Internetconsultatie

Tijdelijke wet onderzoek AIVD en MIVD naar landen met een offensief cyberprogramma

Samenvatting en bespreking van het wetsvoorstel door mr. Peter Koop, Electrospaces.net

16 april 2022

Inleiding en algemene opmerkingen

Om de toenemende cyberaanvallen uit landen als Rusland en China het hoofd te kunnen bieden komt het kabinet met een voorstel voor een tijdelijke wet om de AIVD en de MIVD op dit gebied sneller en flexibeler te kunnen laten opereren. Dit voorstel komt krap vier jaar na inwerkingtreding van de huidige Wiv 2017, terwijl rapporten van toezichthouder CTIVD, de onafhankelijke evaluatiecommissie uit 2020 en de Algemene Rekenkamer inmiddels duidelijk gemaakt hebben dat een meer fundamentele herziening van de Wiv 2017 gewenst is.

Als gevolg van spookbeelden die door de Snowden-onthullingen werden opgeroepen draaide bij het opstellen van de Wiv 2017 alles om de nieuwe bevoegdheid van ongerichte kabelinterceptie, door tegenstanders steevast "het sleepnet" genoemd. Om tegemoet te komen aan de zorgen vanuit de bevolking bouwde het kabinet een complex systeem van toestemmingen in en werd toegezegd dat deze bevoegdheid in principe niet in Nederland ingezet zou worden.

In het nieuwe wetsvoorstel worden deze waarborgen deels weer teruggedraaid omdat ze niet goed aansluiten bij de praktijk en door de diensten als belemmerend worden ervaren. Hiermee erkent het kabinet impliciet dat de huidige Wiv 2017 de nodige gebreken heeft en hoewel het goed is om die te herstellen, moeten we er alert op zijn dat de slinger deze keer ook weer niet teveel naar de andere kant doorslaat. Zo blijkt het voorstel heel wat meer veranderingen aan te brengen dan men zou verwachten als het gaat om adequater optreden tegen cyberaanvallen.

Dat het tegengaan van cyberaanvallen snelheid en flexibiliteit vereist staat buiten kijf, maar ook nu al is op grond van artikel 37 van de Wiv 2017 een spoedprocedure mogelijk. Opmerkelijk genoeg wordt in de Memorie van Toelichting bij het nieuwe wetsvoorstel niet uitgelegd waarom deze spoedprocedure niet zou voldoen als het gaat om de nodige snelheid bij dergelijke cyberoperaties.

Voorts heten de voorgestelde wijzigingen tijdelijk te zijn, in het voorstel staat namelijk, net als in Amerikaanse wetgeving voor de NSA, een artikel dat bepaalt dat de wet na vier jaar vervalt. De vraag is hoe dat in de praktijk uitpakt: een wijziging die de diensten bevalt zal het kabinet niet zo snel meer ongedaan maken, net zo goed als dat waarborgen die nu "tijdelijk" worden afgeschaft waarschijnlijk niet makkelijk weer opnieuw ingevoerd kunnen worden.

We zullen het wetsvoorstel dus eerder moeten beoordelen als een voorschot op de komende grotere of zelfs algehele herziening van de Wiv 2017 waardoor het gevaar dreigt dat een lappendeken ontstaat van aanpassingen die (nog) niet in breder verband zijn afgewogen.

Bespreking van de onderdelen van het wetsvoorstel

Omdat het wetsvoorstel zelf een erg technisch karakter heeft en daardoor voor buitenstaanders bijzonder moeilijk te begrijpen is en ook de bijbehorende Memorie van Toelichting (MvT) behoorlijk taaie kost is, volgt hieronder een korte samenvatting en bespreking van de verschillende onderdelen. Door de tamelijk korte periode van de internetconsultatie is hier zeker geen volledigheid beoogd en kunnen er dingen over het hoofd zijn gezien.

