
WRR
WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID
De publieke kern van het internet
Naar een buitenlands internetbeleid
Amsterdam University Press

De publieke kern van het internet

De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) werd in voorlopige vorm ingesteld in 1972. Bij wet van 30 juni 1976 (Stb.413) is de positie van de raad definitief geregeld. De huidige zittingsperiode loopt tot 31 december 2017.

Ingevolge de wet heeft de raad tot taak ten behoeve van het regeringsbeleid wetenschappelijke informatie te verschaffen over ontwikkelingen die op langere termijn de samenleving kunnen beïnvloeden. De raad wordt geacht daarbij tijdig te wijzen op tegenstrijdigheden en te verwachten knelpunten en zich te richten op het formuleren van probleemstellingen ten aanzien van de grote beleidsvraagstukken, alsmede op het aangeven van beleidsalternatieven.

Volgens de wet stelt de WRR zijn eigen werkprogramma vast, na overleg met de minister-president die hiertoe de Raad van Ministers hoort.

Wetenschappelijke Raad voor het Regeringsbeleid
Buitenhof 34
Postbus 20004
2500 EA Den Haag
Telefoon 070-356 46 00
E-mail info@wrr.nl
Website www.wrr.nl

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

De publieke kern van het internet

NAAR EEN BUITENLANDS INTERNETBELEID

Amsterdam University Press, Amsterdam 2015

Rapporten aan de Regering nrs. 68 t/m 93 zijn verkrijgbaar in de boekhandel of via Amsterdam University Press (www.aup.nl).
Alle *Rapporten aan de Regering* en publicaties in de reeksen *Verkenningen* en *Working papers* zijn beschikbaar via www.wrr.nl.

Vormgeving binnenwerk: Textcetera, Den Haag

OPTE 'The internet 2010'

De illustratie op de kaft van dit rapport, 'The internet 2010', is een visualisatie van het internet op basis van data uit 2010 gecreëerd door Barrett Lyon als onderdeel van zijn Opte project (opte.org). Deze representatie van het internetverkeer is gebaseerd op de werking van het Border Gateway Protocol, een van de dragende protocollen van het internet. De intensiteit van kleur en licht geven aan waar de meeste verbindingen actief zijn.

ISBN 978 94 6298 065 5
e-ISBN 978 90 4853 004 5 (pdf)
NUR 805

WRR/Amsterdam University Press, Den Haag/Amsterdam 2015

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

Aan de Minister-President
Voorzitter van de Ministerraad
De heer drs. M. Rutte
Postbus 20001
2500 EA Den Haag

ons kenmerk
2015020/AK/MvL

direct nummer
070-356 4691

onderwerp
WRR-rapportnr. 94
De publieke kern van het internet

Email
knottnerus@wrr.nl

datum
18 maart 2015

Het doet mij genoegen u hierbij het rapport *De publieke kern van het internet. Naar een buitenlands internetbeleid* aan te bieden. De raad beargumenteert in dit rapport dat er een kern van protocollen en standaarden binnen het internet is aan te wijzen die als een mondiaal publiek goed beschouwd kan worden. Het functioneren van de samenleving en de economie is met het internet vervlochten geraakt, en is afhankelijk van de integriteit van deze publieke kern. Vanwege het grote belang van het internet zijn staten steeds actiever geworden in hun pogingen om het internet mede te sturen. Steeds vaker ook beschouwen ze het beïnvloeden van de infrastructuur en de centrale protocollen van het internet zelf als een legitiem instrument om nationale of economische belangen te verwezenlijken. Dit is vanuit een oogpunt van het beschermen van de publieke kern van het internet ongewenst. Deze kern moet juist gevrijwaard blijven van oneigenlijke interventies door staten en andere partijen.

In dit rapport beveelt de raad aan om het internet nadrukkelijk en eigenstandig tot een speerpunt van het buitenlandbeleid te verheffen. Deze hoofdaanbeveling wordt verder uitgewerkt in drie prioriteiten voor een diplomatieke agenda. In de eerste plaats gaat het om het vastleggen van een internationale norm waarin de centrale protocollen van het internet aangemerkt worden als een neutrale zone, waarin bemoeienis omwille van nationale belangen niet geoorloofd is. In de tweede plaats gaat het om het onderscheiden en afbakenen van verschillende vormen van veiligheid in relatie tot het internet. In de derde plaats gaat het om het verbreden van het diplomatieke werkveld: zowel naar nieuwe coalities tussen staten als naar internetbedrijven, ngo's en de technische gemeenschap.

Ingevolge de Instellingswet ziet de raad graag de bevindingen van de ministerraad tegemoet.

De voorzitter,

Prof.dr. J.A. Knottnerus

De secretaris,

Dr. W. Asbeek Brusse

Buitenhof 34, Postbus 20004, 2500 EA Den Haag
telefoon (070) 356 46 00, website: www.wrr.nl, e-mail: info@wrr.nl

INHOUDSOPGAVE

SAMENVATTING

Dit rapport wil een bijdrage leveren aan het formuleren van de Nederlandse agenda voor een buitenlands internetbeleid. Kerngedachte daarbij is dat de centrale protocollen en infrastructuren van het internet als een mondiaal publiek goed beschouwd moeten worden. Deze publieke kern van het internet moet gevrijwaard blijven van oneigenlijke interventies van staten en andere partijen die schade toebrengen en het vertrouwen in het internet eroderen.

STATEN VERSTERKEN HUN GREEP OP HET INTERNET

Het internet is niet meer weg te denken uit ons dagelijks leven. Het is vervlochten met ons sociale leven, consumptie, werk en relatie met de overheid, en in toenemende ook met steeds meer objecten die we dagelijks gebruiken, van de slimme meter tot de auto waarin we rijden en de ophaalbrug die we onderweg tegenkomen. Het beheer van het internet was lange tijd het exclusieve domein van wat in internetkringen de 'technische gemeenschap' wordt genoemd. Die gemeenschap legde het fundament voor de huidige sociaaleconomische vervlechting van het fysieke leven en het digitale leven. Maar het beheer van dat fundament, met het Internet Protocol als meest prominente onderdeel, is omstreden geraakt. Vanwege de vele belangen, kansen en kwetsbaarheden die het internet inmiddels kent, zijn ook overheden zich met het reilen en zeilen van het internet gaan bemoeien. Daarbij is het beleidsmatige zwaartepunt aan het verschuiven van een primair economische blik op het internet (de interneteconomie, telecommunicatie en netwerken) naar een blik die meer door (nationale) veiligheid wordt bepaald: het internet van de cybercrime, kwetsbare vitale infrastructuren, digitale spionage en cyberaanvallen. Steeds meer landen willen bovendien om uiteenlopende redenen het gedrag van burgers op het internet reguleren: dat loopt van het beschermen van auteursrecht, via de aanpak van cybercrime tot censuur van en controle op de eigen bevolking via het internet.

