Reactie namens CAIW, KPN, de aanbieders verenigd in NLConnect, Tele2, T-Mobile, VodafoneZiggo

Zienswijze naar aanleiding van de consultatie
"Beleidsregel netwerkaansluitpunt"

februari 2018

INLEIDING

Op 13 december 2017 publiceerde het Ministerie van Economische Zaken en Klimaat de consultatie inzake de beleidsregel ten aanzien van het netwerkaansluitpunt. Graag maken de volgende aanbieders gebruik om te reageren op deze consultatie (hierna: **"de Aanbieders"**):

- CAIW;
- KPN;
- de aanbieders verenigd in NLConnect;
- Tele2;
- T-Mobile en
- VodafoneZiggo.

In aanvulling op deze gezamenlijke zienswijze hebben de Aanbieders voor zover relevant ook individuele zienswijzen ingediend.

Deze zienswijze is als volgt opgebouwd. Allereerst betogen de Aanbieders dat de probleemstelling, de oplossing en het effect van deze beleidswijziging onvoldoende onderzocht zijn. Vervolgens onderbouwen de Aanbieders dat de voorgestelde Beleidsregel geen verduidelijking, maar een wijziging van het wettelijk kader is en dat een beleidsregel daarvoor het verkeerde instrument is. Tot slot leggen de Aanbieders uit dat de beoogde Beleidsregel leidt tot ongewenste juridische en technische consequenties.

I. PROBLEEMANALYSE BELEIDSWIJZIGING ONVOLDOENDE

Bij een consultatie als de onderhavige – waarbij de overheid tracht een ontstane praktijk in de markt aan te passen – hoort een duidelijke probleemstelling en een gedegen onderzoek naar de opties en de gevolgen van het voorgestelde beleid. Ondanks dat de Beleidsregel in het najaar van 2016 al is aangekondigd, ontbreekt in deze consultatie elke afgewogen onderbouwing. En dat terwijl de Beleidsregel verregaande consequenties heeft voor alle Aanbieders.

Het Ministerie rechtvaardigt de beleidswijziging vanuit het realiseren van marktwerking voor modems en modem/router combinaties. Het Ministerie stelt in de toelichting: "*Fabrikanten van modem/router apparatuur zien een potentiële markt die door snelle innovatie in deze sector zal uitbreiden, mits zij betere toegang krijgen tot de telecomabonnee. EZK en ACM*

ontvangen signalen van consumenten die door hun telecomaanbieder beperkt worden in het aansluiten van eigen apparatuur. Deze gebruikersgroep wil de functionaliteit van deze apparatuur beter kunnen benutten, bijvoorbeeld om het eigen private netwerk te beheren of om het borgen van privacy in eigen hand te kunnen houden. De mogelijkheid van vrije modemkeuze kan, nog los van het aantal gebruikers dat hier gebruik van wil maken, ook een positieve invloed hebben op de kwaliteit/prijsverhouding van de apparatuur."

Het is goed dat het Ministerie signalen van eindgebruikers serieus neemt, maar het is in dat kader ook van belang dat het Ministerie zich bij het voorbereiden van deze beleidswijziging tevens zoveel mogelijk vergewist van de daadwerkelijke situatie. Dit voorkomt dat het Ministerie het effect van de Beleidsregel op de vrije keuze en de leveranciersmarkt overschat: er is al veel mogelijk[1] en het is niet zo dat de Beleidsregel enig merkbaar effect zal hebben op de internationale markt voor eindapparaten.
Reeds eerder hebben de Aanbieders het Ministerie gevraagd om het probleem dat met de Beleidsregel tracht te worden verholpen, en het effect van de voorgestelde 'oplossing' helder uiteen te zetten in de stukken van de consultatie. In dat kader verwijzen de Aanbieders naar bijlage 1. De Aanbieders hebben een dergelijke heldere uiteenzetting niet kunnen vernemen. Nergens blijkt dat het Ministerie op iets anders is afgegaan dan ‘signalen’ van een beperkt aantal partijen.

Ook blijkt niet dat het Ministerie in dit geval marktonderzoek heeft laten doen of technische expertise heeft gevraagd. Als dergelijke onderzoeken wel zijn gedaan, zouden de resultaten daarvan bij de consultatie dienen te zijn gepubliceerd. Zo is het onduidelijk waarom de prijs/kwaliteitverhouding van eindapparatuur als gevolg van de voorgenomen Beleidsregel significant zou verbeteren. Zelfs in Duitsland, waar de startsituatie was dat eindgebruikers veel minder keuzevrijheid hadden dan thans in Nederland, blijken eindgebruikers niet op grote schaal te kiezen voor alternatieve eindapparatuur. Sterker nog, er zijn aanwijzingen dat het aantal eindgebruikers dat hiervoor kiest juist weer terugloopt. De Aanbieders constateren dat er veel onvoldoende onderbouwde veronderstellingen ten grondslag liggen aan de voorgenomen Beleidsregel. Het is van belang dat adequaat zorg wordt besteed aan het scherp krijgen van zowel de probleemstelling, de oplossing en het effect van het beleid. Hoewel de Aanbieders verwachten dat de huidige consultatie een aanzet zal geven om te komen tot een scherpere onderbouwing, menen zij dat het op de weg van de overheid ligt om juist ook voorafgaand aan een dergelijke ingrijpend voornemen van beleidswijziging beter onderzoek te doen.

De Aanbieders merken voorts op dat er vanuit het Ministerie een diffuus beeld wordt geschetst van de implicaties van de Beleidsregel, terwijl Aanbieders het juist noodzakelijk achten dat de Beleidsregel eenduidig afbakent waar de grens ligt tussen het domein van de eindgebruiker en van de aanbieder. De toelichting bevat de volgende passage op pagina 5:
"*Een (radio)apparaat met een ingebouwde hardwarematige component (chip) met een voor een bepaald netwerk specifieke authenticatie/beveiligingsfunctie behoort evenals wanneer deze authenticatie/beveiligingsfunctie niet specifiek zou zijn voor een specifiek netwerk, dus niet tot een openbaar elektronisch communicatienetwerk. Dit geldt voor alle (radio)apparaten, direct of indirect aangesloten op bedrade of draadloze openbare netwerken, inclusief modems en modem/router combinaties.*"

[1] De meerderheid van de eindgebruikers kiest op basis van prijs, merkperceptie, aangeboden diensten als internet, telefonie en tv, toegevoegde waarde in de vorm van content- en additionele pakketten als beveiliging, cloud opslag en dergelijke. Een andere factoren die doorslaggevend kan zijn bij de keuze is de Wi-Fi performance van de door de aanbieder geleverde apparatuur. Een eindgebruiker kan het ook wenselijk achten dat de aanbieder het Wi-Fi signaal uitzet omdat zijzelf een eigen draadloos netwerk zonder verstoring wil aanwenden. De keuzemogelijkheden zijn daarmee al zeer ruim. Aan de modemkant wordt de keuze gedicteerd door de drager (glasvezel, xdsl, coax) en optimale operabiliteit tussen actieve componenten in het toegangsnetwerk en de actieve apparatuur op locatie van de eindgebruiker.

De Aanbieders bevelen aan dat eerst wordt onderzocht wat de gevolgen in de praktijk zijn als (radio)apparaten met een ingebouwde hardwarematige component (chip) met een voor een bepaald netwerk specifieke authentificatie/beveiligingsfunctie die niet specifiek is voor een bepaald netwerk niet worden gezien als onderdeel van het openbaar elektronisch communicatienetwerk. Daarbij dienen veiligheid, netwerkintegriteit en continuïteit en de reeds geldende regelgeving in ogenschouw te worden genomen.

Hoewel in de communicatie vanuit het Ministerie uitsluitend aandacht wordt besteed aan 'vrije modemkeuze', lijkt uit de (toelichting op) de Beleidsregel voort te vloeien dat aanbieders ook verplicht zouden worden om hun diensten over andere apparatuur van derden aan te bieden (zoals settopboxen voor TV). Dat is een nog veel verdergaande conclusie dan die in Duitsland is getrokken en heeft zo mogelijk nog grotere impact op de bestaande dienstverlening. Ook hier ontbreekt elke analyse van de gevolgen. Er is geen enkele reden of grondslag om aanbieders te verplichten ook apparatuur van derden voor specifieke 'gespecialiseerde' diensten al telefonie of IPTV te ondersteunen. Die apparatuur heeft vaak specifieke functies voor beveiliging, authenticatie of het doorgeven van auteursrechtelijk beschermde content en kan niet 'zomaar' worden losgemaakt van de aangeboden dienst (zie ook hierna).

Ook ten aanzien van ACM merken de Aanbieders op dat er accenten worden gelegd in de berichtgeving ten aanzien van de Beleidsregel die niet voor de hand liggen. ACM wekt in haar nieuwsbericht van 13 december 2017 de suggestie dat eindgebruikers als gevolg van het beleid meer grip op hun privacy zouden krijgen. ACM stelt: "*Als zij gebruik maken van een apparaat van een telecomaanbieder, liggen de klantgegevens bij die telecomaanbieder.*" Deze opmerking gaat er volledig aan voorbij dat telecomaanbieders aan zeer strikte wettelijke normen zijn onderworpen. Het is daarmee een gezochte motivering, die bovendien de onterechte suggestie wekt richting eindgebruikers dat de privacy bij aanbieders onvoldoende geborgd zou zijn. De Aanbieders zijn van mening dat hiermee een onjuist en schadelijk beeld wordt gecreëerd. Aanbieders denken dat eerder het tegendeel het geval kan zijn. Het toestaan van vrije keuze van apparatuur brengt juist veiligheidsrisico's met zich mee als eindgebruikers apparatuur gebruiken die ondeugdelijk is beveiligd of zelf instellingen aanpassen zonder zich van de gevolgen bewust te zijn. Aanbieders vinden het noodzakelijk – zeker gezien de recente ontwikkelingen op het gebied van DDoS aanvallen op banken – dat het Ministerie expliciet stil staat bij de risico's van deze beleidswijziging.

Proces voorafgaand aan de consultatie

Het tot op heden gevolgde proces toont aan dat de besluitvorming weinig zorgvuldig heeft plaatsgevonden. Hieronder is een uiteenzetting opgenomen van het proces voorafgaand aan de consultatie.

- Op 12 september 2016 werd tijdens het OPT overleg enigszins terloops aangegeven dat er een 'verduidelijking' komt in het dan nog niet gepubliceerde maar reeds eind 2016 in werking tredende Besluit eindapparaten die er op neer zou komen dat het netwerkaansluitpunt de passieve interface is.
- Na zorgen die vanuit de markt werden geuit over deze zeer fundamentele wijziging van het wettelijk kader en de grote impact hiervan op de sector, heeft informeel overleg plaatsgevonden tussen enkele aanbieders en vertegenwoordigers van het Ministerie.
- Naar aanleiding van dat overleg heeft het Ministerie besloten om in plaats van de 'verduidelijking' in het Besluit eindapparaten de definitie van het netwerkaansluitpunt vast te leggen in nog op te stellen beleidsregels. Aangegeven werd dat die consultatie alle gelegenheid zou geven om alle aspecten die een rol spelen bij een beleidswij-

ziging in te brengen en dat de overheid op basis van die resultaten pas een definitief standpunt zou innemen.

- Op 21 december 2016 werd het Besluit eindapparaten gepubliceerd. Aan dit besluit ging geen consultatie vooraf. Hoewel het netwerkaansluitpunt uiteindelijk niet is gedefinieerd in dit besluit, is dit besluit wel relevant voor de consultatie van de Beleidsregel. Dit besluit wekt de suggestie dat ook apparatuur die niet aan de technische specificaties voldoet aan een netwerkaansluitpunt mag worden aangesloten. De Aanbieders hebben aangegeven de punten te zullen aanreiken waarvan zij denken dat die in een consultatie ten aanzien van de definitie van het netwerkaansluitpunt in elk geval aan de orde moeten komen.
- Op 20 januari 2017 hebben de Aanbieders het uitgebreide overzicht met de aandachtspunten voor de consultatie toegezonden aan het Ministerie en ACM (opgenomen als bijlage 1). In dit document hebben Aanbieders de volgende opmerkingen gemaakt:
    - In de consultatie dient een heldere probleemanalyse te worden voorgelegd;
    - De juiste partijen dienen betrokken te worden en er moet gedetailleerd advies worden ingewonnen;
    - De reikwijdte van de Beleidsregel moet duidelijk worden vastgesteld;
    - Het is raadzaam om in de consultatie aandacht te besteden aan de verhouding met andere wet- en regelgeving;
    - De consultatie moet inzicht geven in de mate van standaardisatie van de betrokken diensten, netwerkaansluitpunten en randapparatuur;
    - Van Aanbieders kan niet verwacht worden dat zij dezelfde mate van kwaliteit kunnen leveren ten aanzien van klanten die kiezen voor eigen hardware;
    - Er moet duidelijkheid komen over wie er verantwoordelijk is in geval van storing of schade, nu eindgebruikers en leveranciers een grotere rol krijgen;
    - Ook moet er duidelijkheid zijn over het borgen van veiligheid en netwerkintegriteit;
    - Tot slot moet er een realistische overgangstermijn zijn, waarin aanbieders aan de verplichtingen moeten voldoen.
- Op 15 februari 2017 heeft het Ministerie een ronde tafel georganiseerd waarbij vertegenwoordigers van het Ministerie, ACM, leverancier AVM en verschillende telecomaanbieders aanwezig waren. Tijdens deze ronde tafel hebben telecomaanbieders gewezen op de aandachtspunten die het Ministerie zou moeten betrekken in zijn oordeelsvorming.
- Op 8 maart 2017 hebben de Aanbieders eveneens een uitgebreid juridische analyse toegezonden aan het Ministerie inzake het wettelijk kader (opgenomen als bijlage 2). Dit overzicht liet onder meer zien dat hetgeen het Ministerie beoogde geen 'verduidelijking' is van bestaande wet- en regelgeving, maar dat het een ingrijpende wijziging betreft, en dat het Europese Kader waar het Ministerie zich op baseert anders moet worden geïnterpreteerd.
- Gelet op de eerdergenoemde indicatie, verwachtten de Aanbieders dat ze door middel van de consultatie in staat zouden worden gesteld om alle aandachtspunten op een uitvoerige wijze onder de aandacht zouden kunnen brengen en dat het Ministerie pas na afloop van de consultatie een standpunt zou innemen.
- Op 13 december 2017 heeft het Ministerie de consultatie van de Beleidsregel gestart. Verbazend aan deze concept-Beleidsregel is dat deze op geen enkele manier blijk geeft van de discussies en de input die door partijen is gegeven in het hieraan voorafgaande jaar. De consultatie wordt gepresenteerd als een vaststaand beleid, wat nog wordt versterkt door het door het Ministerie uitgebrachte persbericht, waarin wordt aangekondigd dat de regels medio 2018 verwacht worden in werking te treden.

De Aanbieders hebben niet kunnen vernemen dat het Ministerie de in de voorfase aangedragen stukken en argumenten heeft meegewogen bij het opstellen van de Beleidsregel. Daarom hechten de Aanbieders eraan om de voornoemde stukken en argumenten alsnog voor het voetlicht te brengen in deze zienswijze. De Aanbieders adviseren het Ministerie daarbij om te onderzoeken wat de consequenties van de voorgenomen Beleidsregel zijn per type technologie en per type dienst. De voornoemde stukken en argumenten en ook de argumenten die volgen in deze zienswijze tonen aan hoe complex de gevolgen zijn van de voorgenomen beleidswijziging.

Ook adviseren de Aanbieders het Ministerie, voor zover dat nog niet is gebeurd, om vooraf met andere Ministeries, met de Europese regelgevende instanties[2] en met instanties die verantwoordelijk zijn voor het toezicht op cybersecurity of openbare veiligheid de verhouding van deze Beleidsregel met relevante wet- en regelgeving af te stemmen. Ter illustratie wordt hierbij verwezen naar de problematiek omtrent de veiligheid van netwerken. De telecommarkt signaleert dit niet als enige. Ook het Centraal Planbureau (CPB) geeft aan dat er een aantal beleidsrichtingen omgebogen moeten worden om cyberveiligheid te optimaliseren. Bijgesloten als bijlage 3 is de CPB Policy Brief 'Knelpunten op de markt voor cyberveiligheid' van 22 januari 2018. In deze Policy Brief geeft het CBP aan dat vrije modemkeuze niet leidt een betere prijsprestatie-verhouding, maar tot "relatief goedkope maar moeilijk controleerbare producten" met alle veiligheids- en continuïteitsrisico's van dien. Een coherent beleid is cruciaal als het gaat om de bescherming van veiligheid van netwerken.

Aanbeveling:
De Aanbieders vragen het Ministerie om de probleemstelling, de oplossing en het effect van deze Beleidsregel nader te onderzoeken en daarbij alsnog ook in te gaan op de door de Aanbieders in de voorfase aangedragen stukken en argumenten. Mocht het Ministerie op basis daarvan tot de conclusie komen dat een beleidswijziging door een Beleidsregel alsnog noodzakelijk is, dan vragen de Aanbieders het Ministerie om de uitkomsten van dergelijk onderzoek te weerspiegelen in de Beleidsregel en de bijbehorende toelichting.

II. HET GAAT NIET OM EEN VERDUIDELIJKING, MAAR OM EEN WIJZIGING VAN HET WETTELIJK KADER

In de toelichting bij de Beleidsregel stelt het Ministerie dat "*met de onderhavige beleidsregel duidelijkheid wordt geboden over de betekenis van het begrip 'netwerkaansluitpunt"*. Deze formulering geeft een verkeerde voorstelling van zaken. Anders dan het Ministerie hier doet voorkomen gaat het hier niet om een verduidelijking, maar om een nadere invulling die niet in overeenstemming is met de bestaande interpretaties zoals die door aanbieders, toezichthouders, beleidsmakers en rechterlijke instanties werden toegepast.

Eerder hebben de Aanbieders gezamenlijk een zeer uitgebreide juridische analyse opgesteld (opgenomen in bijlage 2), waarbij zij ernaar hebben gestreefd om op objectieve wijze vast te stellen hoe de relevante nationale en Europese wet- en regelgeving ten aanzien van het netwerkaansluitpunt en het aansluiten van apparatuur zich onderling verhoudt.

[2] De Aanbieders verwijzen hierbij naar artikel 59, lid 6, van de EECC (zie ook bijlage 2). BEREC moet na inwerkingtreding van de EECC richtsnoeren geven over dit onderwerp en het is onverstandig dat het Ministerie vooruitlopend daarop al een ingrijpende aanpassing voorstelt waarvan niet duidelijk is of die met de toekomstige invulling overeenstemt.

In die analyse wordt onderbouwd dat het relevante juridische kader ten aanzien van het netwerkaansluitpunt vanaf 1988 niet materieel gewijzigd is. Op grond van dit Europese kader is geen eenduidige conclusie te trekken ten aanzien van de definitie van het netwerkaansluitpunt. Dit wordt ook bevestigd door het voorstel voor de Europese Elektronische Communicatiecode, en de aangekondigde werkzaamheden door BEREC om de zeer verschillende interpretaties die zich in de lidstaten hebben ontwikkeld. Op grond van zowel de Nederlandse wetsgeschiedenis als de jurisprudentie die zich vanaf 1988 heeft ontwikkeld kan zeker niet de conclusie worden getrokken dat het netwerkaansluitpunt zich per definitie achter alle actieve apparatuur op de eindgebruikerslocatie bevindt, integendeel. Het is om die reden niet vol te houden dat het hierbij slechts om een 'verduidelijking' van het bestaande wettelijk kader zou gaan. In plaats daarvan gaat het om een materiële wijziging ten opzichte van de huidige situatie, die ook niet rechtstreeks volgt uit het Europese regelgevend kader. De Aanbieders verwijzen voor de nadere onderbouwing naar de bijgevoegde juridische analyse.

