Toetsingscommissie
Inzet Bevoegdheden

Binnenhof 19
2513 AA Den Haag
www.tib-ivd.nl

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
t.a.v. de Minister van Binnenlandse Zaken en Koninkrijksrelaties

Ministerie van Defensie
t.a.v. de Minister van Defensie

Referentienummer: BWP3221331
Den Haag, 14 april 2022

Betreft: Reactie op het concept wetsvoorstel Tijdelijke wet onderzoek AIVD en MIVD naar landen met een offensief cyberprogramma

Geachte mevrouw Bruins Slot, geachte mevrouw Ollongren,

Met deze brief reageert de TIB op bovengenoemd concept wetsvoorstel. Omwille van de leesbaarheid daarvan wordt in deze brief gesproken over het wetsvoorstel en vangt deze brief aan met een samenvatting van deze reactie.

Samenvatting
Het wetsvoorstel voorziet in een gedeeltelijke verschuiving van de bindende TIB-toets vooraf naar een bindend CTIVD toezicht tijdens de uitoefening van bevoegdheden. Dit vereist een andere, veel intensievere samenwerking en informatie-uitwisseling tussen TIB en CTIVD. Met name artikel 12 lid 2 van het wetsvoorstel staat daaraan in de weg en verhindert effectief toezicht. Het wetsvoorstel is onvoldoende duidelijk met betrekking tot het vermelden van technische risico's in verzoeken. Het wetsvoorstel voorziet in een uitbreiding van een aantal bestaande bijzondere bevoegdheden. Gedurende een toestemmingsperiode kan een bevoegdheid zonder voorafgaande toets uitgebreid worden door zogenaamd "bijschrijven". De kabelbevoegdheid wordt uitgebreid met het intercepteren van internetverkeer van streamingsdiensten en binnenlands internetverkeer.

1. Inleiding

Het wetsvoorstel voorziet in een uitbreiding ten aanzien van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (hierna: Wiv 2017) en in een gedeeltelijke verplaatsing van toets naar toezicht als het gaat om landen met een offensief cyberprogramma. De TIB ziet het niet als haar taak zich in deze reactie uit te laten over de noodzaak daarvan. Wel ziet de TIB het als haar taak uit te leggen wat de uitbreiding betekent. In de Memorie van Toelichting bij het wetsvoorstel (hierna: MvT) is dit niet altijd even duidelijk. De TIB zal zich voorts uitlaten over de voorgestelde verschuiving van toets naar toezicht en het voorgestelde beroep. Tot slot zal de TIB een enkele opmerking wijden aan iets wat niet is voorgesteld, maar wél wettelijk geregeld moet worden.

2. Uitbreiding van bevoegdheden

2.1. Samenloop met de Wiv 2017

De bevoegdheden van de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst (hierna: de diensten) staan in de Wiv 2017. Het wetsvoorstel geeft een regeling die daarop deels in aanvulling en deels in afwijking is. Een uitgangspunt van de Wiv 2017 is dat de

diensten gegevens slechts voor een bepaald doel mogen verwerven. Eenmaal verworven gegevens kunnen onder voorwaarden breder binnen de diensten worden gebruikt. Dat uitgangspunt geldt in dit wetsvoorstel ook. De reikwijdte van het wetsvoorstel is echter beperkt tot onderzoeken van de diensten naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen. Die landen worden door het kabinet aangewezen in de (geheime) geïntegreerde aanwijzing (GA). In de MvT wordt beschreven dat een bevoegdheid alleen onder toepassing van de tijdelijke wet kan worden ingezet als het zwaartepunt van de inzet op onderzoeksopdrachten binnen de reikwijdte van de tijdelijke wet valt. Het daarbij gegeven voorbeeld van een target dat voorkomt in verschillende onderzoeken geeft onvoldoende beeld bij de impact daarvan. Het kan ook gaan om veel bredere inzet dan gericht op één target, zoals kabelinterceptie en bulkhacks. Zolang het zwaartepunt ligt bij een cyberonderzoek, kunnen alle verworven gegevens ook worden bekeken door andere onderzoeksteams. Zo komen alle gegevens, ook die van personen die niet in aandacht van de dienst staan en dat ook nooit zullen staan, breder beschikbaar binnen de diensten. Het betekent een forse uitbreiding van bevoegdheden van de diensten, waarmee waarborgen die in het Wiv 2017 regime gelden buiten toepassing blijven.