Dat nationale staten hun ruimte en rol opeisen op het internet kan gevolgen hebben voor de cruciale onderbouw van het internet. Het internet is gemaakt om internationaal, zonder aanzien des persoons of nationaliteit te functioneren, een basisprincipe dat ten goede komt aan alle gebruikers. Het zijn vooral de diepere technologische lagen van het internet, bestaande uit protocollen en standaarden, die ervoor zorgen dat informatie zijn weg vindt en in alle hoeken van de wereld aankomt. Wanneer deze protocollen en standaarden niet naar behoren werken, komen het functioneren en de integriteit van het gehele internet onder druk te staan. Het internet kan 'kapot' gaan als we er niet meer vanuit kunnen gaan dat de informatie die we verzenden aankomt, dat we bij de sites uitkomen waar we naar

op zoek zijn en dat deze toegankelijk zijn. Recentelijk zijn steeds meer staten juist de diepere lagen van het internet gaan gebruiken als aangrijpingspunt om nationale belangen te behartigen.

Gezien het grote belang van internet is het zaak om nationale en internationale belangen van staten meer gewicht te geven binnen het governance bouwwerk. Tegelijkertijd is het nodig ervoor te waken de technologische kern – waar de groei van het internet op gebouwd is – niet beschadigd wordt en deze en te beschermen tegen oneigenlijk gebruik. De vraag hoe nationale belangen en de governance van het internet als mondiaal publiek goed met elkaar in balans kunnen worden gebracht, moet uiteraard internationaal beantwoord worden. Dat vereist een heldere Nederlandse stellingname.

DE PUBLIEKE KERN VAN HET INTERNET

Dit rapport betoogt daarom allereerst dat delen van het internet kenmerken hebben van een mondiaal publiek goed. Bij mondiale publieke goederen gaat het om baten voor iedereen in de wereld die alleen door gerichte actie en samenwerking te realiseren of te behouden zijn. Deze baten vloeien vooral voort uit de kernprotocollen van het internet zoals de 'TCP/IP protocol suite', verschillende standaarden, het systeem van domeinnamen (DNS) en routing protocollen. Het internet als publiek goed functioneert alleen als het de kernwaarden universaliteit, interoperabiliteit en toegankelijkheid garandeert en als het de kerndoelen van informatieveiligheid, te weten vertrouwelijkheid, integriteit en beschikbaarheid ondersteunt. Het is essentieel dat we – de gebruikers – op de werking van de meest fundamentele protocollen van het internet kunnen vertrouwen omdat daar ook het vertrouwen van afhangt dat we hebben in het sociaaleconomische bouwwerk dat daarbovenop gebouwd is. Hoewel het onvermijdelijk is dat nationale staten 'het internet' meer naar eigen beeltenis vorm willen geven, zullen er manieren gevonden moeten worden om de algemene werkzaamheid van deze 'publieke kern' van het internet te blijven garanderen.

TWEE VORMEN VAN INTERNETGOVERNANCE

Om deze spanning inzichtelijk te maken worden twee vormen van internetgovernance onderscheiden. In de eerste plaats de governance van de internet infrastructuur. Het gaat daarbij over het bestuur, de organisatie en de ontwikkeling van de diepere lagen van het internet, die sturend zijn voor de ontwikkeling van het internet. Hierbij staat het belang van het internet als collectieve infrastructuur voorop. Hiertegenover staat de governance die gebruik maakt van de internet infrastructuur. In dit geval wordt het internet ingezet als een middel in de strijd om inhoud en gedrag op het net te controleren. Dat kan variëren van het beschermen van auteursrecht en intellectueel eigendom tot het censureren en surveilleren van burgers door overheden. Steeds vaker worden de infrastructuur en de centrale protocollen van het internet echter zelf als een legitiem instrument gezien om

nationale of economische belangen te verwezenlijken. Waar internetgovernance voorheen voornamelijk de governance *van* het internet was – waarbij het beheer en functioneren van het internet als infrastructuur voorop staat - is er nu steeds vaker sprake van governance *via* of met gebruikmaking van het internet.

BEDREIGINGEN BINNEN DE GOVERNANCE VAN HET INTERNET

Het beheer van de publieke kern van het internet – de governance *van* het internet – ligt bij een aantal organisaties vaak samengenomen als de 'technische gemeenschap'. Hoewel dat beheer in principe in goede handen is, begint zich vanuit verschillende kanten druk op te bouwen. Politieke en economische belangen en verschillen van inzicht – soms in combinatie met nieuwe technologische mogelijkheden – maken dat het collectieve karakter van het internet uitgedaagd wordt:

- Grote economische belangen – zoals de bescherming van copyright en verdienmodellen voor datatransport – oefenen sterke druk uit op de politiek om netneutraliteit, voorheen een default van het internet, op te heffen of juist met wetgeving te beschermen.
- Het beheer van de namen en nummers van het internet (de IANA functie) is gepolitiseerd geraakt. Om redenen van internationale politieke legitimiteit is de druk groot om dat beheer uit de directe invloedssfeer van de VS te halen: het net is immers van vitaal belang voor vrijwel alle landen. Nederland heeft belang bij een 'agnostische' vormgeving van de IANA functie, waarbij de beheerstaken in handen blijven van de technische gemeenschap en er bij de meer politieke taken ruimte is voor de accommodatie van politieke en economische belangen.
- De discussie over ICANN (die de IANA functie uitoefent) is tevens een belangrijke testcase voor de Nederlandse en Europese internetdiplomatie om internationale coalitievorming voorbij 'the usual suspects' van de trans-Atlantische as te brengen.
- Een andere uitdaging is de opkomst van het nationale veiligheidsdenken op het internet. De ingenieursbenadering van de CERTs (gericht op het 'gezond houden' van het netwerk) en de internationale samenwerking daarbinnen ondervinden hinder van actoren gericht op nationale veiligheid, zoals inlichtingendiensten en militaire cybereenheden. Een vermenging van deze opvattingen van veiligheid is ongewenst omdat het partiële belang van nationale veiligheid botst met het collectieve belang van de veiligheid van het netwerk als geheel.

DREIGINGEN ALS GEVOLG VAN GOVERNANCE VIA HET INTERNET

Staten richten zich vanuit verschillende belangen echter ook rechtstreeks op de publieke kern van het internet. Daarbij raken ze soms aan centrale protocollen. Door dit soort praktijken wordt het functioneren van het gehele internet minder betrouwbaar en veilig. In de eerste plaats in technische zin, maar in het verlengde daarvan ook in economische en sociaal-culturele zin: als we niet uit kunnen gaan

van de integriteit, de beschikbaarheid en de vertrouwelijkheid van het internet heeft dat gevolgen voor de manier waarop we ermee willen en kunnen omgaan. De spanning tussen politieke en economische belangen enerzijds en de belangen van het internet als een publieke infrastructuur anderzijds komen aan de oppervlakte in dossiers als:

- Wetgeving die auteursrecht moet beschermen en gebruik maakt van protocollen en het DNS als middel, zoals de Amerikaanse wetsvoorstellen SOPA en PIPA en het ontwerp verdrag ACTA.
- Verschillende vormen van censuur en surveillance die gebruik maken van vitale protocollen en van de 'diensten' van internetmediairs als ISPs.
- De online activiteiten van inlichtingen- en veiligheidsdiensten en militaire cybereenheden die de integriteit van de publieke kern van het internet ondergraven door hardware, software, protocollen en standaarden te compromitteren en kwetsbaarheden in hard- en software geheim te houden.
- Sommige vormen van internet- en/of datanationalisme waarbij staten een deel van hun internet willen afschermen.

