Bits of Freedom
Prinseneiland 97hs
1013 LN Amsterdam

Lotte Houwing
+31 6 8320 7546
lotte@bitsoffreedom.nl

bitsoffreedom.nl
IBAN: NL73 TRIO 0391 1073 80
KVK: 34 12 12 86, Amsterdam

Geachte Minister van Binnenlandse Zaken en Koninkrijksrelaties, geachte Minister van Defensie,

Bits of Freedom maakt graag van de gelegenheid gebruik om te reageren op het conceptwetsvoorstel Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma.[1]

De reactie die nu voorligt is gestoeld op de bijna decennia-lange betrokkenheid van Bits of Freedom en onze achterban bij de Wet op de inlichtingen- en veiligheidsdiensten. Ook hebben we de zorgen en aandachtspunten meegenomen die, in de behandeling van de Wiv 2017 en het referendum in 2018, door de samenleving zijn geuit.

In onze reactie gaan we eerst kort in op de context waarin het voorstel valt. We bespreken waarom het aannemelijk is dat het voorstel, in tegenstelling tot wat de titel doet vermoeden, zal leiden tot meer structurele aanpassingen aan geldende wetgeving, en we laten zien hoe dit voorstel zich niet beperkt tot één specifieke taak, maar ook daarbuiten grote implicaties heeft voor de rechten en vrijheden van burgers. Vervolgens bespreken we de voorgestelde uitbreidingen met betrekking tot de bevoegdheden van de geheime diensten. Tot slot zullen we stilstaan bij de voorgestelde aanpassingen aan het stelsel van waarborgen en toezicht.

1. Context

1.1 De maatschappelijke discussie rond de Wiv 2017

Dit voorstel moet worden bezien in de context van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017), waar het zich expliciet toe verhoudt. De introductie van de Wiv 2017 was controversieel. De maatschappelijke discussie leidde tot een referendum waarbij burgers zich met een nipte meerderheid uitspraken tegen de Wiv 2017 en voor een betere wet. Na dit zorgvuldige en uitgebreide maatschappelijke debat maken wij ons grote zorgen over dit nieuwe voorstel waarin opnieuw gevraagd wordt om het vergroten van de bevoegdheden van de geheime diensten, het steeds meer ongerichte karakter hiervan en het beknotten van het toezicht. Precies de onderwerpen die van 2015 tot en met 2018 zoveel reuring veroorzaakten.

Opnieuw zetten uw ministeries de fundamentele rechten en vrijheden van burgers onder druk. Daarmee lijken uw ministeries de grenzen niet te respecteren die de samenleving nog geen vijf jaar geleden in het referendum heeft gesteld aan de inbreuk die de diensten mogen maken op de privésfeer van alle inwoners van Nederland.

Sterker nog, met de introductie van dit voorstel wordt vooruitlopend op de aangekondigde wijziging van de Wiv 2017, en de lopende discussie daaromtrent, opnieuw een groot beroep

1 https://www.internetconsultatie.nl/tijdelijkewetcyber/b1

gedaan op de capaciteit van de Tweede Kamer en het maatschappelijk middenveld en de aandacht van de samenleving. Daarnaast staat het voorstel op gespannen voet met een binnen die lopende discussie door de Kamer aangenomen motie waarin de regering is verzocht om de bevoegdheden van de Toetsingscommissie Inzet Bevoegdheden (Tib) op geen enkele manier in te perken.[2] De titel en presentatie van het wetsvoorstel als tijdelijk en taakspecifiek verhullen daarnaast onterecht de daadwerkelijke impact van het voorliggende voorstel en dreigen daardoor aan de aandacht te ontsnappen.

1.2 De reikwijdte van het voorstel

In artikel 2 wordt omschreven dat onderliggend voorstel, in afwijking van de Wiv 2017, van toepassing is bij het verrichten van onderzoek naar door de inlichtingen- en veiligheidsdiensten naar *landen* met een offensief cyberprogramma tegen Nederland of Nederlandse belangen ("*cyber-defence*"). Daarmee laat de wet potentieel erg veel ruimte voor toepassing van de voorgestelde maatregelen. Zijn er tegenwoordig niet erg veel landen met een offensief cyberprogramma? Ook lijkt het voorstel zich niet te beperken tot statelijke actoren, maar lijkt zij ook van toepassing te zijn op instellingen of bedrijven uit een dergelijk land. Wellicht kan het voorstel de inzet van de voorgestelde maatregelen zelfs legitimeren bij onderzoeken naar/in een land, wanneer er in dat land een enkele hackersgroep offensieve activiteiten wenst te ontplooien tegen Nederland(se belangen). Daarmee is de potentiële reikwijdte van het voorstel erg breed en onvoldoende helder afgebakend. Ook wekt dit vragen op over in hoeverre dit aansluit bij de cyberdreiging waar de AIVD zich mee bezig houdt, zoals omschreven op haar website.[3]

