Stichting Digitale
Infrastructuur Nederland

Reactie van Stichting DINL op het concept wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX: Versie juni 2015

Leidschendam, 31-8-2015

Excellentie,

Stichting Digitale Infrastructuur Nederland (DINL) vertegenwoordigt de belangrijkste spelers en organisaties van de Nederlandse digitale infrastructuur. DINL is de spreekbuis van Nederlands derde mainport[1]. De sector vormt het hart van de Nederlandse online economie en heeft een sleutelrol in het wereldwijde internet. Deelnemers van DINL zijn AMS-IX (Amsterdam Internet Exchange), DDA (Dutch Datacenter Association), DHPA (Dutch Hosting Provider Association), ISPConnect, Stichting NlNet, SIDN (Stichting Internet Domeinregistratie Nederland) en SURFnet.

DINL maakt zich grote zorgen om de gevolgen van het 2 juli jongstleden ter consultatie gepubliceerde Kabinetsvoorstel waarin een aanpassing op de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) wordt voorgesteld. Het wetsvoorstel omvat een omvangrijke en ingrijpende uitbreiding van bevoegdheden van de inlichtingendiensten. Een greep:

- Onbeperkte toegang tot communicatie, gegevens, bestanden, databases, versleutelde berichten; niet alleen van Nederlandse burgers en bedrijven; maar ook, in de wetenschap van het internationale karakter van de Nederlandse online economie, van elke buitenlands bedrijf en buitenlandse gebruiker van Nederlandse online diensten en digitale infrastructuur
- Ongericht mogen tappen en afluisteren om (persoons)gegevens te vergaren (‘interceptie in bulk’), op elke mogelijke verbinding, ook internationale verbindingen die door miljoenen gebruikers en bedrijven worden benut
- Mogen inbreken in elk gecomputeriseerd apparaat, in de ruimste zin van het woord, ook die van onschuldige bedrijven en consumenten, om zich via die apparaten toegang te verschaffen tot gewenste informatie
- Jarenlang mogen bewaren en (her)gebruiken van de verzamelde (persoons)gegevens
- Kunnen afdwingen van ontsleuteling van berichten, bestanden, communicatie; zelfs door personen die zelf geen verzender of ontvanger van die de communicatie zijn
- Kunnen afdwingen van het faciliteren van afluisteren en aftappen, bij elk bedrijf en elke organisatie die ook maar iets op het gebied van communicatie organiseert of levert
- Achteraf kunnen doorzoeken van bestanden die voor heel andere doeleinden zijn aangelegd.
- Vrijelijk kunnen delen van vergaarde informatie met andere landen

[1] Deloitte 2013: NL Digitale Infrastructure, our third mainport

Stichting Digitale Infrastructuur Nederland
Overgoo 13 / Postbus 262
2260 AG Leidschendam

T: +31707621070
E: info@dinl.nl

Volgens DINL heeft het wetsvoorstel in huidige vorm de volgende ingrijpende consequenties:

- De sector digitale Infrastructuur, Nederlands derde mainport: een ecosysteem van honderden bedrijven die aan de basis staan van de digitale economie, wordt door de maatregelen hard geraakt. Dat verstoort de hefboomwerking van deze industrie voor de economie. Net als bij de andere mainports: Schiphol en de Rotterdamse haven, werken de negatieve effecten sterk door in de gehele economie.
- Het kabinet schiet zich met deze maatregelen in de voet. Ze schaden het vertrouwen in het imago van de Nederland als een land dat de privacy en de vertrouwelijkheid van gegevens beschermt. Het gevolg is dat de sterke positie van Nederland als Digital Gateway naar Europa[2], de ideale vestigingsplaats voor datacenters, internationale online bedrijven en de basis voor innovatie, wordt geschaad.
- Burgers zullen zich bespied voelen door de overheid en minder vrij en onbevangen in hun hun online activiteiten. Ook dit remt het gebruik van online diensten en daarmee de ontwikkeling van de digitale- en kenniseconomie.
- Door de gehanteerde definitie “aanbieder van openbare communicatie” zullen tienduizenden bedrijven en organisaties die iets doen aan digitale communicatie, klein en groot, moeten meewerken aan het beschikbaar maken van hun bestanden en databases. Ook dienen zij afluisteren en tappen te faciliteren en de significante investeringen en kosten hiervoor zelf op te brengen.
- Het voorstel werpt een forse drempel op voor startups. Deze zullen hun toevlucht zoeken in landen waar zulke verplichtingen niet bestaan.
- Door het ontbreken van degelijk toezicht en controle zullen ongewenste en potentieel onrechtmatige activiteiten van de inlichtingendiensten zich nog meer aan het zicht van de samenleving kunnen onttrekken.

Het verder vergroten van reikwijdte van definities en bevoegdheden wekt de sterke indruk dat niet het verkrijgen van inlichtingen over verdachte personen of organisaties, maar het vergaren van bulk data een doel op zich is geworden. Bij het zoeken naar de speld in de hooiberg is blijkbaar de gedachte dat eerst nog meer hooibergen gecreerd moeten worden.
In de wetenschap dat toekomstige economische groei voor een groot deel afkomstig zal zijn uit de online economie, komt het plan om de bevoegdheden zonder fatsoenlijke risicoanalyse en onderbouwing zo sterk uit te breiden neer op het onverantwoordelijk gokken met de economische toekomst van Nederland.

