Bijlage bij brief Wiv 2017 en regeerakkoord

Betreft: informatie over de Wiv 2017 en specifiek de bevoegdheid tot onderzoeksopdracht gerichte interceptie.

1. Wat verandert met deze nieuwe wet?

- Een onafhankelijke, bindende toets door de TIB voorafgaand aan de inzet van verschillende bijzondere bevoegdheden, waaronder interceptie.
- De bevoegdheid tot interceptie wordt techniekonafhankelijk en op een nieuwe manier met waarborgen omgeven. Hiermee is onderzoeksopdracht gerichte interceptie (OOG-interceptie) ook mogelijk op de kabel. Dit gaat gepaard met een systeem van meerdere fasen voor OOG-interceptie, waardoor de inhoud van communicatie pas in de laatste fase verder kan worden verwerkt en dit door andere personen gebeurt dan die werkzaamheden verrichten in de voorgaande fases (taak- en functiescheiding).
- Voor het eerst zijn er algemene bewaartermijnen: 3 jaar voor gegevens uit OOG-interceptie en 1 jaar voor alle andere gegevens verkregen uit de inzet van bijzondere bevoegdheden.
- De bestaande bevoegdheid tot het toegang verschaffen tot een geautomatiseerd werk (in de volksmond “hacken” genoemd) is duidelijker omschreven en voorzien van meer waarborgen. Zo krijgt bijvoorbeeld de praktijk van het hacken via een derde een grondslag in de wet.
- Rechterlijke uitspraken, zowel van de Europese als de Nederlandse rechter, hebben een plek gekregen in de wet. Hiermee wordt de tijdelijke regeling ter bescherming van advocaten en journalisten vervangen door een permanente wettelijke.
- De introductie van een bindend oordeel in het geval van een klacht over de AIVD of MIVD. Hiertoe is er een onafhankelijke klachtbehandelaar, de CTIVD afdeling klachtbehandeling.

De nieuwe wet introduceert dus een verruiming van de bevoegdheid van interceptie, niet langer afhankelijk van de techniek die bij de communicatie wordt gebruikt: de onderzoeksopdracht gerichte interceptie (OOG-interceptie). Dat gaat gepaard met een groot aantal nieuwe waarborgen (TIB, fasensysteem, taak- en functiescheiding, bewaartermijnen, bindend klachtrecht). Ook voor de bestaande bijzondere bevoegdheden worden de waarborgen daarmee versterkt.

2. Wat is OOG-interceptie?

Wij vragen de AIVD en de MIVD om tijdig dreiging te onderkennen. Dat doen zij door goed te kijken naar de handelingen en communicatie van personen of organisaties. Aan welke personen of organisaties moeten we dan denken?

- Statelijke actoren die heimelijk democratische en rechtsstatelijke processen beïnvloeden.
- Groepen die onze militairen in het buitenland bedreigen.
- Landen of organisaties in het buitenland die vijandig tegenover Nederland en zijn bondgenoten staan.
- Landen die werken aan massavernietigingswapens en personen die hen daarbij helpen.
- Personen die een bedreiging vormen voor de Nederlandse scheepvaart, zoals bij piraterij in Somalië.

- Statelijke actoren die digitale aanvallen plegen, bijvoorbeeld om gevoelige gegevens te stelen van Nederlandse bedrijven.
- Terroristen of personen of organisaties die hen ondersteunen.
- Extremisten: personen die met geweld hun politieke agenda willen doordrijven.

Het is niet altijd op voorhand precies duidelijk van wie de dreiging komt. OOG-interceptie is nodig als je geen naam of technisch kenmerk hebt van degene die een dreiging vormt of als je bij de provider die de communicatie regelt niet kunt aankloppen. Dit speelt bijvoorbeeld bij de volgende fenomenen:

- Men belt steeds minder, en dit geldt ook voor de bovengenoemde targets van de diensten. Hierdoor levert de traditionele telefoontap steeds minder op.
- Het snel wisselen van communicatiedienst, zodat targets de diensten steeds een stap voor zijn.
- Het communiceren via een buitenlandse provider, die geen informatie hoeft te verstrekken.
- Het gebruik maken van communicatiediensten die speciaal zijn gemaakt om veiligheidsdiensten te ontwijken.
- Militaire tegenstanders in operatiegebied maken gebruik van allerlei internettoepassingen voor aansturing en verkrijgen van inlichtingen.
- Een dreiging zonder dat de tenaamstelling bij de provider of het technisch kenmerk bekend zijn.
- Cyberaanvallen: misbruik van het internet om te hacken en/of malware te plaatsen.