Ook roept het vragen op over de afbakening en toepasbaarheid van deze wet dan wel de Wiv 2017 wanneer er onderzoek wordt gedaan vanuit verschillende taken die bij de inlichtingen- en veiligheidsdiensten zijn belegd. Om misbruik van bevoegdheden en het omzeilen van waarborgen te voorkomen en te zorgen voor voldoende duidelijkheid, controleerbaarheid en voorzienbaarheid is het van belang dat er helderder wordt afgebakend wanneer de Wiv 2017, en wanneer dit voorstel, van toepassing is en hoe er wordt omgegaan met een eventuele samenloop.

Bovendien mogen gegevens die met bevoegdheden op basis van het voorliggende voorstel worden verzameld, ook voor andere onderzoekstaken (buiten cyber-defence) worden gebruikt. In dat geval biedt het onderliggende voorstel enkel de legitimatie voor de inzet van de bevoegdheden waarmee grootschalig gegevens kunnen worden verzameld en er minder waarborgen en een ander toezichtsstelsel van kracht is, maar kunnen die vervolgens voor alle onderzoekstaken worden gebruikt. Daarmee heeft het voorstel ook buiten deze specifieke taak grote gevolgen voor de rechten en vrijheden van burgers. En dient het voorstel dus ook niet als een tot cyber-defence beperkt voorstel te worden behandeld.

2 Motie van het lid Leijten over het niet inperken van de bevoegdheden van de Toetsingscommissie Inzet Bevoegdheden, 29 924, ter vervanging van Nr 214 https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z13130&did=2021D28139
3 https://www.aivd.nl/onderwerpen/cyberdreiging

1.3 Stelselwijzigingen maken een (tijdelijke) wet permanent

Het is opmerkelijk dat in een voorstel voor een tijdelijke wet stelselwijzigingen worden geïntroduceerd, bijvoorbeeld het instellen van de mogelijkheid tot hoger beroep bij de Raad van State. Door de introductie van dergelijke grootschalige veranderingen aan het stelsel, en de consequenties voor de betrokken organisaties, is het aannemelijk dat de veranderingen van langere duur zullen zijn dan de vier jaar geldigheidsduur zoals omschreven in dit voorstel. De memorie van toelichting loopt ook al vooruit op verlenging van de voorgestelde maatregelen.[4] Het is daarom van belang om het voorstel ook als dusdanig te behandelen.

2. Uitbreiding van bevoegdheden

2.1 OOG-interceptie

Toen onderzoeksopdrachtgerichte interceptie (OOG-interceptie) in de Wiv 2017 werd geïntroduceerd zijn er door het kabinet een aantal toezeggingen gedaan om aan de zorgen die in de samenleving leefden tegemoet te komen. Zo zou OOG-interceptie heel anders zijn dan ongerichte interceptie, omdat het mogelijk zou zijn de bevoegdheid fijnmazig in te zetten. Dit werd later nog versterkt door het opnemen van de zogenaamde 'gerichtheidseis' in artikel 26 lid 5 van de wet. Op voorhand niet-relevante gegevens, zoals die van streamingdiensten, zouden meteen worden uitgefilterd en vernietigd en het zou vrijwel uitgesloten zijn dat de bevoegdheid ingezet zou worden op binnenlandse communicatie buiten cyber-defence. Ook zou het voor de diensten mogelijk zijn om vooraf aan de inzet de precieze kanalen te duiden waarover relevante communicatie wordt getransporteerd.[5] Deze toezeggingen zouden ervoor zorgen dat OOG-interceptie zou worden onderscheiden van ongerichte interceptie, en het woord sleepnet overtrokken zou zijn. Deze toezeggingen worden in dit voorstel overboord gegooid.

