Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX: een respons van Internet Society Nederland op de consultatieversie juni 2015

Amsterdam, 28 augustus 2015

Internet Society Nederland
bureau@isoc.nl

www.isoc.nl

Over ISOC Nederland

Internet voor iedereen

De Internet Society (ISOC) streeft naar een open, neutraal, gedecentraliseerd en voor iedereen toegankelijk en betrouwbaar internet. ISOC maakt zich sterk voor globale samenwerking op het gebied van internet- en gerelateerde technologieën: ISOC is de moederorganisatie voor een aantal toonaangevende internationale organen die zich bezig houden met het ontwikkelen en bevorderen van het gebruik van open internetstandaarden en –protocollen. Denk aan de Internet Engineering Task Force (IETF), de Internet Architecture Board (IAB), en de Internet Engineering Steering Group (IESG.

Daarnaast is ISOC pleitbezorger van een brede maatschappelijke discussie over internet-gerelateerde onderwerpen waarbij alle belanghebbenden evenredig vertegenwoordigd dienen te zijn.

In dat kader is één van de 'core values' van ISOC is bij uitstek relevant in deze respons :[1]

> 'The social, political, and economic benefits of the Internet are substantially diminished by excessively restrictive governmental or private controls on computer hardware or software, telecommunications infrastructure, or Internet content.'

ISOC is erkend door de Verenigde Naties en actief in 170 landen. Onder het motto 'het internet is voor iedereen' zet ISOC zich onder andere in voor de bevordering van wet- en regelgeving die de verdere ontwikkeling van het grenzeloze internet mogelijk maakt.

Internet Society Nederland is de Nederlandse afdeling ('chapter') van ISOC en als zodanig onderdeel van deze internationale niet-gouvernementele organisatie. Deze respons is echter ingediend namens ISOC Nederland en niet ISOC internationaal.

[1] http://www.internetsociety.org/who-we-are/mission/values-and-principles

Inleiding

Op 2 juli jl. is het wetsvoorstel om de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) aan te passen ter consultatie gepubliceerd.[2] Uiterlijk 1 september kan een ieder reageren op deze kabinetsvoornemens alvorens het concept, al dan niet aangepast naar aanleiding van de respons op de consultatie, naar de Raad van State gaat. Bij deze maakt Internet Society Nederland (ISOC Nederland) een aantal fundamentele zorgen die zij heeft met betrekking tot het wetsvoorstel kenbaar.

Aanpassing bijzondere bevoegdheden van de diensten: interceptie van kabelgebonden telecommunicatie in 'bulk'

Het Kabinet neemt in de 218 pagina's aan Memorie van Toelichting (MvT) bij het wetsvoorstel de conclusies en aanbevelingen uit het Wiv 2002 evaluatierapport van de commissie Dessens [3] 'in algemene zin' over. 'Inhoudelijk is de regeling inzake de verwerking van gegevens door de diensten op diverse onderdelen ingrijpend gewijzigd, met name waar het gaat om de bijzondere bevoegdheden van de diensten', aldus bladzijde 20 van de MvT. En inderdaad, zoals verwacht, op pagina 55 staat dat 'deze bevoegdheden thans technologieonafhankelijk (worden) geformuleerd, waarmee de bestaande beperking tot niet-kabelgebonden telecommunicatie komt te vervallen en derhalve ook kabelgebonden telecommunicatie voor interceptie als hier bedoeld (interceptie in "bulk") in aanmerking komt.'

Er valt wellicht iets voor te zeggen het onderscheid tussen media te laten 'vervallen' vanwege 'technologische ontwikkelingen'[4], maar waarom dan niet de huidige, beperktere kabelgebonden bevoegdheden naar het draadloze domein vertalen in plaats van andersom zoals nu gebeurt? De intentie van het Kabinet met betrekking tot 'kabelgebonden telecommunicatie' is echter heel helder: het gaat om beoogde '*interceptie in "bulk"*'.

Pagina 63 van de MvT zegt dat 'naast een explosieve groei van de hoeveelheid gegevens die in de wereld wordt geproduceerd (en elke twee tot drie jaar verdubbelt) moet worden vastgesteld dat inmiddels ongeveer 90% van alle telecommunicatie via kabelnetwerken verloopt. In de huidige wet is met deze ontwikkeling geen rekening gehouden.' En 'om zicht te houden op de dreigingen zijn de diensten afhankelijk van een adequate toegang tot telecommunicatie. (…) Bijzondere bevoegdheden die het mogelijk maken om – onder strikte

[2] http://www.internetconsultatie.nl/wiv
[3] http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/12/02/rapport-evaluatie-wiv-2002.html
[4] Alhoewel: bij interceptie in het publieke (!) draadloze domein vindt geen schending plaats van de integriteit van apparatuur en/of infrastructuur van een derde. Dat staat ook in zoveel woorden in de MvT op blz 203: 'De huidige wet kent in artikel 27 de bevoegdheid tot ongerichte interceptie van niet-kabelgebonden telecommunicatie, waarbij niet voorzien is in een medewerkingsplicht voor aanbieders van een openbaar telecommunicatienetwerk of openbare telecommunicatiedienst.' Die medewerkingsplicht is namelijk niet vereist om ongericht niet-kabelgebonden telecommunicatie te intercepteren. Daarnaast kan men betogen dat gebruikers van e.g. satellietcommunicatievoorzieningen een duidelijker en in ieder geval beperktere doelgroep vormen. Noodzakelijkheid en proportionaliteit van inzet van bijzondere bevoegdheden zijn in dat geval beter te beargumenteren.

voorwaarden – in bulk te intercepteren in het kabelgebonden domein zijn daarbij onmisbaar.'