2.2. Strategische operaties
In paragraaf 2.2.2. van de MvT is beknopt aangegeven dat het noodzakelijk wordt geacht dat de diensten ook strategische operaties mogen uitvoeren. De paragraaf is kennelijk opgenomen om aan te geven dat de diensten meer moeten kunnen dan onder de Wiv 2017. Dat is ook herhaaldelijk aangegeven door de diensten. Maar wat de diensten meer mogen volgens het wetsvoorstel wordt niet duidelijk gemaakt.

In de inleiding van de MvT is een *supply chain aanval* beschreven. Een supply chain aanval richt zich op een leverancier, teneinde misbruik te maken van de legitieme toegang die de leverancier heeft tot een computersysteem van een target. Via de leverancier wordt het target dan gehackt.
De beschrijving in de MvT heeft betrekking op een in 2020 uitgevoerde supply chain aanval. Er is bij deze aanval een achterdeur ingebouwd in een legitieme update van monitoringsoftware Orion van softwarebedrijf SolarWinds. Deze aangepaste update is vervolgens via het netwerk van SolarWinds wereldwijd verspreid onder haar klanten, waaronder veel overheidsinstellingen en bedrijven in de vitale sector. Eenmaal geïnstalleerd kon de aanvaller via het softwareprogramma binnendringen in de systemen van al deze klanten. Door de Amerikaanse overheid, maar ook door Nederland, is deze aanval geattribueerd aan de Russische inlichtingendienst SVR.

Is het de bedoeling van dit wetsvoorstel om de Nederlandse diensten onder deze tijdelijke wet ook de bevoegdheid te geven een supply chain aanval uit te mogen voeren? Moeten de diensten meer kunnen hacken dan zij nu kunnen binnen de Wiv 2017? Als dat het geval is, dan moet dat ook klip en klaar worden gesteld. Met deze beschrijving in het wetsvoorstel wordt de samenleving onvoldoende geïnformeerd.

De TIB leest geen uitbreiding van bevoegdheden ten opzichte van de Wiv 2017. De TIB ziet in de paragraaf slechts een verduidelijking dat de diensten strategisch mogen opereren. Hoe en wat is niet aangegeven en dat maakt het voor de TIB lastig toetsbaar.

2.3. Verruiming bijschrijfmogelijkheid

Bijschrijven is het proces waarbij de diensten gedurende de uitoefening van een bevoegdheid op een persoon of organisatie die bevoegdheid ook gaan inzetten op andere apparaten die worden gebruikt door die persoon of organisatie. Dat mag op grond van de Wiv 2017 als een persoon of organisatie andere apparaten gaat gebruiken. Bijvoorbeeld: er wordt een tap gezet op het telefoonnummer van een persoon en deze persoon krijgt een nieuw telefoonnummer. De diensten hoeven dan niet langs de minister en de TIB, maar mogen het nieuwe telefoonnummer ook onder de tap zetten. In het wetsvoorstel wordt die bevoegdheid in het kader van de hack- en tapbevoegdheid verruimd. Voor de bevoegdheid tot het geven van opdrachten aan aanbieders van telecommunicatie en gegevensopslag om gegevens te verstrekken, wordt een vergelijkbare ruime bijschrijfmogelijkheid geïntroduceerd.

Wat betekent die verruiming? De TIB heeft de bijschrijfmogelijkheid in de Wiv 2017 zo uitgelegd dat het moet gaan om apparaten die exclusief worden gebruikt door de persoon of organisatie waar het onderzoek zich op richt. Deze exclusiviteitseis vervalt in dit wetsvoorstel. Ook als anderen een apparaat gebruiken, mogen de diensten direct gaan hacken of tappen. Cyberactoren maken ook vaak gebruik van gedeelde infrastructuur. Cyberactoren hacken dan bijvoorbeeld een server bij een hostingprovider, die wordt gehuurd door verschillende klanten zoals de bakker om de hoek, maar ook een huisartsenpraktijk en een kerkgenootschap. Zij gebruiken de serverruimte om hun bestanden op te slaan of om hun website toegankelijk te maken. Ook deze servers zou de dienst, ongeacht van wie er nog meer gebruik maakt van de server, zonder voorafgaande toets van de minister en de TIB mogen hacken of tappen als de cyberactor in onderzoek die server heeft gehackt. Op een server kunnen wel duizenden websites tegelijk toegankelijk gemaakt worden.