Op basis van deze bevindingen trekt dit rapport de conclusie dat overheden uiterst terughoudend moeten zijn met beleid, wetgeving en operationele activiteiten die ingrijpen in de kernprotocollen van het internet. Dit geldt eveneens voor de private partijen die ten aanzien van deze publieke kern een spilfunctie vervullen.

NAAR EEN BUITENLANDS INTERNETBELEID

Welke bijdrage kan Nederland hieraan leveren? Het overkoepelende belang van internetveiligheid veronderstelt allereerst een diplomatieke benadering waarin het internet – nadrukkelijk en eigenstandig – tot een speerpunt verheven wordt. Naast traditionele speerpunten als handel, mensenrechten en vrede en veiligheid zou de regering een buitenlands internetbeleid moeten prioriteren en uitwerken. Voor een kleine, maar potentieel invloedrijke, diplomatieke speler in dit veld als Nederland geldt wel dat 'practice what you preach' de meest solide basis is om als voortrekker te kunnen fungeren. Bij nieuwe nationale wetgeving moet de vraag of Nederland hiermee internationaal voor de dag kan komen derhalve een belangrijke overweging zijn. Op het gebied van de fundamentele rechten en internetbeleid moet Nederland eigenlijk consequent een acht scoren om daadwerkelijk een voortrekkersrol te kunnen claimen.

Inhoudelijk behelst deze rol een diplomatieke inspanning gericht op het beschermen van de publieke kern van het internet. Het beschermen van de publieke kern van de infrastructuur vraagt behalve om politiek optreden van staten tegelijkertijd ook om een grote terughoudendheid van diezelfde staten. Om dit te bereiken moeten er in het internationale domein van de internetgovernance nieuwe vormen van

macht en tegenmacht worden georganiseerd. De principes van *menging*, *scheiding* en *beteugeling*, drie klassieke principes van machtsbinding, moeten daartoe naar de internationale context vertaald worden.

AANBEVELINGEN

De centrale aanbeveling dat het internet nadrukkelijk speerpunt dient te zijn van het buitenlands beleid wordt in dit rapport verder uitgewerkt in drie aanbevelingen:

- Bevorder het vastleggen en internationaal verspreiden van de norm dat de publieke kern van het internet – de centrale protocollen en infrastructuur die een mondiaal publiek goed zijn – gevrijwaard moet zijn van bemoeienis van overheden.

In de eerste plaats gaat het om een internationale norm waarin de centrale protocollen van het internet aangemerkt worden als een neutrale zone, waarin overheidsbemoeienis omwille van nationale belangen niet geoorloofd is. Over vijf jaar heeft een veel grotere groep landen de technische capaciteiten die nu slechts in handen van enkele grootmachten liggen. Als intussen tevens de norm postvat dat nationale staten vrijelijk kunnen bepalen of ze wel of niet willen ingrijpen in de centrale protocollen van het internet om de eigen belangen veilig te stellen, heeft dat een uiterst schadelijk effect op het internet als een mondiaal publiek goed.

Voor het vastleggen en verspreiden van deze norm staan Nederland een aantal belangrijke fora ter beschikking. In de eerste plaats de EU en via de EU ook handelsverdragen waarin een dergelijke norm als clausule opgenomen kan worden. Ook fora als de Raad van Europa, de OESO, de OVSE en de VN bieden mogelijkheden om deze norm te verankeren. Hiermee kan een kiem worden geplant die op termijn uit kan groeien tot een breder regime.

- Bevorder dat verschillende vormen van veiligheid in relatie tot het internet op nationaal en internationaal niveau beter van elkaar onderscheiden worden en door aparte actoren worden geadresseerd.

In de tweede plaats gaat het om het onderscheiden van verschillende vormen van veiligheid in relatie tot het internet. Dat vergt een duidelijke afbakening en scheiding van taken en organisaties en vooral ook een beteugeling van de neiging van staten om nationale veiligheid de dominante visie op het internet te laten worden. Met name de technologische aanpak van de CERTs, die een meer public health-

achtige benadering van de veiligheid van het netwerk als geheel hanteren, en de benadering vanuit de nationale veiligheid, waarin nationale belangen boven de belangen van het netwerk gaan, moeten gescheiden blijven.

- Maak de verbreding van het diplomatieke werkveld onderdeel van de agenda voor internetdiplomatie.

Er speelt zich een demografische verschuiving op het internet af: weg van Noord en West in de richting van Oost en Zuid. Andere stemmen dan de Europese en Amerikaanse zullen in de nabije toekomst harder spreken en daar zullen ook andere economische en politieke ideeën in doorklinken. Het is daarom zaak om een brede diplomatieke inspanning te plegen om met name de zogenaamde *swing states* ervan te overtuigen dat het ongemoeid laten van de publieke kern van het internet een belang van *alle* staten is. Ook gaat het erom private partijen expliciet onderdeel van de diplomatieke inspanning op het gebied van internetgovernance te maken. Gezien de grote macht van internetgiganten als Google en Apple, kunnen overheden deze partijen in diplomatieke zin niet meer negeren. Deze bedrijven zijn meer dan mogelijke investeerders of privacy schenders: het zijn partijen die serieuze diplomatieke aandacht behoeven vanwege hun vitale rol in het digitale leven, met alle tegenstrijdigheden die eigen zijn aan de diplomatie. En tenslotte gaat het om het productief maken van de expertise van ngo's en andere private betrokkenen, zonder daarbij valse verwachtingen te scheppen over hun rol in het beheer van het internet. Zeker waar het gaat om het doordenken van de gevolgen van internetgovernance voor het technisch functioneren van het internet als geheel, valt hier een wereld te winnen.

TEN GELEIDE

Dit rapport is voorbereid door een WRR-projectgroep onder leiding van prof. dr. Dennis Broeders, stafmedewerker van de WRR. De overige leden waren dr. Erik Schrijvers en drs. Lisa Vermeer, beiden lid van de wetenschappelijke staf van de WRR. Prof.dr. Mark Bovens was als lid van de raad bij het project betrokken. Prof.dr. Huub Dijstelbloem, stafmedewerker van de WRR, Wendy Hoogeboom en Liisa Janssens, beiden stagiair, leverden in verschillende fases een bijdrage aan het project.

Tijdens het schrijven van dit rapport is met vele deskundigen uit de wereld van internetgovernance en cyber security gesproken. Deze gesprekken zijn van grote waarde geweest voor het rapport en de raad dankt hen allen voor hun tijd en inzichten. Hun namen staan achterin het rapport vermeld.

Tenslotte danken wij degenen die bereid waren eerdere versies van dit rapport van gedetailleerd commentaar te voorzien: prof.dr.ir. Jan van den Berg, prof.dr. Nico van Eijk, prof.dr. Marieke de Goede, prof.dr.ir. Erik Huizer en prof.mr. Corien Prins.