Oftewel ongericht, in 'bulk via de 'kabel' want 'onmisbaar', en noodzakelijk en proportioneel. Aldus het Kabinet.

Nut en Noodzaak

Op basis van de stukken is ISOC Nederland er echter geenszins van overtuigd dat genoemde noodzakelijkheid is aangetoond en dat deze vervolgens opweegt tegen de potentieel ernstige inbreuk op de persoonlijke levenssfeer van privépersonen, zoals het Kabinet overigens zelf ook vaststelt.

Nederland behoort tot de top in de wereld als het gaat om gebruik van breedband- en mobiel internet door haar burgers, en beschikt over een zeer geavanceerde open en neutrale internetinfrastructuur. Wat betekent de inzet van de nieuwe bijzondere bevoegdheden voor het vereiste vertrouwen van personen, bedrijven en andere organisaties om online te communiceren en zaken te doen in Nederland? Wat zijn de economische consequenties? Dat laatste element ontbreekt geheel in de motivatie van het Kabinet.[5] Terwijl de onthullingen van Snowden over het gedrag van Amerikaanse veiligheidsdiensten er wel degelijk voor gezorgd hebben dat online bedrijvigheid uit de Verenigde Staten verdween.[6]

Voordat het instrumentarium van de diensten uitgebreid wordt zoals voorgesteld, moet volgens ISOC Nederland allereerst grondig en vooral onafhankelijk onderzoek plaatsvinden naar de effectiviteit, en dus proportionaliteit, van ruimere bevoegdheden en het ongericht kunnen tappen op kabelgebonden infrastructuur. Uit studies in andere landen blijkt deze op zijn minst twijfelachtig.[7] Politieke prioriteit en gebrek aan transparantie staat dan hoger op de agenda dan (on)gewenst resultaat. Hoeveel veiliger wordt de situatie? Welke aanslagen zijn daadwerkelijk en aantoonbaar vermeden? Hoe kunnen we beoordelen of geïmplementeerde maatregelen de beoogde (welke?) resultaten realiseren en of deze inderdaad opwegen tegen de 'collateral

---

[5] Zeer opmerkelijk gezien de al in 2011 gestelde ambities van het Kabinet om van Nederland een 'Digital Gateway to Europe' te maken. Zie de Digitale Agenda http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/notas/2011/05/17/digitale-agenda-nl-ict-voor-innovatie-en-economische-groei/282931-e07-digitale-agenda.pdf , en ook de https://digitale-infrastructuur.nl/ rapporten uit 2013 en 2014. Het economische belang van de Nederlandse digitale infrastructuur wordt inmiddels door een ieder erkend: het is een essentiële en snel groeiende 'third mainport', naast de haven van Rotterdam en Schiphol.

[6] http://www2.itif.org/2013-cloud-computing-costs.pdf

[7] Zie het 'Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court' van de Amerikaanse 'Privacy and Civil Liberties Oversight Board https://www.documentcloud.org/documents/1008957-final-report.html op blz 11: 'We have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack.'

damage'? Er zal toch op zijn minst in concreet onderbouwde termen aannemelijk gemaakt moeten worden dat bestaande bevoegdheden ontoereikend zijn.

Ook de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) stelt in haar jaarverslag 2014-2015 dat:[8]

'De Commissie het als een gemis (ervaart) dat in Nederland vooralsnog nauwelijks wordt gediscussieerd over *de vraag in hoeverre het noodzakelijk is bevoegdheden uit te breiden*. De nadruk in de discussies ligt al snel op de rechtmatigheid van het handelen en minder op de doelmatigheid of effectiviteit van interceptiebevoegdheden. *De discussie kan daardoor blijven hangen bij de constatering dat tegenwoordig 90 procent van de communicatie over de kabel gaat en daardoor de 'traditionele' bevoegdheid tot het ongericht intercepteren van satellietcommunicatie (de resterende 10 procent) niet meer volstaat. Maar kan deze constatering alleen de conclusie tot de uitbreiding van de bevoegdheden dragen? Daarvoor moet men toch een beeld hebben van de effectiviteit en/of het gebrek daaraan van de bestaande bevoegdheden?* Ook internationaal is dit een vraag die de gemoederen bezighoudt, maar waarover weinig uitsluitsel wordt gegeven. *Uitgangspunt zou moeten zijn dat eerst de noodzaak voor nieuwe bevoegdheden, ingegeven door tekortschietende effecten van de huidige bevoegdheden, overtuigend moet worden aangetoond voordat sprake kan zijn van een wettelijke uitbreiding*.'

En daar voegt de CTIVD aan toe:

'*Deze effectiviteitstoets wordt ook ingegeven door de rechtmatigheidstoets die artikel 8 van het Europees Verdrag voor de Rechten van de Mens voorschrijft vanuit het oogpunt van privacybescherming. Daarbij staat niet alleen ter beoordeling welke schade aan de nationale veiligheid wordt voorkomen, maar tevens welk nadeel individuen wordt berokkend met de interceptiebevoegdheden*.'

(cursivering en onderstreping door ISOC Nederland)

Integraal Afwegingskader?

