische risico's betreft, (3) artikel 5, tweede lid, inzake de bijschrijfmogelijkheid in het kader van hacken, (4) artikel 6, inzake de beoordelingstermijn voor bulkdatasets die zijn verkregen door hacken, (5) artikel 50, vierde lid, van de Wiv 2017, juncto artikel 9, inzake GDA op OOG, (6) artikel 10, inzake de bijschrijfmogelijkheid in het kader van de toepassing van artikel 47 Wiv 2017 (gerichte interceptie) of (7) artikel 11 inzake de bijschrijfmogelijkheid in het kader van de toepassing van artikel 54 Wiv 2017 (het opvragen van gegevens bij aanbieders van telecommunicatie- en opslagdiensten).

Ad b: indien de afdeling toezicht bij het toezicht op de desbetreffende bepalingen tegen een onrechtmatigheid aanloopt, kan zij daarvan in de vorm van een voorlopig oordeel mededeling doen aan de verantwoordelijke minister. Het is een discretionaire bevoegdheid van de afdeling toezicht; dus geen verplichting. In de praktijk zal naar verwachting pas tot zo'n mededeling worden gekomen indien niet in de reguliere contacten tussen de toezichthouder en de diensten een geconstateerde onrechtmatigheid kan worden weggenomen.

Ad c en d: bij het voorlopige oordeel kan de afdeling toezicht – indien zij daartoe aanleiding ziet – ook aangeven welke gevolgen zij daaraan verbindt. Dat kan uitsluitend betrekking hebben op (1) beëindiging van de desbetreffende bevoegdheid en/of (2) de verwijdering en vernietiging van de bij de uitvoering van de desbetreffende bevoegdheid verwerkte gegevens. Het eerste gevolg is helder: voor zover dat ziet op de uitoefening van de hackbevoegdheid, betekent dit dat die dan gestopt moet worden. Bij de verwijdering en vernietiging van gegevens ligt dit wellicht minder eenduidig. Ingeval van GDA op OOG-metadata betekent dit in ieder geval niet, dat de in GDA betrokken gegevens dienen te worden verwijderd en vernietigd, maar uitsluitend de uit de toegepaste GDA-methodiek voortvloeiende gegevens (de resultaten). Dit brengt met zich mee dat de verplichte verslaglegging inzake de uitoefening van bijzondere bevoegdheden door de diensten (artikel 31 Wiv 2017) al dan niet in combinatie met voorzieningen in het toegepaste informatiesysteem, zodanig dient te zijn dat ingeval aan een bindend oordeel (en daarmee ook bindend) als gevolg de vernietiging van gegevens wordt verbonden, daaraan ook effectief uitvoering kan worden gegeven.

Ad e: Nadat het voorlopig oordeel door de afdeling toezicht aan de minister is medegedeeld, krijgt de minister een termijn van 48 uur (na ontvangst) om op het voorlopig oordeel en de eventueel daaraan te verbinden gevolgen te reageren. Een termijn van 48 uur achten we voldoende lang voor een reactie en ook niet te lang, nu immers een onrechtmatige geachte uitvoering wel zo spoedig mogelijk dient te worden beëindigd.

Ad f: Zodra de afdeling toezicht de reactie van de minister heeft ontvangen of de termijn van 48 uur is verstreken en er is geen reactie ontvangen, dan kan zij overgaan tot het vaststellen van het oordeel. Bij de definitieve oordeelsvorming dient de reactie uiteraard betrokken te worden. Er is geen termijn vastgesteld om tot een vaststelling te komen; dat is ter discretie aan de afdeling toezicht. Dat laat ook ruimte om naar aanleiding van de reactie waar nodig bijvoorbeeld nadere toelichting te vragen of in overleg te treden om te bezien of de geconstateerde onrechtmatigheid op een andere wijze ongedaan kan worden gemaakt. Is men tot vaststelling van een oordeel en de daaraan te verbinden gevolgen gekomen dan dient het oordeel met redenen omkleed schriftelijk aan de minister te worden medegedeeld.

Ad g: na ontvangst van het oordeel begint voor de minister de termijn van zes dagen te lopen om tegen het oordeel beroep in te stellen bij de Afdeling bestuursrechtspraak van de Raad van State. Voor dat beroep geeft artikel 14 een regeling. Tevens is in artikel 15 voorzien in de mogelijkheid om een voorlopige voorziening aan te vragen teneinde schorsende werking te verkrijgen van het oordeel van de afdeling toezicht. Deze voorziening is noodzakelijk om te voorkomen dat lopende onderzoeken van de dienst naar landen met een offensief cyberprogramma nadelige gevolgen ondervinden, bijvoorbeeld omdat de bevoegdheidsuitoefening naar het oordeel van de afdeling toezicht van de CTIVD dient te worden beëindigd waardoor het zicht op het target verloren gaat; met name bij onderzoek in cyberdomein is die kans groot.

Ad h: indien de minister het vastgestelde oordeel alsmede de daaraan door de afdeling toezicht verbonden gevolgen onderschrijft, dan dient de minister daaraan binnen 48 uur uitvoering te geven. Indien de minister het niet eens is met het vastgestelde oordeel en/of de daaraan verbonden gevolgen, dan kan op grond van artikel 14 beroep bij de Afdeling bestuursrechtspraak worden ingesteld.

Ad i: tot slot is bepaald dat van een oordeel van de afdeling toezicht terstond mededeling wordt gedaan aan de beide kamers der Staten-Generaal. Daarbij is artikel 12, derde en vierde lid, Wiv 2017 van overeenkomstige toepassing. Nu het hier om oordelen gaat die betrekking hebben op lopende onderzoeken van de diensten en de toepassing van bepaalde bijzondere bevoegdheden daarin, zal in zijn algemeenheid sprake zijn van een of meer van de in artikel 12, derde lid, Wiv 2017 aangeduide categorieën van gegevens, die ingevolge artikel 12, vierde lid, van die wet, door de minister slechts vertrouwelijk kunnen worden verstrekt. In de praktijk betekent dat, dat de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD) van de Tweede Kamer wordt geïnformeerd.

4.3 Beroep op de Afdeling bestuursrechtspraak

Zoals hiervoor toegelicht voorziet dit wetsvoorstel in een bindende toezichtsbevoegdheid voor de afdeling toezicht van de CTIVD. De ex ante toets van de TIB heeft reeds een bindend