1 INTERNETGOVERNANCE OP EEN KRUISPUNT

> Today's Internet is a fortuitous accident. It came into being through a combination of an initial lack of commercial interests, government benign neglect, military requirements for survivability and resilience, and computer engineers building open systems that worked simply and easily. Battles over its future are going on right now: in legislatures around the world, in international organizations like the ITU, and in Internet organizations like the IGF.
> Bruce Schneier (2013: 13)

1.1 INLEIDING

Het internet is niet meer weg te denken uit onze samenleving. Onze economie, ons sociale leven, onze infrastructuren, ons publieke leven: zij zijn allemaal gerelateerd en vertakt via het internet. In het komende decennium gaat dat internet zich nog verder versterken als trends zoals 'the internet of things', cloud computing en mobiele internettechnologie zich verder doorzetten en aangevuld worden met nieuwe toepassingen die we nu nog niet kennen of kunnen overzien. Ons sociale, publieke en economische leven draait daarmee in toenemende mate op een infrastructuur die de wereld omspant en die in essentie niet territoriaal is. Die infrastructuur is het product van de inspanningen van private partijen en een internationale technische gemeenschap die de belangrijkste software en protocollen waarop – en waarom – het internet functioneert, hebben ontwikkeld. Overheden zijn daar slechts zijdelings bij betrokken geweest, afgezien van aanzienlijke publieke investeringen in met name de begindagen van het internet. De diepe lagen van het internet die bepalen hoe het netwerk functioneert zijn voor de meeste mensen – net als wat zich onder de motorkap van een auto bevindt – onbekend en oninteressant terrein. Het is voor de meeste mensen niet zo belangrijk hoe hun auto werkt, als hij maar werkt, de rest is voor de specialisten. Voor het internet heeft dat ook lange tijd gegolden. Wat begon als een klein netwerk van Amerikaanse universiteiten en het Amerikaanse ministerie van Defensie (ARPANET) was alleen bekend onder de absolute voorlopers, die het netwerk zelf onderhielden, bijstuurden en deden groeien. Met de groei van het internet en met name de introductie van het World Wide Web (WWW) in 1991, waardoor mensen toegang kregen tot de beschikbare informatie via websites waartussen eenvoudig 'gesurft' kan worden, nam het dagelijkse belang van het internet toe. Tegelijkertijd verdwenen de 'motor' en de fysieke infrastructuur van het internet steeds verder uit het zicht van de dagelijkse gebruikers.

De politieke aandacht voor het internet is in het afgelopen decennium sterk toegenomen. Waar het internet vijftien jaar geleden voornamelijk de krant haalde in het licht van de economische mogelijkheden die het bood – met de *dot.com bubble* rond het millennium als oprisping in de opmars van het WWW – figureert het internet nu in vrijwel alle aspecten van het publieke en politieke leven. Politici zien

dat het internet een dragende pilaar van de economie is geworden en een onlosmakelijk onderdeel is van het sociale en werkende leven van hun burgers. Ze zien ook het fenomeen cybercriminaliteit groeien; ze constateren dat eigenlijk alle vitale infrastructuren aan het internet vasthangen; ze beseffen dat Google, Apple en Facebook meer weten van hun burgers dan zij, en dat ook nog eens te gelde kunnen maken; en ze zien de aanwezigheid en bemoeienis van de strijdkrachten en inlichtingendiensten op het internet groeien. Nu het internet zo centraal is komen te staan en zoveel kansen en bedreigingen in zich bergt, zijn steeds meer overheden zich gaan interesseren voor de diepere lagen van het internet en voor de vraag hoe die bestuurd worden.

Het mondiale internet verhoudt zich echter moeizaam tot de wereld waarin nationale staten hun belangen op dat internet veilig proberen te stellen. Hoewel het zeker niet zo is dat nationaal beleid geen invloed heeft op het internet – of beter: op de partijen die het internet vormgeven en gebruiken – is het internationale karakter vaak een grote belemmering om nationale belangen veilig te stellen. Ook internationale samenwerking – laat staan internationale consensus – op het punt van het 'bestuur' van het internet is nog maar nauwelijks van de grond gekomen. Dit wil uiteraard niet zeggen dat het internet niet bestuurd wordt. Integendeel. In de afgelopen dertig jaar is het internet bestuurd, ontwikkeld en uitgebreid door een relatief bottom-up ontstaan netwerk van organisaties, bestaande uit private partijen, ngo's, academici en ook overheden in wat men wel een multistakeholdersysteem noemt (zie bijvoorbeeld Goldsmith en Wu 2008; Mueller 2010; Deibert 2013; DeNardis 2014). Nationale staten eisen echter op dit moment een grotere rol voor zichzelf op, waardoor het bottom-up karakter van dit systeem onder zware druk is komen te staan. Er is geen consensus onder staten, noch onder de andere actoren, over welke keuzes nu gemaakt moeten worden over het toekomstige bestuur van het internet. Sommige keuzes kunnen echter grote gevolgen hebben voor de werking van het internet zelf.

Dit rapport wil bijdragen aan het formuleren van een Nederlandse agenda voor een buitenlands internetbeleid waarin keuzes worden gemaakt. Uitgangspunt daarbij is de noodzaak om een balans te verzekeren tussen het waarborgen en beschermen van het internet als een mondiaal publiek goed enerzijds en het normaliseren van het internet als onderdeel van internationale betrekkingen anderzijds. De vraag hoe nationale belangen en de governance van het internet als internationaal publiek goed met elkaar in balans kunnen worden gebracht, moet uiteraard internationaal beantwoord worden, maar dat vereist een heldere Nederlandse stellingname.

1.2 INTERNETGOVERNANCE OP EEN KRUISPUNT

Dat staten een grotere rol claimen is, gezien het feit dat het internet zo dragend voor economie en samenleving is geworden, geen verrassing. Een laissez-faire-attitude, die lang de norm is geweest voor de meeste landen, wordt nu veelal gezien als onverstandig en ongepast. Dat wil nog niet zeggen dat alle staten een helder begrip hebben van wat het internet is en wat een goede manier van reguleren zou zijn. Bovendien lopen de meningen nogal uiteen over fundamentele zaken als vrijheid van meningsuiting, opsporing van criminelen en het beschermen van intellectueel eigendom. Deze zaken zijn onderdeel van zowel nationale beleidstradities als internationale diplomatieke betrekkingen tussen staten. Het feit dat ze nu ook op het internet spelen maakt ze niet per se anders, maar vraagt soms om een heel andere benadering en vorm van internationale samenwerking. Dit rapport concentreert zich op dat beleid van nationale staten dat raakt aan de diepe, technologische lagen en softwareprotocollen waarop het internet draait. Belangrijke thema's als de vrijheid van meningsuiting op het internet en de grootschalige opslag van persoonsgegevens komen niet eigenstandig aan de orde. Die thema's komen in beeld als het daarop gerichte nationale beleid *gebruikmaakt* van de diepere lagen van het internet en daarmee een bedreiging vormt voor het bredere functioneren van het internet. Het rapport richt zich primair op de vraag wat een goede manier is om deze diepere lagen te reguleren. De betrouwbaarheid van het internet – zowel in technische zin als in de zin van 'vertrouwen' – is afhankelijk van het functioneren van de 'publieke kern' van het internet. Als het internet niet functioneert, niet betrouwbaar is, geldt dat voor elke internetgebruiker, waar ook ter wereld. Hoewel het onvermijdelijk is dat nationale staten 'het internet' meer naar eigen beeltenis vorm willen geven, zullen er manieren gevonden moeten worden om de algemene werkzaamheid van de kern van het internet te blijven garanderen.