2.1.1 'Snapshot'-bevoegdheid; ongerichte interceptie

In artikel 7 wordt de zogenaamde snapshotbevoegdheid omschreven. Deze bevoegdheid maakt het mogelijk om ongericht elke kabel een jaar lang af te tappen en deze gegevens een jaar lang op te slaan. De toezichthouder mag bij de toetsing van de toestemming voor deze bevoegdheid de gerichtheid niet meenemen in haar analyse.

Wettelijke grondslag is geen oplossing OOG-interceptie is bij de introductie van de Wiv 2017 met veel weerstand geïntroduceerd. Steeds meer komt naar voren dat de uitleg die destijds aan de Tweede Kamer en burgers is gegeven onjuist was. Om in de woorden van de toezichthouder te spreken: de uitleg toen "wringt met de aard van de bevoegdheid, het middel en de uitvoering in de (technische) praktijk"[6] In haar toezichtsrapport nr. 75 beveelt de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) daarom aan dat de zogenaamde snapshotbevoegdheid een eigen, expliciete wettelijke grondslag behoeft.

4 Memorie van toelichting, p. 11.
5 CTIVD Toezichtsrapportage nr 75 over de inzet van kabelinterceptie door de AIVD en de MIVD https://www.ctivd.nl/onderzoeken/aivd-mivd-onderzoek-naar-de-inzet-van-oog-i-op-de-kabel/documenten/rapporten/2022/03/15/index.
6 CTIVD Toezichtsrapportage nr 75 over de inzet van kabelinterceptie door de AIVD en de MIVD, p. 6. https://www.ctivd.nl/onderzoeken/aivd-mivd-onderzoek-naar-de-inzet-van-oog-i-op-de-kabel/documenten/rapporten/2022/03/15/index

Dat zou de voorzienbaarheid en de controleerbaarheid van de huidige praktijk ten goede komen. Echter doet het vastleggen van de huidige praktijk in wetgeving geen recht aan de grenzen die de Tweede Kamer en Nederlandse burgers de ministeries hebben meegegeven. In plaats van de praktijk aan te passen aan het gedeelde begrip over wat de aard van de bevoegdheid zou moeten zijn, faciliteert de wet een praktijk waarmee nooit is ingestemd.

Van verificatie naar verkenning De snapshotbevoegdheid is in het regime van de Wiv 2017 een verificatiebevoegdheid, die voorafgaat aan de (verdere) inzet van kabelinterceptie. Dat betekent dat het middel door de diensten enkel wordt ingezet om te testen of ze de juiste gegevensstroom te pakken hebben, en niet om te hengelen naar informatie. Artikel 7 van het voorliggende concept beschrijft echter een bevoegdheid waarbij het snapshotten niet langer plaatsvindt om de relevantie van de gegevensstroom te verifiëren, maar om te verkennen welke gegevensstromen mogelijk relevant kunnen zijn voor een onderzoek, en op welke wijze. Daarmee wordt de bevoegdheid veel ongerichter.

Gerichtheidseis vervalt Naar aanleiding van het referendum is via het Wijzigingsvoorstel in artikel 26 lid 5 van de Wiv 2017 de “gerichtheidseis” geïntroduceerd. Deze eis wordt in dit voorstel met betrekking tot de snapshotbevoegdheid expliciet buiten toepassing gesteld. De bevoegdheid die in artikel 7 wordt omschreven is bedoeld, en volgens de memorie van toelichting per definitie, ongericht.[7] En ook de toezichthouder zal dus niet kunnen toetsen op een voldoende mate van gerichtheid.

Verplichting tot filteren vervalt Volgens het huidige voorstel zouden de diensten niet langer streamingdiensten en binnenlandse communicatie “buiten cyber-defence” hoeven uit te filteren, waarmee ook deze gegevens door middel van de kabelinterceptie door de diensten zullen worden verzameld. Dat is opvallend, gezien het voorstel zich juist richt op cyber-defence. De noodzaak om binnenlandse communicatie *buiten cyber-defence* binnen te halen voor opdrachten in het kader van cyber-defence, lijkt afwezig, oogt tegenstrijdig en wordt onvoldoende toegelicht.