Deze constatering is cruciaal. Wanneer het slechts om een verduidelijking zou gaan, is de impact voor marktactoren van een geheel andere orde van grootte dan in het onderhavige geval. Het gaat immers om een fundamenteel gewijzigde invulling. Een dergelijke invulling die materieel anders is, brengt met zich mee dat de wetgever een zorgvuldig wetgevingstraject dient te doorlopen waarbij de wetgever zich voldoende rekenschap geeft van alle relevante complicaties van deze wijziging. Een beleidsregel is daarom het niet het juiste instrument. Op zijn minst zou het Besluit Eindapparaten moeten worden aangepast, maar het ligt meer voor de hand om de uitkomst van de richtlijnherziening af te wachten en dit in het daaropvolgende implementatietraject mee te nemen.

Het Besluit eindapparaten dient in elk geval ook om een andere reden al te worden aangepast. Daarin wordt ten onrechte ervan uitgegaan dat aanbieders andere apparatuur dan radioapparatuur niet zouden mogen afsluiten als die niet voldoen aan de aangegeven specificaties. Uit de toelichting bij de Beleidsregel valt op te maken dat het Ministerie deze redenering inmiddels niet meer aanhangt, maar die moet dan wel worden gecorrigeerd voordat een Beleidsregel in enige vorm in werking zou treden.

Aanbeveling:
De Aanbieders vragen het Ministerie om voor zover het Ministerie beoogt om het wettelijk kader te wijzingen, dit te doen door het doorlopen van een zorgvuldig wetgevingstraject, bij voorkeur niet voordat de Europese Elektronische Communicatiecode is aangenomen en de implementatie daarvan in werking treedt, waarbij de wetgever zich voldoende rekenschap geeft van alle relevante complicaties van deze wijziging en ook voldoende ruimte biedt voor implementatie van het gewijzigde juridische kader door aanbieders.

III. GEVOLGEN BEOOGDE BELEIDSREGEL JURIDISCH EN PRAKTISCH ONGEWENST

Telecommunicatienetwerken bestaan uit actieve en passieve componenten. Een door de aanbieder beheerde actieve component op het netwerkaansluitpunt stelt de aanbieder in staat een eenduidige scheiding te creëren tussen het eindgebruikersdomein en het domein van de aanbieder. De aanbieder beheert het netwerk tot aan de LAN (Local Area Network, het netwerk van de klant zelf) poort van het actieve apparaat. De eindgebruiker beheert eigen netwerk tot aan de LAN poort van eigen apparatuur. De verbinding wordt gemaakt door een passieve kabel waarmee de eindgebruiker zelf de twee domeinen verbindt.

Een belangrijk gevolg van een actieve, door de aanbieder beheerde component achter het aansluitpunt is dat de aanbieder in staat is de verbinding tot aan het eindpunt te beheren. De voorgenomen Beleidsregel zou ertoe leiden dat een cruciaal deel binnen het telecommunicatienetwerk niet in eigen beheer van de aanbieder is. De Aanbieders achten het noodzakelijk dat het netwerkaansluitpunt een actieve component bevat, omdat alleen dan de aanbieder in staat is de hele keten tussen locatie van de eindgebruiker en het eigen netwerk te bewaken en te besturen. Slechts dan kan de Aanbieder de eindverantwoordelijkheid dragen voor de prestaties van die keten ten opzichte van de verwachtingen van de klant en de eisen van de overheid.

In dat kader brengt de vernieuwde definitie van 'netwerkaansluitpunt' in de Beleidsregel juridische en praktische knelpunten met zich mee. Op 20 januari 2017 hebben de Aanbieders een uitgebreid overzicht van dergelijke knelpunten toegezonden aan het Ministerie en ACM (opgenomen als bijlage 1). De Aanbieders hechten er aan om nogmaals te wijzen op die eerder toegezonden uiteenzetting. Ter onderstreping van die knelpunten wordt hieronder nader ingegaan op i) de veiligheid en continuïteit van het netwerk, ii) de interoperabiliteit en iii) het doorgeven van auteursrechtelijk beschermde content.

Veiligheid en continuïteit

Zoals gezegd hebben de Aanbieders het Ministerie reeds in een vroeg stadium gewezen op de knelpunten van de voorgenomen wijziging van de definitie van het netwerkaansluitpunt in relatie tot de veiligheid en continuïteit van netwerken. Het Ministerie stelt in de toelichting op de consultatie dat hij "*deze signalen zorgvuldig heeft bestudeerd en tot dusverre tot de conclusie komt dat deze risico's voldoende beheersbaar blijven*". Het Ministerie onderbouwt echter op geen enkele wijze hoe hij tot deze conclusie komt, en er wordt geen enkel inzicht gegeven in de mate waarin het Ministerie ook daadwerkelijk onderzoek naar deze aspecten heeft gedaan. Ook wordt uit de beleidsregel niet duidelijk waar precies de grens ligt en om welke apparatuur het gaat. Alleen daarom is het al heel lastig om een dergelijke conclusie te trekken.

De thema's netwerkcontinuïteit en -veiligheid wegen voor telecomaanbieders als vitale sector, zeer zwaar. Dit geldt niet alleen op basis van de maatschappelijke verantwoordelijkheid die op aanbieders rust als aanbieders van een 'vitale infrastructuur. Er is tevens sprake van uitgebreide wettelijke verplichtingen ten aanzien van het waarborgen van netwerkcontinuïteit en -veiligheid. In aanvulling daarop hebben aanbieders ook een inherent en zeer sterk commercieel belang: klanten hebben – terecht - hoge verwachtingen van aanbieders. Incidenten ten aanzien van continuïteit en veiligheid hebben een zeer grote impact op de bedrijfsvoering en concurrentiepositie van aanbieders. Het belang van netwerkcontinuïteit en -veiligheid neemt alleen maar toe gegeven de grote maatschappelijke afhankelijkheid van telecommunicatie infrastructuur, terwijl ook de bedreigingen op het vlak van cybersecurity alleen maar groter worden.

In aanvulling op de eerder toegezonden uiteenzetting van de knelpunten (in bijlage 1), wijzen de Aanbieders nog op de volgende punten ten aanzien van veiligheid en continuïteit:

- Het voeren van meerdere modemtypes zal het aantal storingen omhoog brengen. Er lijkt ten onrecht het beeld te bestaan dat de keuze voor een modem een keuze is van de individuele consument, die slechts operationele gevolgen heeft voor de dienstverlening aan die consument. Dat klopt in een netwerk waar één lijn een verbinding is

richting één ontvanger. Echter, in een hybrid coax-fiber (HFC) netwerk bijvoorbeeld[3] gaat het om zogenoemde 'shared access'. Daarbij is de kwaliteit van de doorgifte van het signaal voor een gehele wijk afhankelijk van het functioneren van alle modems in die wijk. Daardoor kan een 'vreemd', onbekend modem een negatieve impact hebben op de dienstverlening voor alle aangeslotenen in die wijk. Het zoeken naar een storing in zo'n wijk is een hele inspanning. Als niet duidelijk is van welk modem het stoorsignaal afkomstig is, is er geen andere methode dan één voor één de afgaande takken van het netwerk los te maken tot het stoorsignaal verdwijnt.

- Onderhoud modem. Het onderhoud van een modem, zoals beveiligings-upgrades, vindt doorgaans plaats vanaf het netwerk van de aanbieder, voor zover deze modem door de aanbieder ter beschikking is gesteld. Dat kan voor modems die door de eindgebruiker zelf zijn aangeschaft echter niet het geval zijn. De betreffende modemfabrikant zal dus moeten faciliteren dat de eindgebruiker zelf upgrades door kan voeren, en de eindgebruiker is derhalve zelf verantwoordelijk voor het handmatig realiseren van de upgrades. Dat geeft risico's op het gebied van de Internetveiligheid. Niet alleen het nalaten van het doorvoeren van de upgrades, maar ook de upgrade zelf kan problemen veroorzaken. Daarom zou moeten worden gewaarborgd dat de upgrades worden uitgevoerd en ook dat deze upgrades (software) zijn voorzien van een digitale handtekening van de fabrikant en voldoen aan alle andere integriteitseisen die ook in het gangbare proces gewaarborgd zijn voor de eigen modems van de aanbieder. Uiteraard zijn er eindgebruikers en leveranciers die ervoor zorgen dat het modem altijd voldoet aan de laatste updates. In het business model voor de verkoop van modems zit echter geen prikkel voor leveranciers en eindgebruikers om hiervoor te zorgen. In de meeste gevallen gaat het om een eenmalige aanschaf zonder servicecontract en verdere veiligheidsgaranties.

- Open glasnetwerken. Voor aanbieders van open glasnetwerken (zoals CAI Harderwijk, KT Waalre en Reggefiber) geldt dat zij op 2 lagen dienstverlening leveren aan andere ISP's: er zitten op die netwerken ISP's die zelf actieve apparatuur plaatsen in de meterkasten van de eindgebruikers, maar ook (kleinere) aanbieders die gebruik maken van de NT (network termination unit) van de netwerkbeheerder, door achter die NT enkel een eigen router te plaatsen. Indien de eindgebruiker een eigen modem mag plaatsen, kan de aanbieder van het open glasnetwerken niet meer de kwaliteit van de verbinding richting zijn *wholesale* klant (de kleinere aanbieders) monitoren en garanderen.

- Kwaliteit dienstverlening. De keuzevrijheid van eindgebruikers met een derden-modem heeft dus een prijs voor de andere stakeholders, maar ook voor die eindgebruikers zelf. Als de aanbieder het modem niet kent en de technische eigenschappen niet kent noch heeft kunnen testen, dan is het voor de aanbieder niet mogelijk garanties te geven voor de prestatie. Ook hangen de prestaties van een abonnement af van de prestaties van het modem. Voor hogere prestaties kan een krachtiger modem nodig zijn. Het derden-modem beperkt de eindgebruiker dus ook, in die zin dat er logischerwijs een reeks beperkingen qua zekerheid en mogelijkheden volgen uit de keuze voor het derden-modem.

[3] De Aanbieders merken op dat in deze zienswijze verschillende voorbeelden worden genoemd ten aanzien van een concreet type netwerk. De voorbeelden zijn illustratieve knelpunten en spelen in andere typen netwerken op een vergelijkbare wijze.

Bird & Bird

Tot nu toe heeft het Ministerie de Aanbieders niet ervan kunnen overtuigen dat hij voornoemde knelpunten in het kader van de onderhavige Beleidsregel voldoende serieus neemt. Dit geldt ook voor ACM waar zij eenvoudig stelt in haar nieuwsbericht van 13 december 2017: "*de voorgestelde beleidsregel verandert echter niets aan de verantwoordelijkheden voor veiligheid. De telecomaanbieders blijven verantwoordelijk voor de continuïteit en beveiliging van openbare netwerken. Zij mogen dan ook maatregelen blijven nemen om openbare netwerken te* beveiligen." De kern is echter dat de risico's voor netwerken toenemen als aanbieders iedere apparatuur zonder enige beperking, en zonder duidelijk kader moeten aansluiten.

De zorgvuldigheid vereist dat indien het Ministerie besluit de Beleidsregel door te zetten, de knelpunten dienen te zijn verholpen voordat het nieuwe beleid in werking treedt. Zonder te pretenderen dat hiermee alle knelpunten zullen zijn verholpen, zijn de Aanbieders van mening dat daarvoor in ieder geval de volgende maatregelen moeten worden genomen, die per type dienst en type technologie kunnen verschillen.

- In de eerste plaats moet verduidelijkt worden wat de mogelijkheden zijn om eindapparatuur te weren of af te sluiten wanneer de continuïteit of de veiligheid in het geding is. De paradox doet zich voor dat er enerzijds steeds meer druk is op netwerkaanbieders om de toenemende veiligheids- en continuïteitsrisico's te adresseren, en dat anderzijds de mogelijkheden voor aanbieders lijken te worden beperkt om hier daadwerkelijk invulling aan te geven. Zo is het Besluit eindapparaten onvoldoende duidelijk over de mogelijkheden die aanbieders hebben om eindapparaten van hun netwerk te weren of af te sluiten in het geval de netwerkcontinuïteit of – veiligheid in het geding is. In plaats daarvan stelt het Besluit slechts dat het verboden is om eindapparatuur aan te sluiten die niet voldoet aan EMC- of radioapparatuurvereisten.

- In de tweede plaats is het nodig om beter te waarborgen dat eindgebruikers en leveranciers de verantwoordelijkheid kunnen dragen die ze op grond van het gewijzigde beleid wordt toegekend. Het algemeen geaccepteerde probleem is nu juist dat het merendeel van de eindgebruikers zich onvoldoende bewust is van risico's, dat de veiligheidsrisico's van bepaalde apparatuur niet transparant zijn en leveranciers niet per definitie voldoende zorg besteden aan de veiligheidsrisico's. Het Ministerie merkt in dit verband op dat '*inherent aan het beleid van een vrije verhandelbaarheid van eindapparaten is dat fabrikanten en gebruikers (consumenten en bedrijven) een eigen verantwoordelijkheid moeten nemen voor de beveiliging van eindapparaten die zij zelf aanschaffen*'. Het Ministerie heeft echter ook de beleidsverantwoordelijkheid, wanneer hij meer verantwoordelijkheid bij eindgebruikers en fabrikanten neerlegt, te zorgen dat die verantwoordelijkheid door deze partijen voldoende kan worden gedragen.

Wanneer de randvoorwaarden niet duidelijk worden geformuleerd – en dat dient door de beleidsmaker vooraf te worden gedaan en niet achteraf in de toezichtspraktijk door ACM – en wanneer tevens onvoldoende duidelijkheid wordt geboden door het Ministerie en ACM over welke maatregelen toegestaan zijn, dreigen de aanbieders in een catch-22 situatie terecht te komen.

Aanbeveling:
De Aanbieders vragen het Ministerie om, indien het Ministerie besluit de Beleidsregel door te zetten, de genoemde knelpunten te verhelpen en in dat kader in ieder geval de volgende maatregelen te nemen: • te verduidelijken wat de mogelijkheden zijn om eindapparatuur te weren of af te sluiten wanneer de continuïteit of de veiligheid in het geding is; en • te waarborgen dat eindgebruikers en leveranciers de verantwoordelijkheid kunnen dragen die ze op grond van het gewijzigde beleid wordt toegekend.

Het informeren over internetsnelheden

Op grond van de Europese Verordening 2015/2120 over netneutraliteit, de richtsnoeren van BEREC en de ACM Beleidsregel kenbaarheid van internetsnelheden, dienen aanbieders informatie te verstrekken over de minimale, de normaliter beschikbare, de maximale en de geadverteerde download- en uploadsnelheid van internettoegangsdiensten. Daaruit blijkt al dat die internetsnelheden 'op het modem' moeten worden gemeten (en niet in het – al dan niet eigen – Wi-Fi netwerk van de eindgebruiker). De Aanbieders merken op dat wanneer een eindgebruiker een eigen modem kan plaatsen, Aanbieders geen adequate informatie kunnen verstrekken over de genoemde internetsnelheden, omdat die (mede) wordt bepaald door het modem zelf.

Aanbeveling:
De Aanbieders vragen het Ministerie om te onderzoeken wat het effect is van de Beleidsregel op de verplichtingen die gelden op het gebied van netneutraliteit.

Het doorgeven van auteursrechtelijk beschermde content

Hiervoor werd al geconstateerd dat de toelichting op de Beleidsregel aangeeft dat ook apparatuur voor de distributie van TV-diensten (vaak settopboxen genoemd) daaronder zouden vallen en dat – kennelijk – wordt verondersteld dat die diensten ook over apparatuur van derden zou moeten worden geleverd. Om videocontent zoals televisiezenders te mogen doorgeven aan kijkers hebben aanbieders toestemming nodig van zenders en andere auteurs- en naburig rechthebbenden. Als voorwaarde voor toestemming stellen rechthebbenden eisen aan het gebruik van bepaalde hardware, voorwaardelijke toegangssystemen en DRM-systemen (Digital Rights Management). Op dit terrein werken aanbieders nauw samen met de leveranciers van de content-beveiligingssystemen. Rechthebbenden, aanbieders en genoemde leveranciers voorkomen zodoende in belangrijke mate dat content kan worden gekopieerd en online gedeeld door illegale praktijken zoals cardsharing, control word sharing en illegaal streaming aanbod. De Aanbieders wijzen erop dat deze vormen van fraude strafbaar zijn op basis van artikel 326c van het Wetboek van Strafrecht. Dergelijk illegaal gedrag leidt immers tot economische en maatschappelijke schade en benadeelt de gehele mediasector, waaronder makers en rechthebbenden, producenten, omroepen en pakketaanbieders. Met de voorgestelde Beleidsregel wordt de praktijk van content-beveiliging ondermijnd. De aanbieders merken op dat de Beleidsregel niet kan worden vastgesteld zonder dat is onderzocht wat het effect daarvan is op de praktijk van content-beveiliging en daarmee de handhaving van artikel 326c Sr.

Aanbeveling:
De Aanbieders vragen het Ministerie om te onderzoeken wat het effect is van de Beleidsregel op het illegaal delen van auteursrechtelijk beschermde content.

Interoperabiliteit

De praktijk ten aanzien van technische standaarden is weerbarstig. Ook wanneer verschillende fabrikanten 'op papier' dezelfde standaarden toepassen, kunnen interoperabiliteitsissues optreden. De reden hiervoor is dat standaardisatie niet zelden onbedoeld ruimte laat voor verschillende invullingen, en dat fabrikanten bepaalde functionaliteiten kunnen toevoegen die niet of onvoldoende door de standaarden worden ondersteund. De mogelijkheden van aanbieders om in de praktijk de interoperabiliteit te waarborgen worden daarom beperkt. Het is van belang dat er bij aanbieders geen onrealistische verantwoordelijkheden worden neergelegd om te allen tijde te waarborgen dat alle denkbare eindapparatuur interoperabel is met de netwerkinterface.

Juist omdat het geen gegeven is dat eindapparatuur - die in naam gestandaardiseerd is en voldoet aan de netwerkspecificaties - ook daadwerkelijk goed functioneert, werken aanbieders samen met leveranciers om apparatuur te certificeren. Tijdens het certificatieproces kunnen aanbieders de leverancier ondersteunen om eventuele interoperabiliteitsissues die zich onverhoeds voordoen op te lossen, en de certificatie geeft eindgebruikers de garantie dat de aangeschafte apparatuur ook daadwerkelijk naar behoren functioneert op het netwerk. Het is van belang dat bij eindgebruikers geen verkeerde verwachtingen worden gewekt. Mocht het Ministerie bij het standpunt blijven dat een aangesloten apparaat geen onderdeel vormt van het openbare elektronische communicatienetwerk, dan dienen Aanbieders de mogelijkheid te hebben om, voor zover er sprake is van een vrije keuze van eindapparatuur, uitsluitend de correcte werking te waarborgen van eindapparatuur die daadwerkelijk voor het netwerk is gecertificeerd.

Aanbeveling:
De Aanbieders vragen het Ministerie om in de Beleidsregel te verduidelijken dat, voor zover er sprake is van een vrije keuze van eindapparatuur, aanbieders uitsluitend de correcte werking kunnen en hoeven te waarborgen van eindapparatuur die daadwerkelijk voor het netwerk is gecertificeerd.