1.2.1 EEN MONDIALE INFRASTRUCTUUR EN NATIONALE BELANGEN

Sommige auteurs stellen dat het kruispunt waarop internetgovernance is aangekomen tot een clash leidt tussen twee werelden: enerzijds de mondiale en nonstatelijke wereld van het internet en anderzijds de wereld van de natiestaten met nationale soevereiniteit als ordenend beginsel in het internationale domein. Soevereiniteit en het internet lijken onverenigbare grootheden: het internet zelf stoort zich niet aan nationale grenzen en het internetprotocol TCP/IP is technisch zo opgezet dat informatie in principe altijd zijn einddoel zoekt. Of, zoals John Gilmore het formuleert: "The net interprets censorship as damage and routes around it" (geciteerd in Maher 2013). Tegelijkertijd laten staten zich inmiddels niet meer onbetuigd en proberen ze het mondiale internet meer en meer onder controle en binnen de kaders van het eigen nationale beleid te krijgen en/of internationaal te reguleren. Soms gebeurt dat om grip op de eigen bevolking te krijgen, soms om economische belangen te verdedigen en soms zelfs om soevereiniteit in de militaire zin te doen gelden. De trend dat staten grenzen trekken in cyberspace en daar-

mee territorialiteit op het internet introduceren tekent zich duidelijk af. Net zoals het Wilde Westen langzaam opgeslokt en getemd werd door de staat, voorspellen sommigen dat hetzelfde gebeurt met het 'anarchistische' internet. In de literatuur wordt soms wel gesproken van de opkomst van een Westfaals model op het internet. Deze verwijzing naar de Vrede van Westfalen in 1648, waarin soevereiniteit als het legitieme ordenend beginsel van de betrekkingen tussen staten werd vastgelegd, wordt nu gebruikt om aan te geven dat staten hun soevereiniteit op het mondiale internet willen doen gelden. Demchak en Dombrowksi (2011; 2014: 33) waarschuwen dat de opkomst van een cyber-Westfalen niet zonder conflict zal zijn: "het proces waarin staten grenzen trekken op het internet en hun soevereiniteit claimen, zal schoksgewijs, gevaarlijk en langdurig zijn". Deze ontwikkeling past in een bredere trend van renationalisering, waarin het geloof in de voordelen van economische en culturele globalisering – dat lang sterk is geweest en ook veel heeft opgeleverd – in balans wordt gebracht met nationale belangen. Zo wordt, onder de noemer van economische veiligheid, nagedacht over de verhouding tussen enerzijds internationale investeringen, transnationale overnames en geopolitieke ontwikkelingen en anderzijds het beschermen van eigen industrieën en vitale infrastructuren. Hoe moeten landen die sterk in de wereldeconomie geïntegreerd zijn een koers varen tussen naïviteit en paranoia (NCTV 2014)? Ook in relatie tot het mondiale internet moeten staten het nationale belang en het internationale internet tegen elkaar afwegen. De drie onderstaande citaten illustreren hoe sterk de rol van staten en de blik daarop de afgelopen jaren is veranderd.

"We reject: kings, presidents and voting. We believe in: rough consensus and running code"

Zo formuleerde David Clark, MIT-hoogleraar en destijds een van de internetpioniers, in 1992 hoe 'de internetgemeenschap' invulling gaf aan wat nu 'internetgovernance' heet (geciteerd in Goldsmith en Wu 2008: 24). Er was geen behoefte aan democratische besluitvorming over hoe het netwerk zich verder moest ontwikkelen, noch aan politieke toestemming van bovenaf. Afdoende was ruwe consensus onder de ingenieurs en andere stakeholders die het internet hoofdzakelijk als een technologische uitdaging zagen. Het internet was in hun ogen in essentie een non-politiek netwerk dat door technologische doorbraken en een groeiende schare gebruikers langzaam uitgroeide tot een mondiaal netwerk van netwerken. Hoewel het internet zeker in de begindagen mede dankzij de overheid – met name de Verenigde Staten – tot ontwikkeling kwam, hebben de meeste overheden het internet lange tijd gezien als iets dat nauwelijks bestuurd diende te worden en tot op zekere hoogte zelfs onbestuurbaar was.

"Good luck! That's sort of like trying to nail Jell-O to the wall"

In 1998 was ook de Amerikaanse president Clinton er nog van overtuigd dat het internet niet te controleren was. Hij deed zijn uitspraak naar aanleiding van de pogingen van de Chinese overheid om het internet, en dan met name de Chinese

internetgebruikers, te controleren en in de gaten te houden (geciteerd in Goldsmith en Wu 2008: 90). De 'Great firewall of China' is een begrip geworden en wordt beschouwd als een van de vroegste pogingen om het internet en internetgebruikers te controleren en te surveilleren. Ondertussen zijn we vele generaties van internetsurveillance verder en is de technologie om gebruikers te ontdekken en te monitoren steeds verfijnder geworden (Deibert et al. 2008; 2010; 2011). Of, zoals Tim Wu (2010: 309) het formuleert: "The Jello was somehow nailed to the wall". Voor de gebruiker is het internet daarmee steeds minder een vrijplaats waar je anoniem je gang kunt gaan. Bedrijven en overheden houden het gedrag van internetgebruikers gedetailleerd in de gaten. Bedrijven omdat data en kennis over het gedrag van internetters te gelde gemaakt kan worden, overheden omdat zij in die kennis een sleutel zien tot een grotere veiligheid en controle. Wat veiligheid is, wordt in verschillende landen uiteraard zeer verschillend ingevuld. Nederlandse, Iraanse, Amerikaanse en Russische concepties van veiligheid en vrijheid verschillen sterk van elkaar, ook op het internet. In tegenstelling tot zijn voorganger Clinton is de huidige Amerikaanse president Obama ver voorbij elk idee dat het internet een oncontroleerbaar netwerk is. De onthullingen over de mondiale surveillancepraktijken van de Amerikaanse National Security Agency (NSA) hebben het debat over de toekomst van het internet verder op scherp gezet (Greenwald 2014). De mogelijkheden voor een goed gefinancierde dienst als de NSA lijken in ieder geval eindeloos.

"The internet is a CIA project"

Aldus de Russische president Poetin in april 2014 tijdens een mediaforum in Sint-Petersburg,[1] een van de vele indicaties dat het internet steeds minder als een mondiaal, apolitiek netwerk gezien wordt. Of, beter gezegd: door politici niet als zodanig geaccepteerd wordt. De roep van politici om meer grip te krijgen op het internet wordt steeds luider. Een andere, en in vele ogen zorgelijke ontwikkeling, is de militarisering van het internet, waarbij steeds meer landen het internet zien als het vijfde domein van oorlogsvoering (na land, zee, lucht en ruimte) en op hoge snelheid militaire cybercapaciteit en cyberinlichtingendiensten opbouwen (zie bijvoorbeeld Singer en Friedman 2014; Guitton 2013; Deibert 2013; Dunn Cavelty 2013). Het internet is daarmee onderdeel geworden van de hogere politiek van de nationale en internationale veiligheid. Eenmaal op dat niveau aangekomen, is de kans dat staten zich weer terugtrekken naar een houding van 'benign neglect' ten opzichte van het internet goeddeels verkeken.