Toezicht verzwakt De door de Minister verleende toestemming om deze bevoegdheid in te zetten wordt op rechtmatigheid getoetst door de Tib. Door de ongelooflijk ruime formulering van de bevoegdheid blijft er echter weinig voor de toezichthouder over om aan te toetsen.

2.1.2 Toestemmingsniveau van geautomatiseerde data-analyse en selectie

Het toestemmingsniveau voor de inzet van de bevoegdheid tot selectie en meta-data analyse van gegevens die zijn verzameld door middel van onderzoeksopdrachtgerichte interceptie wordt verlaagd van toestemming door de Minister die wordt getoetst door de Tib naar toestemming door enkel het diensthoofd. De nieuwe mogelijkheid voor de CTIVD om tijdens en achteraf toezicht te houden, is onvoldoende waarborg om het verlies van toezicht aan de voorkant op te vangen.

Het is van belang de afschaling van het toezicht op de bevoegdheid tot geautomatiseerde metadata-analyse en selectie te zien in combinatie met de meer ongerichte inzet van de interceptie-bevoegdheid. Dat betekent dat er nog meer gegevens van burgers die geen

7 Memorie van toelichting, p. 23.

onderwerp van onderzoek van de diensten zijn en dat ook niet zullen worden, worden verzameld, maar ook geautomatiseerd zullen worden geanalyseerd, terwijl het toezicht hierop wordt afgeschaald.

2.2 Strategische operaties

In de memorie van toelichting wordt gesproken over zogenaamde "strategische operaties". Het is opvallend dat deze term in het voorstel zelf niet terugkeert. Ook wordt niet duidelijk gemaakt wat hier precies mee wordt bedoeld. Het zou gaan om een "proactieve" inzet van middelen om zicht te krijgen op "toekomstige" aanvallen en de daaraan verbonden technologie, het vergaren van kennis en het ontwikkelen van mogelijkheden ten behoeve van de toekomstige inzet van middelen, mogelijk ook op non-targets. Het is niet duidelijk wat hier precies wel en niet onder moet worden geschaard.

Een mogelijke uitleg is dat hier een offensieve hackbevoegdheid aan de diensten wordt toegekend. Of dat op grond van deze omschrijving de mogelijkheid tot het afgeven van een verplichting tot het inbouwen van een achterdeurtje in encryptie wordt geïntroduceerd. Dat zouden ingrijpende bevoegdheden zijn met mogelijk verstrekkende consequenties voor de veiligheid van onze digitale infrastructuur en onze samenleving. Wanneer dit is wat de ministeries voor ogen hebben, dan is het noodzaak de Tweede Kamer daar goed over te informeren zodat zij een geïnformeerde discussie kan voeren over de wenselijkheid. Het is uit den boze bevoegdheden die potentieel zulke verstrekkende gevolgen hebben enkel in de toelichting te omschrijven.

2.3 Bijschrijven

Bijschrijven is het brengen van bepaalde infrastructuur of apparaat onder de bestaande toestemming een bepaalde bevoegdheid in te zetten. Het voorstel voorziet in de uitbreiding van de mogelijkheid tot bijschrijven van verschillende items. Van geautomatiseerde werken in de hackbevoegdheid, van nummers of technische kenmerken bij de bevoegdheid tot gerichte interceptie, en van de opdracht gegevens te verstrekken aan een aanbieder van een communicatiedienst of een persoon of instantie die de opslag ervan verzorgt. Met deze bijschrijving krijgen de geheime diensten toegang tot het nieuwe item voor de duur van de reeds verleende toestemming, zonder dat de toezichthouder er aan te pas komt.

Het is begrijpelijk dat er snelheid geboden kan zijn met het inzetten van bevoegdheden wanneer bijvoorbeeld een target wisselt van mobiele telefoon, of op reis gebruik maakt van verschillende providers. In de Wiv 2017 is er al de mogelijkheid tot bijschrijven waar het gaat om geautomatiseerde werken, nummers of technische kennis *van* het target. In het concept wordt voorgesteld dit uit te breiden naar geautomatiseerde werken, nummers of technische kenmerken *in gebruik* door het target, zonder dat deze bijschrijving vooraf wordt getoetst. Dit brengt een aantal risico's met zich mee:

- Het gebruik beperkt zich niet tot exclusief of legitiem gebruik. Dat wil zeggen dat het ook gaat om geautomatiseerde werken, nummers of technische kenmerken van openbare, commerciële of persoonlijke infrastructuur en apparaten. Denk bijvoorbeeld aan een server waarop Apple voor duizenden gebruikers haar clouddienst host. Daarop zijn mogelijk (veel) gebruikers actief die geen onderwerp van onderzoek van de geheime diensten zijn en dat ook niet zullen worden. Er wordt onvermijdelijk een inbreuk op de privacy van deze mensen gemaakt, en er zijn mogelijk ook consequenties voor de veiligheid van de door hen gebruikte apparatuur en infrastructuur.