Het wetsvoorstel houdt ook in dat andere gehackte apparaten bijgeschreven mogen worden. In de MvT wordt een digitale aanvalscampagne van cyberactor APT31 besproken, in open bronnen gerelateerd aan China. Beschreven is dat de cyberactor systemen van Europese, ook Nederlandse, burgers hackt en samen gebruikt in haar aanvalscampagne. Recentelijk heeft de MIVD ook bekend gemaakt dat de Russische militaire geheime dienst GRU Nederlandse routers van particulieren en het midden- en kleinbedrijf heeft gehackt in het kader van een aanvalscampagne.[1] De MIVD informeert deze slachtoffers. Dat is een uitzondering. Uit de MvT spreekt nu juist niet het voornemen om gebruikers te waarschuwen, maar te hacken en te tappen (om zo het zicht op de cyberactor niet te verliezen). Het wetsvoorstel betekent concreet dat de diensten, als zij zien dat een cyberactor de thuisrouter van de familie Jansen misbruikt voor een aanvalscampagne zo'n thuisrouter ook mogen hacken en het internetverkeer dat daar overheen gaat mogen tappen. De intentie om te gaan bijschrijven moet dan wel in het verzoek worden opgenomen, de uitvoering daarvan is onderworpen aan toezicht van de CTIVD, maar niet elke router of server wordt vooraf beoordeeld. Als er honderden thuisrouters of routers van het midden- en kleinbedrijf in beeld komen, kunnen al deze routers (dus ook van Nederlandse burgers) direct, zonder voorafgaande toestemming, gehackt en getapt worden.

De CTIVD zal bindend toezicht gaan uitoefenen op deze praktijk. Dat vereist goede werkafspraken tussen de CTIVD, de TIB en de diensten. Deze verruiming is niettemin stevig. Het is een politieke afweging of het belang van een snellere inzet van de diensten zo zwaar moet wegen dat

[1] MIVD ontdekt Russische spionnen in Nederlandse routers, nieuwsbericht ministerie van Defensie, 3 maart 2022.

voorafgaande toetsing moet vervallen. Het huidige systeem voorziet reeds in een snelle toets op noodzakelijkheid en proportionaliteit van bijschrijvingen, door een toezichthouder die 52 weken per jaar toetst. Kan het oordeel van de TIB niet worden afgewacht, dan is er een spoedprocedure waarin de diensten van start kunnen gaan na mondelinge toestemming van de minister.

2.4. Bewaartermijn bulkdatasets verkregen uit een hack

Bulkdatasets zijn grote gegevensverzamelingen van hoofdzakelijk personen die niet in de aandacht van de diensten staan en dat ook nooit zullen staan. Tegelijkertijd kunnen die gegevensverzamelingen wel gegevens bevatten van bepaalde personen waarvan de identiteit pas gedurende het onderzoek wordt achterhaald. De Wiv 2017 bevat een regeling dat bulkdatasets verkregen door (met name) de inzet van de hackbevoegdheid uiterlijk na anderhalf jaar op relevantie dienen te worden onderzocht. Gegevens die niet relevant zijn moeten worden vernietigd. Het belang voor de nationale veiligheid om bepaalde bulkdatasets langduriger te mogen onderzoeken op relevantie wordt door de TIB gezien. Tegelijkertijd maakt het langduriger bewaren van bulkdatasets inbreuk op de grondrechten van vele personen.

In het wetsvoorstel is in artikel 6 een regeling opgenomen waarbij de relevantiebeoordeling uit de Wiv 2017 buiten toepassing wordt verklaard als de bulkdataset is verkregen met toepassing van de tijdelijke wet. De regeling komt erop neer dat gegevens niet meer zo spoedig mogelijk beoordeeld moeten worden op relevantie en een andere termijn gaat gelden, namelijk een termijn van een jaar. Die termijn kan telkens worden verlengd met een jaar. Er geldt geen maximale termijn, ook niet omdat de tijdelijke wet op zichzelf verlengd kan worden. Het roept de vraag op hoe deze regeling zich verhoudt met het in artikel 8 EVRM vastgelegde vereiste van voorzienbaarheid. Een inbreuk op het privéleven is toegestaan voor zover bij de wet is voorzien. Het niet vastleggen in wetgeving van een maximale bewaartermijn van bulkdata kan door het Europees Hof voor de Rechten van de Mens aangemerkt worden als tekortkoming.[2] Het wetsvoorstel voorziet wel in een bindende toets van de CTIVD op een verzoek tot verlenging van de relevantiebeoordeling. Het is de vraag of het bindend toezicht als effectieve remedie kan worden gezien. In het wetsvoorstel is hier geen aandacht aan besteed.