1.2.2 HET INTERNET ALS EEN MONDIAAL PUBLIEK GOED?

Hoewel het internet functioneert in een wereld waarin staten de dienst uitmaken, heeft het een grote mondiale betekenis. In de kern is het internet gemaakt om internationaal, zonder aanzien des persoons of nationaliteit te functioneren, een basisprincipe dat ten goede komt aan alle gebruikers. De kracht van het internet is zijn groei geweest en het indrukwekkende vermogen om in de eerste dertig jaar

van zijn geschiedenis miljarden gebruikers en nieuwe toepassingen te accommoderen. Of zoals Vint Cerf (2013: 7) – een van de 'vaders van het internet' – het formuleert: "de hulpbronnen van het internet, hoewel eindig, worden uitsluitend beperkt door ons vermogen om meer hulpbronnen te creëren om de gedeelde virtuele ruimte van het internet en de bijbehorende applicaties te doen groeien".

Door zijn internationale opzet en mondiale betekenis hebben delen van het internet kenmerken van een mondiaal publiek goed. Bij mondiale publieke goederen gaat het om baten voor iedereen in de wereld, baten die alleen door gerichte actie en samenwerking te realiseren of te behouden zijn. Het 'publieke' van publieke goederen zit in het feit dat deze in principe iedereen raken of voor iedereen beschikbaar zouden moeten zijn. Dat zegt echter nog niets over de wijze waarop daarin voorzien moet worden. Hoe dat gebeurt, kan van geval tot geval verschillen en kan het werk zijn van (combinaties van) zowel private als publieke partijen (WRR 2010: 196-7). Deze redenatie zou van toepassing verklaard kunnen worden op het internet als een netwerk en infrastructuur. Het collectieve is dan niet zozeer de inhoud van het WWW maar juist het functioneren van het internet als *systeem* dat toepassingen als het WWW en inhoud daarvan mogelijk maakt. Laura DeNardis (2014: 17) wijst erop dat het functioneren van dat netwerk een vitaal belang is: "niet minder dan economische veiligheid, het moderne sociale leven, cultuur, het politieke debat en nationale veiligheid staan op het spel bij het wereldwijd operationeel en veilig houden van het internet".

Zuivere mondiale publieke goederen hebben twee essentiële kenmerken: non-exclusiviteit en non-rivaliteit. Ofwel: je kunt niemand uitsluiten van het gebruik en het gebruik door de ene persoon gaat niet ten koste van het gebruik door een ander. Strikt genomen gaat dat niet op voor het internet. Zowel overheden als bedrijven kunnen mensen uitsluiten van het internet. Bovendien is het internet niet gratis, hetgeen in zichzelf al uitsluitend is. Sommige overheden, zoals Egypte in 2011, hebben het internet zelfs een paar dagen uitgezet in tijden van onrust en crisis, door de netwerken buiten werking te stellen. Maar beide principes zijn wel van toepassing op de manier waarop de technische gemeenschap het internet heeft opgezet en tot ontwikkeling gebracht. Om nogmaals DeNardis (2013: 4) te citeren: "met uitzondering van repressieve politieke contexten van censuur, zijn de kernwaarden van het internet universaliteit, interoperabiliteit en toegankelijkheid". Deze kernwaarden zijn allemaal gericht op insluiting en niet op uitsluiting.
De technische en logische kern van het internet, te weten de basisprotocollen die bepalen hoe het net werkt, gaan dus uit van waarden die non-exclusiviteit ondersteunen. De geschiedenis van de groei van het internet heeft laten zien dat het internet de waarde van non-rivaliteit sterk heeft kunnen faciliteren door de capaciteit van het net steeds weer te vergroten. Bij voldoende technische vooruitgang – het uitbreiden van bandbreedte – is het internet zo opgezet dat er genoeg is voor

iedereen. De kern van het internet wordt in dit rapport derhalve opgevat als een onzuiver mondiaal publiek goed[2] – zoals bijvoorbeeld infrastructuur dat ook is (Went 2010).

1.2.3 MONDIAAL VERSUS NATIONAAL ALS KERNPROBLEEM VAN INTERNETGOVERNANCE

Nationale staten eisen steeds meer hun ruimte en rol op het internet op, en met name in zaken van internetgovernance. Deze ontwikkeling kan gevolgen hebben voor het mondiale publieke goed dat de technische kern van het internet is. Het governancebouwwerk dat het internet sinds de jaren tachtig heeft bestuurd en zo sterk heeft doen groeien is slechts zeer beperkt door staten ontworpen en ingericht. Nu die zich melden met een brede waaier aan soms tegenstrijdige nationale belangen en verschillende invullingen van vrijheid en veiligheid is het zaak om nationale en internationale belangen van staten meer gewicht te geven binnen dit governancebouwwerk zonder de publieke kern – waar de groei van het internet op gebouwd is – te beschadigen. Vele wetenschappers omschrijven de huidige tijd als het moment waarop de slag om de toekomst van het internet geleverd wordt. De WRR lecture 2012 van Ronald Deibert droeg de titel 'The global battle for the future of cyberspace'; het eerste hoofdstuk van Milton Muellers boek *Networks and states* (2010) heet 'A battle for the soul of the internet'; en het nieuwste boek van Laura DeNardis (2014) is getiteld *The global war for internetgovernance*. De vraag hoe nationale belangen en de governance van het internet als internationaal publiek goed met elkaar in balans kunnen worden gebracht, is er een die in hoofdzaak internationaal beantwoord moet worden. De bijdrage van Nederland wordt – net als van alle andere landen – bepaald via het buitenlands beleid en via het nationale beleid dat internationale uitstralingseffecten heeft naar andere landen en naar het internationale domein. Die effecten kunnen uiteraard zowel positief als negatief zijn. Dit rapport wil een bijdrage leveren aan het formuleren van wat de Nederlandse agenda voor een buitenlands internetbeleid zou moeten zijn.

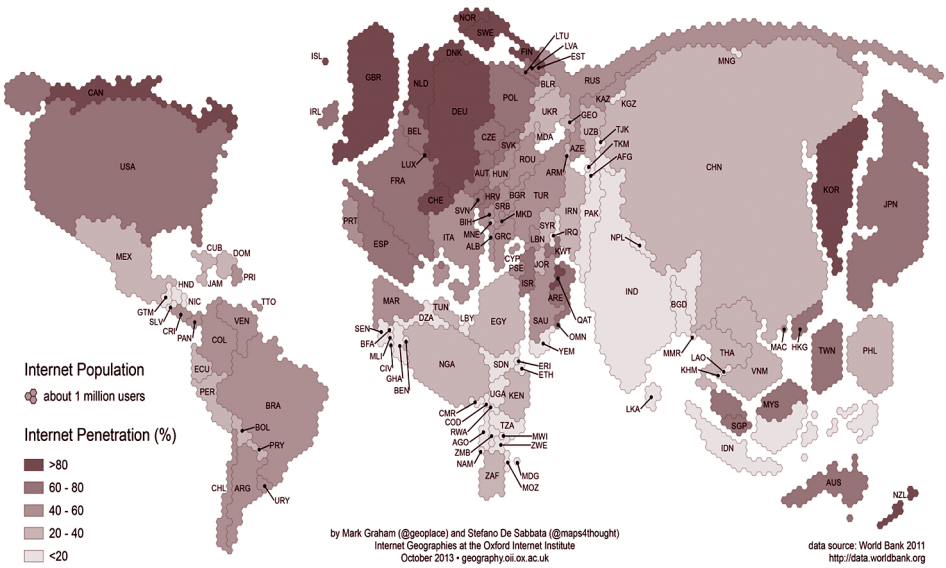
1.3 SETTING THE SCENE: DRIE TRENDS IN CYBERSPACE

De internationale agenda en strijd om de governance van het internet ontwikkelen zich tegen de achtergrond van een drietal trends die van bijzonder belang zijn voor het internationale speelveld. De trends zijn: de demografische verschuiving onder de mondiale internetgebruikers; het veiligheidsdenken en de militarisering van het internet; en de dataficatie van de samenleving. Uiteraard zijn er meer trends die van grote invloed zijn op de ontwikkeling van het internet, met name technologische trends zoals mobiel internet en cloud computing. Zulke trends komen in de tekst ter sprake op de momenten dat ze voor de analyse van belang zijn. De hoofdtrends die hier centraal staan, onderscheiden zich door hun grote invloed op het internationale politieke speelveld waarop Nederland zijn positie moet bepalen.