De bovenstaande fenomenen groeien snel in omvang. Zij zijn zonder OOG-interceptie niet of slechts in beperkte mate te onderkennen. Onderkenning door gerichte inzet van middelen, bijvoorbeeld de inzet van de afluisterbevoegdheid, zou wenselijk zijn, maar dat is gewoonweg niet mogelijk.

OOG-interceptie is geen ‘sleepnet’, maar een methode waarmee deze niet exact gekende dreiging wel kan worden onderkend. Dat komt omdat interceptie zich eerst richt op de datastroom en vervolgens de dreiging uit de datastroom haalt op basis van technische gegevens en onderlinge relaties. Je begint breder en trechtert dan, onder het motto “*select while you collect*”.

Maar wat betekent deze methodiek voor de uitvoeringspraktijk van de kabelinterceptie?

In het werk van de inlichtingen- en veiligheidsdiensten is datareductie een steeds terugkerend element. Om zo doelgericht mogelijk te werken, wordt doorlopend getrechterd.

1. Opdracht kabinet. Het doel van de interceptie moet door het kabinet zijn aangewezen in de Geïntegreerde Aanwijzing Inlichtingen & Veiligheid. De onderwerpen die de AIVD of MIVD onderzoeken zijn hiermee ingekaderd.
2. De noodzakelijkheid, proportionaliteit en subsidiariteit van de interceptie moet worden bepaald: waarom is interceptie in dit geval noodzakelijk? Eerst moet duidelijk zijn dat dit doel niet op een andere manier is te bereiken dan door interceptie van de datastroom. Kan bijvoorbeeld gericht worden getapt of met personen worden

gesproken, dan moet eerst die weg worden doorlopen.

3. Keuze van de kabel en de fiber. Er moet worden bepaald waar in Nederland de datastroom loopt. Dit gebeurt in overleg met de communicatieaanbieders en in opdracht van het hoofd van de dienst. In Nederland liggen vele kabels, en die kabels hebben tientallen fibers. Uiteindelijk komen slechts enkele fibers in aanmerking om te worden geïntercepteerd.
4. Verwerving van data. Verzoek om toestemming aan minister en TIB om data te verwerven. Minister verleent toestemming en TIB voert daarop een rechtmatigheidstoets uit. In het verzoek staat gemotiveerd waar de diensten naar zoeken en waarom, waarom de interceptie van de betreffende datastroom daarvoor noodzakelijk is en hoe de datastroom zo klein mogelijk wordt gemaakt.
5. Filtering van de data. Alle data waarvan aan de buitenkant te zien is dat ze niet relevant zijn (negatieve filtering) worden direct afgebogen. Bijvoorbeeld de data van populaire streaming- en/of downloaddiensten als *netflix, spotify, bit-torrent* en *youtube*. Deze data komen niet in de dataset terecht. Vervolgens wordt er een onderscheid gemaakt tussen metadata en inhoud waarna verdere filtering volgt.
6. De inhoudelijke gegevens worden positief gefilterd op basis van selectiecriteria zoals nummers. Voor het mogen uitvoeren van deze positieve filtering is wederom toestemming van de minister en TIB nodig. De inhoud die niet binnen de filters valt wordt niet opgeslagen en is ook niet meer terug te halen.
7. De door filtering gereduceerde metadata worden gebruikt voor de analyse van netwerken. Voor het mogen uitvoeren van geautomatiseerde metadata-analyse die gericht is op het identificeren van personen of organisaties is toestemming van de minister en TIB benodigd. Indien hierbij metadata worden aangetroffen die toch niet relevant blijken te zijn, worden deze direct vernietigd.

Van de daadwerkelijk geïntercepteerde data wordt naar verwachting 98% direct weer verwijderd en vernietigd. Van de totale data die over de kabel gaat resteert dan minder dan een promille.

3. Waarborgen passend gemaakt

De huidige wet kent al een aantal waarborgen en met de Wiv 2017 wordt er nog eens een aantal toegevoegd. Al deze waarborgen bij elkaar garanderen een zorgvuldige inzet van bevoegdheden. Hierbij zet ik de waarborgen nog eens op een rij:

Begrenzing door de wettelijke taak
In het geval van de AIVD moet ofwel sprake zijn van een ernstig vermoeden dat personen of organisaties vanwege hun doelen of activiteiten een dreiging vormen voor de nationale veiligheid ofwel sprake zijn van onderzoek naar andere landen. De begrenzing is gerelateerd aan die taken, waarbij bijzondere bevoegdheden mogen worden ingezet.

Doelgericht, behoorlijk en zorgvuldig
De verwerking van gegevens vindt slechts plaats voor een bepaald doel en op behoorlijke en zorgvuldige wijze.