Naar het oordeel van DINL bestaan vijf fundamentele problemen met het wetsvoorstel en deze disproportionele uitbreiding van bevoegdheden.

1. Noch noodzaak, noch effectiviteit van de ruime bevoegdheden is, in het licht van de grote gevolgen en impact, onderbouwd.
2. Er is geen analyse van- en onderzoek gedaan naar het risico en de effecten van zulke maatregelen op de digitale- en daarmee de gehele economie.
3. De sterk verouderde definities en omschrijvingen van bedrijven en hun activiteiten laten zien dat de minister geen kaas heeft gegeten van de complexe structuur van de digitale

[2] Zie digitalgateway.eu

economie. De verschillende activiteiten in de online wereld kunnen niet zomaar over een kam worden geschoren. Het creëert een onwerkbare inconsistentie in het domein van wet- en regelgeving en een conflict met de ontwikkelingen bij andere ministeries. Het leidt tot nieuwe verplichtingen, lastendruk en daarmee uitvoerbaarheidsproblemen hoge kosten voor veelal kleine, innovatieve bedrijven. De proportionaliteitstoets wordt blijkbaar omzeild door de lasten bij voorbaat eenzijdig bij bedrijven te leggen.

4. De overheid treedt de eigen principes: de publiek-private samenwerking, multi-stakeholder aanpak en de principes van een vrij, veilig en open Internet met voeten.
5. Het toezicht en controle op het gebruik van de vergaarde data en een juiste toepassing van de bevoegdheden zijn onvoldoende geborgd en georganiseerd. Op geen enkele wijze wordt inzichtelijk gemaakt hoe de enorme verzamelingen van persoonsgegevens zullen worden beveiligd tegen onrechtmatig en ongeautoriseerd gebruik, gebruik anders dan het oorspronkelijke doel, hoe de privacy van burgers wordt beschermd en hoe het vrijelijk delen van informatie met andere landen aan banden wordt gelegd.

In de appendix licht DINL deze vijf issues nader toe. Tegelijkertijd herkent en erkent DINL de noodzaak van goed functionerende inlichtingendiensten en heeft begrip voor de noodzaak van verbetering en modernisering.

DINL stelt voor om werk te maken van de volgende zaken:

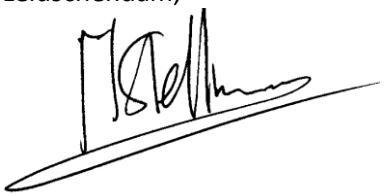
- Pas de eigen uitgangspunten en richtlijnen voor beleidsafwegingen op een juiste en complete manier toe[3]
- Onderbouw bevoegdheden op basis van degelijk onderzoek naar nut, noodzaak en effectiviteit.
- Doe eerst een degelijke economische impact analyse: breng de effecten van vertrouwen en de rol en activiteiten van veiligheidsdiensten op het vestigingsklimaat en economie in beeld.
- Schrap de mogelijkheid van exploiteren van kwetsbaarheden in computers, apparatuur van personen of bedrijven die part noch deel hebben aan verdenkingen
- Schrap de verplichting tot medewerking aan ontsleuteling door personen die niet zelf bij de communicatie betrokken zijn
- Maak vaart, samen met de ministers van EZ en Justitie met de aanscherping van definities zodat de risico's en impact (van de bevoegdheden) op specifieke en essentiële delen van de digitale samenleving beter in kaart kunnen worden gebracht.
- Benoem op basis van de hiervoor genoemde verbeterde definities de zones (m.b.t. risico's voor economie, vertrouwen en imago), waarvoor additionele onderbouwing voor bevoegdheden is vereist c.q. verklaar die tot no-go zones.
- Organiseer in lijn met de eigen kernwaarden van het Kabinet en samen met de collega's van Justitie, een betere afstemming met de telecomsector en de sector digitale infrastructuur; sectoren die door deze maatregelen zwaar worden geraakt. Zorg dat er een voorstel komt dat door overheid én bedrijven kan worden gedragen.
- Regel een fatsoenlijke vergoeding van de door bedrijven te maken kosten voor uitvoering

[3] https://www.kcwj.nl/kennisbank/integraal-afwegingskader-beleid-en-regelgeving

- Geef garanties dat door diensten gevonden kwetsbaarheden onverwijld aan het NCSC de en Abuse-HUB worden gemeld
- Organiseer toezicht en controle conform de door het IVIR ontworpen principes[4] .

DINL is te allen tijde bereid om hierover met u in gesprek te gaan.