karakter. In het kader van deze ex ante toets zijn 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. In het huidige stelsel heeft de TIB hierin het laatste woord. De ECW constateerde in dit verband dat het stelsel van de wet hiermee een weeffout bevat die de komende jaren wellicht opnieuw tot problemen zal leiden, mede gelet op de snelle technologische ontwikkelingen. Immers, ook de verduidelijkingen van begrippen en verhelderingen van procedures zullen weer nieuwe vragen van afbakening kunnen oproepen. De ECW concludeert daarom dat het niet alleen praktisch onwenselijk is, maar ook principieel niet passend dat een toezichthouder het laatste woord heeft over de uitleg van wettelijke begrippen, de invulling van de toetsingsnormen en de intensiteit van de toetsing. Dat is volgens de ECW bij uitstek een rechterlijke taak, waarbij de toezichthouder, gegeven de rechterlijke overwegingen, gaat over de toepassing in concrete gevallen.
De ECW heeft dan ook aanbevolen dat het stelsel van toezicht wordt aangevuld met een rol voor de rechter, die de grenzen van het speelveld bepaalt waarbinnen het toezicht op de bevoegdheidsuitoefening door de diensten plaatsvindt. De ECW verwijst hierbij naar het bestuursrecht waarbij eveneens geschillen tussen toezichthouders en onder toezicht gestelden aan de orde zijn, maar waarbij de bestuursrechter wel de bevoegdheid heeft deze geschillen finaal te beslechten. Ten aanzien van de oordelen van de TIB ontbreekt deze mogelijkheid (of een vergelijkbare procedure) volledig. Dit klemt te meer nu ook de afdeling toezicht van de CTIVD met dit wetsvoorstel een bindende oordeelsbevoegdheid krijgt. Gelet op de in het geding zijnde belangen en omstandigheden (snel duidelijkheid, zo min mogelijk bekendheid van staatsgeheime informatie) heeft de ECW aanbevolen de Afdeling bestuursrechtspraak van de Raad van State in eerste en enige instantie te belasten met de geschillenbeslechting zoals hiervoor bedoeld. De bestuursrechter is bij uitstek geschikt om de rechtmatigheid van overheidshandelen te beoordelen: aan de hand van de beginselen van behoorlijk bestuur en met inachtneming van de bijzondere positie van de democratisch gelegitimeerde overheid. Een rol voor de rechter zou het stelsel ook meer in balans brengen, omdat het probleem wordt neergelegd waar het rechtsstatelijk gezien het beste thuishoort, namelijk de rechter, aldus de ECW.

Gelet op de specifieke aard van de geschillen en de (operationele) noodzaak om zo snel mogelijk tot een finale uitspraak te komen, is het niet wenselijk de daarvoor de in het bestuursrecht gebruikelijke rechtsgang in meerdere instanties open te stellen. De rechter die in eerste en enige instantie oordeelt heeft in dit geval de voorkeur. Omdat naar verwachting veel zaken zullen worden voorgelegd waarin niet zo zeer een feitencomplex, maar de uitleg van wettelijke begrippen centraal zal staan, ligt het voor de hand om de Afdeling bestuursrechtspraak, als hoogste algemene bestuursrechter met een belangrijke rechtsvormende rol, aan te wijzen als bevoegde instantie. De keuze voor de Afdeling bestuursrechtspraak doet ook recht aan het grote maatschappelijke belang dat over de rechtmatigheid van het optreden van de AIVD en de MIVD (relatief) snel een definitief rechterlijk oordeel wordt gegeven. Bovendien heeft de Afdeling bestuursrechtspraak reeds ervaring met AIVD- en MIVD-gerelateerde zaken en de omgang met staatsgeheime informatie die daaraan inherent verbonden is.

Tegen deze achtergrond wordt daarom voorgesteld dat de verantwoordelijke minister beroep kan instellen bij de Afdeling bestuursrechtspraak van de Raad van State tegen een bindend oordeel van de afdeling toezicht van de CTIVD, de daaraan door de afdeling toezicht verbonden gevolgen of beide, alsmede tegen een oordeel van de toetsingscommissie als bedoeld in artikel 3, eerste lid, dan wel tegen een oordeel van de toetsingscommissie inzake een door de minister verleende toestemming in een onderzoek op grond van dit wetsvoorstel. In aanvulling hierop wordt in artikel 15 ook een regeling voorgesteld waarmee een voorlopige voorziening kan worden getroffen voor spoedeisende gevallen die verband houden met een bindend oordeel van de afdeling toezicht en de daaraan door de afdeling toezicht van de CTIVD verbonden gevolgen.

Gelet op de wettelijke taak van de Afdeling bestuursrechtspraak van de Raad van State zoals geformuleerd in artikel 30b van de Wet op de Raad van State, te weten de berechting van de bij de wet aan haar opgedragen geschillen, dient sprake te zijn van een geschil. Deze taak dient nadrukkelijk onderscheiden te worden van de taak van de Afdeling bestuursrechtspraak om te beslissen op aan haar op grond van een wet door een rechtbank gestelde prejudiciële vraag. In de praktijk zal bij de toepassing van de onderhavige regeling sprake zijn van een geschil tussen de afdeling toezicht van de CTIVD of de TIB enerzijds en de verantwoordelijke minister anderzijds over de vraag of de verleende toestemming dan wel de uitvoering van een bevoegdheid in overeenstemming is met het gestelde bij of krachtens de Wiv 2017 en het bepaalde in dit wetsvoorstel. Daarmee is sprake van een geschil zoals bedoeld in artikel 30b van de Wet op de Raad van State.

Benadrukt moet worden dat de thans voorgestelde regeling inzake beroep en de voorlopige voorziening een regeling *sui generis* is. Hoewel veel elementen zijn ontleend aan de Algemene wet bestuursrecht, is de regeling nadrukkelijk geen bijzonder bestuursprocesrecht en de bepalingen uit de Algemene wet bestuursrecht zijn dan ook niet van toepassing. Met deze regeling wordt slechts beoogd een tijdelijke voorziening te treffen die weliswaar in lijn is met de aanbevelingen van de ECW, maar waarmee niet vooruit wordt gelopen op definitieve aanpassingen van het stelsel van toets en toezicht, de rol van de rechter daarin en dienovereenkomstige wijzigingen van de Wiv 2017.

De beroepsprocedure
Artikel 14 bevat een regeling voor het instellen van beroep bij de Afdeling Bestuursrechtspraak van de Raad van State en bevat de volgende, voornamelijk procedurele, voorschriften.
a. een limitatieve opsomming van de oordelen van de TIB en de CTIVD waartegen de verantwoordelijke minister beroep kan instellen;
b. een bepaling waaruit blijkt dat het instellen van beroep geen schorsende werking heeft;
c. een termijn van zes dagen voor het indienen van een beroepschrift door de minister vanaf het moment dat de TIB of de CTIVD het oordeel schriftelijk aan de verantwoordelijke minister heeft medegedeeld;
d. bij indiening van het beroepschrift worden alle relevante gegevens vertrouwelijk aan de Afdeling bestuursrechtspraak verstrekt;

e. behoudens gevallen waarin de Afdeling bestuursrechtspraak kennelijk onbevoegd is, het beroep kennelijk niet-ontvankelijk, kennelijk ongegrond of kennelijk gegrond is, kan de TIB of de CTIVD binnen zes dagen na indiening van het beroepschrift een verweerschrift indienen;
f. bij indiening van het verweerschrift kunnen aanvullende gegevens (d.w.z. gegevens die niet reeds zijn verstrekt bij indiening van het verweerschrift) vertrouwelijk worden verstrekt aan de Afdeling bestuursrechtspraak;
g. de Afdeling bestuursrechtspraak kan zowel de minister als de TIB of CTIVD verzoeken om binnen een door de Afdeling te bepalen termijn aanvullende gegevens te verstrekken;
h. de Afdeling bestuursrechtspraak nodigt de partijen zo spoedig mogelijk uit voor een (inhoudelijke) zitting, tenzij de Afdeling bestuursrechtspraak van oordeel is dat zij kennelijk onbevoegd is, of het beroep kennelijk niet-ontvankelijk, kennelijk ongegrond of kennelijk gegrond is;
i. de behandeling van de zaak vindt plaats met gesloten deuren;
j. de Afdeling bestuursrechtspraak doet binnen twee weken uitspraak, gerekend vanaf de dag na die waarop het verweerschrift is ingediend, of de termijn daarvoor is verstreken. In bijzondere omstandigheden kan deze termijn met een week worden verlengd;
k. de uitspraak wordt gemotiveerd en kan strekken tot gehele of gedeeltelijke onbevoegdverklaring, niet-ontvankelijkverklaring, ongegrondverklaring of gegrondverklaring van het beroep;
l. indien de uitspraak strekt tot gehele of gedeeltelijke gegrondverklaring van het beroep bepaalt de Afdeling zelf wat de gevolgen zijn van de uitspraak;
m. de uitspraak van de Afdeling bestuursrechtspraak is niet openbaar en wordt in afschrift toegezonden aan de verantwoordelijke minister en de afdeling toezicht dan wel de toetsingscommissie;
n. een verplichting tot geheimhouding voor alle betrokkenen;
o. de plicht om de beide kamers der Staten-Generaal te informeren over het oordeel van de afdeling toezicht, waarbij de regeling inzake vertrouwelijkheid onverkort van toepassing is.