- Het feit dat de geautomatiseerde werken, nummers of technische kenmerken worden gebruikt door non-targets en hier (grote hoeveelheden) gegevens op staan van burgers die geen onderwerp van onderzoek van de diensten zijn, brengt een noodzaak met zich mee voor een verzwaarde proportionaliteitstoets. Het hacken van de telefoon van een verdachte is iets heel anders dan het hacken van een server op een universiteit, bijvoorbeeld. Die verzwaarde proportionaliteitstoets hoeft bij de initiële toestemming waarop wordt bijgeschreven niet te zijn gemaakt, en bijschrijving zonder deze voorfgaande toestemming zorgt ervoor dat deze proportionaliteitstoets pas kan worden gemaakt bij het verzoek tot verlenging van de toestemming. Dan is er mogelijk al veel schade geleden.

3. Toezicht en waarborgen

3.1 ‘Verplaatsing’ van het toezicht is in de praktijk afschaling

Er wordt gesproken over een zogenaamde “verplaatsing” van het toezicht van de Tib naar de CTIVD. Ondanks dat de bij de Tib weggehaalde toetsingsbevoegdheden terugkeren bij de CTIVD als toezichtsbevoegdheden, is hier niet (enkel) sprake van een verplaatsing van toezicht, maar van een karakterverandering en afschaling.

Een lagere intensiteit De Tib toetst elk verzoek waarvoor zij een toetsingsbevoegdheid heeft. Die bevoegdheden hebben dus een toetsingsintensiteit van 100%. Het toezicht door de CTIVD heeft een ander karakter. De CTIVD heeft de bevoegdheid om toezicht te houden op meerdere lopende processen van de geheime diensten en doet dat steeksproefsgewijs. Zelfs al zou de capaciteit van de CTIVD toenemen, dan is het nog niet gewaarborgd dat de in artikel 13 van het voorstel beschreven bevoegdheden altijd allemaal getoetst zullen worden. Het is aannemelijk dat de toetsingsintensiteit zal afnemen.

Voorkomen is beter dan genezen De Tib toetst vooraf waar de CTIVD tijdens en achteraf toezicht houdt. Dat betekent dat waar het aankomt op schade die mogelijk voortkomt uit de uitoefening van bevoegdheden door de diensten, de Tib in staat is deze te voorkomen, waar de CTIVD deze enkel kan stoppen. Dit verschil is met name relevant waar het aankomt op de hackbevoegdheid en de daaraan verbonden technische risico’s, bijvoorbeeld bij het bijschrijven van geautomatiseerde werken die niet-exclusief in gebruik zijn door de target en het gebruik van onbekende kwetsbaarheden door de geheime diensten. Dit meenemen in de toetsingsbevoegdheid vooraf dwingt om dit nauwlettend in ogenschouw te nemen en vooraf over na te denken. Ook borgt het een beoordeling van iemand die zelf niet een operationeel belang heeft bij de uitkomst van de afweging. Enkel achteraf de inzet kunnen stopzetten laat het risico dat een onbekende kwetsbaarheid bij een kwaadwillende op de radar komt te staan, of dat bij de inzet van een bevoegdheid disproportionele schade aan de veiligheid van (digitale) infrastructuur ontstaat, onverlet.

Karakter Beide toezichthouders hebben logischerwijs een andere inkleuring van de manier waarop zij toezicht houden op de praktijk van de diensten. Zo toetst de Tib vooraf het concrete verzoek, en dus ook die specifieke inzet van de bevoegdheid die aan hen wordt voorgelegd. En toetst de CTIVD in grote lijnen hoe de diensten omgaan met bepaalde bevoegdheden. Dit zijn twee verschillende manieren van toezichthouden die ervoor zorgen dat een 'verplaatsing' van de toezichtstaak op een (deel van) een bevoegdheid altijd gepaard gaat met een verandering in de wijze van toezichthouden en daarmee de bescherming van de rechten en vrijheden van burgers.