Het is aan het Kabinet om nut en noodzaak van het wetsvoorstel aan te tonen, niet aan derden om aan te geven hoe deze onderbouwing er uit moet zien. Het officiële 'Integraal Afwegingskader' (IAK)[9] kan in deze assistentie verlenen.

'Het IAK is een werkwijze en informatiebron en toe te passen op elk moment in het beleidsproces. Met name in een vroeg stadium van het beleidsproces heeft de toepassing van het IAK meerwaarde. Elk voorstel voor beleid of regelgeving dat wordt voorgelegd aan het parlement moet een adequaat antwoord bevatten op de 7 hoofdvragen van het IAK:

1. Wat is de aanleiding?
2. Wie zijn betrokken?
3. Wat is het probleem?

[8] http://www.ctivd.nl/documenten/jaarverslagen/2014/04/30/jaarverslag-2014 , blz 28
[9] https://www.kcwj.nl/kennisbank/integraal-afwegingskader-beleid-en-regelgeving

4. Wat is het doel?
5. Wat rechtvaardigt overheidsinterventie?
6. Wat is het beste instrument?
7. Wat zijn de gevolgen?'

ISOC Nederland heeft sterk de indruk dat de 'verplichte kwaliteitseisen' waarop het IAK is gebaseerd, niet zijn meegenomen bij de totstandkoming van het wetsvoorstel:[10]

Veiligheidsbewustzijn van targets en hacken van onschuldige technisch zwakkere randgebruikers

De MvT wijst op het 'veiligheidsbewustzijn' van 'targets', en knoopt daar vervolgens een wat ISOC Nederland betreft perverse conclusie aan op blz. 53 dat dit 'kansen' biedt 'tot het benutten van zwakheden bij technische randgebruikers'. Gericht hacken via (apparatuur van) bij voorbaat niet-verdachten en onschuldigen, in de hoop dat men op deze wijze indirect bij de 'targets' kan komen. Zie artikel 30, eerste lid, onder b, van het wetsvoorstel. Los daarvan dient men zich in ieder geval af te vragen in hoeverre massale ongerichte interceptie een toegevoegde waarde levert in termen van het beschermen van nationale veiligheidsbelangen wanneer technisch onderlegde individuen en groepen de vertrouwelijkheid van hun communicatie relatief eenvoudig weten te waarborgen. Voor ISOC Nederland stellen anonimiteit en gebruik van encryptie burgers juist in staat hun recht op vrijheid van meningsuiting en expressie uit te oefenen. En ook in termen van het geven van een 'tegenmacht' richting het opereren van veiligheidsdiensten is ISOC Nederland van mening dat encryptie er voor zorgt dat de kosten van massasurveillance verhoogt worden en diensten dwingt interceptie specifiek te maken en te houden. Anonimiteit en gebruik van encryptie zouden dus vanuit overheidswege beschermd, geborgd en zelfs gepromoot moeten worden.[11] Daar gaan de kabinetsvoornemens echter rechtstreeks tegenin, een algemeen decryptiebevel incluis. Zie bijvoorbeeld artikel 30, lid 5 en 8, en artikel 41.

Effectiviteit bijzondere bevoegdheden

Een feit is daarnaast dat daders van recent gepleegde aanslagen in het buitenland al lang in beeld waren van diensten. Hoe effectief is dan één en ander? Is dit indicatief voor de beperkingen die te ruime bevoegdheden met zich brengen? Men is op zoek naar een speld in een hooiberg maar creëert de facto extra hooibergen. Hoe dan ook, dit soort vragen verdient een fundamentele

---

[10] https://www.kcwj.nl/kennisbank/integraal-afwegingskader-beleid-en-regelgeving/verplichte-kwaliteitseisen : 'Het IAK is gebaseerd op de verplichte kwaliteitseisen, die de ministerraad op 14 april 2011 heeft vastgesteld.

[11] Zie rapport UN rapporteur Freedom of Expression David Kaye 'on the promotion and protection of the right to freedom of opinion and expression van 22 mei 2015 http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc : 'With respect to encryption and anonymity, States should adopt policies of non-restriction or comprehensive protection, only adopt restrictions on a case-specific basis and that meet the requirements of legality, necessity, proportionality and legitimacy in objective, (and) require court orders for any specific limitation' en 'states should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression'

discussie op basis van onafhankelijk gepresenteerd feitenmateriaal. Zolang dat er niet is, en de effectiviteit van nieuwe bevoegdheden dus niet ingeschat kan worden, is uitbreiding van bevoegdheden bij voorbaat niet noodzakelijk en -proportioneel.