De beroepsprocedure vangt aan met het indienen van een beroepschrift. Omdat er in de regel sprake zal zijn van een lopend inlichtingenonderzoek en de (voorgenomen) uitoefening van de bevoegdheid van groot operationeel belang is, zijn de termijnen voor het indienen van een beroepschrift, een verweerschrift en de einduitspraak relatief kort. Deze korte termijnen zijn ook om een andere reden noodzakelijk, namelijk vanwege het feit dat het beroep geen schorsende werking heeft (artikel 14, tweede lid). Wanneer de rechtmatigheid van de uitoefening van een bevoegdheid ter discussie staat, is het van belang op de kortst mogelijke termijn duidelijkheid te verkrijgen over de rechtmatigheid. Zoals hiervoor reeds uiteen is gezet, kan een oordeel van de afdeling toezicht van de CTIVD nadelige gevolgen hebben voor een inlichtingenonderzoek, in het bijzonder wanneer de uitoefening van een bevoegdheid ingevolge artikel 13, eerste lid, juncto tweede lid, onder a, naar het oordeel van de afdeling toezicht van de CTIVD beëindigd dient te worden. Hoewel beroep mogelijk is tegen een dergelijk oordeel, is het onvermijdelijk dat er enige tijd zit tussen het vastgestelde oordeel van de afdeling toezicht van de CTIVD en de uitspraak in beroep. In die tussenliggende periode wordt informatie gemist en kan het zicht op een target verloren gaan. Om dit te voorkomen wordt in artikel 15 een regeling voorgesteld waarmee een voorlopige voorziening kan worden getroffen die ook kan strekken tot het verlenen van

schorsende werking aan het oordeel, de daaraan door de afdeling toezicht van de CTIVD verbonden gevolgen of beide. Deze procedure wordt verderop in deze paragraaf toegelicht.

In de praktijk zal sprake zijn van een geschil tussen de afdeling toezicht van de CTIVD of de TIB enerzijds en de verantwoordelijke minister anderzijds over de vraag of de verleende toestemming dan wel de uitvoering van een bevoegdheid in overeenstemming is met het gestelde bij of krachtens de Wiv 2017 en het bepaalde in dit wetsvoorstel. Het beroepschrift zal derhalve gronden bevatten ter onderbouwing van het standpunt van de minister inzake een verleende toestemming (bij een oordeel van de TIB) dan wel inzake de uitvoering van de in artikel 13, eerste lid, genoemde bevoegdheden (bij een oordeel van de afdeling toezicht van de CTIVD).

Het toetsingskader voor de Afdeling wordt gevormd door het bepaalde bij of krachtens de Wiv 2017, het onderhavige wetsvoorstel en de toepasselijke internationaal- en Europeesrechtelijke normen. Het zwaartepunt van de beoordeling zal naar verwachting liggen bij een oordeel over de juiste toepassing van de vier algemene toetsingsmaatstaven voor de toepassing van bevoegdheden door de diensten, te weten: noodzaak, proportionaliteit, subsidiariteit en gerichtheid en de daarbij behorende belangenafweging. Politiek-bestuurlijke of doelmatigheidsoverwegingen spelen hierbij geen rol.

Vanzelfsprekend staat het de Afdeling vrij om te bepalen op welke wijze en met welke intensiteit zal worden getoetst. Wel is de mate waarin de wetgever marges heeft gelaten in dit kader van belang. In de Wiv 2017 kunnen de marges per bevoegdheid verschillen waardoor de toetsingsintensiteit ook voor de TIB en de afdeling toezicht van de CTIVD kan verschillen. Dit betekent logischerwijs ook dat de marges voor de bij de Afdeling bestuursrechtspraak ter toetsing voorliggende oordelen kunnen verschillen. Binnen zo'n oordeel kunnen er bovendien onderdelen zijn die zich lenen voor verschillende soorten toetsingsintensiteit. Zo zal wetsuitleg doorgaans niet voor marginale toetsing in aanmerking komen, waar dat bij de beoordeling van een feitencomplex soms wel aangewezen kan zijn.

Ten behoeve van de beoordeling dient de Afdeling te beschikken over alle relevante stukken die betrekking hebben op het geschil. Hieronder valt in elk geval het verzoek om toestemming, het (gemotiveerde) oordeel van de TIB of de afdeling toezicht van de CTIVD, alsmede eventuele onderliggende stukken. Vanwege de korte termijnen is het van belang dat de Afdeling direct over alle relevante stukken beschikt, zodat zij op de kortst mogelijke termijn tot een uitspraak kan komen. Ook is voorzien in een bepaling waarmee zowel de minister als de afdeling toezicht en de TIB verplicht zijn op een daartoe strekkend verzoek van de Afdeling bestuursrechtspraak alle door de Afdeling relevante geachte inlichtingen mondeling dan wel schriftelijk, te verstrekken, ook buiten de zitting (artikel 14, zevende lid). Vanwege het staatsgeheime karakter van de stukken, worden de stukken en inlichtingen uitsluitend vertrouwelijk aan de Afdeling ter beschikking gesteld. Hierover zullen nadere (praktische) afspraken worden gemaakt.

De Afdeling bestuursrechtspraak kan tot vier uitspraken komen. Ten eerste de onbevoegdverklaring van de Afdeling. Vervolgens de niet-ontvankelijkverklaring van het

beroep. Hierbij valt te denken aan een te laat ingediend beroepschrift of het ontbreken van procesbelang. Tevens kan het beroep ongegrond verklaard worden. Het oordeel van de TIB of de afdeling toezicht van de CTIVD blijft in dat geval in stand en de verantwoordelijke minister dient alsdan uitvoering te geven aan een oordeel van de afdeling toezicht van de CTIVD als bedoeld in artikel 13, vierde lid. Dit is anders wanneer het beroep gegrond wordt verklaard. In dat geval moet de vraag worden beantwoord welke rechtsgevolgen zijn verbonden aan de uitspraak. Ingevolge het dertiende lid is het in dat geval aan de Afdeling bestuursrechtspraak zelf om te bepalen wat de gevolgen zijn van een gehele of gedeeltelijke gegrondverklaring en waarbij de uitspraak van de Afdeling dus afwijkt van het oordeel van TIB of de afdeling toezicht van de CTIVD. In lijn met artikel 8:72 Awb zijn hierbij meerdere situaties voorstelbaar. Zo kan de Afdeling bepalen dat de rechtsgevolgen (gedeeltelijk) in stand blijven, de Afdeling kan zelf in de zaak voorzien of opdracht geven tot een nieuwe weging waarbij de overwegingen van de Afdeling in acht moeten worden genomen maar de Afdeling kan ook een voorlopige voorziening treffen.