Bits of Freedom adviseert het toezicht, in lijn met de motie Leijten, niet af te schalen door de toetsing van de meeste van deze bevoegdheiden bij de Tib weg te halen. Dit zou eventueel kunnen bij de bevoegdheid tot verkennen zoals omschreven in artikel 45 lid 1 sub a Wiv 2017, uitgevoerd binnen de kaders van deze wet, wanneer die bevoegdheid wordt ingezet om vervolgens te kunnen komen tot een beter en gerichter verzoek met inachtneming van de technische risico's bij de bevoegdheid tot het binnendringen zoals omschreven in artikel 45 lid 1 sub b Wiv 2017, en die te laten toetsen door de Tib. In dit voorstel wordt echter juist de toetsing op technische risico's bij de Tib weggehaald.

3.2 De mogelijkheid tot hoger beroep

Eenzijdig hoger beroep is een tweede kans Het voorgestelde artikel 14 introduceert de mogelijkheid aan de zijde van de Minister om in beroep te gaan tegen het oordeel en/of de daaraan gekoppelde gevolgen van beide toezichthouders. Deze hogerberoepsmogelijkheid is gebaseerd op het idee dat ook deze toezichthouders fouten kunnen maken en zich kunnen baseren op een onjuiste wetsinterpretatie. Dat is natuurlijk waar. Echter geldt ook dat toezichthouders fouten kunnen maken die in het belang van de diensten uitpakken. Het wetsvoorstel houdt nog onvoldoende met deze situatie rekening.

Bits of Freedom adviseert dat wanneer er een mogelijkheid tot hoger beroep wordt geïntroduceerd, het hoger beroep mogelijk te maken ten opzichte van alle oordelen van de toezichthouders, en niet alleen oordelen die uitgaan van een onrechtmatigheid aan de kant van de diensten dan wel de verleende toestemming van de Minister. Ook aan de zijde van de burgers wiens recht op een persoonlijke levenssfeer ten onrechte kan worden geschonden door oordelen van de toezichthouders moet dan een hoger beroep mogelijk zijn.

Geheime wetsuitleg Het hoger beroep zoals dat is voorgesteld in het concept vindt plaats achter gesloten deuren en ook de uitspraak is niet openbaar. Het is volstrekt onduidelijk waarom, wanneer de uitspraak ziet op de uitleg van de wet, deze wetsinterpretatie niet openbaar gedeeld kan worden. Het geheim houden van dergelijke uitspraken schaadt de kenbaarheid en voorzienbaarheid van de wetgeving.

Bits of Freedom adviseert om minimaal de wetsinterpretatie uit de uitspraken van de rechter in hoger beroep openbaar te maken.

Technische expertise Bij de introductie van de Tib werd terecht veel waarde gehecht aan het voldoende borgen van de technische expertise die noodzakelijk is om de verzoeken van de diensten goed te kunnen toetsen. Niet voor niets bestaat die toezichthouder uit twee rechters en een technisch expert. In het voorliggende wetsvoorstel blijkt onvoldoende dat men zich bewust is dat deze expertise bij de Raad van State als hoger beroeps instantie voldoende aanwezig moet zijn.

Bits of Freedom adviseert in het geval dat er een hoger beroepsinstantie wordt ingeroepen die de oordelen van de toezichthouders in deze materie moet kunnen beoordelen en herzien, een voldoende mate van expertise in de technische aspecten van de materie bij deze instantie wordt geborgd.

3.3 Relevantiebeoordeling bulkdatasets

Bulkdatasets zijn per definitie enorm omvangrijk en per definitie hebben ze voor het merendeel betrekking op organisaties of personen die geen onderwerp van onderzoek van de diensten zijn en dat ook niet zullen worden. De waarborgen bij het verzamelen, bewaren en verwerken van deze gegevens zijn dan ook van groot belang om de inbreuken op fundamentele rechten en vrijheden te beperken. Het vervangen van de relevantiebeoordeling ex artikel 27 Wiv 2017 door artikel 6 van dit voorstel bij bulkdatasets die zijn verworven met de hackbevoegdheid levert een lager beschermingsniveau op. De belangrijkste verschillen zijn als volgt.

