Het Europees Hof van de Rechten van de Mensen in *Big Brother Watch* dat de dreiging vanuit staten hoger is door toegenomen digitalisering en technologische ontwikkelingen: “Access to such technology also permits hostile State and non-State actors to disrupt digital infrastructure and even the proper functioning of democratic processes through the use of cyberattacks, a serious threat to national security which by definition exists only in the digital domain and as such can only be detected and investigated there.”[1]
Door buitenlandse inmenging, sabotage, en spionage in het cyberdomein staat onze democratische rechtsstaat onder druk, fundamentele rechten en burgerlijke vrijheden van burgers worden geschaad en het Nederlandse verdienvermogen wordt ondermijnd.[2] Deze wet ter bescherming van burgers en Nederlandse belangen is urgent en noodzakelijk, maar schiet tekort. Drie prioriteiten daarin zijn:

1) Maak onderscheid tussen inzetten in het binnen- en het buitenland,
2) bindend toezicht door de CTIVD en de bindende toets van de TIB zijn onwenselijk, indien onontkoombaar moet flexibiliteit behouden blijven,
3) versterk de argumentatie voor de wijziging in de bevoegdheden.

Advies 1: Maak onderscheid tussen inzetten in het binnen- en het buitenland*

De universele toepassing van de reikwijdte van de Wiv[3] waardoor het rechtsbeschermingsregime voor burgers in het binnen- en buiteland hetzelfde is, is gedateerd en zou moeten worden losgelaten om vier redenen: a) de assertiviteit van geopolitieke machten, b) de grenzeloosheid van het digitale domein, c) onze militairen en onze militaire belangen, en d) effectiviteit.
Nu kan het zelfs zo zijn dat gegevens van Nederlandse burgers makkelijker te verkrijgen zijn dan van inwoners van landen met een offensief cyberbeleid. Gegevens die in Nederland via art. 25 Wiv 2017 kunnen worden verzameld zullen in deze landen via een bijzondere bevoegdheid zoals een hack moeten worden verzameld. Het is bijvoorbeeld onwaarschijnlijk dat de diensten het Russische Kadaster om gegevens vragen. Dit betekent dat vergelijkbare gegevens over Nederlandse burgers via een beperkt toestemmingsniveau worden verkregen, terwijl de inzet van een bijzondere bevoegdheid zoals een hack een toets van de TIB vereist.

1.1 Het tegengaan van assertievere geopolitieke machten is een ongelijke strijd

De Commissie Jones-Bos stelde vast dat verschillende landen een ander regime volgen voor de toepassing van de rechtsbescherming. Landen zoals China, Rusland, Iran en Noord-Korea bekommeren zich niet om de bescherming van fundamentele rechten van hun eigen burgers, laat staan Nederlandse burgers. Deze landen houden zich niet aan dezelfde afspraken waardoor een ongelijke strijd ontstaat. De universele reikwijdte van de Wiv 2017 zou in deze wet niet moeten gelden. Het rechtstatelijk besef bij onze diensten en de betrokken ministeries is hoog waardoor de waarborgen uit de Wiv 2002 voldoende zijn voor buitenlandse inzetten.

1.2 De grenzeloosheid van het digitale domein maakt Nederlandse belangen ongekend kwetsbaar

De wereldwijde online verbinding maakt het eenvoudig om grensoverschrijdend aanvallen uit te oefenen op een ongekende schaal en zonder veel kosten of personele capaciteit. Gezien de geografische locatie zullen de inlichtingen via deze wet voornamelijk op afstand worden verkregen. Dit maakt het effectief inzetten van bevoegdheden tegen offensieve cybermachten urgent. [4]

1.3 De levens van onze militairen en onze militaire belangen wegen zwaarder

Het is wellicht onwaarschijnlijk dat we een militaire aanwezigheid zullen hebben in landen met een offensieve cyberstrategie tegen Nederland, maar dit is niet uitgesloten. De levens van onze militairen

[1] EHRM, case of Big brother wacht and others v. The United Kingdom, overweging 323
[2] Idem.
[3] Evaluatie 2020 Wet op de inlichtingen- en veiligheidsdiensten 2017, p. 19
[4] Big Brother Watch e.a. t. VK (EHRM, 58170/13 e.a.) en | EHRC Updates (ehrc-updates.nl)

en onze militaire belangen zijn te groot om de privacy van inwoners van het betreffende land op eenzelfde wijze mee te nemen in de proportionaliteit of subsidiariteit als Nederlandse burgers.