De behandeling van de zaak geschiedt met gesloten deuren. Het gaat immers om de uitvoering van bevoegdheden door de diensten waarmee per definitie inzicht ontstaat in het actuele kennisniveau van de betreffende dienst, de personen en organisaties die in onderzoek zijn en door de diensten aangewende geheime bronnen. Het behoeft geen betoog dat een openbare behandeling zich niet verdraagt met deze belangen. In het verlengde hiervan is ook bepaald dat de uitspraak van de Afdeling niet openbaar is. Dit roept de vraag op doe deze bepaling zich verhoudt tot artikel 121 van de Grondwet op grond waarvan is bepaald uitspraken in het openbaar geschieden. In dit verband is de bijzondere positie van de Raad van State van belang. De Afdeling bestuursrechtspraak is onderdeel van de Raad van State, maar de Raad van State behoort niet tot de rechterlijke macht (artikel 116 Grondwet juncto artikel 2 Wet op de rechterlijke organisatie). De Raad van State is een Hoog College van Staat waarbij aan de Afdeling bestuursrechtspraak rechtsprekende bevoegdheid is toegekend (artikel 30b Wet op de Raad van State). De Afdeling is dus een rechterlijk college in plaats van onderdeel van de rechterlijke macht. Uit de toelichting op artikel 121 Grondwet volgt dat het gaat om de openbaarheid van terechtzittingen, vonnissen en uitspraken van gerechten die tot de rechterlijke macht behoren.[16] Op grond hiervan is artikel 121 Grondwet dus niet van toepassing op de uitspraken van de Afdeling bestuursrechtspraak. De openbaarheid van zittingen en uitspraken is separaat in de Awb geregeld. In deze regeling is wel voorzien in de verzending van een afschrift van de uitspraak aan de betrokken partijen (artikel 14, veertiende lid).

In het verlengde hiervan is bepaald dat eenieder die betrokken is bij de behandeling van het beroep verplicht is tot geheimhouding. Deze bepaling hangt samen met de geheimhoudingsplicht uit de Wiv 2017 (artikelen 135 en 136) en beoogt een effectieve taakuitvoering van de diensten te bevorderen. Dat kan alleen indien de activiteiten die de diensten verrichten geheim zijn en blijven. De hier bedoelde geheimhouding gaat dan ook verder dan de bij rechtszaken gebruikelijke geheimhouding. In die zaken is er altijd een zekere mate van openbaarheid, bijvoorbeeld op de zitting waar ook stukken uit het dossier worden voorgehouden en besproken. Het gaat hier echter om staatsgeheime informatie die

[16] TK 1979/80, 16162, nr. 3, p. 21 bij artikel 6.9

op geen enkele wijze openbaar mag worden en waarbij schending van de geheimhouding grote gevolgen kan hebben en een ernstig strafbaar feit oplevert.

Tot slot is bepaald dat van een uitspraak van de Afdeling terstond mededeling wordt gedaan aan de beide kamers der Staten-Generaal. Daarbij is artikel 12, derde en vierde lid, Wiv 2017 van overeenkomstige toepassing. Nu het hier om uitspraken gaat over de toepassing van bijzondere bevoegdheden in het kader van lopende inlichtingenonderzoeken is artikel 12, derde lid, Wiv 2017 van toepassing. De informatie kan door de minister daarom vertrouwelijk worden verstrekt. In de praktijk betekent dat, dat de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD) van de Tweede Kamer wordt geïnformeerd.

Zoals hiervoor reeds is toegelicht is de voorgestelde regeling een procedure *sui generis*. Op grond van artikel 30a, vijfde lid, van de Wet op de Raad van State zullen nadere procedurele en praktische afspraken worden gemaakt.

Voorlopige voorziening
Artikel 15 bevat een regeling waarmee een voorlopige voorziening kan worden getroffen naar aanleiding van een vastgesteld oordeel van de afdeling toezicht van de CTIVD als bedoeld in artikel 14, eerste lid, onder a. Het wetsvoorstel laat de inhoud van de voorziening vrij, wel geldt de eis dat ze voorlopig is, in die zin dat de bodemrechter zich er niet door gebonden mag weten. Naar verwachting zal vooral gebruikt worden gemaakt van deze procedure teneinde schorsende werking te verlenen aan het oordeel van de afdeling toezicht, de daaraan door de afdeling toezicht van de CTIVD verbonden gevolgen of beide, zodat onomkeerbare operationele gevolgen voor de diensten voorkomen kunnen worden. Om deze reden bepaalt het derde lid van artikel 15 dat het verzoek om een voorlopige voorziening de werking van een oordeel van de afdeling toezicht van de CTIVD opschort vanaf het moment dat de afdeling toezicht het oordeel heeft vastgesteld totdat de voorzitter van de kamer die over het beroepschrift oordeelt (die in deze regeling optreedt als voorzieningenrechter; hierna: de voorzitter) uitspraak heeft gedaan. Op deze manier wordt voorkomen dat onduidelijkheid ontstaat over de rechtmatigheid van de verwerkte gegevens in het kader van de bevoegdheid die onderwerp van het beroep is.

De procedure voor de voorlopige voorziening is vergelijkbaar met de beroepsprocedure met dien verstande dat de termijnen aanzienlijk korter zijn. De procedure verloopt als volgt:

a. de voorzitter van de kamer die over het beroepschrift oordeelt fungeert in deze procedure als voorzieningenrechter en kan op verzoek van de verantwoordelijke minister een voorlopige voorziening treffen indien beroep is of wordt ingesteld tegen een bindend oordeel van de afdeling toezicht van de CTIVD en onverwijlde spoed dit noodzakelijk maakt;
b. de termijn voor het instellen van beroep is langer (zes dagen, artikel 14, derde lid) dan de termijn voor het verzoek om een voorlopige voorziening. Om te voorkomen dat gegevens verloren gaan in de tussenliggende periode kan het verzoek om een voorlopige voorziening ook gedaan worden voorafgaand aan het instellen van beroep;
c. de termijn voor het verzoek om een voorlopige voorziening is 48 uur en vangt aan op de dag nadat de afdeling toezicht van de CTIVD het vastgestelde oordeel schriftelijk aan de verantwoordelijke minister heeft medegedeeld:
d. het verzoek om een voorlopige voorziening heeft schorsende werking en werkt terug tot het moment dat de afdeling toezicht het oordeel en de daaraan te verbinden gevolgen vaststelt;
e. de bepalingen uit de beroepsprocedure ex artikel 14 zijn van overeenkomstige toepassing

voor zover het gaat om de vertrouwelijke verstrekking van onderliggende en aanvullende stukken (artikel 14, vierde, zesde en zevende lid), de mogelijkheid om een verweerschrift in te dienen waarbij de termijn geen zes dagen maar 48 uur is (artikel 14, vijfde lid), de inhoudelijke zitting behoudens gevallen van kennelijke onbevoegdheid van de voorzitter, kennelijke niet-ontvankelijkheid van het verzoek of een kennelijk ongegrond of kennelijk gegrond verzoek (artikel 14, achtste en negende lid), de bepalingen omtrent geheimhouding (artikel 14, tiende en vijftiende lid) en de verstrekking van een afschrift van de uitspraak (artikel 14, veertiende lid);
f. de voorzitter doet zo spoedig mogelijk gemotiveerd uitspraak en stelt het moment vast waarop de voorlopige voorziening vervalt:
g. de uitspraak kan luiden: de onbevoegdverklaring van de voorzitter, niet-ontvankelijkverklaring van het verzoek, afwijzing van het verzoek of gehele of gedeeltelijke toewijzing van het verzoek;
h. de mogelijkheid om direct uitspraak te doen op het beroep indien nader onderzoek niet noodzakelijk is indien de verantwoordelijke minister en de afdeling toezicht hiermee instemmen.