- Onder artikel 27 Wiv 2017 is de uiterste bewaartermijn 1,5 jaar. De bewaartermijn van de bulkdatasets die door het binnendringen in een geautomatiseerd werk binnen het kader van dit voorstel zijn verworven is potentieel oneindig. De termijn kan immers telkens met een jaar worden verlengd, zonder maximumtermijn. Juist bij bulkdatasets, waarbij het gaat om de gegevens van miljoenen burgers die geen onderwerp van onderzoek van de diensten zijn en dit ook niet zullen worden, is het van belang dat burgers erop kunnen rekenen dat als hun gegevens als bijvangst verzameld worden, die in elk geval na een bepaalde termijn zullen worden vernietigd. De stap van 1,5 jaar naar potentieel oneindig is ons inziens onuitlegbaar en gaat ten koste van de voorzienbaarheid voor burgers.
- De CTIVD krijgt de bevoegdheid toezicht te houden op de verlenging van de bewaartermijn, maar niet op het niveau waarop de relevantiebeoordeling wordt uitgevoerd. Dat terwijl diezelfde toezichthouder al in eerdere rapportages heeft aangegeven dat die beoordeling dient plaats te vinden op het niveau van gegevens, en niet op het niveau van bulkdatasets.[8] Dit om te voorkomen dat gegevens die relevant zijn voor de nationale veiligheid maar zitten in een bulkdataset die dat grotendeels niet is worden vernietigd, en gegevens van burgers die niet relevant zijn voor het onderzoek, maar zitten in een bulkdataset met relevante gegevens worden bewaard. De waarborg die uitgaat van de relevantiebeoordeling op gegevensniveau gaat verloren in het nieuwe voorstel.

Het is helaas moeilijk te voorspellen hoeveel van de bulkdatasets die worden vergaard, zullen worden vergaard binnen dit lagere beschermingsniveau. Dat komt ten eerste door de slechte afbakening van de in dit voorstel beschreven reikwijdte. Daardoor kunnen de diensten in

8 CTIVD Toezichtsrapportage nr 70 over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD. https://www.ctivd.nl/onderzoeken/aivd-mivd-onderzoek-bulkhacks/documenten/rapporten/2020/09/22/rapport-70

potentie dit regime van toepassing verklaren op veel van haar verwerving van bulkdatasets door middel van het binnentreden van een geautomatiseerd werk. Zie punt 1.3 van deze inbreng. Ten tweede komt het door ontbrekende beperkingen op het “hergebruik” van de data die binnen dit regime wordt vergaard. De bulkdatasets die zijn verworven voor onderzoeksopdrachten die binnen deze wet vallen, en waar dus de potentieel oneindige bewaartermijn voor geldt, mogen ook voor onderzoeksopdrachten buiten de reikwijdte van deze wet worden gebruikt.[9] Daarmee verzorgt het voorstel een U-bocht constructie. Immers, de gegevens die gebruikt worden voor de onderzoeksopdracht buiten dit voorstel hadden binnen de regels die gelden voor die onderzoeksopdracht al vernietigd moeten zijn.

Concluderend is het dus aannemelijk dat het lagere beschermingsniveau ver voorbij een specifiek afgebakende taak zal reiken.

Bits of Freedom adviseert daarom de relevantiebeoordeling zoals die is omschreven in artikel 27 van de Wiv 2017 van toepassing te laten zijn op alle gegevens die door de uitoefening van bijzondere bevoegdheden door de diensten worden verworven, en tevens om die op het niveau van de gegevens uit te voeren, zoals de CTIVD in haar rapportages omschrijft. Inclusief een maximale bewaartermijn.