Leidschendam,



Namens het DINL bestuur
M. Steltman Directeur DINL

Het bestuur van DINL
J.W. Des Tombes – Voorzitter en CEO IS Group
J Witteman CEO AMS-IX
R Meijer CEO SIDN
G. van Leeuwen Directeur Amsio
M. Eielts CEO Equinix NL
M. Gauw Directeur NlNet
E. Bleumink Directeur Surfnet

[4] http://www.ivir.nl/nieuws/tenstandards

Stichting Digitale
Infrastructuur Nederland

Appendix A: Toelichting DINL op de fundamentele problemen in het wetsvoorstel WIV juni 2015

Inleiding

De Nederlandse digitale infrastructuur, Nederlands derde mainport[5], vormt het hart van de Nederlandse online economie[6] en heeft een sleutelrol in het wereldwijde internet. De stichting DINL is de vertegenwoordiger en spreekbuis van aanbieders van die digitale infrastructuur. Deelnemers van DINL zijn AMS-IX (Amsterdam Internet Exchange), DDA (Dutch Datacenter Association), DHPA (Dutch Hosting Provider Association), ISPConnect, Stichting NlNet, SIDN (Stichting Internet Domeinregistratie Nederland) en SURFnet. DINL zet zich in voor een vrij, open en veilig Internet als basis voor economische groei, voor de kansen van Nederland als digitale gateway naar Europa[7] en vestigingsplaats voor datacenters, online bedrijven, innovatie en economische groei[8], voor de IT van morgen en voor de kennismaatschappij als geheel.

DINL maakt zich grote zorgen om de gevolgen van het 2 juli jongstleden ter consultatie gepubliceerde Kabinetsvoorstel waarin een aanpassing op de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) wordt voorgesteld. De in het voorstel geformuleerde nieuwe bijzondere bevoegdheden hebben impact op alle gebruikers en aanbieders van diensten die in de Nederlandse digitale economie. Het gaat niet alleen om Nederlandse maar ook om de buitenlandse gebruikers en bedrijven die hun data hebben toevertrouwd aan die Nederlandse aanbieders, dan wel hun data via die Nederlandse infrastructuur transporteren.
Het ingrijpende effect op de persoonlijke levenssfeer van burgers en de ongelimiteerde toegang tot gevoelige informatie van bedrijven, die het gevolg is van de verruiming van bevoegdheden in het wetsvoorstel, brengen ernstige schade toe aan het vertrouwen in Nederland als veilige haven voor online data en toepassingen. Het vermindert het animo van burgers en bedrijven om zaken te doen op het Internet en maakt Nederland een minder aantrekkelijke vestigingsplaats voor datacenters, aanbieders van online diensten en voor startups. Daarmee brengt dit voorstel wat DINL betreft onaanvaardbare risico's met zich mee voor de digitale economie, voor innovatie en daarmee voor de Nederlandse economie als geheel.

Het wetsvoorstel Wiv is door de minister in eerste instantie gepresenteerd als een technische aanpassing. Aanleiding van de modernisering van de bestaande wetgeving was de wens van de inlichtingen-en veiligheidsdiensten om technische beperkingen weg te nemen die te maken hebben met veranderingen in communicatievormen en daarbij gebruikte apparatuur en faciliterende infrastructuur. Genoemd worden de ruimere mogelijkheid voor het aftappen van kabels en het afluisteren van Voice over IP (Internet bellen). De minister illustreerde dit in het AO eerder dit jaar (februari 2015), door de situatie te schetsen waarin een jihadist telefoneert via het Internet. Op zich een plausibele probleemstelling.

---

[5] Deloitte 2013: NL Digital Infrastructure, our third mainport
[6] Deloitte 2014: NL Digital Infrastructure: driver for the online ecosystem
[7] Rijksoverheid.nl: strategisch aanvalsplan Nethelands Digital Gateway to Europe
[8] Rijksoverheid.nl: Digitale agenda ICT voor innovatie en economische groei

Stichting Digitale Infrastructuur Nederland
Overgoo 13 / Postbus 262
2260 AG Leidschendam

T: +31707621070
E: info@dinl.nl

Het wetsvoorstel laat echter een heel ander verhaal zien. Het voorziet in een zeer omvangrijke uitbreiding van de bevoegdheden van de diensten, die veel verder gaan dan het adresseren van de genoemde rol van technologie. De nieuwe bevoegdheden doen sterk denken aan hetgeen naar buiten kwam tijdens de onthullingen over het afluistergedrag van de NSA. Ook Nederland lijkt ten prooi gevallen aan de ongebreidelde verzamel- en afluisterwoede van de geheime diensten en de veronderstelling dat die verzameldrift ons veiligheid brengt.

DINL ziet vijf fundamentele problemen van het wetsvoorstel. Deze worden in de volgende secties nader toegelicht.

1 Nut, noodzaak en effectiviteit

Voor de omvangrijke uitbreiding van zijn bevoegdheden in de digitale wereld draagt de minister nauwelijks onderbouwing aan. Noch voor de noodzaak, noch voor de effectiviteit van de (extra) bevoegdheden, noch hoe deze zich verhoudt tot de bestaande bijzondere bevoegdheden van de diensten. Ook de Commissie van Toezicht op de Inlichtingen- en veiligheidsdiensten (CTIVD) stelt in haar jaarverslag 2014-2015[9] dat nauwelijks discussie plaatsvindt over de uitbreiding van bevoegdheden en dat deze niet wordt onderbouwd.
Dit alles wekt de sterke indruk dat in de afgelopen jaren geen degelijk onderzoek is gedaan naar de werkzaamheid van die bijzondere bevoegdheden. Voor ingrijpende zaken zoals het ongericht vergaren en doorzoeken van persoonsgegevens, het mogen inbreken op computers van onschuldigen en het afdwingen van medewerking door bedrijven mag toch worden verlangd dat die met meer dan anekdoten of causale redeneringen wordt onderbouwd. Het is te kort door de bocht om de diensten en de minister op hun woord te geloven.