1.4 Effectiviteit in het buitenland is 'collateral damage' van binnenlandse beeldvorming

De focus van de gepolariseerde debatten over bevoegdheden van de IenV-diensten ziet voornamelijk op de binnenlandse toepassing. De effectiviteit van onze diensten in het buitenland is dan 'collateral damage'. Deze wet ziet op landen met een offensief cyberprogramma tegen Nederland waardoor de toepassing van de wet voornamelijk in het buitenland zal geschieden. Laat het gepolariseerde debat de effectieve inzet van de noodzakelijke capaciteiten in het buitenland niet schaden.

1.5 Hoe kan het verschil eruitzien?

Het toepassen van art. 19 Wiv 2002, betekent bijvoorbeeld geen bindend toezicht van de CITVD of bindende toets van de TIB, het hoogste toestemmingsniveau is beperkt tot de minister. Daarnaast kan sprake zijn van een andere weging van proportionaliteit en subsidiariteit (de weging van OOG interceptie verandert; het hoeft niet zo gericht mogelijk) en er kunnen andere bewaar- of evaluatietermijnen gelden voor data. Rechtmatigheidstoezicht door de CTIVD blijft bestaan.

Advies 2.a <u>Primair</u>: Geen bindend toezicht door de CTIVD

Er zijn drie redenen waarom de introductie van het bindend toezicht door de CTIVD moet worden teruggedraaid:

2a.1 Bindend toezicht is disproportioneel

Met ex durante bindend toezicht gaat het inlichtingendomein verder dan het strafrecht. Dit is disproportioneel wanneer men zich realiseert dat de uiteindelijke mogelijke gevolgen voor een verdachte in het strafrecht ernstiger zijn dan die van een doelwit van de IenV-diensten. In het strafrecht kan vrijheidsontneming de uitkomst zijn, terwijl bij inlichtingendiensten het beperkt is tot een inbreuk in de persoonlijke levenssfeer.

2a.2 Compromitteer operationele slagkracht niet vanwege beeldvorming

Bindend toezicht is een antwoord op het ongegronde wantrouwen tegen de diensten dat wordt gevoed door een onjuiste voorstelling van de mogelijkheden, capaciteiten en middelen en waarin elke rechtstatelijke waarborg wordt weggewuifd. Bindend toezicht is hierdoor ongerechtvaardigd.

2a.3 Bindend toezicht verhoudt zich niet tot het doel van de wet

Bindend toezicht staat haaks op de gewenste effectiviteit en snelheid om veranderlijke dreigingen te adresseren. Hierdoor wordt immers een bureaucratie opgetuigd die een inzet kan stoppen of data kan verwijderen. Een beroep hiertegen heeft geen schorsende werking.

Advies 2.b <u>Secundair</u>: behoud flexibiliteit en ruimte om te manoeuvreren in het geval van nood of dringende aangelegenheden als bindend toezicht wordt geïmplementeerd

Indien bindend toezicht wordt geïntroduceerd zou voldoende flexibiliteit voor de diensten behouden moeten blijven en moet er voldoende rekenschap zijn van de context waarin inlichtingen worden verworven door de volgende elementen mee te nemen in de vormgeving.

2b.1 Handelingsruimte in het geval van levensbedreigende situaties of uitzonderlijke noodzaak

De CTIVD kan beëindigen of verwijderen en vernietigen. Daarbovenop kent een beroep vanuit de diensten geen opschortende werking. Uitzonderingsgronden op besluiten van de CITVD of TIB bieden handelingsruimte voor de diensten. Er bestaat vertrouwen in de professionals van de diensten.

2b.1.1 Levensgevaar:
Er moet een uitzondering zijn voor de bescherming van 'life and limb'. Eventuele verschillen in inzicht over de dreigingssituatie mogen niet leiden tot vertraging.

2b.1.2 Uitzonderlijke noodzaak:
Een uitzondering is nodig als een zwaarwegend belang dit dringend vordert. Dat wil zeggen dat de operatie tijdsensitief is, er doet zich bijvoorbeeld een zeldzame situatie voor. Plus, de inschatting is dat de te vergaren kennis van aanzienlijk belang is voor de bescherming van de nationale veiligheid.

2b.1.3 Waarborgen:
Voor het negeren van een bindend oordeel is toestemming nodig van de minister en geldt 'comply or explain'. De minister informeert de Staten-Generaal over dit besluit. De CTIVD of de TIB kunnen in reactie een beroepsprocedure of voorlopige voorziening starten zonder schorsende werking .

2b.2 Hoor en wederhoor ten behoeve van zorgvuldige besluitvorming

De CTIVD moet de IenV-diensten de mogelijkheid geven om te reageren op een concept-oordeel. Dit komt zorgvuldige besluitvorming ten goede.