Grondrechten van burgers

Het Kabinet lijkt zich bewust dat 'de uitoefening van deze bijzondere bevoegdheden per definitie raakt aan het recht op bescherming van privacy van de burgers.'[12] Echter, 'gelet op de verantwoordelijkheid en de zorg van de overheid voor de veiligheid van haar burgers is het onontkoombaar dat de diensten persoonsgegevens verzamelen en verwerken.' Sterker nog, 'de overheid beoogt met gepaste en doelgerichte uitoefening van deze bevoegdheden bij te dragen aan het realiseren in een veilige samenleving van grondrechten, waaronder ook het recht op privacy.' De uitbreiding van de bevoegdheden moet er dus komen omdat deze (o.a.) bijdraagt aan de bescherming van het recht op privacy? Dat klinkt voor ISOC Nederland als een drogreden…

Ook in de MvT wordt meerdere keren aan het aspect van (de inbreuk op) grond- en mensenrechten gerefereerd. In hoofdstuk 1 staat bijvoorbeeld:

'Diverse in het wetsvoorstel opgenomen bepalingen inzake de verwerking van gegevens, waarbij naast de algemene bevoegdheid tot gegevensverzameling ook bijzondere bevoegdheden ter zake kunnen worden ingezet, maken – in meer of mindere mate – een inbreuk op relevante grond- en mensenrechten, in het bijzonder de artikelen 10, 12 en 13 Grondwet en artikel 8 EVRM. Bij de uitwerking van de verschillende bevoegdheden en andere relevante aspecten van gegevensverwerking (zoals de verstrekking van gegevens) is op de daaruit voortvloeiende eisen acht geslagen, waarbij op een evenwichtige manier recht is gedaan aan zowel het belang van de nationale veiligheid als aan dat van het recht op bescherming van de persoonlijke levenssfeer.'

In combinatie met het weinig steekhoudende pleidooi dat ongerichte interceptie beoogt 'bij te dragen aan het realiseren in een veilige samenleving van grondrechten', vindt ISOC Nederland niet dat in het voorstel 'op een evenwichtige manier recht is gedaan' aan de bescherming van die grondrechten. Gezien de intenties van het Kabinet ('interceptie in "bulk") mag men terdege rekening houden met een zekere vooringenomenheid in deze. Mede in een context van recente uitspraken door het Hof van Justitie van de Europese Unie[13] en de Haagse Rechtbank[14] zou ISOC Nederland onderbouwing willen zien door een onafhankelijke en deskundige partij hoe de voornemens zich (niet) verhouden tot e.g. een artikel 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM).[15] Alvorens tot

[12] Kamerstukken II 2013/14, 33 820, nr. 4.

[13] http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054nl.pdf
[14] http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2015:2498
[15] Als het gaat om vereist toezicht en bijbehorende transparantie, dan geeft IVIR daar een goede aanzet toe met een op 23 juli jl. gepubliceerd rapport http://www.ivir.nl/nieuws/tenstandards . Wat ISOC betreft neemt het Kabinet de erin opgenomen aanbevelingen één op één over.

een uitbreiding van bevoegdheden van diensten over te gaan[16].

Een pas op de plaats maken

ISOC Nederland is van mening dat er dus nog flink wat huiswerk is te doen: de uitgangspositie van het Kabinet is in de kern niet onderbouwd en gemotiveerd.

Het kan niet zo zijn dat vaag en eenzijdig gedefinieerde nationale veiligheidsbelangen de doorslag geven. Zoals Minister van Defensie Hennis-Plasschaert tijdens een Algemeen Overleg op 10 Februari jl. karikaturaal bevestigde [17]: de MIVD zou 'blind en doof' zijn. Ze noemde een aantal onduidelijke 'voorbeelden' die 'hoewel ik niet helemaal tot in detail kan gaan, er echt toe doen voor de informatiepositie van Nederland, de bescherming van de staatsveiligheid en onze belangen in het buitenland. Ik hoop dat ik daarmee de urgentie hiervan voor het voetlicht heb gebracht.' Oftewel noodzakelijk want 'urgent', volgens de Minister. Maar niet 'noodzakelijk' volgens ISOC Nederland. Men kan niet weg komen met het argument, zonder onderbouwing, dat openheid van zaken de 'informatiepositie van Nederland' schaadt. In een rechtstaat die Nederland pretendeert te zijn, moet als uitgangspunt gelden dat bijzondere bevoegdheden ook bijzondere verantwoording vereisen.

Een aantal specifieke elementen uit het wetsvoorstel

Er zijn vele elementen in het 83 bladzijden tellende wetsvoorstel die gedetailleerd aangevochten kunnen worden dan wel vragen oproepen, hetgeen volgens ISOC alleen maar bevestigt dat *eerst volstrekt helder moet gemaakt moet worden wat nut en noodzaak van de voorgestelde wijzigingen is*. Zoals het er nu staat is het voorstel buitenproportioneel. Er zal dus op zijn minst een pas op de plaats gemaakt moet worden. Enkele voorbeelden:

1. Toestemmingsvereisten

Toestemming voor de uitoefening van een bijzondere bevoegdheid door een dienst wordt verleend voor een periode van maximaal drie maanden, maar er is geen grens ('telkens') aan het aantal keren dat de toestemming verlengd kan worden, Aldus artikel 24 lid 3. Dat geldt ook voor interceptie 'in bulk' op de kabel. Die potentieel eindeloze tap is buitenproportioneel.

'Het nieuwe, technologieonafhankelijke stelsel voor de interceptie van telecommunicatie ("bulk") zal op hoofdlijnen uit een drietal fasen bestaan' Aldus de MvT op blz. 63: interceptie van data, voorbewerking van die data en 'verdere verwerking'. Voor ieder fase is een expliciete toestemming vereist. Echter de Minister kan ook een 'combinatie-last' geven, bijvoorbeeld gelijktijdig voor zowel

---

[16] Het Kabinet heeft na aandringen van de Tweede Kamer wel een 'privacy impact assesment' aangekondigd, 'parallel aan het in consultatie geven van het voorstel voor een nieuwe Wiv'. Aldus Minister Plasterk in een brief aan de Kamer van 17 maart jl (2015-0000158585). Ook de MvT refereert er aan in de titel van hoofdstuk 12: 'Hoofdstuk 12 Consultatie, adviezen en privacy impact assessment **'.** Het hoofdstuk zelf is echter leeg, en vooralsnog zijn doel, methode, tijdslijnen, en wat er met de resultaten gebeurt van genoemde voorgenomen 'assesment', volstrekt onduidelijk.