Redelijke implementatietermijn

In het voorgaande is onderbouwd dat het hier wel degelijk om een beleidswijziging gaat, en dat de gevolgen voor aanbieders, maar in bepaalde gevallen ook voor eindgebruikers, zeer materieel zijn. Voor zover het Ministerie het voorgestelde beleid doorgang wil laten vinden, en ook als de genoemde knelpunten zijn verholpen, gebiedt de redelijkheid dat Aanbieders in de gelegenheid worden gesteld zich aan te passen aan de nieuwe situatie vanaf het moment dat de Beleidsregel definitief van kracht wordt. Vanaf dat moment is immers pas echt duidelijk welke maatregelen genomen zullen

moeten worden. Dat betekent ook dat de Beleidsregel uitdrukkelijk aandacht moet geven aan het toepasselijke overgangsregime. Daarbij moet onder meer duidelijkheid gegeven worden over een redelijke inwerkingtredingstermijn. Het belang van rechtszekerheid brengt met zich mee dat dit overgangsregime niet open kan worden gelaten of dat de invulling hiervan bij ACM als toezichthouder kan worden overgelaten. De Aanbieders zijn van mening dat, mits de genoemde knelpunten zijn verholpen, een redelijke implementatietermijn vereist zal zijn. Wat een redelijke implementatietermijn is, verschilt per type dienst en per type technologie en zal dan ook per type dienst en technologie onderzocht moeten worden.

Aanbeveling:
De Aanbieders vragen het Ministerie om een redelijk overgangsregime vast te stellen.

IV. Mobiele openbare elektronische communicatienetwerken

Niet alleen bij vaste netwerken, maar ook bij mobiele netwerken is er sprake van apparatuur op de locatie van de abonnee die tot het domein van de Aanbieder zou moeten behoren. Het voorgestelde artikel 1 lid 4 van de Beleidsregel luidt: "*Indien een openbaar elektronisch communicatienetwerk gebruik maakt van een draadloze verbinding op de locatie van de abonnee, behoren apparaten of radioapparaten op de locatie van de abonnee, die bedoeld zijn voor communicatie met dit netwerk, niet tot het openbare elektronische communicatienetwerk.*"

In de toelichting bij dit artikel wordt aangegeven dat van een draadloze verbinding op de locatie van de abonnee sprake is. "(…) *bij bijvoorbeeld mobiele netwerken en ook bij netwerken met een draadloze eindaansluiting bedoeld voor gebruik van deze aansluiting op een vaste locatie*". Als voorbeeld van deze laatste categorie worden satellietnetwerken voor de ontvangst van omroep en vaste netwerken met lokale draadloze (4G) verbindingen voor gebruik op specifieke locaties genoemd. De toelichting stelt dat in dat geval "*alle (radio)apparaten op de locatie van de abonnee, die bedoeld zijn voor communicatie met het betreffende openbare elektronische communicatienetwerk, niet tot dat openbare elektronische communicatienetwerk*" behoren.

De Aanbieders gaan er van uit dat artikel 1 lid 4 betrekking heeft op apparatuur die gebruik maakt van (bijvoorbeeld WIFI op) vergunningvrij spectrum, zoals genoemd in de Regeling gebruik van frequentieruimte zonder vergunning en zonder meldingsplicht 2015 (http://wetten.overheid.nl/BWBR0036378/2016-12-28). Op basis van deze regeling kunnen gebruikers zelf bepalen welke apparatuur wordt aangeschaft en op welke wijze zij daar gebruik van maken. Voor de duidelijkheid vragen de Aanbieders het Ministerie om een verwijzing naar dit besluit in de toelichting op te nemen.

De Aanbieders gaan er ook vanuit dat radioapparatuur bedoeld om dekking en/of dienstverlening van mobiele openbare elektronische communicatienetwerken te bieden die gebruik maakt van exclusief aan mobiele operators vergund spectrum of licentie vrij spectrum buiten de werking van de Beleidsregel netwerkaansluitpunt valt, ook als deze apparatuur op de locatie van gebruikers wordt geïnstalleerd. Het gaat hier bijvoorbeeld om (kleine) basisstations bedoeld om de dekking of capaciteit van openbare mobiele elektronische netwerken op een bedrijfsterrein of binnen gebouwen te verbeteren. Het gebruik van frequenties door deze basisstations wordt net zoals bij "grote" basisstations zorgvuldig door de mobiele operators in-

geregeld door middel van radioplanning. Hierdoor kan optimaal gebruik gemaakt worden van de frequenties en wordt storing voorkomen.

Aanbeveling:
De Aanbieders vragen het Ministerie om: • in de toelichting bij de Beleidsregel te bevestigen dat artikel 1 lid 4 betrekking heeft op apparatuur die gebruik maakt van (bijvoorbeeld Wi-Fi op) vergunningvrij spectrum, zoals genoemd in de Regeling gebruik van frequentieruimte zonder vergunning en zonder meldingsplicht 2015 ; • in de toelichting bij de Beleidsregel een verwijzing naar de 'Regeling gebruik van frequentieruimte zonder vergunning en zonder meldingsplicht 2015' op te nemen; en • in de toelichting op de Beleidsregel te bevestigen dat radioapparatuur bedoeld om dekking en/of dienstverlening van mobiele openbare elektronische communicatienetwerken te bieden die gebruik maakt van exclusief aan mobiele operators vergund spectrum of licentie vrij spectrum buiten de werking van de Beleidsregel netwerkaansluitpunt valt, ook als deze apparatuur op de locatie van gebruikers wordt geïnstalleerd.

Bird & Bird

Bijlage 1

Besluit eindapparaten

Suggesties voor onderwerpen die moeten worden meegenomen in de consultatie over de invulling van het 'netwerkaansluitpunt'

Inleiding

EZ heeft aangekondigd een nadere consultatie te houden over de invulling van het begrip 'netwerkaansluitpunt' in Beleidsregels. In een overleg van 20 december 2016 hebben de aanwezige aanbieders aangegeven punten te zullen aanreiken waarvan zij denken dat die in zo'n consultatie in elk geval aan de orde moeten komen. In het voorliggende document geven de aanbieders (CAIW Diensten, KPN Telecom, Tele2, T-Mobile en VodafoneZiggo) een overzicht van deze punten, en treden hierover graag nader in overleg met het Ministerie.

Probleemanalyse

- Om tot een passende invulling te komen moet de voorgestelde invulling van het begrip en het probleem dat daarmee wordt beoogd op te lossen in de consultatie helder worden voorgelegd. Wat is precies het mededingingsprobleem in de markt(en) voor eindgebruikersapparatuur, en hoe kan dit op een passende en proportionele wijze geadresseerd worden?

- Daarbij is vooral van belang om inzicht te krijgen per onderscheiden dienst die over netwerkaansluitpunten worden aangeboden welke technische mogelijkheden en/of problemen er zijn.

- Bij het vaststellen van de passendheid en proportionaliteit van de invulling van de maatregelen kan gebruik worden gemaakt van de praktijkervaring die in Duitsland is opgedaan.

Te betrekken partijen en kennis

- Naast telecomaanbieders dienen ook zowel leveranciers van eindapparaten als leveranciers van netwerkapparatuur betrokken te worden. De door EZ beoogde invulling van Beleidsregels beoogt immers een probleem op te lossen op de markt waarop deze partijen actief zijn. Daarnaast geldt dat voor de praktische uitvoerbaarheid van de voorgenomen Beleidsregel de kennis en ervaring van deze partijen noodzakelijk is.

- In het kader van de consultatie moet gedetailleerd advies worden ingewonnen van technische experts, onder andere naar de mogelijkheden en de onmogelijkheden om op basis van uitsluitend specificaties interoperabiliteit tussen apparatuur en netwerk te waarborgen voor de verschillende betrokken elektronische communicatiediensten. In de praktijk zijn voor sommige van die diensten de standaarden zeer complex en er worden ook proprietary oplossingen gebruikt, in situaties waarin er geen standaarden zijn.

- Het is wenselijk dat technische experts eveneens adviseren over mogelijke veiligheids- en integriteitsproblemen, en hoe hier in de praktijk mee om dient te worden gegaan. Dit om risico's voor eindgebruikers en netwerken aanvaardbaar te houden. Technische vraagstukken vormen een belangrijk onderdeel in de meeste van de hiernavolgende punten, zie ook onder het kopje 'technische aandachtspunten'.

Reikwijdte

- De reikwijdte van de voorgenomen Beleidsregel dient duidelijk te worden vastgesteld.

- Van belang is dat Nederlandse eindgebruikers op dit moment al de vrijheid hebben om zelf hun router te kiezen (daarmee is de Nederlandse situatie anders dan de Duitse situatie die aanleiding heeft gegeven voor het Duitse wetsvoorstel inzake de vrije keuze van de router).

- Het is raadzaam om goed te definiëren wat onder eindapparatuur in de zin van dit besluit moet worden verstaan. Bijvoorbeeld apparatuur die in bruikleen wordt geleverd omdat die niet op de markt beschikbaar is, omdat er geen standaarden zijn of omdat die standaarden niet voldoen, dient buiten de reikwijdte te vallen; daar is immers (nog) geen markt voor eindgebruikersapparatuur..

- De reikwijdte dient zich te beperken tot de residentiële markt, op de zakelijke markt wordt – desgewenst – gekozen voor maatwerk door eindgebruikers.

- Over netwerkaansluitpunten worden naast internettoegangsdiensten ook ‘andere diensten dan internettoegang’ in de zin van Verordening 2015/2120 (‘gespecialiseerde diensten’) geleverd. De Beleidsregel moet duidelijk maken voor welke diensten deze geldt en in de consultatie moet daarom per (type) dienst informatie worden gevraagd over de mogelijkheid om die diensten te leveren op basis van actieve apparatuur van derden. In de BEREC consultatie kwam al naar voren dat ‘gespecialiseerde diensten’ gekoppeld kunnen zijn aan specifieke apparatuur.

- Wenselijk is dat de Beleidsregel de mogelijkheid open laat dat de levering van de CPE nog steeds onderdeel kan blijven uitmaken van het aanbod, de meeste klanten hebben hier immers behoefte aan. Mogelijk zijn niet alle diensten die over één passief netwerkaansluitpunt worden geboden zodanig te specificeren dat die ook geleverd kunnen worden via andere apparatuur (zie vorige punt).

  Verduidelijkt moet worden dat verouderde standaarden niet hoeven te blijven worden ondersteund (en dat de vervanging van de verouderde apparatuur voor rekening van de klant is). Daarnaast geldt ook omgekeerd dat niet verwacht kan worden van aanbieders dat zij zonder meer ook nieuwe standaarden ondersteunen.

Verhouding met regelgeving

- Aanbieders worden in toenemende mate verantwoordelijk geacht en gehouden voor de kwaliteit van diensten, waaronder bijvoorbeeld de snelheid van de verbinding. Daarin wordt een aanbieder soms ook aangesproken op de werking van de dienst incl. de randapparatuur van de klant. Het is raadzaam om in de consultatie aandacht te besteden aan waar van dergelijke relaties met regelgeving sprake is (bijvoorbeeld zoals hiervoor besproken de compensatieregeling, of bijvoorbeeld snelheidsmetingen in het kader van netneutraliteit) en hoe een aanbieder daar mee om kan gaan.

Technische aandachtspunten

- De consultatie moet inzicht verschaffen in de mate van standaardisatie van de betrokken diensten, netwerkaansluitpunten en randapparatuur. Daarbij dient een onderscheid gemaakt te worden naar diensten (internettoegang, SIP Telefonie, TV, beheerde WiFi-routers etc.) en netwerktechnologieën (DOCSIS, DSL, FttH). De veronderstelling dat overal beschikbare openbare specificaties voor bestaan moet worden geverifieerd, daarbij is het inhuren van aanvullende technische expertise wenselijk.

- Het passieve aansluitpunt moet per netwerktechnologie nader onderzocht worden (glas/koper/coax). Voor glas is bijvoorbeeld naast een modem een NT nodig, waarvoor geen standaardisatie bestaat.

- Er moet duidelijkheid komen ten aanzien van proprietary-standaarden, in hoeverre beperkt dit de mogelijkheden om specificaties te delen? Hierbij moeten ook leveranciers van netwerkapparatuur worden betrokken, omdat sprake kan zijn van intellectuele-eigendomsrechten die aanbieders kunnen beletten om bepaalde specificaties te verstrekken.

  Op dit moment bestaan er certificeringsafspraken in de markt voor sommige apparatuur. Die zijn noodzakelijk om verstoringen of niet-werkende diensten te voorkomen. Er zal een basis voor dergelijke certificering moeten komen. Daarbij dient de verdeling van de verantwoordelijkheden, binnen de mogelijkheden, tussen de fabrikant en de netwerkaanbieder te worden verduidelijkt.

Borging van kwaliteit

- De kwaliteit (indien van toepassing: SLA's) ten aanzien van klanten die kiezen voor eigen hardware kan niet volledig worden geborgd omdat de aanbieder minder controle heeft over de geleverde dienst. Dat raakt zowel aan de ondersteuning door monteurs en de helpdesk als aan de kwaliteitsparameters van de dienst zelf (bijvoorbeeld internetsnelheden).

- Klanten zowel als de overheid dienen erop te worden gewezen dat indien storingen worden veroorzaakt door hun eigen eindapparatuur aanbieders hiervoor geen verantwoordelijkheid kunnen dragen.

- Het dient onderzocht te worden in hoeverre diensten door andere, niet-gecertificeerde hardware kunnen worden ondersteund. Niet alle diensten zullen in redelijkheid kunnen worden ondersteund. Er zullen diensten zijn die niet met een andere CPE werken (waarbij bijvoorbeeld wel de internettoegangsdienst wordt ondersteund, maar niet alle gespecialiseerde en aanvullende diensten, zoals SIP telefonie en WifiSpots, maar ook bijvoorbeeld SVOD en uitzending-gemist-diensten).

- Het dient te worden onderzocht hoe met netwerkupgrades dient te worden omgegaan. Netwerkupgrades (bijvoorbeeld ten behoeve van hogere snelheden) vergen vaak vervanging of upgrades van de modems. De aanbieder moet dat eenzijdig kunnen opleggen aan klanten die een eigen modem gebruiken in gevallen dat de generieke netwerkupgrade anders niet door zouden kunnen gaan. Het dient te worden voorkomen dat klanten met zelfgekozen apparatuur netwerkupgrades tegen kunnen houden. Spectrum management op DSL/koper lijnen vraagt extra aandacht. Bijvoorbeeld bij de introductie van VDSL kan een slecht functionerend modem van één gebruiker alle gebruikers op zo'n koperbundel negatief beïnvloeden, met name bij nieuwe technieken zoals vectoring & G.fast, waarbij het cruciaal is dat interferentie op een centrale, gecoördineerde wijze wordt beheerst. Om andere klanten te beschermen zullen specifieke maatregelen tegen een 'vrij' modem noodzakelijk zijn (bijv. 'terugtunen' naar 20 Mbit/s (ADSL snelheid)). Dit wordt nu opgelost in de wholesaleovereenkomsten, maar dit zou bij vrije modemkeuze ook naar eindgebruikerovereenkomsten moeten worden doorgetrokken. Ook ten aanzien van coax-technologie kan apparatuur van individuele eindgebruikers de werking van het netwerk en de aangeboden diensten negatief beïnvloeden.

Verdeling verantwoordelijkheden

- Duidelijk moet zijn dat aanbieder niet volledig kan instaan voor de beveiliging en het voorkomen van storingen van niet door hem geleverde modems. Aanbieders moeten de klant verwijzen naar de fabrikant bij storingen. Dat zal druk op klantrelatie geven, maar dit is niet te voorkomen. Aanbieders hebben immers minder inzicht en kennis bij dit type klant in het functioneren van de dienst dan bij hardware die ze zelf volledig ondersteunen.

- Duidelijk moet zijn dat de eindgebruiker zelf verantwoordelijk is voor het doen van firmware updates.

- Leveranciers van eindapparatuur dienen eindgebruikers voldoende voor te lichten over mogelijke beperkingen die eindgebruikers kunnen ervaren bij het aansluiten van de apparatuur en voldoende ondersteuning bieden aan eindgebruikers bij het oplossen van compatibiliteitsproblemen. Ook dienen ze eindgebruikers te wijzen op hun verantwoordelijkheid voor het erop toezien dat firmware-updates tijdig worden gedaan.

- Er moet duidelijkheid worden gegeven over de verantwoordelijkheden in het geval van storing of schade voor andere eindgebruikers of aanbieders door niet-goed werkende eindapparaten. Aanbieders moeten in dergelijke gevallen worden gevrijwaard van de gevolgen van storingen (zoals compensatie) of schade.

- in bepaalde gevallen kan het wenselijk zijn dat leveranciers van netwerkapparatuur specificaties publiceren, waarnaar hun afnemers (de aanbieders) verwijzen.

Borging veiligheid en netwerkintegriteit

- Als gevolg van het toelaten van allerlei eindapparaten kan het netwerk veel toegankelijker worden voor de buitenwereld, en neemt ook het aantal potentiële veiligheidslekken aanzienlijk toe. Dit vergroot het risico op misbruik en continuïteitsproblemen in het netwerk. Hier moet rekening mee gehouden bij de uitvoering. Indien blijkt dat een bepaald type apparatuur onverantwoorde beveiligingsrisico's met zich meebrengt voor de eindgebruiker zelf of andere eindgebruikers dient deze apparatuur niet langer gebruikt te worden. De vraag is alleen hoe dit gedetecteerd kan worden en of dit juridisch is toegestaan (bijvoorbeeld kan sprake zijn van mogelijke privacy-schending).

- Door toegankelijkheid via kwetsbaarheden in eindapparatuur kan continuïteit van het netwerk in gevaar worden gebracht. Het Agentschap Telecom ziet toe op continuïteit van netwerken (op basis van hoofdstuk 11 van de Tw) en kan handhavend optreden. Vraag is ook hier hoe compensatie ten behoeve van storingen geregeld wordt als de storing of discontinuïteit wordt veroorzaakt door (kwetsbaarheid van) eindapparatuur.

- Het vrijgeven van dienstgegevens (met name ten aanzien van telefonie) brengt aanvullende risico's met zich mee ten aanzien van misbruik. Dit kan leiden tot aanzienlijke financiële en andere gevolgen voor de eindgebruiker (zowel de eindgebruikers met eigen apparatuur als overige eindgebruikers). Ook beperkt het de mogelijkheid van een aanbieder om controle te houden over het gebruik van een dienst, zelfs als dit in strijd zou kunnen zijn met bijvoorbeeld regels over nomadisch nummergebruik. Met dit aspect dient rekening mee te worden gehouden bij de uitvoering.

Overgangsregelingen

- Er dient een realistische overgangstermijn te worden gesteld waarin aanbieders op basis van heldere eisen de implementatie van de verplichtingen kunnen realiseren. Aanbieders moeten voordat diensten beschikbaar worden gesteld, de specificaties publiceren. Echter, ook ten aanzien van diensten die nu reeds beschikbaar worden gesteld dient een duidelijke en haalbare invulling te worden gegeven aan de verplichtingen.

Implementatie-impact

- In de consultatie zal inzicht moeten worden gekregen in de impact op operationele processen voordat realistische planning kan worden bepaald. Rekening moet bijvoorbeeld worden gehouden met: (i) online selfcare tools die niet meer werken voor alle klanten (ii) aanpassing van de instructies van callcenters in het kader van storingen en leveringen, (iii) aanpassing van de inzet van installatie-, storings- en servicemonteurs, (iv) andere specifieke bedrijfsprocessen (indienststelling diensten via modems etc.), v) aanpassing van voorwaarden en dergelijke die moeten worden aangepast.

- Informatie van aanbieders die het noodzakelijke inzicht geven moeten in de consultatie vertrouwelijk kunnen worden ingebracht.

Bird & Bird

Bijlage 2

Juridische analyse ten aanzien van het 'netwerkaansluitpunt' (en het Besluit eindapparaten)

A. Inleiding

1. Op 28 december 2016 trad het Besluit eindapparatuur in werking. Van het besluit werd voorafgaand aan publicatie en inwerkingtreding geen ontwerp geconsulteerd. De aanbieders CAIW diensten, KPN, Tele2, T-Mobile en VodafoneZiggo maken daarom graag nog van de mogelijkheid gebruik om hun interpretatie van het juridische kader voor te leggen.