De verantwoordelijke minister kan een verzoek om een voorlopige voorziening indienen bij de voorzitter indien onverwijlde spoed, gelet op de betrokken belangen, dat vereist. Wanneer sprake is van onverwijlde spoed zal per geval worden beoordeeld, maar daarvan zal in de regel al snel sprake zijn bij een oordeel en daaraan verbonden gevolgen door de afdeling toezicht, aangezien het bestreden oordeel en de daaraan verbonden gevolgen per definitie leidt tot onomkeerbare gevolgen, namelijk de uitoefening van een bevoegdheid moet worden beëindigd of bepaalde gegevens moeten worden verwijderd en vernietigd. Hiermee wordt immers informatie gemist, het zicht op een target kan verloren gaan en het verwijderen en vernietigen van gegevens kan niet meer ongedaan worden gemaakt.

De voorlopige voorziening kan ook tegelijkertijd met het instellen van het beroep worden aangevraagd waarbij tevens de mogelijk bestaat voor 'kortsluiting' (artikel 15, zesde en zevende lid). Dit houdt in dat wanneer, hangende het beroep, een verzoek om een voorlopige voorziening wordt gedaan en de voorzitter van oordeel is dat na de daartoe gehouden zitting nader onderzoek redelijkerwijs niet kan bijdragen aan de beoordeling van de bodemzaak, hij daarin direct uitspraak kan doen. Wel is vereist dat een zitting heeft plaatsgevonden waar ook de hoofdzaak aan de orde is gekomen. Bepalend is uiteindelijk of de informatie die schriftelijk en ter zitting is verkregen van dien aard is dat mag worden aangenomen dat nader onderzoek geen relevante nieuwe gegevens of argumenten zal opleveren.

5. Grondrechtelijke en mensenrechtelijke aspecten

De in het wetsvoorstel voorziene afwijkingen dan wel aanvullingen ten opzichte van hetgeen in de Wiv 2017 is bepaald, voldoen als zodanig aan de eisen die daaraan vanuit nationaal als internationaal recht worden gesteld. Een en ander ziet met name op aanvulling dan wel verduidelijking van aspecten van bijzondere bevoegdheden die reeds in de Wiv 2017 zijn geregeld, waarbij met name wordt gewezen op de in dit wetsvoorstel voorziene bijschrijfmogelijkheden (de artikelen 5, tweede lid, 10 en 11) alsmede op de introductie van een zelfstandige grondslag voor de bijzondere bevoegdheid tot verkenning met het oog op de toepassing van artikel 48 Wiv 2017, die uitsluitend binnen de kaders van de tijdelijke wet

kan worden ingezet (artikel 7). Daarnaast worden enkele afwijkingen voorgesteld ten aanzien van in de Wiv 2017 opgenomen regelingen voor de verdere verwerking van verworven gegevens en enkele procedurele eisen (o.a. de artikelen 4, 5, eerste lid, 6, 9). Tot slot wordt voor de toepassing van hetgeen in deze tijdelijke wet is geregeld, voorzien in extra rechtswaarborgen door de invoering van bindend toezicht door de afdeling toezicht van de CTIVD en een beroepsmogelijkheid bij de Afdeling bestuursrechtspraak van de Raad van State ter zake van aangewezen oordelen van de TIB en de afdeling toezicht.

Overeenkomstig artikel 10, eerste lid, van de Grondwet wordt met de regeling in het wetsvoorstel voorzien in een formeel-wettelijke grondslag die is vereist ingeval sprake is van een beperking van het recht op bescherming van de persoonlijke levenssfeer. Bij de hiervoor genoemde aanvullingen die zijn opgenomen in het wetsvoorstel gaat het om situaties waarbij (veelal) sprake zal zijn van de verwerking van persoonsgegevens, waarmee eo ipso sprake is van een beperking van het hiervoor genoemde grondrecht.

Tevens wordt voldaan aan de eisen die artikel 8 van het Europees verdrag tot bescherming van de rechten van de mens (EVRM) stelt. Allereerst wordt opgemerkt dat bij de totstandkoming van de Wiv 2017 reeds is geoordeeld dat die wet aan artikel 8 EVRM en het door het Europees Hof voor de Rechten van de Mens (EHRM) ter zake uitgebrachte jurisprudentie voldoet. In hoofdstuk 9 van de memorie van toelichting bij het voorstel van wet die tot de Wiv 2017 heeft geleid is uitvoerig stilgestaan bij de grondrechtelijke en mensenrechtelijke aspecten van de in dat wetsvoorstel voorgestelde regeling voor de activiteiten van de inlichtingen- en veiligheidsdiensten, ook waar het gaat om de bevoegdheid tot het binnendringen van geautomatiseerde werken. De in dit kader voorgestelde aanvullingen ten opzichte van de (bijzondere) bevoegdheden die de diensten reeds op grond van de Wiv 2017 toekomen, zijn noodzakelijk om de aan de diensten opgedragen taken in het kader van de nationale veiligheid effectief te kunnen uitvoeren. Zoals in hoofdstuk 1 van deze memorie van toelichting is uiteengezet zijn de dreigingen in het cyberdomein van zo'n ernstige aard dat het noodzakelijk is om de mogelijkheden om daar onderzoek naar te kunnen doen ter voorkoming (dan wel mitigering) van mogelijke schade aan Nederland of Nederlandse belangen van essentieel belang is. Voor een deel betreft het, zie de voorgestelde bijschrijfmogelijkheden, een aanvulling op reeds bestaande bevoegdheden om deze – rekening houdend met de snelheid en wendbaarheid van de actoren in het cyberdomein – effectiever in te kunnen zetten, waar naar hun aard geen andere, minder belastende alternatieven bestaan. De inzet zal – overeenkomstig de in artikel 26 van de Wiv 2017 neergelegde eisen – altijd proportioneel dienen te zijn. Waar het gaat om de bijschrijving zal aan het voldoen aan deze en andere eisen conform artikel 31 Wiv 2017 aantekening dienen te worden gehouden. Daarenboven zal ook van de uitoefening van deze bijschrijfmogelijkheden de afdeling toezicht van de CTIVD terstond worden geïnformeerd, zodat ze daar ook – indien de afdeling dat nodig acht – hun aandacht direct op kunnen richten teneinde de rechtmatigheid daarvan te beoordelen en zonodig deze te doen beëindigen. Met de voorgestelde bevoegdheid tot verkenning met het oog op de toepassing van artikel 48 Wiv 2017 (interceptie in bulk van telecommunicatie) wordt – vooralsnog beperkt tot de toepassing in het kader van deze wet - een zelfstandige grondslag geïntroduceerd, die uitsluitend in het teken staat aan een effectievere toepassing van de bevoegdheid tot OOG-interceptie. Ook deze bevoegdheid is noodzakelijkheid in verband met

de aan de diensten opgedragen taak in het kader van de nationale veiligheid. Naar zijn aard bestaat voor de met deze bevoegdheid te verwerven gegevens geen alternatief. Het geen hiervoor is gesteld met betrekking tot het voldoen aan de eisen van artikel 26 Wiv 2017 geldt mutatis mutandis ook voor de uitoefening van deze bevoegdheid.