Zorgplicht
In het wetsvoorstel is de algemene zorgplicht van de diensthoofden tot technische, personele en organisatorische maatregelen vastgelegd. Deze zorgplicht omvat ook de kwaliteit van de

gegevensverwerking inclusief algoritmen en modellen. De diensten zorgen ervoor dat bij inwerkingtreding van de wet een instrumentarium gereed is waarmee gegevensbescherming is geborgd.

Noodzakelijkheid, proportionaliteit en subsidiariteit
Voor de inzet van bijzondere bevoegdheden moet altijd voor het lichtste middel worden gekozen en het middel moet in verhouding staan tot het doel. Ingevolge de aangenomen motie Recourt moet een bijzondere bevoegdheid ook zo gericht mogelijk worden ingezet.

Onvermijdelijkheid voor gevoelige persoonsgegevens
Voor verwerking van gegevens over iemands godsdienst of levensovertuiging, ras, lidmaatschap van een vakvereniging, gezondheid en seksuele leven gelden verzwaarde eisen: dit vindt enkel plaats in aanvulling op andere gegevens en als dat onvermijdelijk is.

Toestemming van de minister vereist
Voor de inzet van de meeste bijzondere bevoegdheden geldt een ministeriële toestemming vooraf die beperkt is in de tijd. Ook is voorafgaande en in de tijd begrensde toestemming benodigd voor bijzondere bevoegdheden die niet op ministerieel niveau zijn belegd.

TIB
Eén van de belangrijkste nieuwe waarborgen is de introductie van een bindende, onafhankelijke toets voorafgaand aan de inzet van bepaalde bijzondere bevoegdheden:

- De benoemingsprocedure garandeert zorgvuldigheid en onafhankelijkheid. De vice-president van de Raad van State, de president van de Hoge Raad der Nederlanden en de Nationale ombudsman doen een aanbeveling aan de Tweede Kamer. De Tweede Kamer doet een voordracht aan de regering, die vervolgens instemt. Benoeming vindt plaats bij koninklijk besluit. De TIB wordt uitgebreid ingewerkt voordat zij van start gaat.
- De leden van de TIB worden voor een vaste periode van zes jaar benoemd en kunnen niet zomaar tussentijds uit hun functie worden gezet.
- Twee van de leden hebben ruime rechterlijke ervaring, het derde lid heeft een andere relevante deskundigheid, bijvoorbeeld op het gebied van techniek.
- De leden worden ondersteund door een staf. Hiervoor is het budget recentelijk verhoogd.
- De TIB bepaalt zelf binnen de grenzen van het redelijke hoe snel zij beslist. Dit is enkel anders bij een spoedprocedure. In dat geval beoordeelt de TIB niet alleen of de inzet rechtmatig is, maar ook of terecht is gekozen voor een spoedprocedure.
- De TIB beschikt voor haar rechtmatigheidstoetsing over dezelfde informatie die ook de minister heeft.
- Indien de TIB geen toestemming geeft, wordt de gevraagde bijzondere bevoegdheid niet ingezet. Er is geen beroep mogelijk.
- De TIB brengt eens per jaar in het publiek verslag uit over haar werkzaamheden.
- Mede naar aanleiding van de aangenomen motie Schouten is voorzien in ruim budget voor de TIB om te kunnen voorzien in de wettelijke taken en de benodigde ondersteuning daarbij.

Onafhankelijk toezicht (CTIVD)
Op de rechtmatigheid van de uitvoering van de wet houdt de CTIVD toezicht. De CTIVD heeft voor haar onderzoek rechtstreekse toegang tot alle gegevens bij de diensten en een ieder die betrokken is of is geweest bij de uitvoering van de wet. Zij publiceert hierover openbare rapporten. Mede naar aanleiding van de aangenomen motie Schouten is het budget van de CTIVD ten behoeve van de Wiv 2017 verhoogd.

Onafhankelijke klachtprocedure met bindende uitspraak
Als iemand van mening is dat de AIVD of MIVD ten onrechte onderzoek naar hem heeft gedaan, kan hij een klacht indienen bij de afdeling Klachtbehandeling van de CTIVD. Deze doet bindend uitspraak.

Parlementaire controle
De Tweede Kamer controleert de uitvoering van de wettelijke taakuitvoering door de diensten zowel in het openbaar als achter gesloten deuren (CIVD). Zij heeft hiervoor de beschikking over de rapporten van de CTIVD en de jaarplannen en – verslagen van de diensten, TIB en CTIVD. Tevens heeft zij een belangrijke rol bij de benoeming van de leden van de TIB en de CTIVD.

Notificatie
Over de inzet van bepaalde bijzondere bevoegdheden (openen van brieven, afluisterbevoegdheid en het binnentreden van woningen) dienen personen in beginsel na vijf jaar te worden genotificeerd.