1.3.1 DEMOGRAFISCHE VERSCHUIVING

Het internet verovert de wereld in rasse schreden. In 2012 waren wereldwijd een kleine tweeënhalf miljard mensen verbonden met het internet. In westerse landen is het bereik (*penetration rate*) het grootst en varieert van 63,2 procent in Europa tot 78,6 procent in de Verenigde Staten.[3] Het Westen nadert zijn verzadigingspunt. De grote groei in de westerse landen zit hem vandaag de dag voornamelijk in de toename van het aantal apparaten met een internetaansluiting dat we per persoon hebben. In Afrika (15,6%) en Azië (27,5%) is het bereik veel lager maar het absolute aantal gebruikers ligt daar veel en veel hoger: Azië herbergt meer dan een miljard internetgebruikers, waarvan China een half miljard voor zijn rekening neemt. In de cijfers van 2011 bleef het Engels als de dominante taal op het internet het Chinees nog net voor, maar de groeipercentages laten zien dat die koppositie waarschijnlijk al is overgenomen. In de periode 2000-2011 groeide het aantal Engelssprekende internetgebruikers met 301 procent, terwijl het aantal Chinees sprekenden in dezelfde periode met 1478 procent en het aantal Arabisch sprekenden met 2501 procent groeide (Choucri 2012: 61). Deibert (2013) stelt dat het internet bezig is aan een demografische verschuiving, waarbij het zwaartepunt zich verlegt van Noord en West naar Oost en Zuid. Figuur 1 laat goed zien hoe de wereld eruitziet in termen van internetpenetratie en waar de ruimte voor groei zit: hoe lichter de kleur, hoe meer ruimte voor uitbreiding van het aantal internetgebruikers.

Figuur 1.1 Internetgebruikers en internetpenetratie wereldwijd, 2011



Bron: Graham (2014)

Die verschuiving heeft grote gevolgen voor de machtsverhoudingen binnen en de culturele blik op het internet. Het volgende miljard internetgebruikers komt uit relatief arme landen, met andere culturele en politieke tradities en met regeringen die deels andere ideeën hebben over veiligheid en vrijheid op het internet. Dat heeft gevolgen voor het Nederlands, Europees en 'westers' buitenlands beleid inzake het internet. Een recent rapport van de Amerikaanse denktank Council on Foreign Relations (2013: 67) roept de Amerikaanse overheid op om deze nieuwe realiteit het vertrekpunt van zijn buitenlands internetbeleid te maken: "The United States can no longer rely on its role as progenitor of the internet to claim the mantle of leadership". De dominantie van de 'westerse' stem in het debat over internet is geen gegeven meer. Als het gaat om internetgovernance zijn er twee duidelijke kampen: een kamp dat het huidige bottom-upmodel met veel stakeholders wil versterken en een kamp dat juist veel meer invloed voor staten wil. Daartussen bevindt zich een grote groep van landen die wel 'swing states' of 'fence sitters' worden genoemd en die nog geen duidelijke opvatting en keus hebben gemaakt (zie bijvoorbeeld Maurer en Morgus 2014; Clemente 2013). Dat andere stemmen en ideeën over wat het internet is en zou moeten zijn meer politiek gewicht krijgen, heeft gevolgen voor hoe Nederland zijn ideeën over vormgeving en toekomst van het internet kan bewerkstelligen in het internationale domein en voor de mogelijkheden om een veilig en betrouwbaar 'Nederlands' internet te realiseren.

1.3.2 'SECURITISATION' VAN HET INTERNET

Het veiligheidsdenken viert hoogtij op het internet. Er is een duidelijke toename van cybercriminaliteit en door het grote aantal bedrijven dat zich op het internet begeeft – vaak zelfs met de meest primaire processen – neemt de kwetsbaarheid verder toe. Ook overheden zien de bedreigingen groeien. Naast economische bedreigingen als cybercrime en diefstal van bedrijfsgeheimen maken overheden zich steeds vaker zorgen over de kwetsbaarheid van vitale infrastructuren en over economische en politieke spionage door staten. Het *Nederlandse Cyber Security Beeld* dat het Nationaal Cyber Security Centrum (2013) net voor de Snowden-onthullingen publiceerde, noemde in dat kader China, Rusland, Iran en Syrië al met naam en toenaam. Inmiddels kunnen daar de bondgenoten Amerika en Groot-Brittannië aan toegevoegd worden. Hoewel de onveiligheid op het internet toeneemt, is het lastig om in te schatten in welke mate dat gebeurt – omdat veel data ontbreken of gekleurd zijn[4] – en welke scenario's realistisch zijn. Daardoor is het lastig om te zien of de toenemende budgetten en beleidsaandacht voor cybersecurity in verhouding staan tot de reële onveiligheid en/of de juiste dreiging. Het begrip 'dreigingsinflatie' wordt vaak gebruikt als verklaring voor de snel oplopende budgetten en wettelijke bevoegdheden, zeker in de Verenigde Staten (Libicki 2012; Lin 2012; Rid 2013).

In recente jaren is het internet bovendien doorgedrongen in de hoogste regionen van het veiligheidsbeleid. Cybersecurity en cyberwarfare zijn snel groeiende beleidsterreinen die – zeker internationaal gezien – op aanzwellende begrotingen en bevoegdheden kunnen rekenen (Bauman et al. 2014; Guiton 2013; Severs 2013). Het feit dat het internet ook als een domein van oorlogsvoering wordt gezien, is van invloed op hoe staten het internet zien. Vele landen, inclusief Nederland, hebben het internet inmiddels na land, water, lucht en ruimte tot het vijfde domein voor oorlogsvoering verklaard. De taal van oorlog en nationale veiligheid doet iets met de manier waarop overheden naar het internet kijken. In overheidskringen zeggen sommigen dat die taal hoge noodzaak is omdat de onveiligheid hand over hand toeneemt, terwijl anderen, ook uit de militair-strategische hoek, vraagtekens zetten bij het nut van deze framing. Het gebruik van terminologie als 'cybergeddon' (World Economic Forum 2014), 'digitaal Pearl Harbor' (Clarke en Knake 2010) draagt echter sterk bij aan wat de Kopenhagen School van de Internationale Betrekkingen 'securitisation' noemt. Deze school gaat ervan uit dat bedreigingen van veiligheid geen natuurlijk gegeven zijn maar worden geconstrueerd door middel van het politieke discours. Ontwikkelingen worden op die manier gepolitiseerd – zodat ze op de politieke agenda komen – en in extreme gevallen zelfs 'securitised' (Lawson 2013: 88). Wanneer dat laatste gebeurt, wordt het onderwerp eigenlijk niet langer meer "besproken als een politiek vraagstuk, maar versneld behandeld en op manieren die gangbare wettelijke en sociale regels schenden" (Buzan et al. 1998: 23, geciteerd in Hansen en Nissenbaum 2009: 1158). Bij 'securitisation' bestaat het risico dat vitale rechtstatelijke waarborgen, democratische controle en openbaarheid van bestuur verzwakt worden omwille van snelle besluitvorming en nationale veiligheid. Een goed voorbeeld is de politieke, militaire en wetgevende reactie van de Amerikaanse overheid en andere landen op de aanslagen van 9/11.[5]