Een belangrijk element ter versterking van de waarborgen waarmee beperkingen op het recht op persoonlijke levenssfeer dienen te worden omgeven, is in de Wiv 2017 gerealiseerd door de introductie van de TIB en de door deze instantie uit te voeren bindende toets ex ante. Daarmee werd een waarborg bij de toepassing van bijzondere bevoegdheden geïntroduceerd, die overigens op meer bevoegdheden ziet dan waartoe gelet op de huidige stand van zaken van de jurisprudentie van het EHRM daarin voorzien moet zijn. Bij de voorbereiding van onderhavig wetsvoorstel is ook acht geslagen op de recente jurisprudentie van het EHRM die betrekking heeft op de bevoegdheden tot bulkinterceptie en de verwerking van bulkdatasets en welke gevolgen daaraan verbonden moeten worden. [17] Uit de analyse van die jurisprudentie, die ook aan beide kamers der Staten-Generaal is toegezonden, is gebleken dat de huidige wet ter zake nog steeds voldoet aan de eisen van het EVRM. Die conclusie is ook van belang voor de regeling van onderhavig wetsvoorstel mede in het licht van de aard en inhoud van de voorgestelde bepalingen in relatie tot de Wiv 2017. Een bindende ex ante toets wordt door het EHRM op dit moment slechts in een beperkt aantal gevallen geëist, te weten bij bulkinterceptie (in de Wiv 2017 aangeduid als onderzoeksopdrachtgerichte interceptie; OOG-interceptie) en de vaststelling van categorieën van selectoren toe te passen op de in bulk geïntercepteerde gegevens. Daarnaast geldt dat de inzet van bijzondere bevoegdheden jegens journalisten die gericht zijn op het achterhalen van de bron van een journalist ook een bindende toets vooraf vereist; in de Wiv 2017 is die toets – evenals die welke ziet op de inzet van bijzondere bevoegdheden die kunnen leiden tot de verwerving van vertrouwelijke communicatie tussen een advocaat en cliënt – in de handen gelegd van de rechtbank Den Haag; die rechtbank verleent overigens de toestemming en toetst dus niet – zoals bij de TIB – een door de minister verleende toestemming. Uit recente jurisprudentie van het Hof van Justitie van de Europese Unie (HvJEU), waar het gaat om de zogeheten e-privacyrichtlijn, vloeit inmiddels voort dat de zogeheten stomme tap, te weten de real time interceptie van uitsluitend verkeersgegevens (dus geen inhoud), ook een vooraf bindende toets door een onafhankelijke instantie vergt.[18] Bij de eerstvolgende wijziging van de Wiv 2017 zal wettelijk worden geregeld. Voor de tussenliggende periode wordt bezien op welke wijze aan deze eis kan worden voldaan.

De in dit wetsvoorstel opgenomen wijzigingen waar het gaat om de ex ante toets door de TIB betreffen op een enkele uitzondering na, te weten de bevoegdheid tot verkennen met het oog op de toepassing van artikel 48 Wiv 2017 (zie artikel 7), wijzigingen waarvoor vanuit perspectief van het EVRM en de jurisprudentie van het EHRM geen noodzaak bestaat om die te onderwerpen aan een bindende voorafgaande toets. De bijzondere bevoegdheid ex artikel 7 van het wetsvoorstel is op een vergelijkbare manier geregeld als andere (vergelijkbare)

[17] Uitspraken van EHRM van 25 mei 2021 in de zaken Big Brother Watch and others v. The United Kingdom (application nos. 58170/13, 62322/14 en 24960/15) en Centrum for Rättvisa v. Sweden (application no. 35252/08).
[18] Uitspraken van HvJEU van 6 oktober 2020 in de zaak Privacy International v. UK (C-623/17) en de gevoegde zaken Quadrature du Net e.a. (C-511/18 en C-512/18). Een regeling ter zake in de Wiv 2017 wordt in het kader van de herziening van de Wiv meegenomen en vooruitlopend daarop zullen met de TIB afspraken worden gemaakt over de toets met betrekking tot de real time interceptie van verkeersgegevens.

bijzondere bevoegdheden in de Wiv 2017. Niet alleen is voorzien in toestemming van de minister en een bindende toets van de TIB ter zake, maar ook overigens zal aan de algemene eisen voor de (verdere) verwerking van gegevens – zoals de toets aan noodzakelijkheid, subsidiariteit en proportionaliteit - moeten worden voldaan. Voorts wordt gewezen op de strikte doelbinding bij de verwerking van de gegevens (geen gebruik van de gegevens voor het inlichtingenproces) en de beperkte kring van personen die van de geïntercepteerde gegevens kennis mogen nemen.

Bij de andersoortige wijzigingen is voorzien in adequaat toezicht. Daar waar de eis van toestemming van de minister dan wel de toetstaak van de TIB komt te vervallen, wordt voorzien in bindend toezicht door de afdeling toezicht van de CTIVD. Dat geldt ook in andere gevallen, waarbij voorzien is in aanvullende mogelijkheden tot bijschrijving. Waar aan de orde is voorzien in een meldplicht voor de minister dan wel de TIB aan de afdeling toezicht opdat daarmee van meet af aan het toezicht kan worden geactiveerd.

Dit past ook in het streven te komen naar een dynamisch toezicht op de taakuitvoering van de diensten, waarbij de gehele keten aan activiteiten – van begin tot eind - aan toezicht is onderworpen. Door aan de oordelen van de afdeling toezicht een bindend karakter toe te kennen, betekent dat een forse versterking van het toezicht en wordt daarmee ook het recht op bescherming van de persoonlijke levenssfeer – waarop dat toezicht voor een groot deel betrekking heeft – adequaat geborgd.

Naar ons oordeel vallen de in het wetsvoorstel voorziene wijzigingen binnen de reikwijdte die aan bij het verdrag aangesloten staten is gelaten om in het kader van de nationale veiligheid maatregelen te nemen die een gerechtvaardigde beperking van het door artikel 8 EVRM gegarandeerde recht op – kort gezegd – privacy met zich brengen. De voorgestelde regeling – inhoudende enerzijds de zeer beperkt inperking van de toetsbevoegdheid van de TIB voorafgaand aan de bevoegdheidsuitoefening die anderzijds wordt vervangen door bindend toezicht in de fase van uitvoering van de bevoegdheid – betekent per saldo dat het geheel van waarborgen bij de uitoefening van de bevoegdheden waarop onderhavig wetsvoorstel specifiek betrekking heeft tenminste gelijk blijft.

De in dit wetsvoorstel voorziene inperking van de toetsbevoegdheid van de TIB waarvoor een bindende toezichtsbevoegdheid van de afdeling toezicht voor in de plaats treedt betreft een tijdelijke voorziening en loopt daarmee niet vooruit op mogelijke aanpassingen van het stelsel van toets en toezicht mede naar aanleiding van de aanbevelingen van rapport van de ECW en het daaromtrent nader in te nemen kabinetsstandpunt. Het is dan ook een voorziening in het kader van deze tijdelijke wet en naar zijn aard dus ook tijdelijk van karakter. Bij de herziening van de Wiv 2017 naar aanleiding van het rapport van de evaluatiecommissie zal immers het gehele stelsel van toets en toezicht, de eventuele samenvoeging van TIB en CTIVD, alsmede de (positionering van de) behandeling van klachten en vermoedens van misstanden op zijn merites en in onderlinge samenhang bezien dienen te worden. Daarbij zullen uiteraard ook de ervaringen die worden opgedaan bij de toepassing van deze wet worden betrokken.