[17] http://www.tweedekamer.nl/vergaderingen/commissievergaderingen/details?id=2015A00163

fase 1 als 2. Hetgeen ook logisch klinkt want als men tot interceptie overgaat dan is dat natuurlijk enkel en alleen ten behoeve van de analyse van de inhoud van onderschepte data. Maar dit maakt de beoogde afbakening en de daarbij gesuggereerde controle wel minder expliciet en plausibel. Terwijl het Kabinet zelf aangeeft dat 'van fase tot fase derhalve in oplopende mate inzicht (wordt) verkregen in de persoonlijke levenssfeer. De waarborgen die in de wet zullen worden opgenomen, worden zwaarder naarmate de persoonlijke levenssfeer van individuen indringender in beeld komt'.[18] In de praktijk zal toestemming voor fase 1 dus het belangrijkst zijn voor de uitoefening van de analyse in fase 2 en 3.

Als de Minister besluit om toestemming te verlenen voor het uitoefenen van een bijzondere bevoegdheid door een dienst, dan kan de CTIVD, die daarvan op de hoogte gesteld wordt, aangeven wanneer zij van mening is dat die toestemming onterecht is. De Minister heeft dan een ´heroverwegingsplicht´, maar kan het oordeel van de CTIVD desalniettemin naast zich neer leggen. Vervolgens is het aan de fractievoorzitters in de Tweede Kamer (de zo geheten 'commissie Stiekem') om te oordelen of de Minister al dan niet terecht het oordeel van de CTIVD naast zich neer heeft gelegd. De uiteindelijke beslissing komt dus niet bij een rechter of een onafhankelijke toezichthouder te liggen, maar bij politici. ISOC Nederland vindt het een zeer slechte zaak dat de toestemmingsvraag en het bijbehorende toezicht daarmee een fundamenteel politieke component hebben gekregen.[19]

2. Waarom uitzonderingen?

Waarom is er een uitzonderingspositie voor journalisten, waarbij in het kader van bronbescherming toetsing door rechter moet plaatsvinden (artikel 24 lid 4 van het wetsvoorstel) alvorens bijzondere bevoegdheden ingezet worden? Rechtelijke toetsing is natuurlijk prima, maar dat zou dan ook in alle andere gevallen zo moeten zijn. Terwijl dan toestemming van de Minister, of zelfs een aangewezen ambtenaar, toereikend is.

Artikel 29 stelt dat het briefgeheim ('het openen van brieven en andere geadresseerde zendingen, zonder goedvinden van de afzender of de geadresseerde') door diensten slechts te schenden is indien daartoe de rechtbank Den Haag een last heeft afgegeven. Waarom is dat ook niet zo bij andere, digitale vormen van communicatie, zoals email?[20] Daarnaast: het is toch

[18] Brief aan de Tweede Kamer 2014-0000622926, Kabinetsstandpunt herziening interceptiestelsel Wiv 2002, 21 november 2014

[19] Dit staat nog los van het ernstige feit dat het staatsgeheime informatie kan betreffen, en de Kamer bij een motie van wantrouwen, of zelfs in het uiterste geval bij het dwingen tot aftreden van een Minister, niet een publieke discussie kan voeren. En als het niet zover komt, en het Kabinet kan steunen op een meerderheid in de Tweede Kamer, dan mag men veronderstellen dat dit ook zo is in de 'Commissie Stiekem'. Hetgeen de oppositie in dat geval monddood maakt.

[20] Zie ook blz 195 van de MvT: 'Artikel 8 EVRM is niet alleen van toepassing op het brief-, telefoon- en telegraafgeheim, maar ook op inhoud van communicatie die via andere communicatiemiddelen wordt getransporteerd. Het thans aanhangig zijnde herzieningsvoorstel voor artikel 13 Grondwet stelt voor alle inhoud van communicatie, ongeacht met welk communicatiemiddel deze wordt overgebracht, aan dezelfde eisen te onderwerpen. Artikel 8 EVRM kent een hiermee vergelijkbare benadering. Artikel 8 EVRM vereist daarnaast dat een

de uitdrukkelijke intentie om de wet 'technologieonafhankelijk' te maken? Waarom dan een uitzondering voor 'brieven en andere geadresseerde zendingen'?

3. Hackbevoegdheid

Artikel 30 beschrijft het verkennen en binnendringen van geautomatiseerde werken inclusief een decryptiebevel (lid 5 en lid 8). Zoals gezegd, diensten moeten ook de gelegenheid krijgen om, gericht via het hacken van onverdachte derden, dichter bij 'targets' te komen (omschreven als 'operationele kansen tot het benutten van zwakheden bij technische randgebruikers'). Dit zonder die onschuldige 'randgebruikers' daarover in te lichten.