Daarnaast moet worden opgemerkt dat het verzoek om de bewaartermijn met een jaar te verlengen ook mag worden onderbouwd met de noodzaak voor onderzoeksopdrachten die niet onder de tijdelijke wet vallen. Hiervoor gelden de opmerkingen die in paragraaf 2.1 zijn gemaakt. Ook dit is een verruiming.

2.5. Kabelinterceptie

In het wetsvoorstel wordt een aantal wijzigingen voorgesteld voor onderzoeksopdrachtgerichte interceptie. Dat is niet alleen de interceptie van satellietverkeer, maar gaat vooral over het intercepteren van internetverkeer op de kabel. Daarom gaat het in deze reactie alleen over kabelinterceptie.

Het wetsvoorstel kent een nieuwe, aparte regeling voor de verkenning van gegevensstromen. In de MvT is aangegeven dat het noodzakelijk is om in een aanvraag voor daadwerkelijke kabelinterceptie

[2] Big Brother Watch e.a. t. VK (EHRM, 58170/13 e.a.) en Centrum för Rättvisa t. Zweden (EHRM, 35252/08), r.o. 423.

("productie") zo goed mogelijk te kunnen omschrijven op welke gegevensstromen zal worden geïntercepteerd. Dat is dan ook het doel.

Dat een aparte, zelfstandige wettelijke regeling wordt gegeven voor de verkenning van gegevensstromen wordt door de TIB als een welkome wijziging gezien. Goed in ogenschouw moet echter genomen worden dat de bevoegdheid ten opzichte van het huidig wettelijk kader wordt verruimd. Niet alleen in gebruikte termen is dat zichtbaar. Waar in de Wiv 2017 gesproken wordt over "snapshotting" (een momentopname om de potentiële inlichtingenwaarde van verkeer vast te stellen) wordt hier gesproken over verkenning. Nadrukkelijker ziet men de verruiming in het buiten toepassing verklaren van het vereiste van gerichtheid. Het gerichtheidsvereiste is op 6 april 2018 als beleidsregel vastgelegd en van toepassing verklaard bij de voorafgaande toets van de TIB op verzoeken tot kabelinterceptie. Dat was één van de waarborgen die het kabinet introduceerde na het raadgevend referendum in maart 2018, waarbij een meerderheid tegen de Wiv 2017 stemde.[3] Door de TIB is het criterium gehanteerd "in hoeverre is bij verwerving sprake van het tot een minimum beperken van niet strikt voor het onderzoek noodzakelijk gegevens, gelet op de technische en operationele omstandigheden van de casus". Door de regering werd dit een bruikbaar criterium geacht. Bij de behandeling in de Eerste Kamer van de wijzigingswet Wiv 2017 op 8 juni 2021 noemde de minister van Binnenlandse Zaken en Koninkrijksrelaties de eis van gerichtheid een hele belangrijke waarborg die moest worden verankerd in de Wiv 2017. Dat is ook gebeurd. Op 14 juli 2021 kwam de eis van gerichtheid in de Wiv 2017. Deze waarborg wordt met dit wetsvoorstel bij kabelinterceptie buiten toepassing gesteld. De verkenning voor kabelinterceptie is bedoeld om een aanvraag voor daadwerkelijke kabelinterceptie goed te kunnen onderbouwen. Waarom het vaststellen van potentiële inlichtingenwaarde op een gegevensstroom niet zo gericht mogelijk kan plaatsvinden maakt de MvT onvoldoende inzichtelijk. Het thans buiten toepassing stellen van de waarborg, in combinatie met de maximale bewaartermijn van 12 maanden, maakt dat het te verwachten is dat de diensten langdurig zullen gaan beschikken over zeer veel (internet)gegevens van burgers. Wat de wijziging voor de toetsing van de verzoeken door de TIB betekent is niet geheel op voorhand te zeggen. De gerichtheidseis heeft weliswaar een zelfstandige betekenis, maar ook als het wetsvoorstel tot wet wordt verheven zal de TIB nog altijd de proportionaliteit dienen te beoordelen.