2. Bestudering van het besluit roept vragen op over enkele van de interpretaties van Europees recht, zoals die blijken uit de toelichting. Omdat die interpretaties van belang zijn bij de toepassing van het besluit en bij de door het Ministerie van EZ voorgenomen consultatie met het oog op een beleidsregel over de afbakening van het begrip 'netwerkaansluitpunt' worden in deze notitie de belangrijkste punten besproken.

3. In het licht van de voorgenomen consultatie over de invulling van het begrip 'netwerkaansluitpunt' is het goed de juridische context en de ontwikkeling voor ogen te houden. Conclusies over het juridische kader moeten worden getrokken op basis van een goede analyse (van de ontwikkeling) daarvan.

4. In deze analyse wordt ingegaan op de relevante bijbehorende Europese en nationale regelgeving, de ontwikkelingen die in de telecommunicatiemarkt heeft plaatsgevonden en de invloed die dit heeft gehad in het nu voorliggende Besluit eindapparaten en zal krijgen in de voorgenomen publicatie van beleidsregels. Om tot een goed afgeronde analyse te komen is er voor gekozen om ook in te gaan op de wetshistorie inzake dit onderwerp.

5. De aanbieders zijn zeer bereid om deze notitie nader toe te lichten en naar aanleiding van deze analyse in gesprek te treden om tot een gedeeld beeld te komen ten aanzien van het juridische kader.

B. Richtlijnen 88/301/EEG van de Commissie. 86/361/EEG van de Raad en de Wet op de Telecommunicatievoorzieningen (Wtv)

6. In 1988 werden twee richtlijnen uitgevaardigd om de randapparatuurmarkt in de EU te liberaliseren (richtlijn 88/301/EEG van de Commissie) en de procedures te harmoniseren (richtlijn 86/361/EEG van de Raad).

7. Al vanaf deze eerste richtlijnen is gebruik gemaakt van twee te onderscheiden grondslagen; (a) de 'harmonisatie-richtlijnen' van de Raad (en later mede het Parlement; op basis van het huidige art. 114 VWEU en voorlopers daarvan) en (b) de 'liberalisatie-richtlijnen' van de Commissie (op basis van het huidige art. 106 lid 3 VWEU en voorlopers daarvan). Die beide soorten richtlijnen moeten goed onderscheiden worden, zowel in effect als in werking:

a. *Harmonisatierichtlijnen* zijn instructies aan lidstaten om hun wetgeving aan te passen aan de Europese regels en geven zo concreet mogelijk aan welke normen moeten worden geïmplementeerd. Hoewel de normen vaak rechtstreeks marktpartijen regarderen zijn de richtlijnen gericht tot de lidstaten en (anders dan verordeningen) niet rechtstreeks bindend. Lidstaten moeten die bepalingen vertalen in voor ondernemingen bindende nationale regels.

b. *Liberalisatierichtlijnen* op grond van (het huidige) art. 106 lid 3 VWEU, zijn een uitwerking van het mededingingsrecht. In dit artikel wordt het lidstaten verboden om aan *openbare ondernemingen* ('ondernemingen aan wie de staat bijzondere of uitsluitende rechten verleent') *bijzondere rechten* te verlenen ten aanzien van (in dit geval) de levering en aansluiting van randapparatuur. In lid 3 van ditzelfde artikel wordt aan de Commissie de bevoegdheid gegeven richtlijnen uit te vaardigen. Deze richtlijnen zijn een eigen bevoegdheid van de Commissie. In procedures tegen de eerste randapparatuur-liberalisatie richtlijn 88/301/EEG heeft het HvJ EU de rechtsgeldigheid van dit instrument aangenomen om lidstaten te verbieden randapparatuur voor te behouden aan de toen nog bestaande ondernemingen met bijzondere rechten (de oude 'staatsmonopolisten').[1] Het Hof maakt daarbij uitdrukkelijk uit dat het slechts kan gaan om overheidsmaatregelen en dat handelen van individuele ondernemingen slechts met de artikelen (thans) 101 en 102 VWEU kan worden aangepakt. De hierboven genoemde richtlijnen zien dan ook alleen op het (verbod op) het opleggen van overheidsmaatregelen die marktwerking belemmeren en niet op procedures die ondernemingen in een vrije markt moeten volgen. Bepalingen uit de oorspronkelijke richtlijn die dat doel hadden werden daarom door het Hof dan ook onverbindend verklaard in de uitspraak in zaak C-202/88.

8. In Nederland werden de beide richtlijnen geïmplementeerd in de Wet op de telecommunicatievoorzieningen (Stb. 1988, 520; 'Wtv'), in het bijzonder hoofdstuk IV (art. 29). Tevens werden de begrippen 'aansluitpunt' en 'randapparatuur' geïntroduceerd.

> Het aansluitpunt werd gedefinieerd als: *een eindpunt van de telecommunicatie-infrastructuur, dat dient voor de aansluiting van randapparatuur* (art. 1 onder j Wtv).
>
> Randapparatuur werd gedefinieerd als: *een inrichting of samenstel van inrichtingen, bestemd voor rechtstreekse aansluiting op de telecommunicatie-infrastructuur door middel van een aansluitpunt* (art. 1 onder k Wtv).

9. In de parlementaire behandeling is uitvoerig ingegaan op de vraag wat bij digitale verbindingen het 'aansluitpunt' is waar de 'randapparatuur' op moet worden aangesloten. Geconstateerd werd dat dit – anders dan bij traditionele analoge telefonie – een complexere afweging was, waarbij uit oogpunt van standaardisatie, beveiliging en efficiency voor een actief koppelvlak werd gekozen. Zie uitvoerig de MvA[2]:

> *Het aansluitpunt op het telefoonnet voor enkelvoudige apparatuur wordt in de huidige situatie gevormd door de eerste contactdoos (stopcontact) op de lokatie van de gebruiker. Via een (nationaal) gestandaardiseerde stekker aan het aansluitsnoer van de randapparatuur, wordt daarop direct toegang verkregen tot de lokale abonneelijn naar de nummercentrale.*
> *De toelatingseisen voor aansluiting van randapparatuur op het telefoonnet zijn mede gebaseerd op de eigenschappen van die lijn en van de daarover te transporteren signalen ten behoeve van de verbindingsopbouw en gegevensoverdracht. Door de historische ontwikkeling van de telefonie zijn een aantal van deze eigenschappen typisch nationaal. Er bestaat dan ook geen wereldwijde standaard voor telefoonapparatuur. Dat niettemin ook buitenlandse*

[1] Zie uitspraken van 19 maart 1991 (C-202/88) inzake Frankrijk (e.a.)/Commissie en (n.a.v. telecomdiensten-richtlijn) 17 november 1991 ((Gevoegde zaken C-271/90, C-281/90, C-289/90).
[2] *Kamerstukken II* 1987/88, 20369, nr. 6, p. 7-8.

apparatuur redelijk op het Nederlandse net functioneert is een gevolg van het feit dat de afwijkingen ten opzichte van de in ons land geldende eigenschappen voornamelijk gevolgen hebben voor de kwaliteit van de overdracht en in veel mindere mate voor de verbindingopbouw.
Voor meervoudige telefoonaansluitingen ten behoeve van bedrijfstelefooncentrales geldt een vergelijkbare situatie als voor enkelvoudige aansluitingen, zij het dat daar geen contactdoos maar een andere afwerkingsvorm van de abonneelijnen is gekozen. De situatie voor telexaansluitingen en voor analoge vaste verbindingen is conform het hierboven beschrevene.
Voor digitale vaste verbindingen en voor aansluitingen op het Datanet-1 moeten de door de apparatuur van de abonnee in standaardvorm geproduceerde digitale gegevens eerst worden aangepast aan de eigenschappen van de gebruikte abonneelijn (bijvoorbeeld koper- of glaskabel). De voor deze omzetting gebruikte apparatuur is onderdeel van het aansluitpunt op het Datanet-1. De gebruiker wordt hiermee een uniform en gestandaardiseerd koppelvlak geboden, onafhankelijk van de door de houder van de concessie gebruikte transportmiddelen (bijvoorbeeld type en lengte van de kabel, glasvezel etc).
Dat wil dus zeggen, dat bij het aansluiten van randapparatuur géén rekening behoeft worden gehouden met het in de infrastructuur toegepaste transportmedium: als aan de toelatingseisen wordt voldaan is het transport van de gegevens verzekerd. Voor de netwerkbeheerder bestaat hierbij tevens de mogelijkheid om, zonder gebruik behoeven te maken van de aangesloten apparatuur, op afstand de goede werking van de infrastructuur, en met name van het traject naar het aansluitpunt, te beheersen en te controleren.
In de nabije toekomst zal er sprake zijn van een geïntegreerd netwerk voor de afwikkeling van vele verschillende diensten (waaronder uiteraard ook telefonie), het zogenaamde Integrated Services Digital Network (ISDN). Dit netwerk verzorgt digitaal transport van gebruiker naar gebruiker: deze dient dus digitale informatie aan te bieden c.q. te ontvangen, die over het netwerk wordt getransporteerd. De vorm waarin deze informatie wordt aangeboden of afgenomen is internationaal gestandaardiseerd in de beschrijving van de eigenschappen van het zogenaamde S/T-referentiepunt en de daarbij behorende afspraken over de wijze van verbindingsopbouw en bewaking (het zogenaamde D-protocol).
Feitelijk ontstaat er derhalve een zelfde situatie als boven beschreven bij het Datanet-1 en de digitale vaste verbinding. Het S-referentiepunt is bedoeld als «stopcontact» voor toestellen of terminals. De eigenschappen zijn zodanig gedefinieerd dat er meer toestellen tegelijkertijd (voor telefonie, fax, teletex etc.) op kunnen worden aangesloten. Het T-referentiepunt is gedefinieerd voor de aansluiting van bedrijfscentrales en netwerken (PABX-en of LAN's). In het geval van een enkelvoudige aansluiting (die in het ISDN twee 64 kbit/s kanalen en een apart 16 kbit/s signaleringskanaal biedt) zijn de eigenschappen op deze referentiepunten overigens identiek. Er is dus in de praktijk geen sprake van twee fysiek te onderscheiden soorten «stopcontacten».
De overgang tussen het S/T-punt waarop de apparatuur wordt aangesloten aan de gebruikerszijde en de abonneelijn c.q. de rest van de infrastructuur wordt gerealiseerd door een zogenaamde «Network Termination Unit» (NT). Deze bevat de elektronica die nodig is voor de vertaling van de door de apparatuur aangeboden digitale gegevens (0-en/1 -en) naar over de lijn te transporteren signalen, en vice versa. Bovendien kan ook hier op afstand bestuurd vanuit de infrastructuur een scheiding worden gerealiseerd tussen het aansluitpunt en de daarop aangesloten randapparatuur, zodat de beheerder van de infrastructuur (PTT) de goede werking daarvan kan bewaken of controleren in geval van klachten.
De netwerkzijde van de NT wordt als U-referentiepunt aangeduid. De eigenschappen van dit punt zijn echter, in tegenstelling tot het S/T-punt, niet internationaal gestandaardiseerd. Dat is ook begrijpelijk omdat het aangepast moet zijn aan de eigenschappen van het abonneenet in een bepaald gebied en/of van de toegepaste verbindings- middelen (koper, glas, radio) waarvoor (nog) geen internationale standaardisatie bestaat en ook veel minder nodig is. Door het gestandaardiseerde S/T-punt kan immers alle apparatuur worden gebruikt die aan de, in toenemende mate internationaal gestandaardiseerde, aansluiteisen voldoet. Wel worden in West Europa nationale standaarden voor dit punt gehanteerd.
De Europese PTT's, verenigd in de CEPT, en de Europese Commissie hebben gekozen voor een Europese standaard op het S/T-koppelvlak. Daarmee is het doel van een open Europese markt voor (fabrikaatonafhankelijke) telecommunicatie-randapparatuur het beste gediend.
Zoals uit het voorgaande blijkt kan (en behoeft) de netwerkzijde van de NT (het U-punt), niet internationaal (te) worden gestandaardiseerd. Het inbouwen in de randapparatuur van een gestandaardiseerde NT, welke suggestie wordt gedaan in de reactie van de leden van de fractie van D66, is dan ook niet wenselijk vanuit de optiek van een open Europese markt.

Voorts behoeft een dergelijke handelwijze niet te leiden tot lagere kosten voor de gebruiker, gezien onder andere de relatief korte economische levensduur van randapparatuur vergeleken met die van infrastructuur.
Er wordt wel aangevoerd tegen het beschouwen van de NT als onderdeel van het aansluitpunt, dat niet duidelijk is of in de in de NT ondergebrachte elektronica niet meer functies zouden kunnen zitten c.q. door de netwerkbeheerder daarin zouden kunnen worden aangebracht dan voor de toegang tot en het transport over het netwerk nodig is. In de internationaal vastgelegde (CCITT, CEPT) S/T-standaarden worden echter alléén transportfuncties gedefinieerd (OSI-laag 1).
Dat op een S-koppelvlak meer apparaten tegelijk kunnen worden aangesloten doet daar niets aan af. Door het «meer-diensten» karakter van het ISDN is dat een vanzelfsprekende noodzaak. Anders zou ook van de meervoudigheid van het ISDN (twee 64 kbit/s kanalen en een 16 kbit/s kanaal) geen gebruik kunnen worden gemaakt. Het is echter niet zo dat de NT ook onderlinge communicatie tussen de op een aansluiting aangesloten terminals mogelijk maakt: er wordt alleen een verbinding met het netwerk gevormd.
Samenvattend meen ik het volgende te mogen stellen. Het in de voorgestelde regelgeving gebruikte begrip aansluitpunt geeft de gebruiker de beste garantie voor uniformiteit, los van landsgrenzen en technologische ontwikkeling, en daarmee vrijheid van keuze van randapparatuur, zonder daarmee de mogelijkheden van het gebruik van de infrastructuur te beperken. Bovendien wordt de netwerkbeheerder een scheidingsvlak geboden, dat het mogelijk maakt om de verantwoordelijkheid voor de kwaliteit en de integriteit van het netwerk volledig te kunnen dragen. Noch in de huidige, noch in de toekomstige (ISDN) situatie legt de voorgestelde regelgeving oneigenlijke beperkingen op aan het gebruik van de transportmogelijkheden welke de houder van de concessie verplicht is aan te bieden. Het inbouwen van een NT in randapparatuur behoeft niet te leiden tot lagere kosten voor de gebruiker, te meer niet daar de afschrijvingsperiode van randapparatuur over het algemeen aanzienlijke korter is dan die van de infrastructuur.

10. Voor ISDN is in lijn met bovenstaande uitleg vanaf het begin aangenomen en geaccepteerd dat het NT-1 aansluitpunt het netwerkaansluitpunt is waarop randapparatuur wordt aangesloten.

11. Mede op basis van deze uitleg is in een procedure, die door Racal Datacom werd aangespannen tegen de Staat en PTT Telecom in 1993, beslist dat het netwerkaansluitpunt van digitale ('Digistream') huurlijnen zich niet bevindt op het passieve vlak van het netwerk, maar op het (actieve) modem.[3] Voor zover bekend is dit de enige rechterlijke uitspraak waarin de bepaling van het (netwerk-) aansluitpunt uitdrukkelijk is getoetst.

C. Invoering van de Telecommunicatiewet (Tw)

12. Per 15 december 1998 werd de Wtv vervangen door de Telecommunicatiewet ('Tw'). De definitie van 'aansluitpunt' werd vervangen door die van 'netwerkaansluitpunt': waar het een openbaar telecommunicatienetwerk betreft, het geheel van verbindingen, met hun technische toegangsspecificaties, die deel uitmaken van dit openbaar telecommunicatienetwerk, en nodig zijn om toegang te verkrijgen tot dit netwerk en om efficiënt via dit netwerk te communiceren (art. 1.1 onder h Tw). Deze definitie beoogde aan te sluiten bij art. 1 van de (de toen nog geldende) Richtlijn 90/388/EEG van de Commissie (de 'Telecommunicatie-dienstenrichtlijn').

[3] Uitspraken in kort geding en bodemprocedure Rechtbank 's-Gravenhage, voor zover nagegaan niet gepubliceerd.

13. In de toelichting daarop wordt niet aangegeven dat enige inhoudelijke wijziging ten opzichte van de definitie en toepassing van de Wtv is beoogd. Er wordt slechts vermeld:[4]

> *Om efficiënt te kunnen communiceren dient elk type (rand)apparaat te worden aangesloten op het daarvoor bedoelde netwerkaansluitpunt, dat qua eigenschappen c.q. karakteristieken zodanig is dat het (rand)apparaat en het telecommunicatienetwerk compatibel zijn. Dit houdt bijvoorbeeld in dat ISDN-apparatuur, om efficiënt, dat wil zeggen conform zijn bestemming, te kunnen communiceren via een openbaar netwerk, specifiek aangesloten moet worden op een ISDN-aansluitpunt. GSM-apparatuur moet, teneinde een efficiënte communicatie mogelijk te maken, op een speciaal GSM-aansluitpunt worden aangesloten. Het gaat er in de definitie om dat de toegepaste technieken in de telecommunicatienetwerken en de (rand)apparaten op elkaar aansluiten zodat ook werkelijk telecommunicatie tot stand kan komen. Het aspect «efficiënt via het netwerk kunnen communiceren» heeft dan ook geen betrekking op een aspect van de communicatie tussen mensen, maar is een technische kwalificatie.*

14. Mede op basis van het ontbreken van een aanwijzing dat de voorafgaande interpretatie werd gewijzigd heeft de praktijk zich onverminderd gebaseerd op het uitdrukkelijke uitgangspunt dat de infrastructuur eindigt op een actief netwerkaansluitpunt.

D. Richtlijn 99/5/EEG van de Raad

15. De drie opvolgende randapparatuur harmonisatierichtlijnen (86/361/EEG, 91/263/EEG en 98/13/EG) zijn in 1999 vervangen door de zogenaamde RTE-richtlijn (99/5/EG). De doelstelling daarvan was niet wijziging te brengen in de regels m.b.t. het netwerkaansluitpunt, maar om telecommunicatie-eindapparatuur en radioapparatuur in dezelfde regeling onder te brengen. Het begrip netwerkaansluitpunt werd als onderdeel van de definitie van 'interface' gedefinieerd als een netwerkaansluitpunt dat een fysiek verbindingspunt is waar een gebruiker toegang heeft tot een openbaar telecommunicatienet, (….)en hun technische specificaties (art. 2 onder e (i)). Nergens blijkt dat bedoeld werd een technische invulling van die definitie als Europese norm op te leggen. De Telecommunicatiewet werd op dit punt dan ook niet aangepast aan de nieuwe richtlijn.

16. Wel trad ter implementatie van de RTE-richtlijn een nieuw Besluit randapparaten en radioapparaten (Stb. 2000, 143) in werking. Dit besluit en de toelichting daarop, geven geen nieuw inzicht in de bepaling van de technische invulling van het netwerkaansluitpunt. Wel bevat art. 15 Besluit een verplichting voor aanbieders van openbare telecommunicatienetwerken om op verzoek van OPTA de specificaties van netwerkaansluitpunten bekend te maken. Dit ter implementatie van art. 4 RTE-richtlijn, waarin lidstaten worden verplicht dergelijke specificaties aan de Commissie te melden. Voor de inwerkingtreding van dit besluit gold die verplichting slechts voor telefonie (op grond van art. 26 Besluit ONP huurlijnen en telefonie). De vervanging van dit Besluit door het Besluit randapparaten en radioapparaten 2007 (Stb. 2007, 20) had slechts wetstechnische redenen en wijzigde de materiële regeling niet. Art.15 van het voorafgaande besluit werd (behoudens het overgangsrecht van het laatste lid) ongewijzigd overgenomen in het nieuwe art. 14.