In het algemeen zal een hackbevoegdheid een prikkel zijn voor diensten om kwetsbaarheden te zoeken en zo mogelijk gebruik te maken van zogenaamde zero day vulnerabilities. Dit is echter zeer ongewenst volgens ISOC Nederland: dergelijke zwakheden kunnen door een ieder uitgebuit worden, ook door de targets, terroristen en buitenlandse mogendheden waar de diensten juist tegen in het geweer (willen) komen. Indien dergelijke kwetsbaarheden niet bekend gemaakt worden en niet direct worden gerepareerd, dan is dat schadelijk en gevaarlijk voor iedereen. 'The vulnerabilities they discover affect the security of us all', zoals security expert Bruce Schreier aangeeft.[21] Daarnaast is er een paradox: enerzijds moet een overheid-gerelateerde dienst kunnen hacken, en deze heeft er dus belang bij dat kwetsbaarheden (blijven) bestaan. Terwijl gelijktijdig bedrijven wettelijk verplicht zijn alle mogelijke maatregelen te treffen om hun netwerken te beveiligen inclusief een meldingsplicht wanneer het toch mis gaat. Hoe daarmee om te gaan? Dit is niet de betrouwbare en transparante overheid die we zouden willen zien, vindt ISOC Nederland.

4. Bewaartermijnen

Bewaartermijnen in het wetsvoorstel worden niet gemotiveerd en zijn daarom buitenproportioneel. In artikel 33 staat dat in bulk onderschepte en nog niet 'verwerkte' data drie jaar mogen worden opgeslagen. Als ze na die periode niet relevant blijken te zijn dan 'worden ze terstond vernietigd'. Hetgeen suggereert dat 'relevante data' wel langer dan 3 jaar bewaard worden. Een uiterste periode wordt niet vermeld. En in artikel 30 lid 9 (hackbevoegdheid) staat: gegevens 'worden zo spoedig mogelijk op hun relevantie voor het onderzoek waarvoor ze zijn verworven onderzocht. Gegevens, waarvan is vastgesteld dat deze niet relevant zijn voor het onderzoek dan wel niet op hun relevantie voor het onderzoek zijn onderzocht, worden na een periode van ten hoogste twaalf maanden vernietigd.' Waarom niet-relevante gegevens een jaar bewaren? En gegevens moeten direct worden onderzocht, maar als dat niet gebeurt (?) dan kunnen ze alsnog 12 maanden worden bewaard?

---

inbreuk op het in artikel 8 EVRM neergelegde recht een legitiem doel moet dienen, bij wet moet zijn voorzien en noodzakelijk moet zijn in een democratische samenleving.' Artikel 8 EVRM verwijst niet expliciet naar een vereiste voorafgaande toestemming van een onafhankelijke rechter, maar wat ISOC NL betreft is dat wel de lijn die het Kabinet dient te kiezen wanneer 'alle inhoud', 'ongeacht het communicatiemiddel', 'aan dezelfde eisen' onderworpen wordt.

[21] https://www.schneier.com/blog/archives/2014/05/disclosing_vs_h.html

5. Doelgerichtheid interceptie in bulk en onderverdeling in fasen

De ongerichte en technologie-neutrale ('bulk') interceptiebevoegdheid uit artikel 33 lid 1 kan alleen met voorafgaande toestemming van de Minister worden ingezet. Zie de opmerking hierboven over een voorkeur van ISOC voor een onafhankelijke toetsing vooraf, bij uitstek relevant voor wat betreft deze ultieme bevoegdheid. Daarnaast, als het gaat om de zogenaamde vereiste 'doelgerichtheid' van de inzet van deze bevoegdheid: 'Zo zal in het verzoek onder meer het onderzoek waarvoor de bevoegdheid moet worden ingezet dienen te worden omschreven alsmede het doel wat met de bevoegdheidsuitoefening wordt beoogd. Daarbij kan niet worden volstaan met een globale aanduiding, maar moet dit zo concreet als mogelijk is, dienen te worden ingevuld.' Aldus de MvT op pagina 67. Dat is voor ISOC Nederland een te vage en ruim gedefinieerde en 'ongerichte' doelopvatting. Het is volstrekt onduidelijk aan welke vereisten de formulering van 'onderzoek' en 'doel' moet voldoen, op basis waarvan toestemming verleend wordt.

Artikel 34 richt zich op fase 2, de zogenaamde 'voorverwerking'. Dat suggereert dat die voorverwerking betrekking heeft op de in fase 1 geïntercepteerde data. Dat is ook het geval, echter daarnaast hebben de diensten uit hoofde van artikel 34 ook een bevoegdheid met betrekking tot 'beoogde activiteiten (…) in het cyberdomein waar het gaat om netwerkmonitoring of netwerkdetectie'. De Mvt zegt op blz 71 dat dan 'bijvoorbeeld door de inzet van Deep Packet Inspection-apparatuur, *realtime* en *online* het dataverkeer (wordt) geanalyseerd.' Het is voor ISOC Nederland niet duidelijk hoe deze bevoegdheid zich verhoudt tot de gedefinieerde fasen en de daarbij behorende toestemmingsvereisten. Als zodanig lijkt deze 'cyber' bevoegdheid zelfs verborgen. Is dat de intentie van de wetgever?