Beperking tot onderzoeken naar cyberaanvallen

Om te beginnen is het opmerkelijk dat, volgens artikel 2 van het wetsvoorstel, de meeste wijzigingen alleen gelden voor "onderzoeken van de diensten naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen." Dit kan zowel gaan om landen die met name genoemd staan in de geïntegreerde aanwijzing (GA) van het kabinet, als om cyberaanvallen waarvan niet meteen duidelijk is welk land er achter zit. Dat laatste roept de vraag op wat er moet gebeuren als een bepaalde aanval achteraf toch een andere oorsprong of doelstelling blijkt te hebben dan aanvankelijk gedacht, iets dat in de cyberwereld niet ongebruikelijk is.

Voor alle andere operaties van de diensten blijven dus de bestaande regels van kracht en alleen voor de genoemde cyberoperaties zouden dan de nieuwe versoepelingen gelden. Dit maakt de toch al complexe Wiv 2017 nog ingewikkelder dan hij al is, iets dat de door het Europese Hof voor de Rechten van de Mens vereiste kenbaarheid en voorzienbaarheid niet ten goede komt.

Geen externe toestemming meer voor verkenning bij hackoperaties

Artikel 4 bepaalt dat voor de verkennende fase die voorafgaat aan een hackoperatie alleen nog toesteming van het hoofd van de AIVD c.q. de MIVD vereist is, in plaats van toestemming van de minister plus toetsing door de TIB, zoals nu in de wet staat. Deze verandering is overeenkomstig de aanbevelingen van de evaluatiecommissie en de CTIVD die betoogden dat de huidige regeling tamelijk zwaar is vergeleken bij de geringe impact voor de privacy. In plaats van de toets door de TIB stelt het kabinet voor om de CTIVD bindend toezicht te geven op deze bevoegdheid, maar de vraag is of dat wel nodig is als het verkennen inderdaad slechts relatief geringe inbreuk maakt.

Geen omschrijving van technische risico's meer vereist

Artikel 5 bepaalt dat wanneer de diensten om toestemming verzoeken voor een hackoperatie, zij daarbij niet meer de technische risico's hoeven te omschrijven, bijvoorbeeld welke defecten er in andermans computersystemen kunnen optreden. Dit werd door de diensten als een knelpunt ervaren omdat vooraf vaak nog niet duidelijk is welke risico's zich gaandeweg de hackoperatie kunnen voordoen.

De vraag is of deze verplichting daarom maar helemaal geschrapt moet worden: het is niet ondenkbaar dat aan bepaalde hackoperaties wel degelijk vooraf bekende, danwel specifieke of relatief grotere risico's zitten die van belang kunnen zijn voor de voorafgaande toetsing. Wel wil het kabinet ook dit weer onder bindend toezicht van de CTIVD plaatsen.

Uitbreiding van hackoperaties naar gehackte apparaten

Belangrijker is dat in artikel 5 ook staat dat de diensten voortaan een toegestane hackoperatie mogen uitbreiden naar andere apparaten of systemen die door hetzelfde

target in gebruik zijn. Als dus tijdens een hackoperatie blijkt dat bijvoorbeeld Russische hackers vanaf een eerder onbekende server opereren, mag ook die server in de toestemming worden "bijgeschreven".

Dit bijschrijven mocht al als het ging om een apparaat dat alleen (exclusief) door het target zelf gebruikt werd, maar nu zouden de Nederlandse diensten dus ook apparaten mogen gaan hacken die door het target gehackt zijn, en dat zullen dus vaak apparaten van willekeurige burgers of bedrijven zijn. Hier is het voorgestelde bindende real-time toezicht door de CTIVD dus wel op zijn plaats.

Een concreet voorbeeld hiervan werd eerder deze maand onthuld, namelijk de operatie waarbij de FBI uit computernetwerken van over de hele wereld malware verwijderd heeft om daarmee cyberaanvallen van de Russische militaire inlichtingendienst GRU te voorkomen. De FBI verkreeg in het geheim rechterlijke machtiging om deze malware ook zonder medeweten van Amerikaanse bedrijven van hun netwerken te mogen verwijderen. In het buitenland kreeg de FBI hiertoe medewerking van buitenlandse overheden.