17. Een wijziging in de wettelijke definitie werd pas aangebracht per 19 mei 2004, bij de implementatie van de het nieuw Europees regelgevingskader (Stb. 2004, 189) om aan te

[4] *Kamerstukken II* 1996/97, 25 533, nr. 3, p. 73.

sluiten bij de nieuwe definitie van art. 2 onderdeel e van de Universeledienstrichtlijn (2002/22/EG), een harmonisatierichtlijn van de Europese Raad en het Europese Parlement. De belangrijkste wijziging was – zoals volgt uit de toelichting – dat de definitie werd beperkt tot aansluiting van eindgebruikers en niet (langer) tot de onderlinge koppeling van netwerken.

18. De definitie van netwerkaansluitpunt luidt sindsdien: *fysiek punt waarop een abonnee de toegang tot een elektronisch communicatienetwerk wordt geboden; in het geval van netwerken met schakelings- of routeringsfuncties wordt het netwerkaansluitpunt bepaald door middel van een specifiek netwerkadres, dat met een abonneenummer of -naam kan zijn verbonden*.

19. Die wettelijke definitie is daarmee materieel ten aanzien van de invulling van het koppelvlak ongewijzigd gebleven en er zijn geen openbare discussies bekend over de inhoud daarvan. Ook is er geen openbare handhaving door OPTA/ACM bekend die een nadere invulling van het technische koppelvlak bepaald heeft.

E. Wijzigingen in markt en techniek sinds de RTE-richtlijn

20. Uit het voorgaande overzicht blijkt dat in Nederland de wetgever sinds 1988 geen verdere inhoudelijke verduidelijking heeft gegeven van de technische invulling van het begrip '(netwerk) aansluitpunt'. Voor dat begrip werd destijds niet gekozen voor een passief koppelvlak, maar voor een – waar mogelijk gestandaardiseerd – (actief) NT koppelvlak. De discussies van destijds zagen op ISDN, de toen bestaande datanetten en digitale huurlijnen. Sindsdien zijn er veel ontwikkelingen geweest.

21. De eerste op te merken ontwikkeling is dat de markt een grotere diversiteit van technologieën in aansluitnetten kent. Traditionele spraaktelefonienetwerken en – koppelvlakken waren relatief simpel, maar zijn vervangen door op IP gebaseerde netwerken op basis van verschillende transmissiemiddelen (koper, coax, glas) en verschillende standaarden (DOCSIS, xDSL, FttH, e.a.). Een deel van de ontwikkelde technieken is gebaseerd op internationale standaarden, met algemene requirements en gaan niet in op detailniveau. Hierdoor hanteren verschillende aanbieders verschillende detailspecs. Apparatuur in het netwerk moet samenwerken met de modems bij klanten. Door de snelle ontwikkelingen op dit gebied wordt apparatuur in netwerken veel sneller vervangen dan in traditionele netwerken.

22. Een tweede ontwikkeling is dat het historische netwerkaansluitpunt werd gezien als een '*socket-in-the-wall*' gekoppeld aan een specifieke infrastructuur en dienst (telefonie, data, huurlijn). In moderne op IP transmissie gebaseerde netwerken worden vanuit één infrastructuur meerdere diensten geboden (in de consumentenmarkt: internettoegang, telefonie en TV). In de infrastructuur en op het koppelvlak bij de klant worden die diensten gescheiden op actief niveau (en niet op passief niveau).

23. Een derde ontwikkeling is dat naast de telecommunicatiediensten die vanuit het netwerk worden aangeboden ook 'Over-The-Top' diensten worden aangeboden die voor klanten aan de traditionele diensten (en de technische opvolgers daarvan) soms gelijkwaardig zijn, maar vanuit de regelgeving daarvan wel worden onderscheiden. Zo wordt (in het kader van de Netneutraliteitsverordening) aangenomen dat aanbieders van digitale IP-

TV diensten een managed TV dienst bieden die op sommige terreinen wel concurreren met OTT TV diensten (zoals Netflix, Apple e.a.), maar in een ander regime vallen. Hetzelfde geldt voor de IP Telefoniediensten van aanbieders, die wel op sommige gebieden concurreren met OTT VOIP diensten, maar daaraan niet gelijk zijn. De 'managed' diensten van telecomaanbieders vanuit het netwerk zijn gebonden aan aanvullende regels die zien op continuïteit, kwaliteit en veiligheid van diensten en netwerken. De waarborging daarvan vergt nadere maatregelen in de infrastructuur en daarmee ook in de desbetreffende regelgeving.

24. De simpele vraag van 1988 of het netwerkaansluitpunt op 'passief' niveau kan worden gedefinieerd of op een specifiek NT-punt was in 1988 al complex, en is daarmee alleen nog maar complexer geworden. De markt heeft zich ontwikkeld zoals dat is gebeurd en wellicht kan achteraf worden geconstateerd dat de consequenties daarvan voor de technische invulling van het begrip 'netwerkaansluitpunt' niet expliciet genoeg onder de aandacht van aanbieders, toezichthouders en beleidsmakers zijn geweest, maar dat kan geen rechtvaardiging zijn voor een onverhoedse invulling daarvan, zonder de consequenties voor implementatie van zo'n keuze in detail te onderzoeken en daarbij – als een nieuwe keus wordt gemaakt - de noodzakelijke implementatietermijnen te bepalen.

25. In lijn met die conclusie is eerder al verwezen naar de voorstellen van de Europese Commissie van 14 september 2016 voor een Voorstel voor Richtlijn tot vaststelling van het Europees wetboek voor elektronische communicatie (de 'EECC'), ter vervanging van het huidige EU regelgevingskader. In overweging 19 daarvan staat:

> *(19) Het netwerkaansluitpunt vormt voor regelgevingsdoeleinden een grens tussen het regelgevingskader voor elektronische communicatienetwerken en -diensten en de regeling voor telecommunicatie-eindapparatuur. Bepaling van de locatie van netwerkaansluitpunten valt onder de bevoegdheid van de nationale regelgevende instantie. In het licht van de praktijk van de nationale regelgevende instanties en de verschillende situaties inzake vaste en draadloze netwerken, moet het Orgaan van Europese regelgevende instanties voor elektronische communicatie (Berec), in nauw overleg met de Commissie, richtsnoeren vaststellen voor de bepaling van het netwerkaansluitpunt overeenkomstig deze richtlijn en in diverse concrete situaties.*

26. Ter uitwerking daarvan is in het voorgestelde art. 59 lid 6 opgenomen:

> *6. Uiterlijk op [inwerkingtreding plus 18 maanden] stelt Berec, na raadpleging van de belanghebbenden en in nauwe samenwerking met de Commissie, richtsnoeren vast inzake gemeenschappelijke benaderingen betreffende de identificatie van het netwerkaansluitpunt in verschillende netwerktopologieën, teneinde bij te dragen tot een consistente omschrijving van de locatie van netwerkaansluitpunten door de nationale regelgevende instanties. De nationale regelgevende instanties houden zoveel mogelijk rekening met deze richtsnoeren bij de omschrijving van de locatie van netwerkaansluitpunten.*

27. Hoewel dit artikel staat in het hoofdstuk met betrekking tot toegang en interconnectie vult het de definitie van 'netwerkaansluitpunt' (zoals opgenomen in art. 2, onderdeel 9, van het voorstel) nader in:

> *9) "netwerkaansluitpunt" of "NAP": het fysieke punt waarop een eindgebruiker de toegang tot een openbaar communicatienetwerk wordt geboden; in het geval van netwerken met schakelings- of routeringsfuncties wordt het NAP bepaald door middel van een specifiek netwerkadres, dat met een nummer of naam van een eindgebruiker kan zijn verbonden;*

28. Voor radioapparatuur zouden een dergelijk invulling mogelijk ook onder Richtlijn 2014/53/EU kunnen worden ingevuld, maar bij gebreke van een harmonisatierichtlijn

voor vaste eindapparatuur, is duidelijk dat verdere invulling alleen onder deze nieuwe grondslag kan plaatsvinden. De Commissie vreest kennelijk dat afzonderlijke lidstaten tot verschillende nationale invulling kunnen komen en creëert hiermee de grondslag voor hernieuwde harmonisatie.

29. Duidelijk is dat deze invulling thans nog geen geldend recht is, maar er zit wel de erkenning in dat de implementatie en interpretatie van het begrip in de huidige markt niet eenduidig is en dat er een voorafgaand onderzoek nodig is voordat die invulling van worden vastgesteld. Dat is precies waarover de aangekondigde consultatie moet gaan.

30. Daarbij is tevens van belang dat er in de toekomst van de EU coördinatie komt op de invulling 'in verschillende netwerktopologieën'. Het zou onwenselijk zijn om nu een invulling te bepalen die in de nabije toekomst weer aangepast zou moeten worden. Dat vergt terughoudendheid met het opleggen van een invulling die op korte termijn grote gevolgen voor de markt heeft.

F. Richtlijn 2008/63/EEG van de Commissie

31. Deze richtlijn van de Commissie is een codificatie van de eerdere richtlijn 88/301/EEG en de daarin nadien aangebrachte wijzigingen (aldus overweging 1). De grondslag is art. 86 lid 3 van het EG Verdrag (het huidige art. 106 lid 3 VWEU) en de richtlijn kan daarom opnieuw alleen inhoudelijke voorschriften geven ten aanzien van het beperken van bijzondere rechten voor openbare ondernemingen. Nu in Nederland geen openbare ondernemingen meer bestaan en geen bijzondere rechten ten aanzien van infrastructuur, diensten of apparatuur worden verleend, voldoet Nederland aan de richtlijn en behoeft deze in beginsel niet geïmplementeerd te worden.

32. Art. 4 van deze richtlijn zou daarom logischerwijs ook niet gelezen kunnen worden als een algemene instructie aan lidstaten om ten aanzien van alle ondernemingen bijzondere publicatieplichten in het leven te roepen, hoewel de tekst wel als zodanig is geformuleerd en in overweging 5 van Radioapparatuurrichtlijn 2014/53/EU – die per 13 juni 2016 de RTE-richtlijn heeft vervangen – wel zo wordt gelezen. Volgens deze overweging van de Radioapparatuurrichtlijn zou de publicatieplicht van technische specificaties van 'interfaces' nog de enige reden zijn om regels te stellen voor eindapparatuur op vaste netwerken. Het is daarom begrijpelijk dat die publicatieplicht – ook al is twijfelachtig of een art. 106-richtlijn daartoe een bindende grondslag kan bieden, in nationaal recht wordt neergelegd.

33. Voor het overige moet evenwel worden geconstateerd dat deze mededingingsrichtlijn, gezien de grondslag, geen bepalingen kan bevatten over de relatie tussen aanbieders en eindgebruikers. Zoals ook uit de hiervoor aangehaalde uitspraak van het HvJ (zie voetnoot 1) blijkt, zijn instructies, die de richtlijn zou bevatten buiten het kader van verplichtingen van lidstaten jegens openbare ondernemingen met bijzondere rechten, niet verbindend. Art. 106 lid 3 VWEU biedt immers simpelweg geen grondslag voor de Commissie om dergelijke regels te stellen en aan het ontbreken daarvan kunnen dan ook geen inhoudelijke argumenten worden ontleend voor een bepaalde invulling van nationale regels.

G. Het Besluit eindapparatuur

34. Per 28 december 2016 is het Besluit randapparaten en radioapparaten 2007 vervangen door het Besluit radioapparatuur 2016 en het Besluit eindapparatuur. Omdat de EU regels alleen nog gelden voor radioapparatuur, zijn regels met betrekking tot vaste eindapparatuur in een apart besluit opgenomen.

35. Het aanvankelijk informeel aangekondigde voornemen om in de toelichting van het besluit te 'verduidelijken' dat het netwerkaansluitpunt zich 'op passief niveau' bevindt werd uiteindelijk niet opgenomen, omdat dit vragen bij marktpartijen opriep en een voorafgaande consultatie zal plaatsvinden voordat die invulling verder plaatsvindt. Voor die consultatie is het echter wel van belang dat de juridische kaders eenduidig zijn. De aanbieders zien het daarom als zeer belangrijk dat er kennis wordt genomen van het voorgaande als achtergrond voor de verdere invulling van het besluit.

36. In het licht van de hiervoor beschreven Europese en Nederlandse wettelijke regels bevat het Besluit eindapparatuur een aantal in het oog springende bepalingen en toelichtingen. Voor een deel werd daarop ook al gewezen door de Raad van State.[5] De Afdeling constateerde dat meer dan voorheen werd gekozen voor een 'strikte interpretatie van richtlijn 2008/53/EG' en heeft geadviseerd de inhoudelijke wijzigingen in de toelichting te benoemen en daadkrachtig te motiveren. De aanbieders zijn er niet ten volle van overtuigd dat hier in voldoende mate aan tegemoet is gekomen .

37. Naast een (ten opzichte van art. 14 BRRA 2007 iets gewijzigde) publicatieplicht voor technische specificaties van netwerkaansluitingen in art. 2 bevat het besluit in de art. 3 en 4 regels over het aansluiten van eindapparatuur, welke voldoet aan de te stellen eisen. Deze bepalingen houden alleen in dat apparatuur moet voldoen aan de eisen gesteld in het Besluit EMC 2016 of het Besluit radioapparaten 2016. De enige beperking die artikel 3 kent is dat het moet gaan om aansluiting op 'daartoe geschikte netwerkaansluitpunten.' Logischerwijs zou dat moeten meebrengen dat alleen apparatuur die voldoet aan de door de aanbieder gepubliceerde technische specificaties mag worden aangesloten. De toelichting (p. 5-6) lijkt dat ook te ondersteunen, maar de tekst van het Besluit lijkt verder te gaan. Het is slechts verboden (art. 4 Besluit) om apparatuur die niet aan EMC- of radioapparatuur-eisen voldoet aan te sluiten op het netwerkaansluitpunt. Naar de letter zou het daarmee niet verboden zijn – om maar een veraf gelegen voorbeeld te noemen - een EMC-goedgekeurd strijkijzer op het netwerkaansluitpunt aan te sluiten, ook al zou dat de veiligheid van het netwerk en andere gebruikers in gevaar kunnen brengen. Het moge duidelijk zijn dat de Europese regels nooit zo kunnen worden uitgelegd dat een dergelijke absurde conclusie getrokken kan worden.

38. Ook aanbieders van vaste netwerken behoren de bescherming van hun netwerken centraal te kunnen stellen. Dat richtlijn 2008/53 een dergelijke grond voor afsluiten van apparatuur en klanten niet kent wordt meegebracht door de bijzondere wettelijke grondslag ervan – zie hiervoor – en niet doordat de Europese wetgever de bescherming van de continuïteit en veiligheid van netwerken heeft willen beperken. De conclusie op pagina 6 van de Nota van Toelichting (slot paragraaf 4) dat deze richtlijn aanbieders in dit opzicht zou beperken getuigt van onjuist begrip van de richtlijn en het regelgevend kader en moet worden hersteld. De verantwoordelijkheid voor de continuïteit en veiligheid van netwer-

[5] Advies RvS No. W15.16.0310/IV, 11 november 2016, *Stcrt*. 2017, 48.

ken is juist een op vele plaatsen in de regelgeving steeds sterker bij de aanbieder van netwerken en diensten neergelegde verplichting en de uitleg dat de oude liberalisatierichtlijn 2008/53 afbreuk zou doen aan latere regels en 'de verantwoordelijkheid in deze gevallen ook bij gebruikers komt te liggen' is niet alleen onjuist, maar ook niet maatschappelijk verantwoord in het licht van het toenemende belang van de continuïteit van telecommunicatienetwerken en diensten.

39. Voor zover het gaat om het bepalen van de technische specificaties van het netwerkaansluitpunt bevat de toelichting inderdaad niet de aangekondigde 'verduidelijking' dat die zich op het passieve niveau bevindt maar veel van de voorbeelden op pagina 5 zijn daaraan nog wel ontleend. In dat opzicht loopt die toelichting toch vooruit op de consultatie die nog volgt.

40. Een detailopmerking betreft nog de opmerking onder punt 3 van de toelichting dat artikel 4 van Richtlijn 2008/53 verplicht de fysieke eigenschappen van het netwerkaansluitpunt te publiceren. Die weergave is correct, maar illustreert tegelijkertijd dat een beroep op de letterlijke tekst van die richtlijn onhoudbaar verouderd is. De tekst dateert uit de tijd dat het er vooral om ging de fysieke eigenschappen van de telefoonstekker te bepalen (hoeveel polen, met welke afstand van elkaar, etc). In de huidige op IP communicatie gebaseerde netwerken zou het passieve niveau worden gecommuniceerd als 'glasvezel', 'coax', of 'een koperpaar'. Met zo'n aanduiding kan immers geen enkel apparaat worden aangesloten, omdat het juist gaat om heel andere dan 'fysieke' specificaties.

H. Een geharmoniseerde EU interpretatie?

41. Uit het hiervoor weergegeven art. 59 lid 6 van de voorgestelde EECC blijkt dat de Commissie onderkent dat de oorspronkelijke doelstelling van de harmonisatie van de randapparatuurmarkt door de veelheid van technologieën en nationale keuzes van regulering gevaar loopt. Dat kan leiden tot argumenten om in lidstaten tot vergelijkbare interpretaties van de regels voor vergelijkbare technologieën te komen. Tot op heden hebben noch de Commissie, noch BEREC, daarin inhoudelijk technisch voldoende duidelijke keuzes gemaakt.

42. In een land als Duitsland heeft dat er recent toe geleid dat - sinds 1 augustus 2016 – na een ruime tijd van voorbereiding de wetgeving zodanig is gewijzigd dat aanbieders klanten de keuze moeten laten om in plaats van meegeleverde 'Routerboxen' eigen boxen te installeren. Daaraan voorafgaand ging een ruime tijd van consultatie en vervolgens implementatie. De regels geven klanten een recht om bepaalde eigen apparatuur in te zetten, maar verbieden aanbieders niet die als geïntegreerde dienstverlening mee te leveren.

43. De Duitse oplossing is nog slechts kort geleden in werking getreden en de marktteffecten lijken op basis van openbare bronnen gering. Voordat zonder meer een dergelijk voorbeeld zal worden gevolgd zal echter moeten worden onderzocht in hoeverre de feitelijke situatie in Nederland geheel vergelijkbaar is.[6] Dit zijn onderwerpen die wat de aanbieders betreft in de aangekondigde consultatie eerst in detail dienen te worden onderzocht voordat op voldoende zorgvuldige wijze definitieve besluiten kunnen worden ingevoerd.

[6] Zo geldt dat in Nederland de uitrol van kopernetwerken historisch afwijkend is van Duitsland, waardoor andere xDSL diensten worden aangeboden dan daar. Ook kent Duitsland niet de mate van FttH uitrol en de daarvoor in Nederland veelal gekozen NT oplossingen.

I. Conclusies en aanbevelingen voor consultatie

44. Uit het voorgaande vloeit voort dat de informeel ingenomen stelling dat 'met regels steeds beoogd is om het passieve aansluitpunt als netwerkaansluitpunt te beschouwen' onvoldoende steun vindt. Noch in EU verband, noch in Nederland is daarvoor immers ooit uitdrukkelijk gekozen. In Nederland heeft zelfs sinds 1988 een uitdrukkelijk ander uitgangspunt gegolden waarbij werd uitgegaan van een 'NT' functie, die zich in elk geval niet op passief niveau bevindt. Het Europese kader ten aanzien van de technische invulling van het netwerkaansluitpunt is sinds 1988 niet materieel veranderd. Er is daarmee, anders dan de suggestie die naar voren komt uit de Memorie van Toelichting bij het Besluit Eindapparaten 2016 geen aanleiding vanuit een gewijzigd Europees kader om tot een andere of nadere technische invulling te komen van het netwerkaansluitpunt.[7] Het Europese kader levert ook geen concrete aanknopingspunten om te komen tot de zeer strikte interpretatie dat er bij het netwerkaansluitpunt sprake moet zijn van een passief koppelvlak.