6. Verruiming van medewerkingsplicht voor bedrijven: introductie 'aanbieder van communicatiedienst'

In de Telecommunicatiewet (Tw) is bepaald dat de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten verplicht zijn medewerking te verlenen aan de uitvoering van een toestemming tot het aftappen of opnemen van telecommunicatie die over hun telecommunicatienetwerken wordt afgewikkeld dan wel via hen verzorgde telecommunicatie. In artikel 32, zevende lid, wordt voor wat betreft de Wiv de medewerkingsplicht uitgebreid tot de 'aanbieders van een communicatiedienst' op wie niet reeds een medewerkingsverplichting ex artikel 13.2 Tw rust. Op basis van artikel 31 kan men niet anders dan vaststellen dat het de intentie van de wetgever is om *iedere* 'aanbieder', natuurlijk- of rechtspersoon, onder de reikwijdte van de wet te laten vallen: het gaat om een ieder 'die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of die gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst'. Of het nu een zorgaanbieder is of een online-winkel, een onderwijsinstelling of sportclub. Deze categorie aanbieders is in principe grenzeloos, iedere organisatie communiceert met de buitenwereld via een website, en daarom is deze categorie veel te ruim.

7. 'Kostendragerschap'

De kostenregeling voor 'openbare' aanbieders die vallen onder de Telecommunicatiewet, wordt voor die nieuwe uitgebreide categorie 'aanbieders van een communicatiedienst' overgenomen. Zoals de MvT zegt op blz. 61: 'Kort gezegd komt die regeling erop neer dat deze aanbieders de investerings-, exploitatie- en onderhoudskosten die zij moeten maken om (technisch) aftapbaar te zijn, zelf dienen te dragen'. Een eenzijdige last voor deze zeer brede groep van natuurlijke- en rechtspersonen dus. ISOC Nederland daarentegen zou het een goede zaak vinden als de overheid zelf deze (voor een aanbieder aanzienlijke) kosten op zich neemt. Het zou namelijk indirect als een proportionaliteitstoets fungeren: staan de te maken kosten van interceptie echt in verhouding tot de beoogde baten? Wanneer deze kosten eenzijdig bij de aanbieders worden neergelegd dan is van een dergelijke afweging geen sprake.

Daarnaast is het zeer zorgelijk dat de wetgever geen besef heeft van de mogelijke financiële impact voor genoemde aanbieders, zie de Mvt op bladzijden 201 en 202:

'Een gedetailleerd inzicht in de kosten van interceptie van telecommunicatie op kabelgebonden netwerken als hier bedoeld is op dit ogenblik echter nog niet mogelijk. Deze kosten zullen de komende periode in nauw overleg met relevante aanbieders in de telecomsector in kaart worden gebracht. Het overleg met relevante aanbieders in de telecomsector is tevens vereist om te achterhalen hoe deze bevoegdheid in een technisch complexe omgeving op de meest doeltreffende en doelmatige manier kan worden toegepast, met zo min mogelijk inbreuken op de persoonlijke levenssfeer van burgers. Bij de implementatie van de interceptie van telecommunicatie op kabelgebonden netwerken in het kader van de nieuwe wet is voorts sprake van schaalbaarheid in omvang en tijd. De keuzes die hierbij worden gemaakt hebben vanzelfsprekend gevolgen voor het financiële beslag. Mede om ervaring op te doen op grond waarvan gerichte vervolgstappen kunnen worden genomen, zal de interceptie na inwerkingtreding van de wet in de aanvangsjaren tot enkele fysieke toegangspunten beperkt blijven.'

Het lijkt ISOC Nederland erg onwaarschijnlijk dat er bereidwilligheid zal bestaan bij 'relevante aanbieders' om hierover in 'nauw overleg' met de diensten te treden.

Veel erger is dat het hierbovenstaande suggereert dat de diensten 'tevens' niet weten hoe die kabelgebonden interceptie in te richten. En dat de aanbieders daarom moeten bijdragen aan ontwerp en inrichting 'om te achterhalen hoe deze bevoegdheid in een technisch complexe omgeving op de meest doeltreffende en doelmatige manier kan worden toegepast'. Hetgeen de diensten de gelegenheid moet geven om in de 'aanvangsjaren' wat te testen op 'enkele' onduidelijke 'fysieke toegangspunten', 'om ervaring op te doen', waarna de 'beperking' opgeheven kan worden en de inzet van de bevoegdheid uitgebreid kan worden. Dit kan toch niet waar zijn…

8. Delen gegevens met buitenlandse diensten

Artikel 49 beschrijft het delen van onderschepte gegevens met buitenlandse

diensten, enkel met toestemming van de Minister. Zie de eerder aangegeven gewenste onafhankelijke toetsing. 'Bulk' data kunnen worden gedeeld met andere diensten zonder dat deze geëvalueerd zijn door de Nederlandse diensten. Dus wat men deelt is dan niet bekend. ISOC Nederland beseft dat er uitwisseling tussen diensten moet (kunnen) plaatsvinden, indien noodzakelijk. Maar dan wel gericht, met kennis van de inhoud.

Artikel 76 lid 3 zegt dat alvorens tot 'samenwerking' wordt overgegaan met ene buitenlandse dienst, er eerst een 'weging' plaats vindt op basis van een aantal 'criteria': wat is de 'democratische inbedding' van betreffende buitenlandse dienst, hoe zit het met de 'eerbiediging van de mensenrechten' in het land, en hoe zit het met de 'professionaliteit en betrouwbaarheid' van die dienst. Niet alleen worden de termen als 'democratische inbedding', 'professionaliteit' en 'betrouwbaarheid' niet ingevuld, ook niet in de MvT, ernstiger is dat de doorslag om tot samenwerking over te gaan niet expliciet afhankelijk is van deze criteria. Indien noodzakelijk dan vindt 'samenwerking' gewoon plaats. Immers, zie MvT op blz 137, het Kabinet heeft 'aangegeven dat wereldwijde internationale samenwerking voor de inlichtingen- en veiligheidsdiensten een *conditio sine qua non* is'. Het is dus slechts een intentieverklaring, en kan daarom als artikel ook weg gelaten worden want een wassen neus volgens ISOC Nederland.