Tot slot. Hetgeen is bepaald in het Grondrechtenhandvest van de Europese Unie blijft hier buiten toepassing. De voorgestelde regeling betreft een maatregel in het kader van de

nationale veiligheid, waarvoor ingevolge artikel 4, tweede lid, van het Verdrag van de Europese Unie de uitsluitende verantwoordelijkheid berust bij de lidstaten.

6. Gevolgen verbonden aan de uitvoering van de wet

6.1 Algemeen

In het kader van de uitvoerbaarheid van de wet heeft een ketentest met de TIB, CTIVD en de diensten plaatsgevonden. In deze ketentest is aan de hand van het concept van het wetsvoorstel bezien of de wet een oplossing biedt voor de geconstateerde problematiek en uitvoerbaar is. Er volgt een aanvullende ketentest ten aanzien van het beroep bij de Afdeling bestuursrechtspraak van de Raad van State. Over het gehele wetsvoorstel vindt een uitvoeringstoets plaats waar in meer detail de uitvoerbaarheid van de wet en de impact op de zowel de diensten als TIB, CTIVD en Raad van State wordt bezien.

1.2 De uitvoeringsconsequenties voor de diensten

PM

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

PM

1.4 Regeldruk

In het wetsvoorstel wordt in een tweetal artikelen, te weten artikel 7 (de zelfstandige grondslag voor de bevoegdheid tot verkennen met het oog op toepassing van artikel 48 Wiv 2017) en artikel 11 (aanvulling bijschrijfmogelijkheid bij artikel 54 Wiv 2017), voorzien in een beperkte verruiming van de medewerkingsplicht van derden bij de toepassing van het bepaalde in deze artikelen. Het betreft een verruiming ten opzichte van de verplichtingen (informatieverplichtingen en inhoudelijke verplichtingen[19]) die reeds uit de toepassing van de Wiv 2017 voortvloeien. In paragraaf 3.3.2 van deze memorie is ingegaan op hetgeen de bevoegdheid ex artikel 7 van het wetsvoorstel inhoudt en in paragraaf 3.5 op de aanvulling van de bijschrijfmogelijkheid van artikel 54 Wiv 2017. In beide gevallen is medewerking vereist van een aanbieder van een communicatiedienst[20] en bij de toepassing van artikel 54 daarnaast ook van personen of instanties die – kortgezegd – beroeps- of bedrijfsmatig opslagdiensten voor gegevens[21] aanbieden.

Bij de bevoegdheid ex artikel 7 van het wetsvoorstel is medewerking van de communicatie-aanbieder vereist bij de uitvoering van een door de verantwoordelijke minister verleende (en

[19] In het kader van onderzoek naar de regeldrukeffecten van een regeling wordt onderscheid gemaakt naar verplichtingen tot het verschaffen van inlichtingen (informatieverplichtingen) en verplichtingen tot het doen of nalaten van handelingen of gedragingen (inhoudelijke verplichtingen).

[20] Een aanbieder van een communicatiedienst is in artikel 46 Wiv 2017 als volgt gedefinieerd: de natuurlijke of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of die gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst.

[21] In artikel 54, eerste lid, onder b, Wiv 2017 is deze – naast de aanbieder van een communicatiedienst aangewezen instantie - als volgt omschreven: een persoon of instantie die in het kader van de uitoefening van een beroep of bedrijf de opslag verzorgt van door derden via geautomatiseerde werken verwerkte gegevens en waartoe voor die derde rechtstreeks geautomatiseerde toegang bestaat.

door de TIB rechtmatig geachte) toestemming voor het verkennen ten behoeve van de inzet van de bijzondere bevoegdheid tot onderzoeksopdrachtgerichte interceptie ex artikel 48 Wiv 2017. Voor de uitoefening van deze bevoegdheid is waar het gaat om verkenning op de kabelgebonden infrastructuur de medewerking vereist van de desbetreffende aanbieder. Hij krijgt daartoe een opdracht en is verplicht medewerking te verlenen. Hiervoor bestaat geen alternatief. Het betreft hier een inhoudelijke verplichting. Deze situatie is vergelijkbaar met de medewerking die bij de uitoefening van artikel 48 Wiv 2017 aan de orde is. In artikel 7, vijfde lid, van het wetsvoorstel is dan ook artikel 53 van de Wiv 2017 van overeenkomstige toepassing verklaard. Dat betekent onder meer dat de aanbieder die verplicht is medewerking te verlenen naar redelijkheid aanspraak heeft op vergoeding uit ’s-Rijks kas van de investerings-, exploitatie- en onderhoudskosten voor de technische voorzieningen die zijn of worden gemaakt teneinde te kunnen voldoen aan de opdracht, alsmede van de door de aanbieder gemaakte administratie- en personeelskosten rechtstreeks voortvloeiend uit het voldoen aan de opdracht; in de Regeling kosten aftappen Wiv 2017 zijn nadere regels gesteld met betrekking tot de vaststelling en vergoeding van de kosten. De inzet van de bijzondere bevoegdheid van artikel 48 Wiv 2017 op de kabelgebonden infrastructuur en daarmee ook de toepassing van artikel 7 van het wetsvoorstel is vooralsnog beperkt tot een enkele aanbieder. De daaraan verbonden kosten zijn operationele kosten voor de diensten die uit de geheime begroting van de diensten worden bekostigd en daarmee als staatsgeheim gekwalificeerd. De omvang van deze kosten zijn evenwel inzichtelijk voor de Commissie voor de Inlichtingen en Veiligheidsdiensten van de Tweede Kamer. De Algemene Rekenkamer houdt daarop toezicht.

Bij de bevoegdheid ex artikel 11 van het wetsvoorstel wordt de uitoefening van de bijzondere bevoegdheid van de diensten om – mits met een verkregen toestemming van de minister en een rechtmatigheidsoordeel van de TIB – zich te wenden tot kortgezegd de aanbieder van een opslagdienst voor gegevens met de opdracht om die gegevens te verstrekken (zogeheten disk images) ook mogelijk gemaakt ingeval het target tussentijds van aanbieder verandert of naast een bestaande opslagdienst ook van een andere opslagdienst gebruik gaat maken. Op deze wijze wordt voorkomen dat hiervoor de hele toestemmingsprocedure moet worden doorlopen, waardoor kostbare tijd bij het verkrijgen van voor het onderzoek noodzakelijke gegevens verloren gaat. Het gaat ook hier om inhoudelijke verplichtingen. En ook hier geldt dat voor het voldoen aan die opdracht ingevolge artikel 54, zesde lid, artikel 13.6, tweede en derde lid, van de Telecommunicatiewet van overeenkomstige toepassing is. Dat betekent dat men aanspraak hebben op vergoeding uit 's Rijkskas van de door hen gemaakte administratiekosten en personeelskosten rechtstreeks voortvloeiend uit het voldoen aan een opdracht op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2017. Omtrent het aantal gevallen waarin van de voorgestelde mogelijkheid gebruik wordt gemaakt alsmede de daaraan verbonden kostenvergoeding kan vanwege het staatsgeheime karakter geen openbare informatie worden verschaft.