Dat het hier daadwerkelijk gaat om het ongericht vergaren van persoonsgegevens, (i.e. gegevens die kunnen worden herleid naar een natuurlijk persoon) en andere data van alle burgers en bedrijven die gebruik maken van internet en digitale infrastructuur in Nederland, illustreert DINL bij deze met een uitleg van de werking van die infrastructuur.

> In de Informatiemaatschappij gebruiken burgers en bedrijven allerlei communicatie-middelen en –methoden. Denk aan mailen, bellen, sms, skype, whatsapp, facebook, chatten; maar ook navigeren, belastingaangifte doen, betalen, winkelen en bankieren zijn vormen van communicatie. Ze laten daarbij digitale sporen na – de zogenaamde metagegevens, die enige tijd opgeslagen blijven bij aanbieders om hun gebruikers te kunnen factureren en in sommige gevallen om aan andere wettelijke verplichtingen te kunnen voldoen.
> Dat communiceren door Burgers is overigens geen vrije keuze, het is ook de overheid zelf die haar burgers steeds meer verplicht om langs digitale weg met hen te communiceren.
> Steeds meer organisaties bieden communicatiediensten aan. Wat te denken van een

[9] Jaarverslag CITVD 2014-2015

sportvereniging die mailboxen inricht voor haar bestuursleden, of een startup die haar klanten laat communiceren via chat.
Al die communicatie vindt plaats over gedeelde verbindingen en met gedeelde apparatuur. Via kabels, computers en datacenters, via ISP's, internet exchange points en aanbieders van internationale communicatie via kabels en glasvezels. De gebruikers en bedrijven zijn niet slechts Nederlandse bedrijven. Nederland is een knooppunt van honderden internationale internet verbindingen; tienduizenden internationale bedrijven en tientallen miljoenen gebruikers maken impliciet gebruik van die digitale infrastructuur.
Het wetsvoorstel geeft de inlichtingendiensten - i.e. de overheid- de mogelijkheid om al die communicatie af te luisteren, de vergaarde data en persoonsgegevens op te slaan en te verwerken, om in te breken in alle daarbij betrokken apparatuur en al die informatie in te zien. Dat gaat ook om apparatuur, data en communicatie van bedrijven of personen, Nederlands of niet, die niets met het directe onderzoeksdoel te maken hebben. De inlichtingendiensten doen dat niet zelf. Ze kunnen een bedrijf dat communicatiediensten "levert" verplichten om een "tap" te plaatsen, dan wel ze opdragen hen rechtstreeks van informatie te voorzien. De kosten voor het tappen, dat betreft de aanschaf van dure apparatuur en de kosten van de tap zelf, moeten door die bedrijven bedrijf zelf worden gedragen.
Het effect is dat zodra een inlichtingendienst of een bedrijf op hun aanwijzing een stekker in een netwerk apparaat steekt, de diensten direct al het internetverkeer "zien" en daarmee dus alle data en persoonsgegevens van honderden, duizenden, of zelfs miljoenen gebruikers tegelijk kunnen opvangen. Vaak wordt eerst de vergaarde communicatie volledig opgeslagen en op een later tijdstip wordt de relevante data er alsnog uit gevist. De vergaarde data kan op een later tijdstip worden doorzocht - mocht zich later een andere aanleiding of gelegenheid voordoen, of worden overgedragen aan andere inlichtingendiensten.

Met deze forse ingrepen op de levenssfeer van burgers in het achterhoofd, in de wetenschap dat bedrijven op flinke kosten worden gejaagd en dat elke burger een potentieel onderzoeksobject wordt, is het van groot maatschappelijk belang dat de vraag wordt gesteld waar dit alles goed voor is. Hoe precies zal een verdere verruiming van bevoegdheden bijdragen aan de veiligheid van Nederland? Moeten burger en het bedrijfsleven werkelijk zo'n hoge prijs betalen voor die vermeende veiligheid? Waartoe leiden al die bevoegdheden en die enorme bergen informatie nu echt? En is dit alles waard om mogelijk de economische toekomst van Nederland op het spel te zetten?
Men zoekt een speld in een hooiberg, maar creëert de facto eerst meer hooibergen. Het is allemaal niet onderzocht en onderzoek elders trekt wel degelijk de effectiviteit in twijfel[10].

10 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

> *Pg 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.'*

Het blijft ook in Nederland bij niet te verifiëren anekdotes. Dit is op zich al eigenaardig. Als het tappen en afluisteren werkelijk tot grote successen hebben geleid, dan heeft de minister toch een belang om dat te onderbouwen. Het ontbreken van de onderbouwing versterkt de twijfel aan de effectiviteit. Recente incidenten doen ook het ergste vermoeden: ze tonen aan dat eerder een goede internationale samenwerking dan het vergaren van nog veel meer informatie preventief had kunnen werken. "De veiligheidsdiensten in Frankrijk hadden meneer X op het oog, Nederland en België wisten daar echter niets van"

2 Economische effecten

De onthullingen door Edward Snowden met betrekking tot de activiteiten van een NSA zouden ons, het kabinet incluis, nog vers in het geheugen moeten liggen. Belangen en privacy werden verkwanseld bij de ongebreidelde verzamelwoede van de Amerikaanse inlichtingendiensten. Volkomen onschuldige burgers werden het slachtoffer van algoritmen [11] die hun gedrag aanmerkten als verdacht en werden slachtoffer van ingrijpen en arrestaties. De vele false positives en de onmogelijkheid hun records te wissen maken het voor honderden personen nog steeds lastig of zelfs onmogelijk om überhaupt te kunnen reizen. Een bekend geval is de popartiest Cat Stevens. Het NSA verhaal is in de ogen van de Nederlandse burger het meest afschrikwekkende voorbeeld van een 'Big Brother' scenario. De overheid die alle burgers bespiedt en vrijwel alles mag en kan, en de effecten op onschuldigen afdoet als collateral damage.