Practice what you preach: bescherm de publieke kern van het internet

Nogmaals, wat ISOC Nederland betreft is het uitgangspunt van het voorstel, dat wil zeggen de nut en noodzaak er van, niet onderbouwd en is het dus niet aan de orde om over gedetailleerde invulling te spreken. Een volledige heroverweging van de voornemens verdient de voorkeur. ISOC Nederland wijst de Nederlandse regering in dat kader graag op het uit onverdacht neutrale hoek komende rapport 'De publieke kern van het internet' van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR).[22] Volgens de WRR is er een kern van centrale protocollen en technologie van het internet aan te wijzen die als een *mondiaal publiek goed* kan worden aangemerkt. Het internet als publiek goed functioneert alleen als het de kernwaarden universaliteit, interoperabiliteit en toegankelijkheid garandeert en als het de kerndoelen van informatieveiligheid, te weten vertrouwelijkheid, integriteit en beschikbaarheid ondersteunt. Nederland zou als onderdeel van haar diplomatieke agenda de vereiste neutraliteit van die kerninfrastructuur van het internet moeten opnemen:

'Het beschermen van de publieke kern van het internet is bovendien voor Nederland een verlengd nationaal belang. Een dergelijk belang ligt op een lijn met strategische mondiale vraagstukken die als internationaal publiek goed gedefinieerd kunnen worden, zoals het mitigeren van klimaatverandering of de stabiliteit van het financiële systeem. *Voor Nederland is het betrouwbaar functioneren van het internet van vitaal belang voor zijn economie, economische groei en het functioneren van de (digitale) samenleving*. Nederland scoort zeer hoog op internationale ranglijsten over internettoegang en breedbandverbindingen en bevindt zich in de top van OECD-landen met het hoogste percentage van de bevolking dat online aankopen doet. Nederland heeft een levendige internetindustrie en de AMS-IX is een van de grootste Internet

[22] http://www.wrr.nl/publicaties/publicatie/article/de-publieke-kern-van-het-internet-1/

Exchange Points ter wereld. (…) Nederland heeft niet alleen veel mee in termen van een levendige internetindustrie en -cultuur en politiek leiderschap op een aantal dossiers als netneutraliteit, maar kent ook een traditie van idealisme en pragmatisme. Deze traditie zorgde in eerdere tijden voor een relatief vrije informatiecultuur en bloeiende economie in Nederland. Dat kleine staten aan de wieg van internationale normen of diplomatieke doorbraken staan, is bovendien geen uitzondering. *Voor Nederland is het uitwerken en uitdragen van een nieuwe agenda voor internetdiplomatie, met als uitgangspunt het waarborgen van de kern van het internet als een mondiaal publiek goed, een passende nieuwe ambitie. Dat het waarborgen van de publieke kern van het internet ook voor andere staten een verlengd nationaal belang is, kan als frame voor de internationale agenda dienen.'*[23]

Nederland moet niet willen deelnemen aan de wedloop tussen verschillende staten en hun veiligheidsdiensten: de onthullingen van Snowden hebben de schade van de inzet van ongerichte en massale interceptiebevoegdheden door diensten wel voldoende aangetoond, in combinatie met een daarmee samenhangend gebrek aan transparantie en onafhankelijk toezicht. Bovendien is 'het risico levensgroot dat het cumulatieve effect van nationale maatregelen – waarbij staten in toenemende mate tegen elkaar opbieden – resulteert in grote kwetsbaarheden van de kern van het internet als een publieke infrastructuur. In aanvulling hierop *ontstaat op nationaal niveau de paradox dat sommige delen van de overheid dagelijks proberen een betrouwbaar en veilig internet te waarborgen terwijl andere delen van de overheid op dit gebied de risico's juist vergroten*.'[24]

(cursivering door ISOC Nederland)

De WRR stelt in dat kader terecht dat 'Nederland zich met de oprichting van *Freedom Online Coalition* opgeworpen (heeft) als een voorloper op het gebied van de digitale mensenrechten. Nederland zou ook het voortouw kunnen nemen bij een diplomatieke inspanning die het waarborgen van de publieke kern van het internet als centrale inzet heeft.'[25]

ISOC Nederland is het geheel met de WRR eens dat het van zeer groot belang is het functioneren en de integriteit van die publieke kern van het internet, de protocollen en infrastructuur, veilig te stellen en te beschermen tegen oneigenlijke interventies door staten en andere partijen. Waarbij Nederland dan inderdaad goed gepositioneerd is een internationale rol als gidsland op zich te nemen, mits 'we practice what we preach'. Dat laatste is echter niet wat het Kabinet met het wetsvoorstel voor ogen lijkt te hebben…

Namens het bestuur van ISOC Nederland,

Bastiaan Goslings

[23] WRR (2015), *De publieke kern van het internet*, Amsterdam University Press, blz 100
[24] Idem, blz 103
[25] Idem, blz 110