In artikel 8 van het wetsvoorstel, waar het gaat om de daadwerkelijke kabelinterceptie voor het inlichtingenwerk, wordt de TIB opgedragen twee aspecten bij haar beoordeling te betrekken. Dat zijn een indicatie van de te verwerven gegevensstromen en een indicatie van de wijze waarop de reductie van gegevens binnen de gehele keten van verwerving invulling krijgt. Volgens de MvT is dit een verduidelijking van de eisen die bij de invulling van de eisen van proportionaliteit en gerichtheid moeten worden betrokken. Tegelijkertijd geeft het voorgestelde wetsartikel, maar ook de toelichting, de TIB de ruimte ook andere aspecten te betrekken in die toets. De MvT stelt verder dat vanwege het dynamisch karakter van kabelinterceptie de diensten slechts een indicatie van die reductie van gegevens kunnen geven. De TIB ziet in het artikel en de toelichting geen beperking in haar beoordelingsruimte van de proportionaliteit en gerichtheid.

Waar de bevoegdheid voor daadwerkelijke kabelinterceptie voor het inlichtingenwerk wel significant wordt uitgebreid is als het gaat om streamingsdiensten en Nederland-Nederlandverkeer.

[3] Brief van de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie van 6 april 2018 (Kamerstukken II 2017-2018, 34 588, nr. G).

Het voorstel betekent dat alle verkeer van en naar streamingsdiensten (zoals Netflix, Spotify, YouTube e.d.) ook getapt mag worden. Ook internetverkeer met oorsprong en bestemming Nederland (Jan uit Amsterdam bezoekt Nu.nl) mag in bulk getapt gaan worden. Er wordt met dit wetsvoorstel teruggekomen op eerdere toezeggingen, gedaan door de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie, dat dit internetverkeer niet getapt zal worden.[4] Gelet op de samenloop met de Wiv 2017 (besproken in paragraaf 2.1) heeft ook deze verruiming betekenis in onderzoeken die niet vallen onder de reikwijdte van deze wet.

2.6. Overzicht

De belangrijkste wijzigingen in het wetsvoorstel die een verruiming van bevoegdheden van de diensten tot gevolg hebben staan hieronder uitgewerkt in een tabel.

Wiv 2017	**Tijdelijke wet**
Bijschrijfmogelijkheid alleen voor exclusief in gebruik zijnde infrastructuur	Bijschrijfmogelijkheid ook voor gehackte servers, thuisrouters en andere apparaten
Maximale termijn beoordeling relevantiebepaling 1,5 jaar, zo spoedig mogelijk uitvoeren, niet bindend toezicht CTIVD	Beoordeling op relevantie niet langer zo snel mogelijk, geen maximale termijn, bindend toezicht CTIVD
Verkennen gegevensstromen kabelinterceptie gericht en ter verificatie	Verkennen gegevensstromen kabelinterceptie ongericht en ten behoeve van verkenning
Kabelinterceptie voor inlichtingenwerk alleen onderzoeksopdrachtgericht	Ongerichte kabelinterceptie voor inlichtingenwerk
Kabelinterceptie van verkeer streamingsdiensten en Nederland-Nederlandverkeer (buiten cyber defence onderzoek) direct vernietigd	Kabelinterceptie van verkeer streamingsdiensten en Nederland-Nederlandverkeer

3. Toets en toezicht

De hiervoor benoemde verruiming van de bijzondere bevoegdheden van de diensten gaat gepaard met een gedeeltelijke verplaatsing van het toezicht. Van belang is dat de CTIVD daarover een daadwerkelijk bindende toetsbevoegdheid krijgt. Over het geheel genomen acht de TIB het voorgestelde stelsel onder voorwaarden toezichtbaar.

3.1. Scannen en GDA

In het wetsvoorstel staat dat de TIB niet langer voorafgaand bindend toetst over de rechtmatigheid van de toestemming voor het zogenaamde scannen in het kader van de hackbevoegdheid. Met deze bevoegdheid kunnen de diensten voorafgaand aan het daadwerkelijk hacken een scan uitvoeren om in te schatten wat de mogelijkheden voor de hack zijn. Bijvoorbeeld welke applicaties benaderbaar zijn en of er poorten open staan. Het toezicht verschuift, door de CTIVD hierop bindend toezicht te geven. De TIB kan zich vinden in deze wijziging, gelet op de zeer beperkte inbreuk die het scannen oplevert. Met een voorafgaande toestemming van de minister en toetsing daarvan door de TIB is die bevoegdheid thans te zwaar belegd.