In de VS is het effect van de NSA bevoegdheden en de onthullingen hierover onderzocht door de ITIF [12]. Daaruit bleek dat veel Amerikaanse bedrijven oplossingen hebben gezocht voor het opslaan van hun data en die van hun klanten, door datacenter, hosting en cloud providers te kiezen in landen met minder verregaande bevoegdheden. Daar heeft onder andere Nederland van geprofiteerd doordat Amerikaanse bedrijven zaken zijn gaan doen met Nederlandse hosting- en cloud-bedrijven en daarmee hun data hier bewaren. Ze wilden verschoond blijven van de verregaande bevoegdheden en ingrepen van de NSA. De economische schade die het gevolg was van dat beschadigde vertrouwen bedroeg volgens de ITIF maar liefst 25 tot 35 miljard dollar aan gederfde inkomsten voor Amerikaanse bedrijven die wel waren onderworpen aan de bevoegdheden van de NSA.

Er wordt gesuggereerd dat de situatie in Nederland onvergelijkbaar is, dat Nederland de privacy van haar burgers goed beschermt, en dat het hier niet zo'n vaart zal lopen. Dat is naïef. Want er

[11] http://www.nrc.nl/nieuws/2013/08/02/waarom-je-nooit-zomaar-snelkookpan-en-rugzak-kan-googlen
[12] "How Much Will PRISM Cost the U.S. Cloud Computing Industry? "http://www2.itif.org/2013-cloud-computing-costs.pdf

is per saldo maar weinig verschil met de bevoegdheden die de Nederlandse diensten met dit voorstel ter beschikking krijgen, ten opzichte van die van de NSA.
In de afgelopen jaren hebben toonaangevend digitale merken als Google, Microsoft, Facebook, Twitter, Spotify, Netflix en vele anderen Nederland als de thuisbasis gekozen voor hun Europese activiteiten. De digitale economie heeft een omvang van 5,6% van het BNP en is zo'n beetje de enige sector die forse economische groei laat zien.
Het NFIA[13] (Netherlands Foreign Investment Agency van MinEZ) onderzocht de factoren die bijdragen aan de keuze voor Nederland als vestigingsplaats voor zulke digitale diensten. Het vertrouwen in de bescherming van privacy door de overheid is daarbij als factor genoemd. Belangrijk te noemen in dat kader is dat voor een optimaal vestigingsklimaat voor buitenlandse bedrijven aan alle voorwaarden voldaan moet zijn. Neem een voorwaarde weg en het vestigingsklimaat leidt direct schade.

Het is belangrijk om ons te realiseren hoe de economische hefboomwerking van bedrijven in de sector digitale infrastructuur werkt. Dat werkt net als bij de Rotterdamse haven of bij Schiphol. Een datacenter, hosting- of cloud bedrijf faciliteert duizenden, soms honderdduizenden sites. Internet knooppunten in Nederland faciliteren communicatie van honderden miljoenen gebruikers. Daar zitten ook de huidige en toekomstige Ubers en Netflixes bij. Het wegvallen van vertrouwen in de Nederlandse digitale infrastructuur leidt ertoe dat zelfs bij een klein percentuele afname, Nederland enorme aantallen sites en toepassingen mist omdat de bedrijven die ze exploiteren hun sites zullen verplaatsen naar een ander land, en misschien zich daar dan ook vestigen.
Vertrouwen komt, als bekend, te voet en gaat te paard, zo leert ons het Amerikaanse scenario. Lichtzinnige besluiten kunnen de sterke positie van Nederland als Digital Gateway gemakkelijk schaden. In het licht van de bevindingen van de ITIF , NFIA en het voorgaande is het zeer aannemelijk om te veronderstellen dat ook de Nederlandse bedrijven in de digitale infrastructuur, en dus de digitale economie schade zal ondervinden van de enorme uitbreiding van bevoegdheden van de inlichtingendiensten.
Het schrikbeeld is dat grote internationale afnemers de Nederlandse aanbieders van digitale infrastructuur en dus Nederland als vestigingsplaats, zullen mijden. Ze zullen, net als destijds in Amerika, hun toevlucht zoeken in landen die de privacy van hun klanten en gebruikers wel willen beschermen tegen het graaigedrag van de overheid.
Tijdens een recente handelsmissie naar San Diego werd in gesprekken met buitenlandse investeerders en potentiele afnemers de vraag naar de plannen van de Nederlandse overheid op het gebied van privacy en de inlichtingendiensten veelvuldig gesteld. Dit is een heldere illustratie van het gegeven dat deze kwesties en materie top of mind is bij menig bestuurder en ondernemer.