Bepaalde bulkdatasets mogen langer bewaard worden

Artikel 6 zegt dat bulkdatasets die via de hackbevoegdheid zijn verkregen voortaan langer bewaard mogen worden: na de huidige termijn van 1 jaar kan de minister toestemming geven om deze telkens opnieuw een jaar te bewaren, ook zonder dat de inhoud op relevantie beoordeeld hoeft te worden.

Volgens de MvT geldt dit echter alleen voor "bulkdatasets die gegevens bevatten die verworven zijn in onderzoeken naar landen met een offensief cyberprogramma" - een formulering die niet helemaal lijkt te kloppen, want gaat het alleen om datasets die tijdens hackoperaties jegens dergelijke offensieve landen zijn binnengehaald, of om datasets die tijdens alle hackoperaties van de Nederlandse diensten zijn verworven en waarin zich toevallig ook (relevante?) gegevens over dergelijke offensieve landen bevinden?

Opgemerkt moet worden dat voor bulkdatasets die via de ongerichte (kabel)interceptie verworven worden er een aparte maximale bewaartermijn van drie jaar geldt. Wat de tijdelijke wet voorstelt maakt de omgang met bulkdatasets dus nog meer versnipperd, terwijl er, zoals de evaluatiecommissie al adviseerde, juist behoefte is aan een meer uniforme regeling voor bulkdatasets, ongeacht hoe ze verkregen zijn.

Verkennen ten behoeve van ongerichte interceptie

Artikel 7 van het wetsvoorstel bepaalt dat ongerichte interceptie mag worden toegepast om in kaart te brengen wat voor soort datastromen er over bepaalde internetverbindingen lopen, het zogeheten verkennen. Dit is nodig om te kunnen bepalen op welke kabels, resp. kanalen de daadwerkelijke ongerichte interceptie ter vergaring van inlichtingen het beste kan worden toegepast.

In de huidige Wiv 2017 is deze mogelijkheid tot verkennen (als "search gericht op interceptie") er alleen nadat reeds toestemming voor de daadwerkelijke interceptie is gegeven, wat betekent dat het ook "zo gericht mogelijk" dient plaats te vinden, iets dat in de praktijk uit de aard der zaak niet te realiseren valt, zo constateerde de CTIVD onlangs in rapport 75.

Een aparte regeling voor het vooraf verkennen is dus wenselijk, alleen stelt het wetsvoorstel er vreemd genoeg nauwelijks beperkingen aan, waardoor de diensten datastromen een jaar lang volledig zouden mogen aftappen en opslaan. Op z'n minst zou bepaald moeten worden dat het verkennen alleen mag gebeuren door middel van steekproeven, of zoals het nu al wordt genoemd: "snapshotten", bijvoorbeeld door het hooguit twee uur per dag te doen, zoals nu als voorwaarde is gesteld.

Wellicht zouden de onderliggende data zelfs al vernietigd kunnen worden zodra de nodige technische informatie over de datastromen gerapporteerd is. Na korte of langere tijd zullen die immers toch weer anders verlopen. Overigens blijft voor het verkennen wel voorafgaande toestemming door de minister plus aansluitende toets door de TIB vereist.

Minder beperkingen bij de ongerichte interceptie

Artikel 8 zegt dat voor de beoordeling van de proportionaliteit en gerichtheid van een aanvraag voor ongerichte interceptie de diensten een indicatie moeten geven van de te verwerven gegevensstromen alsmede van de wijze waarop de reductie van gegevens binnen de gehele keten van ingevuld gaat worden.

Opmerkelijker is dat de MvT bij artikel 8 bijna terloops vermeldt dat in principe ook dataverkeer van streamingdiensten (zoals Netflix en Youtube) en binnenlandse

communicatie ongericht kan gaan worden afgetapt. Na het referendum over de Wiv 2017 hadden de ministers aanvankelijk nog toegezegd dat dit niet zou gaan gebeuren, met name om tegemoet te komen aan de zorgen over vermeende massasurveillance.