In het wetsvoorstel wordt daarnaast voorgesteld de TIB niet langer voorafgaand bindend te laten toetsen over de toestemming voor geautomatiseerde data-analyse op gegevens verkregen met kabelinterceptie. Deze verschuiving van toezicht verdedigbaar, gelet op de aard van de

[4] Idem.

bevoegdheid die meer het karakter heeft van verdere verwerking van gegevens. De CTIVD zal hier bindend toezicht op houden.

3.2. Informatie-uitwisseling TIB en CTIVD
De gedeeltelijk verplaatsing van het toezicht betekent de introductie van dynamisch toezicht op het werk van de diensten. Er zal door de CTIVD veel meer toezicht moeten worden gehouden op handelingen binnen lopende operaties, die zonder voorafgaande rechtmatigheidstoets van de TIB zijn gestart. Informatie-uitwisseling tussen de TIB en CTIVD is dan essentieel.

De TIB acht het voorgestelde stelsel toezichtbaar, mits artikel 3 lid 3 wordt gewijzigd en artikel 12 lid 2 wordt geschrapt. In beide artikelen is een informatieplicht bepaald. Indien de TIB de CTIVD wil wijzen op mogelijk voor het toezicht relevante aandachtspunten moet de TIB dat volgens artikel 3 lid 3 doen onder gelijktijdige melding aan de minister.

Daarnaast moet de TIB volgens artikel 12 lid 2 het diensthoofd vooraf informeren over de te verstrekken inlichtingen aan de CTIVD. Deze bepalingen staan effectief en onafhankelijk toezicht in de weg. Als de TIB vooraf de ondertoezichtgestelde moet informeren over informatie-uitwisseling met de andere toezichthouder, weet de ondertoezichtgestelde al waar het toezicht zich op richt.

3.3. Technische risico's en onbekende kwetsbaarheden
In het wetsvoorstel vervalt de voorafgaande, bindende toets van de TIB op de technische risico's van een hackoperatie en wordt het toezicht daarop bindend bij de CTIVD belegd. In de praktijk betekent dit dat het vereiste vervalt dat een verzoek tot toestemming een omschrijving van de technische risico's bevat. Het wetsvoorstel is op dit punt wat de TIB betreft onvoldoende duidelijk.

Ten eerste zal de TIB bij de bindende toets vooraf nog steeds de proportionaliteit van een hackoperatie moeten toetsen. Voor deze toets is van belang dat duidelijk wordt gemaakt wat en wie gehackt gaan worden, maar deels ook hoe dat zal gebeuren en welke risico's daarbij aanwezig kunnen zijn. Bijvoorbeeld het risico dat een kritiek computersysteem van een derde onbedoeld zou uitvallen tijdens de hack. Dat lijkt ook nog steeds de bedoeling te zijn, als gekeken wordt naar de passage in paragraaf 3.2.4.1 van de MvT waarin wordt opgemerkt dat de TIB nog steeds de op het moment van het verzoek om toestemming voor inzet van de bevoegdheid voorzienbare risico's van de inzet van de bevoegdheid kan betrekken. Vervolgens staat echter beschreven dat het een beperkt en hoger abstractieniveau zal hebben en voorts is aangegeven dat niet meer hoeft te worden beschreven dat een onbekende kwetsbaarheid wordt ingezet. De MvT mist op dit punt de scherpte die nodig is om precies te duiden wat wel en wat niet door de TIB mag worden gevraagd en moet worden beoordeeld.

Ten tweede valt het volgende op. Als niet meer hoeft te worden beschreven wat de diensten in technisch opzicht gaan doen, weet de minister feitelijk ook niet waarvoor zij toestemming verleent. Daarmee lijken de technische risico's buiten het zicht van de minister te komen. Geeft de minister met haar toestemming dan een carte blanche aan de diensten? Met name bij de inzet van onbekende kwetsbaarheden in relatie tot het onderzoeksgebied van het wetsvoorstel roept dat vragen op. Als in een verzoek niet opgenomen hoeft te worden of onbekende kwetsbaarheden ingezet kunnen worden, valt de inzet daarvan dus ook buiten de toestemming van de minister. De CTIVD zal uiteraard toezicht houden, maar, is het de bedoeling van het wetsvoorstel dat de inzet van een onbekende kwetsbaarheid buiten de toestemming van de minister zal worden gehouden?