7. Advies en consultatie

PM consultatie CTIVD, TIB, Afdeling bestuursrechtspraak; advies RvS; ATR

8. Overgangsrecht

In artikel 16 van het wetsvoorstel is voorzien in een overgangsrechtelijke regeling met als strekking dat op de bij de TIB voor toetsing aanhangige toestemmingen op het moment van inwerkingtreding van de wet de in het onderhavige wetsvoorstel opgenomen regeling niet van toepassing is.

II. Artikelsgewijze toelichting

In het algemeen deel van de memorie van toelichting is reeds bij de bespreking van de verschillende onderwerpen reeds uitvoerig ingegaan op de inhoud van de meeste artikelen, zodat daarnaar wordt verwezen.

Artikel 2

In artikel 2, derde lid, is bepaald dat de diensten in verzoeken om toestemming voor de inzet van een bijzondere bevoegdheid in aanvulling op het bepaalde in artikel 29, tweede lid, Wiv 2017 dienen aan te geven of daarbij uitvoering wordt gegeven aan het bepaalde in onderhavig wetsvoorstel. Op deze wijze is kenbaar voor zowel de TIB als de CTIVD dat in het kader van de toets en het toezicht het bepaalde in dit wetsvoorstel in acht genomen dient te worden.

Artikel 3

In artikel 3, eerste lid, wordt aan de TIB de bevoegdheid toegekend indien zij van oordeel is dat met betrekking tot een aan haar voorgelegde toestemming ten onrechte wordt gesteld dat daarmee uitvoering wordt gegeven aan het bepaalde in de tijdelijke wet, zij de minister hiervan terstond op de hoogte stelt. Dit is een oordeel dat buiten het reguliere toetsingskader van de TIB valt. Deze bevoegdheid is aan de TIB toegekend, omdat toepassing van de tijdelijke wet haar bevoegdheid op onderdelen rechtstreeks raakt. Tegen het oordeel van de TIB staat beroep open bij de Afdeling bestuursrechtspraak. De TIB toetst vervolgens de voorgelegde toestemming, waarbij ze het bepaalde in de tijdelijke wet buiten toepassing laat.

Artikel 12

Met het oog op een goede uitvoering van de aan hen opgedragen taak in het kader van de toepassing van de tijdelijke wet is het noodzakelijk dat de TIB en de afdeling toezicht inlichtingen kunnen verstrekken daar waar de taak van de TIB (ex ante toets in de autorisatiefase, noodzakelijk voor het kunnen inzetten van een bevoegdheid) raakt aan die van de afdeling toezicht van de CTIVD (ex durante, te weten bij de uitvoering van de bevoegdheid) en vice versa. Het gaat dan om inlichtingen betreffende bevindingen die de toetsingscommissie onderscheidenlijk de afdeling toezicht bij de uitvoering van hun taak in het kader van deze wet hebben opgedaan en die voor de taakuitvoering van de ander van belang kan zijn. Nu de Wiv 2017 een gesloten stelsel van gegevensverstrekking kent, ook waar het gaat om verstrekking door de TIB aan de afdeling toezicht en vice versa, dient daarvoor een wettelijke grondslag te worden gecreëerd. Artikel 12 voorziet daarin.

Een voorbeeld van toepassing van de bevoegdheid tot het verstrekken van inlichtingen betreft de situatie, waarbij het noodzakelijk wordt geacht om een nadere toelichting op de

door de TIB aangegeven aandachtspunten te geven in het kader van de meldingen die de TIB op grond van artikel 3, tweede en derde lid, alsmede artikel 7, derde lid, aan de afdeling toezicht van de CTIVD heeft gedaan inzake door haar uitgesproken rechtmatigheidsoordelen. Dat kan bijdragen aan een effectievere uitvoering van de aan de afdeling toezicht opgedragen taak.

Een ander voorbeeld betreft de situatie, waarbij de TIB en de afdeling toezicht van de CTIVD in het kader van een aan de TIB voorgelegde toestemming, inhoudende een verlenging van de bijzondere bevoegdheid als bedoeld in de artikelen 45, eerste lid, onder b, 47, of 54 van de Wiv 2017, inlichtingen van de afdeling toezicht wenst te ontvangen voor zover de toestemming tevens betrekking heeft op situaties waarbij eerder toepassing is gegeven aan de in artikelen 5, tweede lid, 10, eerste lid, en 11, eerste lid, van deze wet bedoelde bevoegdheid en de desbetreffende gegevens noodzakelijk zijn voor een effectieve uitvoering van de aan de TIB opgedragen taak. Het gaat dan om situaties die vanwege het feit dat het bijschrijvingen betreft op eerder door de TIB beoordeelde en rechtmatig geachte toestemmingen van de minister voor de toepassing van de desbetreffende bevoegdheden en die bijschrijvingen deel uit kunnen maken van een voor goedkeuring voorgelegde toestemming tot verlenging van de desbetreffende bevoegdheid, de noodzaak bij de TIB aanwezig wordt geacht om ter zake van de afdeling toezicht nadere inlichtingen over de bijschrijvingen verstrekt te krijgen. Immers de bijschrijvingen hebben plaatsgevonden tijdens de uitvoering van de desbetreffende bevoegdheid waarop – mede door de voorgeschreven melding – de afdeling toezicht van de CTIVD actief toezicht heeft kunnen houden. Met name in de gevallen dat een bijschrijving die eerder door de afdeling toezicht onrechtmatig is gevonden, maar wel is opgenomen in een verleende toestemming tot verlenging van de inzet van de bevoegdheid, kan het voor de TIB relevant zijn om van de overwegingen van de afdeling toezicht ter zake kennis te kunnen nemen. Dat laat onverlet dat de TIB vervolgens een onafhankelijk rechtmatigheidsoordeel over de voorgelegde toestemming tot verlenging dient te geven.

In artikel 23 van de Wiv 2017 is aan de hoofden van de diensten de wettelijke plicht opgedragen om zorg te dragen voor de geheimhouding van daarvoor in aanmerking komende gegevens, de geheimhouding van daarvoor in aanmerking komende bronnen waaruit gegevens afkomstig zijn alsmede de veiligheid van de personen met wier medewerking gegevens worden verzameld. Het gaat hier om gegevens die door de diensten ten behoeve van de aan de TIB onderscheidenlijk de afdeling toezicht opgedragen taken zijn verstrekt conform de daartoe bestaande wettelijke verplichtingen. Nu verstrekking van gegevens tussen de TIB en de afdeling toezicht wordt mogelijk gemaakt, is het wenselijk dat met het oog op de wettelijke plicht van de diensthoofden inzichtelijk blijft welke gegevens bij welke instantie berusten. Hiertoe bepaalt artikel 12, tweede lid, dat het hoofd van de betrokken dienst omtrent de te verstrekken gegevens wordt geïnformeerd.

Tot slot is het wenselijk dat omtrent de toepassing van de in artikel 12 opgenomen regeling door de TIB en de afdeling toezicht voldoende transparantie wordt betracht teneinde te voorkomen dat er discussie ontstaat omtrent de onafhankelijkheid van beide instanties in

hun oordeelsvorming. Voorgesteld wordt om dat in het jaarlijks uit te brengen verslag van werkzaamheden te doen opnemen.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,

De Minister van Defensie,