2b.3 Geen definitieve gevolgen aan bindend toezicht totdat de rechter zich heeft uitgesproken

2b.3.1 Opschortende werking
Wanneer een dienst in beroep gaat tegen de beslissing van de CTIVD of de TIB dan moet dit opschortende werking hebben. De mogelijkheden van de CTIVD zijn definitief: verwijdering of beëindiging. Geen opschortende werking is operationeel onverantwoord en onzorgvuldig.

2b.3.2 Bewaren van data en behoud van de strategische positie
Bewaar de betwiste informatie in een 'escrow account' in plaats van de informatie te verwijderen. Als de inzet ziet op het verkrijgen van stromende data kunnen deze blijven worden ontvangen. Behoud de operationele positie. Een operatie moet kunnen worden bevroren in afwachting van de rechter of ingeperkt door de rechter. Een strategische positie hoeft niet te worden opgegeven. **

2b.4 Besluitvorming CTIVD zou unanimiteit moeten vereisen

Ex durante bindend toezicht is moeilijk denkbaar, maar als daar toch voor wordt gekozen is het duidelijk dat dit een bijzonder zwaar middel is. De mogelijkheden van de CTIVD zijn te verstrekkend: beëindiging van de desbetreffende bevoegdheid en/of de verwijdering en vernietiging van de bij de uitvoering daarvan verwerkte gegevens. Daarbovenop heeft beroep geen opschortende werking: Dit vereist hoge eisen aan de besluitvorming, namelijk unanimiteit.

2b.5 De aangewezen rechtbank zou een inlichtingenofficier moeten bevatten

Er zijn militaire rechtbanken omdat het voor burgerrechters moeilijk is te oordelen over een situatie waarin in een milliseconde wordt besloten over leven of dood. Hetzelfde geldt voor inlichtingenwerk. Het is moeilijk voor te stellen waarom het nodig is om bulkdata te vergaren waarin voor het overgrote deel onschuldige burgers in zitten, dat bewaring van data langer nodig is omdat deze later van onschatbare waarde kan zijn, of dat hacken van populaire app's proportioneel kan zijn.

Advies 3: Versterk de argumentatie voor de wijziging in de bevoegdheden

Wanneer verdergaande bevoegdheden worden voorgesteld lijkt het vanzelfsprekend om ook de waarborgen te verhogen om een balans te creëren tussen macht en tegenmacht. De noodzaak voor macht en tegenmacht staat niet ter discussie, maar bindend toezicht zorgt voor een disbalans die met de adviezen 1,2 en 3 kan worden hersteld. De toegenomen dreiging is te hoog[5], om bindende bevoegdheden van de TIB of de CTIVD te legitimeren. Bindend toezicht zal ook het negatieve effect

[5] Dreigingsbeeld statelijke actoren, 3 februari 2021; Jaarverslag AIVD 2020; Jaarverslag MIVD 2020

niet wegnemen van de Wiv 2017 op de operationele teams in hun onderzoek naar nieuwe of verborgen dreigingen, het verkrijgen van strategische posities en internationale samenwerking.[6] Om de winsten uit deze wet te verzilveren zou de argumentatie voor de rechtmatigheid van de voorstellen en de noodzaak ervoor beter kunnen worden onderbouwd.

3.1 De inbreuk op de persoonlijke levenssfeer kan een gradueel proces zijn, een lichte inbreuk rechtvaardigt zware restricties zoals strikte bewaartermijnen niet. Onderbouw dit beter.

Toegang tot elektronisch bewijs is cruciaal in een gedigitaliseerde wereld. Door vereisten van data minimalisatie, toegenomen versleuteling en privacy by design is deze toegang steeds beperkter. Bevoegdheden en doelen zoals genoemd in de wet die voorligt zijn des te noodzakelijker. Inzake bulkinterceptie wordt dit bijvoorbeeld ook onderkend door het EHRM: “Consequently, the Court is required to carry out its assessment of Contracting States’ bulk interception regimes, a valuable technological capacity to identify new threats in the digital domain, for Convention compliance by reference to the existence of safeguards against arbitrariness and abuse, on the basis of limited information about the manner in which those regimes operate.”[7]

Het bulkinterceptiesysteem is een gradueel proces van een initiële fase van verwerving tot aan het onderzoek en gebruik van specifieke gegevens, waarbij de mate van inbreuk toeneemt naarmate het proces verder wordt doorlopen. De noodzaak van robuuste waarborgen is volgens het Hof het grootst in de stadia waarin specifieke gegevens van personen worden onderzocht en gebruikt, omdat daar de inbreuk op de rechten van individuele burgers het grootst is.