Ten derde wordt in de MvT niet voldoende ingegaan op de betekenis van de verplaatsing van het toezicht op technische risico's en het gebruik van onbekende kwetsbaarheden. De MvT spreekt over het toezicht van de CTIVD op logging van de uitvoering van de hackbevoegdheid. Dat betekent feitelijk dat een handeling reeds is uitgevoerd (want de handeling is weggeschreven in de logging van het computerssysteem waarop de hack wordt uitgevoerd). De CTIVD zou juist in staat moeten worden gesteld om (near) real time toezicht uit te kunnen voeren. Uitsluitend toezicht achteraf is vanwege de aard van hacken en de risico's daarvan onvoldoende. De hacker maakt immers afwegingen en keuzes op basis van zijn kennis en ervaringen, op basis waarvan hij overgaat tot talloze handelingen. Als er iets mis gaat (per ongeluk kan bijvoorbeeld een systeem van een derde omvallen) is toezicht uitsluitend op basis van logging onvoldoende. Dit om te voorkomen dat risico's zich daadwerkelijk manifesteren.

De CTIVD zal daarom in de gelegenheid gesteld moeten worden om vooraf goede afspraken te maken met de diensten over de invulling van dit toezicht, waarbij met name duidelijk is binnen welke kaders en/of bandbreedtes de diensten mogen opereren.

Op die manier kunnen de risico's door het vervallen van de toets vooraf gemitigeerd worden. In die kaders worden bandbreedtes verwoord, bijvoorbeeld een categorisering van soorten hackmethodes. In een verzoek tot toestemming wordt vervolgens een indicatie gegeven hoe de diensten voornemens zijn te opereren, op basis van de informatie die dan bekend is (wellicht uit een eerdere scan op het netwerk, zie paragraaf 3.1.). Daarin wordt dan tevens aangegeven dat, mocht het anders lopen, de diensten zullen opereren binnen een bepaalde bandbreedte zoals verwoord in het kader. Deze werkwijze geeft de diensten meer flexibiliteit, terwijl de minister haar afweging in volle omvang kan maken. De bindende toets vooraf van de TIB is gebaseerd op de indicatie die de diensten kunnen geven, terwijl de CTIVD bindend toezicht kan houden of de uitvoering blijft binnen de afgesproken kaders en daarmee rechtmatig is.

3.4. Beroep

De TIB heeft eerder, ook in haar gesprek met de Evaluatiecommissie Wiv 2017 die de beroepsprocedure voorstelde, aangegeven niet principieel tegen de introductie van een beroepsprocedure te staan. Wel is de TIB verrast dat niet is ingegaan op een recent verschenen rapport van een commissie bestaande uit drie hoogleraren (hierna: commissie Bovend'Eert), die op verzoek van de minister van Binnenlandse Zaken en Koninkrijksrelaties hebben gekeken naar recente uitspraken van het EHRM en het stelsel van toezicht.

De commissie Bovend'Eert plaatst vraagtekens bij de introductie van een aanvullende voorziening van geschilbeslechting bij de Afdeling bestuursrechtspraak. Niet alleen omdat de commissie niet overtuigd is van de noodzaak daarvan. Het introduceren van beroep kan het stelsel van toezicht ook fundamenteel veranderen. Het risico bestaat dat zich de facto een procedure in twee instanties ontwikkelt, waar alleen de diensten gebruik van kunnen maken.[5] De TIB onderschrijft dit punt. Personen die worden geraakt door inzet van de diensten, weten dat over het algemeen niet. Het beroep staat alleen open voor de diensten. Zij zullen die mogelijkheid alleen benutten als zij het niet eens zijn met het oordeel van de TIB. Daar waar de TIB te weinig ruimte zou geven en de diensten iets niet mogen, voorziet de wet dus in een snelle herkansingsmogelijkheid. Daar waar de

[5] Adviesrapport Naar een duurzaam en effectief stelsel van toezicht op de inlichtingen- en veiligheidsdiensten, Bovend'Eert, Lawson en Winter (2022), p. 37.

TIB teveel ruimte zou geven en de diensten meer mogen, kunnen de burgers die daardoor geraakt worden niet tegen die beslissing opkomen.