Kortom, er zijn meer dan voldoende redenen om aan te nemen dat significant risico bestaat dat uitvoering van het wetsvoorstel in huidige vorm schade zal berokkenen aan de digitale economie. Net als bij de Rotterdamse haven of bij Schiphol zal het afnemen van de activiteit een flinke uitstraling hebben op de bedrijven die daar hun activiteiten op baseren. Het zal de

[13] http://investinholland.com/infrastructure/broadband/ en http://www.nfia.nl

positie van Nederland als digitale gateway en daarmee als digitale innovator ondermijnen. Dat is een onaanvaardbaar risico voor de economische toekomst van Nederland.

Een ander, direct gevolg van het voorstel betreft de economische schade aan kleine bedrijven door het opleggen van de verplichting om taps te faciliteren. Elk bedrijf dat communicatiefaciliteiten aanlevert of organiseert, zal op verzoek van een inlichtingendienst moeten meewerken. Conform de definitie zou het om maar liefst 360.000 bedrijven kunnen gaan, omdat elk bedrijf, stichting of vereniging wel iets aan communicatie faciliteert. De investeringen in apparatuur bedragen gemakkelijk tienduizenden euro's en de kosten per tap lopen al snel in de honderden tot duizenden euro's. Die kosten zullen niet door de overheid worden vergoed. Het gaat daarbij vooral om MKB bedrijven, de door het kabinet steeds bewierookte ruggengraat van innovatie[14] en toekomstige economische groei. Het is een onaanvaardbare lastenverzwaring voor bedrijven.
Door niet over vergoedingen en kosten te spreken, laadt de minister ook de verdenking op zich dat hij de proportionaliteitstoets omzeilt. Immers, indien substantiële kosten voor de overheid zijn gemoeid met de uitvoering zal zij moeten afwegen[15] hoe de kosten tegen de baten opwegen.

In dat licht moeten we ons ernstig afvragen of de vermeende, niet onderbouwde verbetering van de veiligheid in Nederland zodanig is, en zoveel waarde heeft, dat we bereid zijn onze economische toekomst hiervoor in de waagschaal te stellen door vertrouwen te schaden, het MKB en innovatieve bedrijven op hoge kosten te jagen en buitenlandse bedrijven te ontmoedigen om hier zaken te doen of zich hier te vestigen. Er is een niet denkbeeldige kans dat de overheid zo de spreekwoordelijke kip met de gouden eieren aan het slachten is.

Naar de stellige overtuiging van DINL vereist een voorstel als dit een gedegen onderbouwing en onderzoek. Een onderzoek vooraf naar noodzaak, effectiviteit, maar ook naar de economische effecten op het vertrouwen en op de kleine ondernemingen, mag beslist niet achterwege blijven. De overheid zal voor elk van de bevoegdheden eerst klip en klaar moet aantonen dat het echt niet anders kan en dat een dergelijk ingrijpen zonder economische gevolgen zal blijven. Tevens zal de overheid de bedrijven die het treft fatsoenlijk moeten compenseren voor hun investeringen en inspanningen.

3 Verruiming van begrippen

Langzaam maar zeker beseft ook de overheid dat de digitale economie meer omvat dan een willekeurige verzameling van computers en de verbindingen daartussen. Er is sprake van een gelaagdheid in de technologie, een specifieke inrichting van besturing en regie en er ontstaan tal van sociaaleconomische structuren die gebaseerd zijn op het internet en de digitale online economie. Sommige wetgevingstrajecten houden al rekening met die gelaagde indeling van het internet, diensten en het gebruik. Ter illustratie: Netneutraliteit adresseert het verschil tussen

[14] http://www.startupdelta.org
[15] http://www.minbuza.nl/binaries/content/assets/ecer/ecer/import/icer/handleidingen/2009/icerleidraadeu-hoofdstuk3.pdf

toegang tot het internet en de daarover geleverde diensten. Het ministerie van EZ hanteert een model voor het online waardeweb waarin de verschillende rollen zoals toegang, toepassingen, transport en datacenters worden onderscheiden. Ook in Europees verband wordt nagedacht over nieuwe begrippen en wordt duidelijk dat niet alles over 1 kam kan worden geschoren. De Europese e-commerce richtlijn onderscheidt partijen op basis van “mere conduit”, het faciliteren van content.
Van belang is ook het recent verschenen rapport van het WRR, dat onomwonden stelt dat het publieke internet een internationaal, beschermd goed is dat door overheden moet worden ontzien, net als andere infrastructuur. Want die bescherming en het vertrouwen in het functioneren en de veiligheid zijn essentieel voor economische groei .
Ook DINL staat voor het belang van een vrij, open en veilig internet als de basis van economische groei en de kenniseconomie van morgen. Vrij, open en veilig betekent ook: vrij van overheidsingrepen in besturing en vrij van het beschadigen van de integriteit en vertrouwelijkheid van dat Internet. Dus vrij van ingrepen door justitie of inlichtingendiensten. Dit standpunt werd door de minister president met verve uitgedragen tijdens de opening van de wereldwijde conferentie over cyberspace, de GCCS2015, in maart J.L. in Den Haag. Nederland wierp zich op als de voorstander en hét grote voorbeeld hoe de wereld met vrijheid en veiligheid van internet en cyberspace om dient te gaan.