Dwingende bewaar- en vernietigingstermijnen.
Binnen een jaar en bij OOG-interceptie binnen drie jaar moet zijn onderzocht of de gegevens verkregen vanwege bijzondere bevoegdheden relevant zijn. Anders moeten deze worden vernietigd. De bewaartermijn van drie jaar is noodzakelijk omdat vaak lange tijd onduidelijk is welke exacte betekenis gegevens hebben. Zo werd na de aanslagen in Parijs en Brussel duidelijk dat ISIS al jaren bezig was geweest aanslagplegers naar Europa te sturen. Direct na de aanslagen hebben Europese inlichtingen- en veiligheidsdiensten de gegevens die zij in deze jaren hebben vergaard (nogmaals) uitgekamd op zoek naar verbanden tussen de aanslagplegers en nog onbekende derden. Gegevens die tot dan toe zonder betekenis waren, kregen die in het licht van de aanslagen en hetgeen daaromtrent bekend werd plotseling wel. Enkel omdat deze gegevens konden worden bewaard, konden nieuwe cellen van ISIS in Europa worden ontdekt en aanslagplots worden verijdeld.

Functie- en taakscheiding
Voor OOG-interceptie gelden functie- en taakscheiding c.q. compartimentering. De medewerkers die de technische interceptie uitvoeren zijn anderen dan de medewerkers die de gegevens na selectie inhoudelijk onderzoeken. Slechts een beperkt aantal medewerkers heeft toegang tot de dataset (set 1) die in de eerste fase wordt geïntercepteerd.

Toestemming van de minister vereist voor verstrekking ongeëvalueerde gegevens
Voor het verstrekken van ongeëvalueerde gegevens aan buitenlandse partnerdiensten geldt het vereiste van een voorafgaande en in de tijd begrensde ministeriële toestemming. In het geval deze gegevens uit OOG-interceptie zijn verkregen, moet bovendien de CTIVD hiervan terstond in kennis worden gesteld.

4. Internationale vergelijking

Nederland sluit zich met de nieuwe wet aan bij de ons omringende landen. Landen om ons heen kennen soortgelijke interceptiebevoegdheden alsmede waarborgen, zoals een toets vooraf en dwingende bewaartermijnen. Het onderstaande schema laat dit zien:

Onderwerp	Duitsland	Verenigd Koninkrijk[1]	Frankrijk	België	Nederland
Toestemming interceptie					
• Wie verleent toestemming?	Minister	Minister	Premier	Minister	Minister
• Wie toetst?	G10-commissie	Commissioner	CNCTR	BIM-commissie	TIB
• Adviserend / bindend (A/B)	B	B	A	B	B
• Onderscheid binnen- en buitenland? wel (X) of geen (0)	X (buitenland geen G10-commissie)	X (buitenland geen Commissioner)	X (buitenland geen CNCTR)	X (buitenland geen BIM-commissie)	0
Toezicht					
• Wie houdt toezicht?	G10-commissie / PKGr	Commissioner / ISC	CNCTR	VCI	CTIVD / CIVD
• Adviserend of bindend (A/B)	B / A	A	A	B	A
• Onderscheid binnen- en buitenland? wel (X) of geen (0)	X (buitenland geen G10-commissie)	X (buitenland geen Commissioner)	X (buitenland geen CNCTR)	0	0
Klachtbehandeling					
• Wie behandelt klachten	Bestuursrechter	IPT	Conseil d'État	VCI	CTIVD
• Adviserend / bindend (A/B)	B	B	B	B	B
Bulkinterceptie					
• Toestemming buitenland	Ja	Ja	Ja	Ja	Ja
• Toestemming binnenland	Ja	Ja, enkel metadata	Ja	Nee	Ja
• Onderscheid kabel/niet-kabel?	Nee	Nee	Nee	Nee	Nee
• Bewaartermijn buitenland	Geen	Geen	4 jaar inhoud 6 jaar metadata	Geen	3 jaar
• Bewaartermijn binnenland	Restrictief regime[2]	Geen	Gedifferentieerd[3]	Nvt	3 jaar
• Onkostenvergoeding	Naar redelijkheid/ tarieven	Naar redelijkheid	Naar redelijkheid	Onbekend	Naar redelijkheid

[1] Met betrekking tot het VK is uitgegaan van het beschreven wetvoorstel.
[2] Verwerking van binnenlandse data geschiedt in beginsel op basis van voorafgaande toestemming (G-10) dat sterk lijkt op gerichte interceptie.
[3] Het varieert van 1 maand tot enkele jaren (cybersecurity) afhankelijk van de bevoegdheid op basis waarvan de gegevens zijn verkregen alsmede of het metadata dan wel ook inhoud betreft.