45. De stelling dat het Europese kader zich onmiskenbaar beweegt in de richting van de lezing dat het netwerkaansluitpunt zich 'op passief niveau' moet bevinden vindt dan ook geen enkele steun in de daadwerkelijke wet- en regelgeving op Europees niveau. De bestaande Europese wet- en regelgeving is op dit vlak niet alleen zeer statisch (sinds 1988 niet materieel gewijzigd), maar geeft bovendien geen concrete voorschriften ten aanzien van de technische uitwerking. Het aansluitpunt eenvoudig benoemen als een 'socket in the wall' maakt de discussie wat betreft de aanbieders niet helderder, omdat – afhankelijk van de invulling – een dergelijk 'socket' op passief niveau voor breedbandnetwerken niet gestandaardiseerd bestaat en ook op actief niveau kan worden ontwikkeld.[8]

46. De enige afwijking in dit statische beeld wordt gevormd door het voorstel in het kader van de EECC. Daarin onderkent de Europese Commissie:

    - dat het vaststellen van het aansluitpunt niet eenduidig is;
    - dat dit voor verschillende netwerktopologieën anders kan zijn;
    - dat de interpretatie tussen lidstaten hierdoor aanmerkelijk verschilt;
    - dat er behoefte is aan harmonisatie;
    - dat BEREC hiertoe richtsnoeren dient op te stellen;
    - dat NRA's op basis van deze richtsnoeren het netwerkaansluitpunt dienen te definiëren.

    De voorgenomen publicatie van beleidsregels door het Ministerie van Economische Zaken staat daarmee haaks op het voorstel van de Commissie.

[7] De Memorie van Toelichting bij het Besluit Eindapparaten 2016 stelt dat dit besluit de artikelen 14 tot en met 17 van het Besluit randapparaten en radioapparaten 2007 vervangt, en strekt ter implementatie van Richtlijn 2008/63/EG. In het licht van het voorgaande, waarbij is vastgesteld dat de Richtlijn 2008/63/EG geen materiële wijzigingen met zich meebrengt ten opzichte van de eerdere richtlijnen ten aanzien van de identificatie van het netwerkaansluitpunt, is het niet te volgen wat de rechtvaardiging is voor het Besluit Eindapparaten 2016.

[8] Zo moet bij glasnetwerken het getransporteerde lichtsignaal per definitie worden omgezet in een elektronisch signaal voor verder transport en hoort die functie logischerwijs bij de netwerkfunctie.

Het Besluit Eindapparaten 2016, aangevuld met de nog te publiceren beleidsregels, brengt het risico met zich mee dat aanbieders grote inspanningen moeten doen om te voldoen aan nationale wetgeving die vervolgens door Europese wetgeving in combinatie met richtsnoeren van BEREC zal worden ingehaald. Voor zover hier toch voor gekozen wordt is van belang dat recht wordt gedaan aan het feit dat de markt heeft zich in Nederland nu eenmaal heeft ontwikkeld op basis van een – al of niet juiste – interpretatie, die ook in beleid en toezicht nooit is weersproken. Het is van belang om in de voorgenomen consultatie diepgaand te analyseren welke gevolgen een te maken keuze heeft. Daarbij is niet ondenkbaar dat ervoor verschillende technologieën verschillende gevolgen zijn.

47. De interpretatie van het 'netwerkaansluitpunt' kan, mede gezien het bovenstaande, niet los worden gezien van het verdere regelgevende kader. De toegenomen aandacht voor continuïteit en veiligheid van netwerken en diensten legt verplichtingen op aanbieders die ze moeten kunnen naleven jegens alle klanten. Daarnaast is er druk op innovatie en verbetering van gebruikerservaringen. Oplossingen die een algemene uitrol van nieuwe technologieën zouden bemoeilijken zouden daarmee in strijd geacht moeten worden. Dat kan op detailniveau invloed hebben op de exacte technische niveaus waarop de scheiding tussen infrastructuur en randapparatuur kan worden gelegd.

48. Het kan zijn dat de uitkomst van de consultatie zal zijn dat het netwerkaansluitpunt ligt op een technisch niveau dat thans nog niet apart is gedefinieerd en aangeboden. In dat geval dient er een redelijke termijn in acht te worden genomen om de noodzakelijke voorzieningen te ontwikkelen en uit te rollen.

49. In elk geval dient het Besluit eindapparatuur te worden aangepast in die zin dat alleen apparatuur die voldoet aan de, door de aanbieder bekend gemaakte specificaties, mag worden aangesloten. De Europese regels verzetten zich – anders dan eerder verondersteld – daar niet tegen.

50. De aanbieders beogen met de bovenstaande analyse van het juridisch kader een positieve bijdrage te leveren aan het vraagstuk ten aanzien van het netwerkaansluitpunt. Zoals gesteld zijn de aanbieders zeer bereid om hierover nader in gesprek te treden om eraan bij te dragen dat tot een constructieve en zorgvuldige invulling van het juridische kader zal worden gekomen.

Bijlage 3

Centraal Planbureau

Achterstand Europees aanbod | *Vergroot volume en vertrouwen*

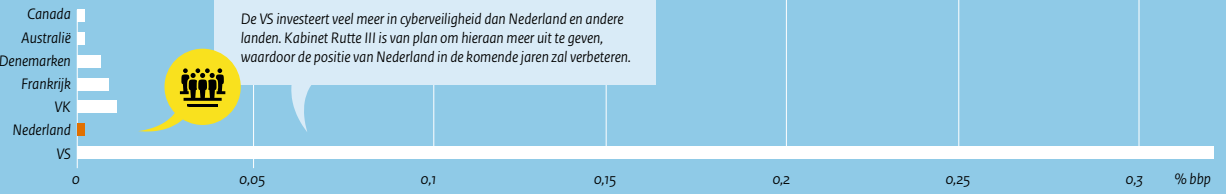
CPB Policy Brief | 2018/01

Knelpunten op de markt voor cyberveiligheid

Bastiaan Overvest
Anne Marieke Braam
Rinske Windig
Emilie Bartels

Knelpunten op de markt voor cyberveiligheid

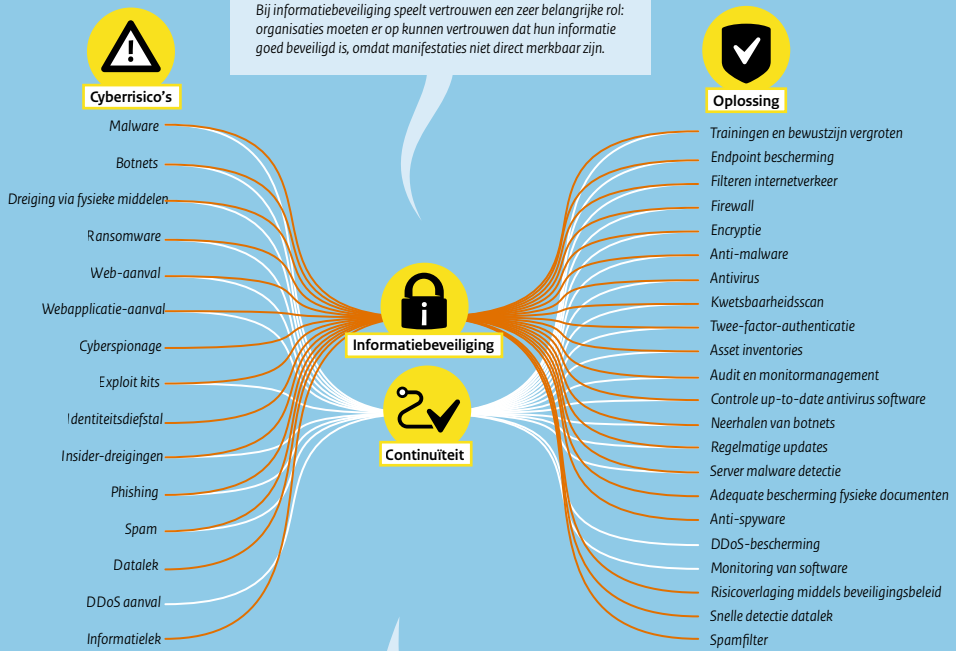
Hoe zorgen we voor een goed functionerende markt voor cyberveiligheid in Nederland en Europa?



De VS investeert veel meer in cyberveiligheid dan Nederland en andere landen. Kabinet Rutte III is van plan om hieraan meer uit te geven, waardoor de positie van Nederland in de komende jaren zal verbeteren.

1 Minder vertrouwen in buitenlandse cyberveiligheidsproducten

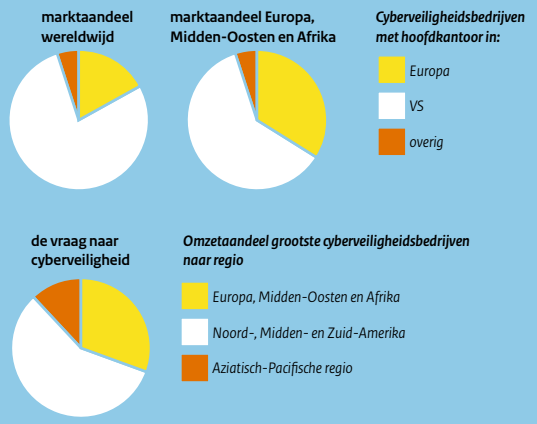
Bij informatiebeveiliging speelt vertrouwen een zeer belangrijke rol: organisaties moeten er op kunnen vertrouwen dat hun informatie goed beveiligd is, omdat manifestaties niet direct merkbaar zijn.



*Cyberdreigingen en oplossingen bestaan grofweg uit twee categorieën: ze vormen een gevaar voor de **informatiebeveiliging** of voor de **continuïteit** van een systeem.*

Er is sprake van informatie-asymmetrie: afnemers weten vaak niet goed welk product of welke dienst het best beschermt door de grote verscheidenheid aan dreigingen en oplossingen.

Deze investeringsvoorsprong vertaalt zich in een dominant marktaandeel van de VS, zowel wereldwijd als in Europa, Midden-Oosten en Afrika. Ook de vraag naar cyberveiligheidproducten is veel groter in de VS. Dat levert schaalvoordeel op. Nederland en andere Europese landen kunnen minder goed gebruik maken van schaalvoordelen.



2 Schaalvoordelen worden niet optimaal benut

Producten en diensten uit de VS kunnen door hun schaalvoordeel een stuk goedkoper zijn. Dit stelt afnemers van hoogwaardige informatiebeveiliging voor een dilemma: kiezen zij voor vertrouwde, nationale maar duurdere aanbieders, of voor goedkopere producten waarvan de betrouwbaarheid moeilijker gecontroleerd kan worden?

Om vertrouwen te vergroten kunnen in Europa (internationale) afspraken worden gemaakt over cyberveiligheid, zoals een digitale variant op de Geneefse Conventies. Hierin kunnen bijvoorbeeld afspraken worden gemaakt over het gebruik van 'zero-days' en achterdeurtjes door inlichtingendiensten.

De bewustwording over cybergevaren, en daarmee de vraag naar cyberveiligheidsproducten, kan worden vergroot door bedrijven bijvoorbeeld een 'cyberveiligheidsparagraaf' in hun jaarverslag te laten opnemen. Een grotere markt stelt Europese cyberveiligheidsbedrijven meer in staat te profiteren van schaalvoordelen.

Samenvatting

In Europa werkt de markt voor cyberveiligheid nog niet optimaal. Het gevolg is dat afnemers de keuze hebben tussen dure, maar gecontroleerde nationale oplossingen en relatief goedkope, maar moeilijk controleerbare buitenlandse producten. Voor een goed functionerende markt zijn er verschillende beleidsrichtingen. Zo kunnen (internationale) afspraken gemaakt worden over cyberveiligheid. Hierbij kan bijvoorbeeld gedacht worden aan afspraken over het gebruik van 'zero-days' en achterdeurtjes. Ook kan de bewustwording en daarmee de vraag naar cyberveiligheidsproducten worden vergroot door bedrijven een 'cyberveiligheidsparagraaf' in hun jaarverslag te laten opnemen.

De belangrijkste twee knelpunten waardoor de markt nog niet optimaal werkt, zijn onvoldoende vertrouwen in het aanbod van buitenlandse cyberveiligheidsbedrijven en onvoldoende mogelijkheden voor Europese aanbieders om schaalvoordelen te creëren. Om het (internationale) vertrouwen te vergroten zijn afspraken nodig over het gedrag van landen in het 'cyberdomein' (IT-netwerken zoals het internet, het telefonienetwerk en gesloten netwerken).

Om schaalvoordelen te creëren, moet de markt voor cyberveiligheid 'volwassen' worden. Hiervoor is meer informatie nodig over de kosten en baten van cyberveiligheid. Dit kan door bedrijven te stimuleren om een 'cyberveiligheidsparagraaf' in hun jaarverslagen op te nemen en door het verzamelen van meer Europese statistieken. Verder is het belangrijk dat de overheid op het terrein van cyberveiligheid een goede opdrachtgever is. Hierbij hoort ook adequaat toezicht op de cyberveiligheid van vitale processen.

Nu ontbreekt vertrouwen in buitenlandse cyberveiligheidsoplossingen. Hierdoor hebben Nederlandse aanbieders soms moeite om over de grens te verkopen. Dit vertrouwenstekort speelt vooral bij afnemers met een behoefte aan hoogwaardige cyberveiligheid. Dit zijn bijvoorbeeld bedrijven die beschikken over gevoelige informatie. Het vertrouwenstekort wordt daarnaast gevoed door incidenten waaruit blijkt dat inlichtingendiensten ook bevriende landen bespioneren. Schaalvoordelen ontbreken in Nederland, en mogelijk in Europa, doordat de markt voor cyberveiligheid hier relatief klein is en later op gang kwam dan in de VS. Het creëren van schaalvoordelen is dan ook nodig om te kunnen concurreren met de grote (met name) Amerikaanse aanbieders. Dit vergroot het vertrouwen in, en de kwaliteit van het Europese cyberveiligheidsaanbod.

De beleidsopties in deze *Policy Brief* kunnen helpen om de markt voor cyberveiligheid beter te laten functioneren. Hierdoor neemt uiteindelijk het algemene niveau van cyberveiligheid toe en kunnen we de economische vruchten van de digitalisering plukken.

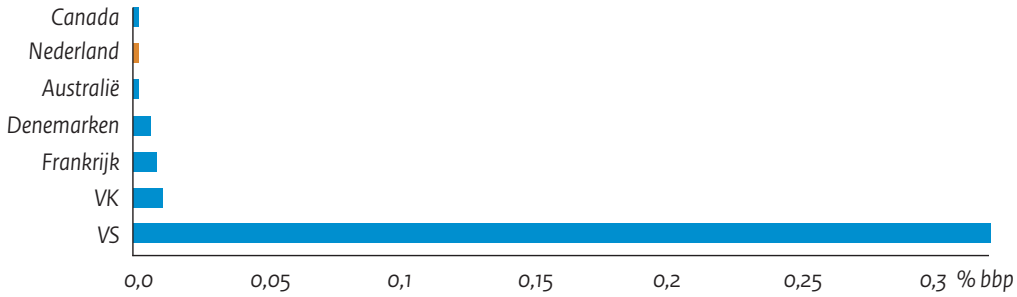
1. Marktwerking voor meer cyberveiligheid

In 2015 berichtte de Nederlandse chipmachinefabrikant ASML te zijn aangevallen door Chinese staatshackers. Hierbij hebben hackers mogelijk bedrijfsgeheimen over nieuwe technologieën buitgemaakt. De economische gevolgen van een hack kunnen groot zijn. Zo legde de gijzelsoftware 'non-Petya' in juni 2017 een containerterminal van AMP Terminals enkele dagen plat. De schade voor het bedrijf liep op tot 300 miljoen dollar.

Deze incidenten laten zien dat ICT kwetsbaar is. Dit is verontrustend, omdat onze economie en dagelijkse levens steeds meer digitaliseren. Digitalisering biedt kansen, maar het potentieel ervan kunnen we alleen optimaal benutten als we weerbaar zijn. Daarvoor moet de markt voor cyberveiligheid goed functioneren.

Hoe goed werkt die markt? Onvoldoende – volgens verschillende recente rapporten. Munnichs et al. (2017) concluderen bijvoorbeeld dat huishoudens, bedrijven en de overheid in Nederland te weinig investeren in cyberveiligheid en dat ze zich onvoldoende bewust zijn van het belang van cyberveiligheid. En Rademaker et al. (2016) wijzen op de relatief lage uitgaven van de Nederlandse overheid (zie figuur 1).

Figuur 1 De Nederlandse overheid investeert relatief weinig in cyberveiligheid



Bron: Rademaker et al. (2016).

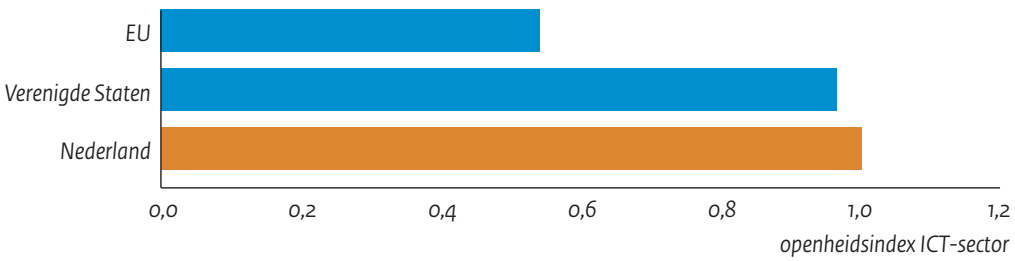
De Nederlandse uitgaven aan cyberveiligheid bedroegen in 2016 0,002 procent van het bbp.[1] In de Verenigde Staten lag dit percentage op 0,3 – hoger dan in een aantal Europese landen.

Momenteel werkt de Europese markt voor cyberveiligheid nog niet optimaal. Dit leidt tot een ongunstige *trade-off* tussen relatief dure maar betrouwbare producten en producten met een gunstige prijs-kwaliteitsverhouding, maar waarvan de betrouwbaarheid lastig te controleren valt. Deze *Policy Brief* geeft inzicht in de knelpunten op de markt voor cyberveiligheid en doet beleidsvoorstellen. Voor dit onderzoek hebben we gesprekken gevoerd met verschillende experts uit zowel het bedrijfsleven als de publieke sector (zie bijlage A).

[1] Overigens is het kabinet Rutte III van plan om hieraan meer uit te geven: structureel 95 miljoen euro vanaf 2021. Hierdoor verbetert de positie van Nederland in de komende jaren.

Daarnaast hebben we de markt in kaart gebracht op basis van cijfers uit jaarverslagen van de 21 grootste cyberveiligheidsaanbieders.

Figuur 2 ICT-sectoren Europese landen over het algemeen geslotener dan in de VS



Bron: UNCTAD World Development Indicators, bewerking CPB. NB. De figuur geeft de mate van openheid per land van de ICT-sector, gecorrigeerd voor de omvang van de economie en de openheid van andere sectoren in het land volgens de *Relative Comparative Advantage* maatstaf van Vollrath (1991).

Op basis van de gesprekken en onze eigen analyse hebben we zes mogelijke knelpunten geïdentificeerd: 1) handelsbarrières, 2) onvoldoende ICT-afgestudeerden, 3) onvoldoende bewustwording van cyberveiligheidsrisico's, 4) ongunstige randvoorwaarden, 5) onvoldoende mogelijkheden om schaalvoordelen te creëren, 6) onvoldoende vertrouwen in (met name) buitenlands aanbod. Als fundamentele knelpunten zien we *onvoldoende vertrouwen* en *onvoldoende schaal*.