Zo is niet het geval bij het ministerie van BZK, zoals uit het wetsvoorstel blijkt. Het komt haar blijkbaar erg goed uit om die gelaagdheid, structuur en discussie over vrijheid en veiligheid compleet te negeren door de gehele digitale economie over één kam te scheren. In het wetsvoorstel wordt slechts gesproken over “geautomatiseerde werken” : alle soorten van digitale apparaten in de breedst mogelijke zin, en over “aanbieders van openbare communicatie”: dat is elk bedrijf of organisatie dat aan het publiek diensten aanbiedt of organiseert waarmee kan worden gecommuniceerd. Geen woord over internet of een onderverdeling van rollen en typen van gebruik. Het omvat dus per saldo de gehele digitale economie. Van ISPs, banken en zorgverzekeraars, van mobiele telefoons, routers en internet verbindingen, online pacemakers en koelkasten, de computers in kerncentrales, google autos, internet verbindingen, de door de sportvereniging aangeboden email, tot en met de miljoenen servers in Nederlandse datacenters.
Zo’n verbreding en verruiming van de “scope” van de maatregelen is uiteraard disproportioneel, onacceptabel en ongewenst. Het is volstrekt duidelijk dat in de digitale economie gebieden zijn die speciale bescherming en status vereisen. Een mobiele telefoon van een Syriëganger is nog wel iets anders dan een functie die essentieel is voor het functioneren van het gehele internet, of een kabelverbinding die door miljoenen binnenlandse en buitenlandse burgers en bedrijven worden gebruikt.
Het recente AO[16] over dit onderwerp illustreerde de lacunes in het gebruik van passende definities, kaders en terminologie toen de minister zich haastte te zeggen “dat uiteraard niet de hele AMS- IX zal worden afgetapt”. Maar het wetsvoorstel maakt dit wel degelijk mogelijk en moeten we de minister dan geloven dat het ‘uiteraard’ niet gaat gebeuren, en dat de minister onder de politieke druk van een actualiteit de verleiding om die snoepwinkel te gaan grutten kan weerstaan?

[16] http://www.volkskrant.nl/dossier-kabinet-rutte-ii/kabinet-verder-met-plan-voor-aftappen-kabel~a3848693/

DINL stelt dat het wetsvoorstel niet kan passeren zonder een veel scherpere afbakening van de gebieden waar de diensten wél en niet mogen komen. In concreto: De minister dient zich aan te sluiten bij de ontwikkelingen binnen het ministerie van EZ en niet op eigen houtje eigen definities aan te passen en te verbreden. Hij dient zich voorts rekenschap te geven van het WRR rapport en het bestaan van de daarin beschreven digitale infrastructuur, i.e. de publieke kern van het internet en die te definiëren zoals het internet werkelijk functioneert. Vervolgens dient hij het voorstel zo aan te passen dat de beschermde gebieden worden ontzien.

4 Waar is de multi-stakeholder aanpak?

Nederland is dé promotor van het zogenaamde multi stakeholder model. Op de recente wereldwijde conferentie over cyberspace, de GCCS2015, werden die aanpak en de privaat publieke samenwerking in Nederland door Minister Koenders gepresenteerd als hét grote voorbeeld voor de wereld.
Het succes en groei van het internet worden grotendeels verklaard doordat geen enkel groot bedrijf of overheid “de baas” is over dat internet. Het vrije en open karakter maakt het een platform voor activiteiten van allerlei aard en voor de economische groei van morgen. Het eerder genoemde WRR rapport beschrijft het model in detail.
Ook bij de aanpak van ongewenste fenomenen in cyberspace blijken de multi stakeholder benadering en PPS (privaat-publieke samenwerking) instrumenteel. Het kan ook niet anders: slechts de betrokken bedrijven en organisaties zelf begrijpen de technologie en kunnen veiligheid en beschikbaarheid garanderen. Voor maatregelen zoals het offline brengen van content of het opvragen van informatie over bij concrete verdenkingen is het handelen en medewerking van organisaties in de digitale infrastructuur nodig. Niemand wil dat de overheid zelf aan de knoppen zit. Een voorbeeld van een succesvolle multi stakeholder samenwerking in Nederland is de bescherming van de samenleving tegen cybercrime. We noemen de gedragscode Notice and Take Down, het barrièremodel, de gezamenlijke bestrijding van botnets, diverse overleg organen rond bestrijding van fraude, de samenwerking met het meldpunt Kinderporno, de samenwerking met gespecialiseerde diensten van politie bij concrete cases, het NCSC. En zo zijn er meer.
Een consequentie van zo’n model is dat de overheid rekening moet houden met de belangen van alle stakeholders, niet slechts die van de overheid of van een individueel ministerie of dienst.

Het met de mond belijden van de multi stakeholder aanpak valt dan ook niet te rijmen met de eenzijdige aanpak die geschetst wordt in de beoogde nieuwe Wiv. Op geen enkele manier wordt rekening gehouden met de belangen van de betrokken bedrijven en stakeholders. Erger, ze worden met voeten getreden. De diensten eigenen zich de mogelijkheid toe om zelf aan de knoppen te zitten (het mogen inbreken in apparaten en computers). De betrokken faciliterende bedrijven worden gedwongen op eigen kosten mee te werken aan afluister- en aftappraktijken en hun medewerkers lopen het risico te worden gedwongen om mee te werken aan ontsleuteling van bestanden of berichten. Dat is een aanpak die beslist niet past in het uitgedragen beleid van minister Koenders, maar eerder past bij de landen met een eenzijdig en repressief beleid met betrekking tot het Internet. “You can’t have it both ways”: enerzijds multi-stakeholder bepleiten, anderzijds op een moment dat het blijkbaar even niet uitkomt een

eenzijdige aanpak kiezen in hetzelfde domein, is voor DINL een onbegaanbare weg, die een zorgvuldig opgebouwde samenwerking schaadt.