3.4 Technische risico’s

Onder de Wiv 2017 moeten de diensten, in het verzoek om toestemming tot het binnendringen van een geautomatiseerd werk, de technische risico’s van die handeling beschrijven. Onder dit nieuwe regime zou dat niet langer verplicht zijn. De Tib kan de technische risico’s dan ook niet meenemen in haar toetsing. Dat is extra zorgelijk in het licht van de uitbreiding van de bevoegdheid tot het bijschrijven van geautomatiseerde werken naar ook niet-exclusief gebruik. Een afweging over wat een aanvaardbaar risico is om bepaalde informatie te vergaren, valt wellicht anders uit wanneer je de smartphone van een target binnendringt, dan wanneer je een hele server binnendringt. Dit geldt ook ten aanzien van de mogelijkheid van het gebruik van onbekende kwetsbaarheden, en wellicht ook voor (bepaalde invullingen van) de “strategische operaties”. Het weghalen van het toezicht bij de Tib betekent een verminderde toetsing van de noodzakelijkheid, subsidiariteit, proportionaliteit, evenredigheid en dus aanvaardbaarheid van de technische risico’s die gepaard gaan met de inzet van deze bevoegdheden. Dit wordt niet ondervangen door de “verplaatsing” van dit toezicht naar de CTIVD. En dat terwijl dit verstrekkende gevolgen kan hebben voor de veiligheid van de digitale infrastructuur.

Bits of Freedom adviseert daarom de eis de technische risico’s in het verzoek op te nemen en daarmee ook ter toetsing aan de Tib voor te leggen zoals omschreven in de Wiv 2017 in stand te laten.

3.5 Slachtofferdata

Bij het verkrijgen van inzicht in een cyberaanval of target verschaffen de geheime diensten zich de toegang tot de gehackte infrastructuur of apparatuur en verwerven zij bulkdatasets met gegevens van personen, bedrijven, overheden of organisaties die toevallig gebruiker zijn

9 Memorie van toelichting, p. 20.

van de gehackte infrastructuur of apparatuur. Wanneer de diensten toegang krijgen tot dergelijke *slachtofferdata* vanuit de taak om inzicht te krijgen in een cyberaanval of target, moet helder en met waarborgen omkleed worden vastgelegd hoe er met de verworven slachtofferdata wordt omgegaan.

Bits of Freedom adviseert helder vast te leggen dat deze gegevens niet voor onderzoekstaken kunnen worden gebruikt en deze gegevens zo snel mogelijk moeten worden vernietigd.

3.6 Informatiepositie en samenwerking toezichthouders

Voor de rechtseenheid en effectiviteit van het toezicht is overleg en samenwerking tussen beide toezichthouders van groot belang, zeker wanneer hun toezichtsgebieden complexer met elkaar verstrengeld raken. Het huidige concept stelt een onverklaarbare en onacceptabele beperking van de mogelijkheid tot (vertrouwelijke) samenwerking en informatieuitwisseling tussen beide toezichthouders voor. Volgens het voorstel zou het hoofd van de betrokken dienst vooraf moeten worden geïnformeerd over de informatie die de toezichthouders met elkaar willen uitwisselen. Ook zou er een register moeten worden gevormd van alle uitgewisselde informatie. Dit belemmert een open en vertrouwelijke uitwisseling tussen de toezichthouders en daarmee het effectieve toezicht.

De beperking die het voorstel de beide toezichthouders stelt op het verstrekken van inlichtingen aan elkaar in het kader van de in het voorstel aan hun opgedragen taken is des te opvallender nu ditzelfde voorstel zoveel toezichtstaken van de Tib naar de CTIVD overhevelt. De beperkingen die hen op het uitwisselen van informatie gesteld worden bemoeilijken een goede overdracht van deze taken.

Daarnaast introduceert dit wetsvoorstel de verplichting van de Tib om, wanneer zij de CTIVD wijst op mogelijk relevante aandachtspunten in verband met de uitvoering van een verleende toestemming, gelijktijdig hiervan melding te doen bij de betrokken Minister. Ook dit komt het effectieve toezicht niet ten goede. Het creëert namelijk een prikkel voor de diensten om meer middelen in te zetten op verbeteringen in specifiek aangewezen gebieden, in plaats van een zelfkritische houding aan te nemen ten opzichte van alle onderdelen van het inlichtingenwerk.

Bits of Freedom adviseert om samenwerking en overleg tussen beide toezichthouders juist aan te moedigen zodat dit een goede rechtseenheid en effectief toezicht ten goede komt.

We gaan er vanuit u met onze inbreng te hebben voorzien van inzichten en handvatten om het conceptwetsvoorstel Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma te versterken. Vanzelfsprekend zijn wij graag bereid tot een nadere toelichting, mocht daaraan behoefte bestaan.

Met vriendelijke groet,
namens Stichting Bits of Freedom,

Lotte Houwing