Handelsbarrières, zoals importheffingen, kunnen een hindernis vormen voor de internationale markt voor cyberveiligheid. Specifiek voor cyberveiligheid kan het Wassenaar Arrangement een barrière vormen. Volgens deze regeling is voor producten zowel civiel als militair gebruikt kunnen worden (*dual-use*) een exportvergunning nodig. Hieronder vallen ook sommige cyberveiligheidsproducten. In de gesprekken met experts werden dergelijke handelsbarrières echter niet als knelpunt gezien.[2] Dit beeld wordt bevestigd door figuur 2.**Error! Reference source not found.** Deze geeft voor de VS, de EU en Nederland de relatieve openheid van de ICT-sector weer. Nederland heeft een relatief open ICT-sector. Opvallend is dat de EU als geheel in vergelijking met de VS een gesloten ICT-sector heeft.

Een veelgenoemd knelpunt in de gesprekken met experts is een tekort aan ICT- of cyberveiligheidsafgestudeerden. Dit knelpunt hangt samen met het feit dat de grootste werkgevers voor deze afgestudeerden in de VS (*Silicon Valley*) en, in toenemende mate, in Duitsland (zoals het *Helmholtz-Zentrum für IT-Sicherheit*) zitten. Deze grote organisaties bieden hogere salarissen en hebben meer ontwikkelingsmogelijkheden dan relatief kleine Nederlandse organisaties. Een tekort aan ICT'ers *an sich* lijkt daarom niet het probleem. Ook veel genoemd is een gebrek aan '*awareness*'. Het Nederlandse mkb zou bijvoorbeeld cyberveiligheidsrisico's te laag inschatten. Uiteindelijk beperkt dit de vraag naar cyberveiligheid. Paragraaf 3 gaat dieper in op de vraagzijde. Verder zijn volgens experts de randvoorwaarden voor startende (cyberveiligheids-)bedrijven in Nederland relatief

[2] Door beveiligingsonderzoekers wordt het Wassenaar Arrangement wel gezien als barrière bij het internationaal delen van kennis over softwarekwetsbaarheden.

ongunstig. Voor deze bedrijven is er bijvoorbeeld te weinig financiering beschikbaar in de vorm van durfkapitaal om een goede start te maken.[3] Goede randvoorwaarden zijn belangrijk voor een dynamisch ondernemingsklimaat, maar niet specifiek voor cyberveiligheid en komen daarom in dit stuk verder niet aan de orde.

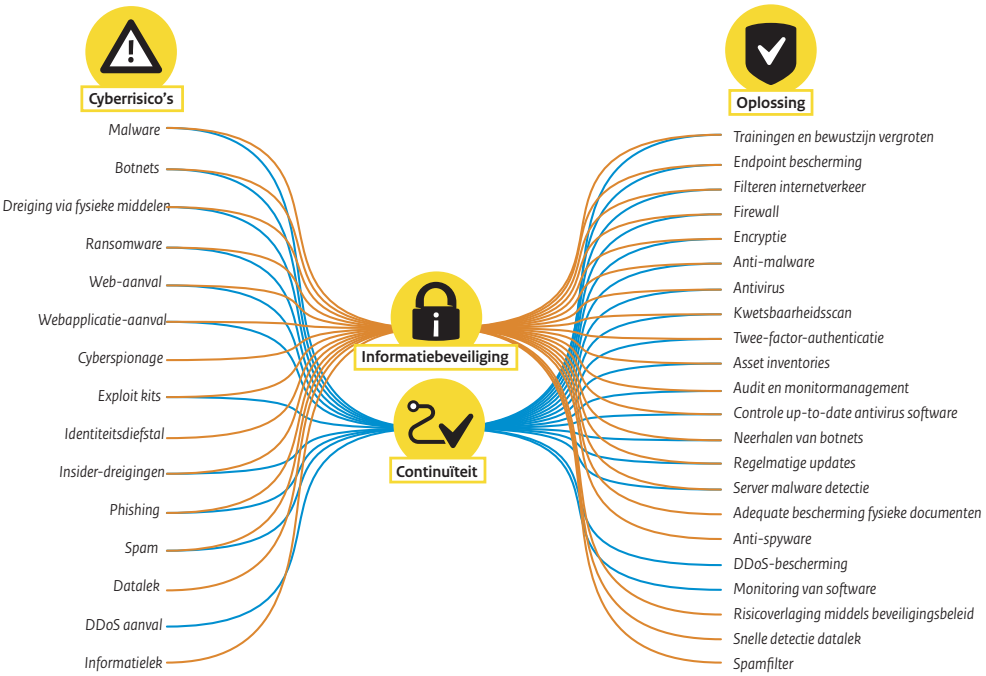
Om de markt voor cyberveiligheid beter te laten functioneren, zou het beleid zich meer kunnen richten op de twee fundamentele knelpunten: vergroten van het (internationale) vertrouwen in het cyberveiligheidsaanbod en creëren van schaal aan de aanbodzijde. Het internationale vertrouwen kan omhoog door afspraken te maken over statelijke verantwoordelijkheden en bevoegdheden. Ook kan gedacht worden aan een evaluatie van het Nederlandse certificeringssysteem voor hoogwaardige oplossingen (zoals beveiliging van staatsgeheimen) en een verdere harmonisatie van Europese certificeringssystemen. De mogelijkheden om schaal te creëren kunnen worden vergroot door te zorgen voor een maatschappelijk optimale vraag naar cyberveiligheid. Dit kan via goed opdrachtgeverschap van de overheid[4] en een stevig toezicht op de cyberveiligheid van vitale processen. Daarnaast kunnen bedrijven meer openheid geven in een ´cyberparagraaf´ in het jaarverslag.

2. Het belang van vertrouwen

Het vertrouwen in buitenlandse cyberveiligheidsoplossingen is soms laag – vooral als het om de staatsveiligheid gaat. Zo verbood de Amerikaanse overheid in september 2017 het gebruik van Russische beveiligingssoftware vanwege twijfels over de betrouwbaarheid. Ook zou de Amerikaanse inlichtingendienst NSA in Europa hebben gespioneerd, waaronder bij kanselier Angela Merkel en vliegtuigbouwer Airbus.[5] Dit soort incidenten vergroten de behoefte aan betrouwbare cyberveiligheidsoplossingen, liefst uit eigen land. Uit onze gesprekken met experts komt vertrouwen dan ook naar voren als een belangrijk knelpunt. Zonder buitenlands vertrouwen houdt voor Europese cyberveiligheidsbedrijven de groei op bij de landsgrens.

[3] Ook in Nederland is er durfkapitaal voor cyberveiligheidsbedrijven. In november 2017 werd bekend dat EclecticIQ een injectie kreeg van 14 miljoen euro. Straathof en Van Veldhuizen (2015) laten zien dat het volume van de Nederlandse durfkapitaalinvesteringen sinds 2010 sterk stijgt.
[4] Zie ook VKA/SEO (2016) voor suggesties rondom opdrachtgeverschap van de overheid.
[5] Zie bijvoorbeeld dit artikel in de Volkskrant.

Figuur 3 Cyberdreigingen en oplossingen



NB. De lijst van dreigingen en mogelijke oplossingen komt uit ENISA Threat Landscape Report 2016.

Op de markt voor cyberveiligheid bieden cyberveiligheidsbedrijven diverse oplossingen aan voor allerlei cyberdreigingen (zie figuur 3). Cyberdreigingen vormen een gevaar voor informatiebeveiliging en/of de continuïteit van de ICT van een afnemer.

In hoeverre vertrouwen voor een afnemer een rol speelt, is afhankelijk van meerdere factoren. Ten eerste is het belang van vertrouwen extra groot bij informatiebeveiliging, omdat het soms maanden of jaren kan duren voordat een informatielek wordt ontdekt, als het al wordt ontdekt. Dit in tegenstelling tot een verstoring van de continuïteit van een bedrijf – dat is meestal wel direct merkbaar. Wanneer er geen direct signaal is, is het belangrijk dat organisaties vertrouwen hebben dat de informatie goed is beveiligd.

Ten tweede verschilt het belang van vertrouwen per type afnemer. Voor sommige afnemers is de te beveiligen informatie bijzonder gevoelig of kostbaar. Denk hierbij aan staatsgeheimen of waardevolle *know-how*. Ook de continuïteit van systemen is soms essentieel. Bijvoorbeeld voor een vitaal proces als het betalingsverkeer, of de levering van stroom. Niet alleen zijn de behoeftes van deze afnemers anders dan van het gemiddelde huishouden, ook het dreigingsniveau verschilt per type gebruiker. Zo is een organisatie met gevoelige of verhandelbare informatie een aantrekkelijk doelwit voor een gerichte aanval. Deze afnemers hebben dus behoefte aan hoogwaardige cyberveiligheid. Tussen deze 'hoogwaardige' afnemers van cyberveiligheid en aanbieders speelt vertrouwen een essentiële rol.

Een gebrek aan vertrouwen hangt daarnaast samen met een gebrek aan informatie. Op de markt voor cyberveiligheid is sprake van informatieasymmetrie: Afnemers hebben meestal minder informatie over nut en noodzaak van een product dan aanbieders. Daarnaast is het verschil in beveiligingsniveau tussen producten voor afnemers moeilijk in te schatten. Een mogelijk gevolg van deze 'averechtse selectie' is dat alleen de goedkoopste aanbieders met de laagste kwaliteit overblijven – een *lemons market*. Aan de aanbodzijde bestaat het risico op moreel gevaar. Een buitenlands cyberveiligheidsbedrijf kan in het geheim samenwerken met een inlichtingendienst, of met een concurrent van de afnemer. In verschillende landen zijn bedrijven en burgers immers al verplicht om, al dan niet heimelijk, medewerking te verlenen aan inlichtingendiensten.

Afnemers en aanbieders gaan op verschillende manieren om met het vertrouwenstekort. Nationale overheden kunnen voor bepaalde producten controles verplichten of producten uit verdachte landen weren. In Nederland worden cyberveiligheidsproducten beoordeeld door de AIVD en de MIVD. Andere landen hebben vergelijkbare controles. Ook kunnen overheden controles en beperkingen instellen voor IT-bedrijven en voor de handel in veiligheidsproducten. De *International Traffic in Arms Regulations* (ITAR) en de *Export Administration Regulations* (EAR) zijn voorbeelden van Amerikaanse wetgeving voor import en export van veiligheidsproducten. In Duitsland kan de overheid een buitenlandse deelname van meer dan 25 procent in een IT-bedrijf blokkeren, met het *Außenwirtschaftsgesetz*. In Nederland gaan ook stemmen op voor een dergelijke wet sinds de overname van Fox-IT door een Brits bedrijf in 2015, maar deze wet bestaat nog niet. Een andere mogelijkheid is om zelf cyberveiligheidsoplossingen te (laten) ontwikkelen. In Nederland gebeurt dat sinds 2012 via de 'Small Business Innovation Research' regeling.[6] Het Verenigd Koninkrijk stimuleert bijvoorbeeld via *grand challenges* nieuwe cyberveiligheidsoplossingen[7] en in Duitsland wordt een groot onderzoekscentrum voor cyberveiligheid opgericht.

Aanbieders kunnen het vertrouwenstekort tegengaan door meer transparantie of zekerheden te bieden. Kaspersky heeft bijvoorbeeld in september 2017 aangeboden om voor het Amerikaanse Congres te getuigen en de software te laten controleren.[8] En Apple verklaarde in 2016 niet mee te werken aan een FBI-verzoek over het ontgrendelen van een iPhone van een terrorist. In Rusland weigerde chatapp Telegram publiekelijk medewerking aan de Russische inlichtingendienst FSB. Microsoft, als laatste voorbeeld, heeft een Duits cloudcentrum ondergebracht bij Deutsche Telekom. Hierdoor kan Microsoft niet of moeilijker meewerken aan Amerikaanse informatieverzoeken. Ook kunnen bedrijven investeren in het laten certificeren van hun producten. Een andere mogelijkheid is het onder opensource-licentie uitbrengen van technologie.

Uiteindelijk kan het vertrouwenstekort gevolgen hebben voor de markt voor cybersecurity als geheel. Als kwaliteit niet zichtbaar is, loont het voor aanbieders niet om te investeren in

[6] Zie bijvoorbeeld dit bericht van dcypher.
[7] Zie de National Cyber Security Strategy van het VK.
[8] Zie dit nieuwsbericht van Kaspersky.

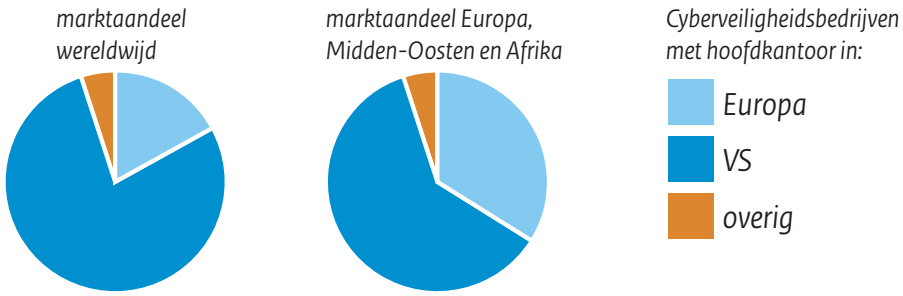
veiligere ICT-producten. Als binnenlandse aanbieders meer vertrouwd worden dan buitenlandse aanbieders, brengt dat een concurrentienadeel met zich mee voor cyberveiligheidsbedrijven met internationale ambities. Europese cyberveiligheidsbedrijven met een product waarbij vertrouwen essentieel is, kunnen dus relatief minder groeien. De markt voor dat type hoogwaardige oplossingen is dan mogelijk nationaal.

Een oplossing voor deze problemen ligt in het vergroten van het internationale vertrouwen in het cyberveiligheidsaanbod. Dit is vooral belangrijk voor producten waarbij vertrouwen een grote rol speelt, zoals technologie die gebruikt wordt voor staatsgeheimen, continuïteit van vitale processen en waardevolle bedrijfsgeheimen. Internationale afspraken over gedrag en taken van landen in het cyberdomein helpen hierbij. Deze en andere opties worden verder uitgewerkt in paragraaf 4.

3. Het belang van schaal

Als (internationaal) vertrouwen het belangrijkste knelpunt is, dan leidt dit tot nationaal afgebakende markten. Dat zien we echter niet. De helft van de grootste cyberveiligheidsbedrijven komt uit de Verenigde Staten. Het wereldwijde marktaandeel van Amerikaanse bedrijven is maar liefst 78 procent (zie figuur 4). Europese cyberveiligheidsbedrijven hebben een aandeel van 17 procent wereldwijd – en in Europa, het Midden-Oosten en Afrika 34 procent. Hoe kan het dat Amerikaanse bedrijven de internationale markt voor cyberveiligheid zo beheersen?

Figuur 4 De Verenigde Staten domineren de markt voor cyberveiligheid



NB. De figuur laat het marktaandeel zien van cyberveiligheidsbedrijven uit Europa, de VS en overige economieën. Het marktaandeel is weergegeven voor de wereldwijde markt en voor EMEAR (Europa, Midden-Oosten en Afrika). Marktaandelen zijn berekend met gegevens uit jaarverslagen van de 21 grootste aanbieders.[9] Cijfers zijn voor 2016 of meest recent beschikbaar.

[9] Deze lijst is samengesteld op basis van de concurrentieanalyse uit jaarverslagen, de Cybersecurity 500, een besluit van de Europese Commissie, en Worldwide Endpoint Security 2010-2014 Forecast. 'Multiple product' bedrijven waarbij het cyberveiligheidsaandeel niet is gespecificeerd, zijn weggelaten.

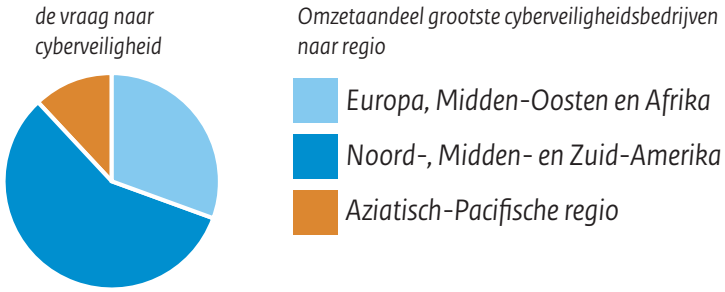
Het korte antwoord is: schaal.[10] Een bedrijf heeft schaalvoordelen als de gemiddelde kosten lager zijn naarmate het meer produceert. Software en digitale platformen zijn voorbeelden van producten met schaalvoordelen. De marginale productiekosten voor een softwarekopie zijn namelijk bijna nul. Ook bij cyberveiligheidsoplossingen – zoals antivirussoftware, monitoringsdiensten en gegevensbeheersystemen – zijn schaalvoordelen daarom belangrijk. Een extra reden waarom grotere bedrijven een voordeel hebben, is dat afnemers erop willen vertrouwen dat een aanbieder tijdens een crisissituatie voldoende menskracht heeft. Op zo'n markt kan slechts een handvol grote bedrijven overleven.

Waarom slagen Europese bedrijven er minder goed in om schaalvoordelen te creëren? Dit heeft meerdere oorzaken. Ten eerste hebben de Verenigde Staten een voorsprong: de ICT-sector is daar groter en de vraag naar cyberveiligheid kwam daar eerder op gang. Op het gebied van wetgeving in de ICT-sector zijn de Verenigde Staten ook een voorloper. Bedrijven zijn al vanaf 2003 wettelijk verplicht om een datalek te melden, terwijl in Nederland deze generieke verplichting er sinds 2016 is. Vanaf 25 mei 2018 gaat de Algemene verordening gegevensbescherming (AVG) in, waarmee in elke EU-lidstaat een meldplicht geldt.

Ten tweede is de Amerikaanse thuismarkt groter. De economieën in de afzonderlijke Europese lidstaten zijn kleiner dan de Amerikaanse economie. Cyberveiligheidsbedrijven in de VS kunnen daardoor laagdrempeliger groeien en schaalvoordelen behalen, zonder het product te moeten aanpassen.

Een derde verklaring is dat de vraag naar cyberveiligheid in de Verenigde Staten groter is. Figuur 1 laat al zien dat de Amerikaanse overheid daar relatief veel aan uitgeeft. En de omzet van de grootste cyberveiligheidsbedrijven wordt voor het grootste deel behaald in de "AMER"-regio; meer dan op basis van bbp verwacht mag worden (figuur 5).

Figuur 5 Vraag cyberveiligheid relatief hoog in Noord- en Zuid-Amerika



NB. Het diagram geeft het volumeaandeel van de top 21 cyberveiligheidsbedrijven in drie economische regio's.

Waarom de vraag naar cyberveiligheid in de Verenigde Staten groter is, kan ten eerste verklaard worden door de verschillen in wetgeving. Denk bijvoorbeeld aan het Amerikaanse productaansprakelijkheidsrecht. Deze verschillen leiden niet zozeer tot handelsbarrières, maar tot verschillen in omvang van de vraag. Ten tweede ervaren de Verenigde Staten (maar

[10] Ook VKA/SEO (2016), p. 53, wijst op het belang van schaalgrootte.

ook Israël) mogelijk een hoger dreigingsniveau dan Nederland en andere Europese landen. Amerikaanse overheden en bedrijven verwachten of ervaren bijvoorbeeld dreiging vanuit Noord-Korea, Rusland of terroristische groepen. De defensie-uitgaven van de VS zijn met 3,3 procent bbp dan ook hoger dan in Nederland of Duitsland (beide 1,2 procent bbp). Ten derde kan de vraag in Europa relatief laag zijn als ICT-gebruikers binnen huishoudens, bedrijven en overheden de cyberrisico's te laag inschatten. Vaak wordt het mkb gezien als een (te) weinig digitaal bewuste sector – cijfers die dit kunnen onderbouwen, zijn er echter nog niet. Mogelijk verandert dit met de Algemene verordening gegevensbescherming (AVG) die bedrijven dwingt om digitale (persoons-)gegevens goed te beveiligen.