Wat betreft het uitsluiten van binnenlandse communicatie heeft de CTIVD in rapport 75 opgemerkt dat die toezegging kennelijk meer ging om dat die communicatie niet onderzocht wordt, in plaats van dat die niet binnengehaald wordt. Dit mede omdat het voor internetverkeer technisch vaak lastig is om binnenlands en buitenlands verkeer goed van elkaar te scheiden, een probleem dat we ook bij de Amerikaanse en Duitse diensten zagen.

Geen TIB-toetsing meer van data-analyse bij ongerichte interceptie

Artikel 9 van het wetsvoorstel bepaalt dat voortaan geen toetsing door de TIB meer nodig is als de diensten "geautomatiseerde data-analyse" (GDA) willen toepassen op de metadata die via ongerichte interceptie zijn verzameld. In plaats daarvan zal de CTIVD bindend toezicht houden op deze bevoegdheid.

Volgens de MvT is deze wijziging nodig omdat toetsing door de TIB niet goed past bij het "dynamische proces van gegevensverwerking", maar tegelijk blijft voorafgaande toestemming door de minister nog wel vereist, dus waar dan de gewenste flexibilisering ligt is niet duidelijk. Bovendien doorbreekt deze wijziging het systeem van dat voor alle fases van de ongerichte interceptie toestemming van de minister plus toetsing door de TIB nodig is. Ook deze voorgestelde wijziging zou dus beter in het kader van een algehele herziening ingebracht kunnen worden.

Uitbreiding van gerichte interceptie naar gehackte apparaten

Artikel 10 maakt het mogelijk om de traditionele gerichte interceptie ook toe te passen op aansluitingen die door een target "in gebruik worden genomen", wat in de praktijk zal neerkomen op apparaten van derden die door een target worden gehackt. Het was al mogelijk om bijv. andere telefoonnummers en e-mailadressen van een target zelf op de taptoestemming "bij te schrijven", maar nu wordt dat dus ook mogelijk voor verbindingen die door een target gekaapt worden. Voor dergelijke bijschrijving is alleen interne toestemming vereist, maar de CTIVD krijgt hier wel bindend toezicht over.

De diensten krijgen dus de keuze om ofwel (op grond van art. 5 van het wetsvoorstel) iemands computer te hacken, danwel (op grond van art. 10) diens internetverbinding af te tappen wanneer zij zien dat een target die computer gehackt heeft. Ook wanneer dit nog slechts alleen geldt voor hackers uit landen met een offensief cyberprogramma en de basiscriteria van noodzakelijkheid, proportionaliteit en subsidiariteit er op van toepassing zijn, is dit een tamelijk vergaande wijziging die er toe kan leiden dat onze Joint Sigint Cyber Unit (JSCU) en de Russische GRU in de computer van een willekeurige burger of onderneming digitaal met elkaar in gevecht raken.

Uitbreiding van de opvraagbevoegdheid naar gehackte servers

Artikel 11 biedt een vergelijkbare bijschrijfmogelijkheid als art. 10, maar dan voor bedrijven als hostingproviders waar ondernemingen en particulieren serverruimte kunnen huren. Ook daar konden de diensten nu al data van een target opvragen (in de vorm van disk-images van servers aldus de MvT), maar voortaan kan dat ook voor andermans serverruimte die door een target gehackt is. Ook hier geldt dat voor een dergelijke bijschrijving alleen interne toestemming vereist is, maar de CTIVD hier wel bindend toezicht over krijgt.

Toezicht en beroepsprocedure

De resterende artikelen 12 t/m 15 van het wetsvoorstel behandelen wijzigingen in het toezicht en introduceren een geheel nieuwe beroepsprocedure voor het bindende toezicht. Daarover zijn door andere deskundige partijen al nuttige dingen opgemerkt, dus ik zal daar hier niet verder op in gaan.