Om dit te illustreren schetsen wij een consequentie van de slechte afweging van belangen. Door het wetsvoorstel ontstaat een zorgelijke paradox met betrekking tot de informatieveiligheid en privacybescherming van bedrijven. De overheid verplicht bedrijven middels de WBP (wet bescherming persoonsgegevens) en de aanstaande Europese DPD (Data protectie directive) om al het mogelijke te doen de privacy van hun gebruikers te beschermen door het beveiligen van informatie en systemen tegen ongeautoriseerde toegang.
Echter, de inlichtingendiensten krijgen in het voorstel de mogelijkheid om kwetsbaarheden in willekeurige computers uit te nutten om toegang te krijgen tot informatie. Dat betekent dat inlichtingendiensten een belang hebben om kwetsbaarheden onder de pet te houden, zolang zij zelf de toegang nodig hebben.
Kwetsbaarheden in systemen worden echter niet slechts gebruikt door de “good guys”[17] en het feit dat de overheid kwetsbaarheden niet direct met het bedrijfsleven deelt verzwakt de informatieveiligheid van de gehele digitale economie. Het roept ook vragen op. Hoe wordt het een bedrijf beoordeeld dat gehackt blijkt, als later bekend wordt dat informatie over de uitgebuite kwetsbaarheid al wel bij de overheid bekend was? Zal er sprake zijn van een vrijwaring tegen boetes? Of hoe zal de samenleving oordelen als door een gehackte auto doden vallen, en blijkt dat de diensten al op de hoogte waren van het feit dat de door die hacker gebruikte kwetsbaarheid bestond, maar die hack zelf nog even nodig had?

De overheid moet het multi-stakeholder model serieus nemen. Dat betekent dat bedrijven niet slechts kunnen worden benoemd als objecten die gewoon moeten meewerken aan hetgeen de minister wil. De overheid moet serieus rekening houden met de belangen van bedrijven die verantwoordelijk zijn voor een belangrijke functie in de economie.
Met betrekking tot het genoemde voorbeeld zou de rol van de overheid dan ook moeten zijn dat de gevonden kwetsbaarheden onverwijld gedeeld worden en beschikbaar komen voor die bedrijven. Informatieveiligheid en privacy behoren vóór de informatiepositie van de diensten te gaan. Dit is voor DINL een fundamenteel en principieel uitgangspunt: safety first, en pas daarna security. Het wetsvoorstel gaat in elk geval compleet voorbij aan deze belangenafweging. Met de huidige, verkeerde keuzes zal onomkeerbare schade worden toegebracht aan Informatieveiligheid en privacy.

5 Toezicht en controle

De samenleving hecht grote waarde aan bescherming van privacy en de persoonlijke levenssfeer. Het is niet voor niets dat de overheid er van alles aan doet om die privacy in het digitale domein te beschermen. Er zijn op nationaal- en Europees niveau allerlei vormen van wetten, regels, verplichtingen en verantwoording, en zelfs boetes voor overtredingen ontstaan. De normen en richtlijnen voor informatiebeveiliging en toegang tot persoonsgegevens

[17] The vulnerabilities They discover affect the security of us all’, https://www.schneier.com/blog/archives/2014/05/disclosing_vs_h.html

omvatten zonder uitzondering maatregelen voor de inrichting van onafhankelijk toezicht en controle.
Zoniet als het gaat om data die door de inlichtingendiensten worden vergaard. De enige vorm van toezicht bestaat uit de instanties die door de minister zelf worden bestuurd, en de CITVD . Het argument is dat met de parlementaire controle het toezicht voldoende is geregeld. Dat is uiteraard een veel te gemakkelijke voorstelling van zaken. De CITVD heeft de mogelijkheid de minister te verzoeken een ander besluit te nemen, maar de minister kan dat naast zich neerleggen. Het is dan aan de fractievoorzitters om hierover een oordeel te vellen. En verder is de complexiteit van de uitvoering zo omvangrijk dat controle door commissieleden beslist niet voldoende is. Het is sowieso discutabel of het toezicht op een bevoegdheid waarmee privacy op zo'n grote schaal kan worden geschonden, en economische belangen kunnen worden geschaad, slechts in de handen van de politiek ligt.

DINL is dan ook van mening dat er voor toezicht en controle een betere organisatie kan en moet worden ingericht. Het IVIR heeft hiervoor een handzaam en goed uitgewerkt model ontwikkeld, gebaseerd op 10 principes.[18] DE Minister zou er goed aan doen dat voorstel ter harte te nemen en het toezicht op deze wijze te organiseren.

--

[18] http://www.ivir.nl/nieuws/tenstandards
Wat DINL betreft neemt het Kabinet de erin opgenomen aanbevelingen één op één over.