De Amerikaanse 'dominantie' heeft belangrijke gevolgen voor de markt. Het grootste deel van de wereldwijde omzet komt namelijk bij Amerikaanse bedrijven terecht. Uit de gesprekken kwam naar voren dat zij hierdoor innovatiever zijn en gemiddeld een hogere kwaliteit kunnen bieden. Europese aanbieders hebben veelal onvoldoende schaal, waardoor ze relatief duur zijn en maar een beperkt aantal producten kunnen aanbieden. Voor grotere afnemers zijn deze kleine cyberveiligheidsbedrijven bovendien minder aantrekkelijk vanwege hun beperkte capaciteit.

Een ander gevolg van de verschillen in schaalgrootte is dat talent wegtrekt. Grote cyberveiligheidsbedrijven en kennisinstellingen zitten vooral in de Verenigde Staten, maar ook steeds meer in het Verenigd Koninkrijk of Duitsland. Deze organisaties bieden doorgaans hogere salarissen en betere opleidingsmogelijkheden dan kleine Nederlandse cyberveiligheidsbedrijven.

De twee knelpunten van vertrouwen en schaal samen hebben gevolgen voor de Nederlandse markt. De vraagzijde, en dan vooral afnemers met een hoogwaardige behoefte, staan namelijk voor een ongemakkelijke keuze: tussen enerzijds vertrouwde, maar relatief dure, nationale producten en anderzijds ogenschijnlijk kwalitatief hoogwaardige en gunstig geprijsde producten met onzekerheid over de betrouwbaarheid. Deze *trade-off* leidt tot een segmentering van de markt: hoe gevoeliger of hoogwaardiger de vraag, hoe hoger het marktaandeel van nationale aanbieders zal zijn.

Een vergroting van de vraag stelt Nederlandse cyberveiligheidsbedrijven in staat om schaalvoordelen te creëren. Of de vraag momenteel 'te laag' is weten we niet. Wel zijn er aanwijzingen dat de vraagzijde nog niet volwassen is. Meer informatie voor ICT-gebruikers over cyberrisico's vergroot mogelijk de vraag. Ook kan de vraag worden vergroot wanneer de overheid meer doet om cyberveiligheid van de eigen organisatie en van vitale processen te borgen.

4. Beleidsopties

Voor een goede werking van de markt voor cyberveiligheid zijn voldoende *schaal* en *vertrouwen* essentieel. Als de marktvraag onvoldoende volwassen is en als het vertrouwen in

buitenlandse producten (al dan niet terecht) ontbreekt, ontstaan onnodige risico's voor gebruikers van ICT en voor vitale processen die van ICT afhankelijk zijn.

Het huidige beleidspakket zorgt al grotendeels voor meer schaal en vertrouwen. Zo vergemakkelijkt de EU-Dienstenrichtlijn grensoverschrijdende dienstverlening en stimuleert de AVG organisaties om veilig met (digitale) persoonsgegevens om te gaan. Verder schrijft de Europese NIB-richtlijn beveiligingsvereisten voor, die momenteel worden omgezet naar nationaal recht met het wetsvoorstel voor de Cybersecuritywet. We zien een aantal opties om de markt nog beter te laten werken:

1. Maak internationale afspraken over statelijke verantwoordelijkheden en bevoegdheden in het cyberdomein.
2. Harmoniseer het Europese certificeringssysteem.
3. Evalueer het Nederlandse certificeringssysteem.

Om Nederlandse en andere Europese cyberveiligheidsbedrijven in staat te stellen om schaalvoordelen te creëren, zien we deze beleidsopties:

4. Stimuleer het opnemen van een 'cyberparagraaf' in jaarverslagen.
5. Verzamel Europese statistieken over cyberveiligheid bij bedrijven.
6. Vergroot cyberexpertise bij de overheid.
7. Denk goed na over benodigde kennis en producten ('vraagarticulatie').
8. Zorg voor een cyberveilige digitale overheidsinfrastructuur. Bijvoorbeeld via 'security by design' en/of als gunningscriterium bij de aanbesteding.
9. Zorg voor goede afstemming en organisatie van het toezicht op cyberveiligheid van vitale processen.

Deze beleidsopties helpen om de markt voor cyberveiligheid beter te laten werken. Positieve gevolgen daarvan zijn dat Nederlandse cyberveiligheidsbedrijven meer mogelijkheden krijgen om (internationaal) door te groeien. Ook krijgt de vraagzijde meer keuze, waardoor het algemene niveau van cyberveiligheid kan toenemen.

De negen opties worden hieronder verder uitgewerkt.

Ad 1) Het internationale vertrouwen kan worden vergroot door afspraken over de bevoegdheden en werkwijze van inlichtingen- en opsporingsdiensten in het cyberdomein. Hierbij kan worden gedacht aan een EU-standpunt over encryptie en de voorwaarden waaronder inlichtingen- en opsporingsdiensten digitaal onderzoek mogen doen. Staan we bijvoorbeeld toe dat inlichtingendiensten 'zero-days' (weeffoutjes in software die onbekend zijn bij de leverancier en waardoor digitaal kan worden ingebroken) of achterdeurtjes (bewust ingebouwde technieken om bijvoorbeeld een wachtwoord te omzeilen) in software mogen gebruiken? Afspraken hierover kunnen ook, als begin, bilateraal worden gemaakt of opgesteld als niet-bindende principes.[11] Om de naleving van internationale afspraken te

[11] Een voorbeeld van niet-bindende regelgeving is de Tallinn-handleiding. Deze bevat een richtinggevende analyse van de toepassing van het internationaal recht op het cyberdomein.

borgen kan een onafhankelijke autoriteit worden ingesteld – zoals de OPCW (chemische wapens) en de IAEA (atoomenergie).

Ad 2 en 3) Veel landen kennen een certificeringssysteem voor cyberveiligheidsproducten die zij gebruiken voor de bescherming van staatsgeheimen of defensiemiddelen. In Nederland worden cyberveiligheidsproducten beoordeeld door de AIVD en de MIVD. Het is belangrijk dat dit systeem goed werkt. Een strenge (en mogelijk langdurige) beoordeling voorkomt dat onbetrouwbare producten gebruikt worden, maar heeft ook het risico dat gebruikers van nuttige producten lang moeten wachten of dat het product technologisch achterhaald is op het moment dat de goedkeuring er is. Een goed certificeringssysteem maakt de maatschappelijk optimale afweging tussen deze voor- en nadelen.

Het zou nuttig zijn om te evalueren hoe de afweging tussen betrouwbaarheid en tijdigheid in het Nederlandse systeem wordt gemaakt. Hierbij kan ook worden gekeken naar aspecten als de toelating tot de beoordeling, de vergoeding van de kosten en de termijn waarbinnen het onderzoek is afgerond.

Een andere route is om het Europese stelsel van certificering verder te harmoniseren. Lidstaten vertrouwen nu vooral op eigen controles.[12] Als hetzelfde product meermaals gecertificeerd moet worden, en op steeds weer een andere manier, brengt dat extra kosten met zich mee. En als een bedrijf erin slaagt om een buitenlandse goedkeuring te krijgen betekent dat niet dat het product ook gekocht zal worden. De internationale effectiviteit van het certificeringssysteem kan worden vergroot door verdergaande harmonisatie.[13] Hierbij kan worden gedacht aan uniforme producteisen, een open toegang en, uiteindelijk, een 'Single Passport' – zoals dat al bestaat voor de bancaire sector op de Interne Markt.

Ad 4) Bedrijven zijn huiverig om openheid te geven over cyberincidenten. Om bedrijven aan te zetten tot meer transparantie kan overwogen worden om een 'cyberparagraaf' in het jaarverslag verplicht te stellen. In zo'n paragraaf geeft het bedrijf inzicht in de maatregelen die zijn genomen om cyberrisico's in te perken en welke incidenten zich hebben voorgedaan. Dit vergroot niet alleen het maatschappelijke inzicht in de cyberveiligheid, maar zet bedrijven er ook toe aan om bewust na te denken over cyberrisico's en interne maatregelen te nemen. Meer informatie over cyberveiligheid kan de vraag naar cyberveiligheid vergroten, waardoor uiteindelijk schaal wordt gecreëerd.

Op grond van de Wet gegevensverwerking en meldplicht cybersecurity zijn bedrijven die een vitaal proces aanbieden, verplicht om bij het Nationaal Cyber Security Centrum (NCSC) melding te doen van ernstige cyberincidenten. Deze meldingen helpen het NCSC om haar coördinerende en hulpverlenende rol goed in te vullen.

Ad 5) Op het niveau van bedrijven en overheden zijn geen cijfers over de frequentie en de aard van cybercriminaliteit en de kosten en baten van cyberveiligheidsmaatregelen beschikbaar. Om deze kennislacune op te vullen kan meer en gerichter statistisch onderzoek

[12] Het Verenigd Koninkrijk kent bijvoorbeeld de 'Commercial Product Assurance' en Frankrijk de Certification Sécuritaire de Premier Niveau.
[13] De Europese Commissie kondigde in september 2017 hiervoor voorstellen aan. [link]

gedaan worden. Het is wenselijk om dit voor een langere periode en op Europees niveau te doen. Het onderzoek kan niet alleen worden uitgevoerd onder bedrijven en huishoudens, maar ook via uitvragen bij cyberverzekeraars of ISACS (samenwerkingsverbanden tussen organisaties om informatie uit te wisselen). Beter statistisch onderzoek helpt bovendien om na te gaan in hoeverre de bewustwording binnen de samenleving onvoldoende is.

Ad 6, 7 en 8) Een aanbeveling voor goed opdrachtgeverschap door de overheid op het terrein van cyberveiligheid komt voort uit drie beleidsopties: 'Vergroot cyberexpertise bij de overheid', 'Denk goed na over benodigde kennis en producten (vraagarticulatie)' en 'Zorg voor een cyberveilige digitale overheidsinfrastructuur'. De overheid is een van de grootste vragers van ICT en zou daarom ook een van de grootste vragers moeten zijn van cyberveiligheidsoplossingen. Om een goede opdrachtgever te zijn, is voldoende kennis vanuit de overheid noodzakelijk. Deze expertise kan vervolgens worden ingezet om een duidelijke visie op te stellen en na te denken over welke kennis, diensten of producten nodig zijn; ook wel de vraagarticulatie genoemd. Verschillende ministeries zijn hier nu al actief mee bezig en hebben een 'Strategische Kennis- en Innovatieagenda' (SKIA) opgesteld, waarin onder andere de visie op veiligheid staat beschreven.[14]

De vraagarticulatie helpt vervolgens om doelgericht op een passende manier kennis of kunde in te kopen of zo nodig te laten ontwikkelen.[15] Bij het ontwikkelen van nieuwe producten kan gedacht worden aan instrumenten als SBIR, PCP of een innovatiepartnerschap.[16] Als ICT-diensten worden ingekocht dan is het belangrijk om al in een vroeg stadium na te denken over de cyberveiligheid. Bijvoorbeeld door te eisen dat het in te kopen product '*by design*' veilig is of door cyberveiligheid als expliciet criterium te laten meewegen bij de gunning[17]. Ook is het soms wenselijk om meerdere producten kleinschalig naast elkaar te testen.[18]

Ad 9) De cyberveiligheid van de vitale processen (zoals elektriciteits- en drinkwatervoorziening, of betalingsverkeer) is essentieel voor het goed functioneren van de maatschappij. Vitale bedrijven zijn in eerste instantie zelf verantwoordelijk voor hun cyberveiligheid. Het toezicht op de cyberveiligheid zal (volgens het wetsvoorstel Cybersecuritywet) sectoraal bij bestaande toezichthouders worden belegd. Het risico dat kan ontstaan, is dat vitale bedrijven onvoldoende investeren in cyberveiligheid en dat de sectorspecifieke toezichthouders dat onvoldoende zien of kunnen bijsturen, met als gevolg dat potentiële schaalvoordelen onbenut blijven.

Om dit risico te beperken hebben sectorale toezichthouders kennis en informatie nodig. Deze expertise kan worden opgebouwd door het aantrekken van cyberdeskundigen en door samenwerking met het NCSC en sectorspecifieke toezichthouders. Hierbij kan gedacht worden aan een werkgroep van toezichthouders en de publicatie van formele afspraken tussen het NCSC en toezichthouders. Zulke afspraken kunnen bijvoorbeeld duidelijk maken welke informatie wél en welke vooral níet gedeeld wordt.

---

[14] Zie bijvoorbeeld de SKIA's van het ministerie van Defensie en van Justitie en Veiligheid.
[15] Zie Van Elk et al. (2017) voor een kader voor doelgericht onderzoeksbeleid.
[16] De site van Pianoo geeft meer informatie over innovatiegericht inkopen.
[17] Een klassiek voorbeeld van hoe het mis kan gaan, is 'Diginotar'.
[18] Bij technologische onzekerheid en padafhankelijkheid is het optimale beleid een combinatie van vroegtijdig ingrijpen en ruimte voor experimenten. Zie Bijlsma et al. (2016).

Bijlage A Gesprekspartners

Naam	Organisatie	Functie
Hans de Vries	Nationaal Cyber Security Centrum	Directeur
Hans van Loon	Van Loon Cyber	Strategy & business consultant
Hoi Wah Yip	AON	Manager
Jeremy Maginot	AON	Director
Mark Buningh	AON	Cyber Risk Practice Leader
Thijs de Boer	AON	Strategy director
Jan Piet Barthel	dcypher	Directeur
Kas Clark	Nationaal Cyber Security Centrum	Senior onderzoeker
Lars van Willigen	Ministerie van Economische Zaken	Beleidsadviseur
Maarten van Wieren	Deloitte	Senior manager
Maxwell Keyte	CapGemini	Lead cybersecurity
Michel Rademaker	The Hague Centre for Strategic Studies	Deputy director
Muhittin Hasancioglu	Shell	Vice president
Petra van Schayik	Compumatica	CEO
Sjoerd Peerlkamp	Alliander	CISO
Tim van Essen	Ministerie van Buitenlandse Zaken	Beleidsadviseur
Yori Kamphuis	CoBlue	Chief business development officer
Philip Meijer	Innovation Quarter	Account manager safety & security
Eric van Pelt	Netherlands Foreign Investment Agency	Senior project manager
Richard Franken	The Hague Security Delta	Directeur
Nathalie Falot	Considerati	Senior legal consultant
Marcel van Oirschot	Fox-IT	Commercieel directeur

Bijlage B Overzicht cybersecurity bedrijven

Bedrijfsnaam	Hoofdvestiging	Omzet (in mln.$)	Marktaandeel (%)
BAE Systems	Verenigd Koninkrijk	1.601,10	3,69
Booz Allen Hamilton	Verenigde Staten	5.804,28	13,38
CA Technologies	Verenigde Staten	4.036,00	9,30
Check Point Software Technologies	Israël	1.740,30	4,01
Cisco Systems	Verenigde Staten	1.969,88	4,54
CyberArk	Verenigde Staten	216,60	0,50
FireEye	Verenigde Staten	714,11	1,65
F-Secure	Finland	158,29	0,36
IBM Security	Verenigde Staten	7.192,71	16,57
Intel	Verenigde Staten	2.375,48	5,47
Kaspersky Lab	Rusland	644,00	1,48
Mimecast	Verenigd Koninkrijk	186,60	0,43
NCC Group	Verenigd Koninkrijk	241,90	0,56
Palo Alto Networks	Verenigde Staten	1.761,60	4,06
Rapid7	Verenigde Staten	157,44	0,36
Raytheon	Verenigde Staten	561,00	1,29
SecureWorks	Verenigd Koninkrijk	262,13	0,60
Sophos	Verenigd Koninkrijk	407,87	0,94
Symantec	Verenigde Staten	4.019,00	9,26
Thales	Frankrijk	8.186,75	18,87
Trend Micro	Japan	1.159,06	2,67

NB. * jaarverslag 2016, ** jaarverslag 2017. Sommige bedrijven zijn actief op meer markten dan alleen die voor cyberveiligheid: BAE Systems heeft een onderdeel *Cyber & Intellegence* (9%); Booz Allen Hamilton heeft *Cyber* als een van de vijf onderdelen; CA Technologies heeft de onderdelen *Mainframe Solutions* (54%), *Enterprise Solutions* (38%) en *Services* (8%) waar cyberveiligheid allemaal onder valt; Check Point Software Technologies is nagenoeg volledig gericht op cyberveiligheid; Cisco Systems heeft een onderdeel *Security* (4%); CyberArk is nagenoeg volledig gericht op cyberveiligheid; FireEye is nagenoeg volledig gericht op cyberveiligheid; F-Secure is nagenoeg volledig gericht op cyberveiligheid; IBM Security heeft een onderdeel *Cognitive Solutions* waar cyberveiligheid onder valt (12%); Intel heeft de *Data Center Group* (55%) en de *Security Group* (4%) waar cyberveiligheid onder valt; Kaspersky Lab is nagenoeg volledig gericht op cyberveiligheid; Mimecast is nagenoeg volledig gericht op cyberveiligheid; NCC Group is nagenoeg volledig gericht op cyberveiligheid; Palo Alto Networks is nagenoeg volledig gericht op cyberveiligheid; Rapid7 is nagenoeg volledig gericht op cyberveiligheid; Raytheon heeft het onderdeel *Forcepoint* waar cyberveiligheid onder valt (6%); SecureWorks is nagenoeg volledig gericht op cyberveiligheid; Sophos biedt hardware (20%), cyberveiligheidsproducten (77%) en overige diensten (3%) aan; Symantec is nagenoeg volledig gericht op cyberveiligheid; Thales heeft het onderdeel *Defence & Security* (55%) waar cyberveiligheid onder valt; Trend Micro is nagenoeg volledig gericht op cyberveiligheid.

Literatuur

Bijlsma, M., B.M. Overvest en S.M. Straathof, 2016, Marktordening bij nieuwe ICT-toepassingen, CPB Policy Brief.

Elk, R.A. van, A.M. Braam, B.M. Overvest en S.M. Straathof, 2017, Integraal onderzoeksbeleid: doelen en instrumenten, CPB Policy Brief.

ENISA, 2017, Threat landscape report 2016.

Ministerie van Defensie, 2016, Strategische kennis- en innovatieagenda 2016-2020.

Ministerie van Veiligheid en Justitie, 2013, Nationale cybersecurity strategie 2.

Ministerie van Veiligheid en Justitie, 2017, Strategische kennis- en innovatieagenda.

Munnichs, G., M. Kouw. en L. Kool, 2017, A never-ending race; On cyberthreats and strengthening resilience. Den Haag, Rathenau Instituut.

Rademaker, M., L. Faesen, K. van Lieshout en M. Abdalla, 2016, Dutch investments in ICT and cybersecurity. Putting it in perspective, The Hague Centre for Strategic Studies.

Straathof, S.M. en S. van Veldhuizen, 2015, Financiering van start-ups en venture capital, CPB Notitie.

United Kingdom Cabinet Office, 2017, National cyber security strategy 2016 to 2021.

Verdonk Klooster & Associates en SEO Economisch Onderzoek, 2016, Economische kansen Nederlandse cybersecurity-sector.

Vollrath, T.L., 1991, A theoretical evaluation of alternative trade intensity measures of revealed comparative advantage, *Weltwirtschaftliches Archiv*, vol. 127(2): 265-280.

Dit is een uitgave van:

Centraal Planbureau
Postbus 80510 | 2508 GM Den Haag
T (088) 984 60 00

Januari 2018