Aan het bezwaar van het eenzijdig beroep wordt in het voorstel geen aandacht besteed. Niet is beschreven waarom het niet mogelijk zou zijn om de belangen van de burger op dit punt te kunnen laten behartigen. Bijvoorbeeld door een onafhankelijke vertegenwoordiger van de burger aan te stellen, die in de gevallen die hij opportuun acht namens de burger beroep instelt.[6]

Over de regeling die thans in het wetsvoorstel is opgenomen merkt de TIB verder op dat de voorgestelde stelselwijziging alleen toezichtbaar is indien de CTIVD daadwerkelijk bindend toezicht verkrijgt. Essentieel daarbij is dat beroep niet per definitie opschortende werking heeft, anders zou het bindend toezicht geen echt bindend toezicht zijn. Indien de diensten onomkeerbare gevolgen willen voorkomen, staat nu de mogelijkheid van een voorlopige voorziening open. Dit is goed beschreven in het wetsvoorstel.

3.5. Effecten op de TIB

De introductie van het beroep levert meer werk op. Er is meer en intensiever overleg nodig met de CTIVD om dynamisch en effectief toezicht mogelijk te maken. Rechtseenheid tussen de TIB en CTIVD zorgt voor rechtszekerheid voor de diensten. Als de TIB en CTIVD tot dezelfde te hanteren kaders komen, zorgt dat er voor dat de diensten weten waar zij aan toe zijn. De motivering van beslissingen zal meer aandacht vragen, niet in de laatste plaats met het oog op een mogelijke beroepsprocedure in de concrete zaak. Ook de beroepsprocedure zelf zal werk opleveren, in de voorbereiding maar ook in de uitvoering. De TIB moet 52 weken per jaar in staat zijn om een beroepsprocedure te kunnen voeren.

De TIB zal dus in staat gesteld moeten worden om additioneel juridische ondersteuning in te kunnen zetten, zodat het toetsingsproces kan worden voortgezet zoals de diensten mogen verwachten: professioneel, snel en adequaat. Dit vormt een tweede belangrijke voorwaarde om te kunnen spreken van een toezichtbaar stelsel.

4. Grondrechtelijke en mensenrechtelijke aspecten

In deze paragraaf in de MvT is meegedeeld dat nog geen gevolg wordt gegeven aan de uitspraak van het Hof van Justitie van de Europese Unie van 6 oktober 2020.[7] Uit deze zaak, zo wordt in de MvT ook erkend, blijkt dat een zogeheten stomme tap (een real time tap op de verkeersgegevens van telecommunicatie, waaronder locatiegegevens) moet worden voorzien van een vooraf bindende toets door een onafhankelijke instantie. Deze toets zou door de TIB kunnen worden uitgevoerd. Aangekondigd is echter dat dit pas bij de eerstvolgende wijziging van de Wiv 2017 geregeld gaat worden. De implicatie van deze uitspraak is echter al langer bekend. Er lijkt tot nu toe niets gedaan te zijn met het invullen van een vereiste van nota bene het Hof van Justitie van de Europese Unie strekkende ter waarborging van grondrechten van de burger. Dat is opvallend.

[6] Een dergelijke vertegenwoordiger vertoont raakvlakken met de amicus curiae. De Algemene wet bestuursrecht is op dit punt zeer recent aangepast, waardoor de Afdeling bestuursrechtspraak andere dan partijen in de gelegenheid kan stellen opmerkingen te maken, zodat deze de Afdeling kan informeren en een beter, breder inzicht kan geven op de mogelijke maatschappelijke gevolgen van een te nemen beslissing. Zie Stb. 2020, 416.

[7] Uitspraken van het Hof van Justitie van de Europese Unie van 6 oktober 2020 in de zaak Privacy International t. Verenigd Koninkrijk (C623/17) en de gevoegde zaken Le Quadrature du Net e.a. (C511/18, C512/18 en C520-18).

5. Conclusie

Het voorstel voorziet in een uitbreiding van een aantal bijzondere bevoegdheden, zodat de diensten de dreiging die uitgaat van landen met een offensief cyberprogramma sneller kan aanpakken. Over de vraag of de voorgestelde uitbreiding noodzakelijk is laat de TIB zich niet uit. Dat is vooral een politieke vraag. Het geheel is naar oordeel van de TIB toezichtbaar, mits de informatieplicht wordt geschrapt en de benodigde additionele capaciteit voor de TIB wordt gerealiseerd.

Handtekening:

mr. M. Moussault
Voorzitter Toetsingscommissie Inzet Bevoegdheden