Het kunnen analyseren van grote datasets is van belang voor het identificeren van de ongekende dreigingen. De Algemene Rekenkamer beschrijft de uitdagingen waar de diensten voor staan: “de I&V-diensten [staan] voor belangrijke strategische veranderopgaves om hun wettelijke taken in het kader van de nationale veiligheid blijvend goed te kunnen uitoefenen. Deze opgaves worden gedreven door technologische ontwikkelingen en een verslechterend dreigingsbeeld.”[8]

Tevens concludeert de Algemene rekenkamer: “Toenemende en veranderende dreiging vraagt om innovatie en intensievere samenwerking (zowel tussen de I&V-diensten zelf, met ministeries en met internationale partners). De nadruk op toepassing van datareductie in de afgelopen jaren heeft tot verdringingseffecten geleid waar met name het lerend en innoverend vermogen van de I&V-diensten onder te lijden heeft gehad. Innovatie ten behoeve van het versterken van de inlichtingenpositie staat hierdoor bij veel operationele teams stil.”[9] Het verdringingseffect houdt in dat Wiv 2017 *compliant* werken een zodanige wissel trekt op de capaciteit en beschikbare applicaties dat dit capaciteit voor innovatie en de inlichtingenpositie verdringt. De wijziging in de Wiv 2017 die wordt voorgesteld brengt hier verandering in.

De toenemende dreiging zoals genoemd in diverse dreigingsanalyses en de rechtspraak, de noodzaak voor analyse van datasets beschreven in de Memorie van Toelichting van het voorstel, het gradueel proces dat wordt beschreven door het Europese Hof van de Rechter van de mens, en de dringende behoefte voor administratieve lastenverlichting voor de slagkracht beschreven door de Algemene Rekenkamer zijn belangrijke fundamenten van dit wetsvoorstel. Om de winsten te verzilveren is het nodig om tegenwicht te bieden tegen de maatschappelijke beeldvorming door de noodzaak en rechtmatigheid beter te onderbouwen.

[6] Algemene Rekenkamer, 2021, Slagkracht AIVD en MIVD – de wet dwingt, de tijd dringt, de praktijk wringt, p. 63

[7] EHRM, case of Big brother wacht and others v. The United Kingdom, overweging 323

[8] Algemene Rekenkamer, 2021, Slagkracht AIVD en MIVD – de wet dwingt, de tijd dringt, de praktijk wringt, p. 10

[9] Algemene Rekenkamer, 2021, Slagkracht AIVD en MIVD – de wet dwingt, de tijd dringt, de praktijk wringt, p. 45, 46

Addendum

* Advies 1: Maak onderscheid inzetten in het binnen- en het buitenland
Extra toelichting: Locatiebepaling in het digitale domein kan lastig zijn, er kan sprake zijn van ‘ loss of location’ wanneer je een inzet pleegt het onmogelijk is om na redelijke inspanning om uiteenlopende redenen de locatie te bepalen. Daarbovenop, is het mogelijk dat je je op Nederlandse infrastructuur bevindt, terwijl je een geautomatiseerd werk in een ander land bent binnengetreden, zie het voorbeeld van de Nederlandse servers die door Rusland kunnen worden gebruikt. Hier kan het locatiecriterium worden toegepast: wanneer je, na redelijke inspanning, erachter komt dat het doelwit zich in NL bevindt geldt het binnenlands regime; bij onzekerheid of bevestiging dat men in het buitenland actief is geldt het buitenland regime. Gebruik van de NL infrastructuur zoals vermeld in p. 4 en 5 van de MvA geldt als ‘het buitenland’ de locatie van het doelwit/herkomst van de aanval staat centraal, niet de locatie van de infrastructuur of data.

** Advies 2b.3.2 Behoud van de strategische positie
Extra toelichting: Het belang hiervan kan worden toegelicht naar aanleiding van het voorbeeld van p. 31 in de Memorie van Toelichting, hierin staat dat de inzet van de hackbevoegdheid wordt gestopt als de CTIVD daartoe besluit. Dit is onwenselijk doordat het een aanzienlijke verspilling is van capaciteit, tijd en middelen indien de rechter de CTIVD ongelijk geeft. Het verkrijgen van toegang tot een geautomatiseerd werk kan zeer arbeids- en tijdsintensief zijn. Als het bindende toezicht behouden blijft in deze wet moet het onderzoek in het geautomatiseerde werk worden stilgelegd (tenzij sprake is van ‘life or limb’ of uitzonderlijke noodzaak), maar de aanwezigheid in het geautomatiseerde werk moet kunnen worden behouden.