Ook cybersecurity en cyberwarfare zijn in de ogen van sommige onderzoekers onderdeel geworden van een 'securitised' discours (Hansen en Nissenbaum 2009; Dunn Cavelty 2013; Singer en Friedman 2013). Het feit dat overheden momenteel grote stappen zetten op het gebied van nationale en internationale veiligheid inzake het internet, tegen een achtergrond van een relatief slecht in kaart gebrachte dreiging en veel onenigheid over een aantal vitale kernvragen als 'wat is een cyberaanval?' en 'wat is een cyberoorlog?' heeft potentieel grote gevolgen. Het leidt wellicht tot een vergaande militarisering van het cyberdomein (Libicki 2012; Dunn Cavelty 2012) en tot het ontstaan van een nieuw cybermilitair-industrieel complex (Brito en Watkins 2011; Deibert 2013). Het leidt wellicht ook tot een wapenwedloop in cyberspace (Nye 2011). En, zoals vaker is gebeurd, kan het er zelfs toe leiden dat de reactie op het gevaar op zichzelf weer nieuwe gevaren oplevert. De opkomst van veiligheid als centraal thema op het internet – in plaats van de

economische invalshoek van staten op het internet in de beginperiode – heeft uiteraard grote gevolgen voor de manier waarop verschillende staten hun visie op internetgovernance bepalen en welke prioriteiten ze stellen.

1.3.3 DE DATAREVOLUTIE

De derde ontwikkeling die van belang is voor de toekomst van internetgovernance is 'dataficatie'. Dataficatie kent drie aspecten: de omvang van de data, de aard en de analyse ervan, en het toepassingsbereik (Van Dijck 2014; Mayer-Schönberger en Cukier 2013). De enorme toename van data over menselijk gedrag – al dan niet vrijwillig afgestaan – en de registratie en opslag van data en metadata door zowel bedrijven als overheden hebben het internet en de manier waarop we het internet ervaren veranderd. Data zijn het bloed van internetbedrijven geworden. Bedrijven als Facebook, Twitter en Google verzamelen data over personen in ruil voor hun toepassingen die 'gratis' mogen worden gebruikt. Dankzij mobiele internettechnologie zijn die data allang niet meer beperkt tot gedrag op het internet. De data worden vervolgens gebruikt om adverteerders en klanten zo scherp mogelijk op elkaar af te stemmen. In het huidige tijdperk van big data heeft het adagium dat 'meer beter is' zich ook vertaald in de manier waarop we naar de wereld kijken. Met de toename is eveneens de aard van de dataverzamelingen en de analyse daarvan veranderd. Het combineren van zoveel mogelijk data om daar door middel van statistische analyse – soms onverwachte – correlaties en antwoorden uit te destilleren, wordt gezien als een bron van nieuwe toepassingen en markten in de interneteconomie (Degli Esposito 2014). Ook overheden zien legio toepassingen voor de analyse van grote hoeveelheden gegevens: in de volksgezondheid, in het bestuur van steden en niet in de laatste plaats in het domein van de veiligheid. De dynamiek van big data heeft grote gevolgen voor vraagstukken van privacy en gegevensbescherming (waarover de WRR later in 2015 zal rapporteren),[6] voor de wijze waarop onderzoek wordt verricht (meer datamining en minder hypothesegedreven), alsook voor internationale machtsverhoudingen op en rondom het internet.

Dataficatie is in toenemende mate 'overal'. Typerend is de opkomst van het 'Internet of Things' (kortweg vaak IoT). Cisco Systems, een van de grote spelers, gaat al een stap verder en spreekt van het 'Internet of Everything'. Het IoT verwijst naar de verbindingen tussen tal van apparaten die online met elkaar kunnen 'communiceren'. Dat kunnen telefoons zijn, maar ook koelkasten en auto's en op industrieel niveau kan het gaan om machines en logistieke processen. Een treffende illustratie van deze ontwikkeling en van wat het gebruik van data vermag is Apple Watch. Het horlogeachtige apparaat meet en communiceert de identiteit van de drager, zijn locatie, de activiteiten die hij verricht (via gyroscoop en accellerometer) en pretendeert zelfs de gezondheid en de gemoedstoestand te kunnen nagaan. Met deze ontwikkelingen verplaatsen vragen rond databeheer en veiligheid zich van computer en telefoon naar andere apparaten en gebruiksdoeleinden. Daarmee

wordt tevens het onderscheid tussen online- en offlineactiviteiten verder gerelativeerd, een ontwikkeling waar verschillende onderzoekers in een advies aan de Europese Commissie in 2014 aandacht voor hebben gevraagd in een publicatie met de treffende titel 'Onlife manifesto'.[7]

Nu data zo centraal zijn komen te staan in de manier waarop bedrijven naar hun klanten kijken en overheden naar hun burgers – en die van andere landen – zijn de opslag en huishouding van gegevens ook van belang geworden in het internationale domein. Privacy en databescherming zijn in Europa relatief sterk ontwikkeld en uitgewerkt in wet- en regelgeving, maar de nieuwe werkelijkheid van de datificatie zet grote druk op de waarborgen die daarin zijn vastgelegd. De Europese regels voor databescherming uit 1995 hadden een uitstralingseffect naar de rest van de wereld (een 'Brussels effect' – Bradford 2012). Sinds 2012 wordt in Brussel over nieuwe regels onderhandeld en het is de vraag of de nieuwe verordening eenzelfde werking kan hebben. Sommige aspecten ervan, zoals de omvang van boetes bij misbruik van data, kunnen grote consequenties hebben. De potentie om wereldwijd de standaard te zetten enerzijds en de enorme toename van het gebruik en de waarde van gegevens anderzijds leiden ertoe dat er grote belangen gemoeid zijn met deze nieuwe Europese wetgeving.

Sommige bedrijven weten veel meer van burgers dan overheden, die voorheen eigenlijk de grootste dataverzamelingen onder hun hoede hadden. Dit is overheden uiteraard niet ontgaan. Een van de meest opmerkelijke onthullingen over de NSA was de mate waarin die zijn surveillanceactiviteiten richtte op informatie die door private internetpartijen was verzameld en de mate waarin met name Amerikaanse bedrijven de dienst daarin hielpen (Greenwald 2014). Historicus Timothy Garton-Ash stelde onlangs in een ingezonden stuk in *The Guardian* dat de conclusie eenvoudig was: "were Big Brother to come back in the 21st century, he would return as a public-private partnership" (zie ook Lyon 2014). De onthullingen hebben laten zien hoe sterk de informatiepositie van een aantal hoofdzakelijk Amerikaanse bedrijven is en wat de toegang van overheden daartoe is. Bruce Schneier (2013) stelt dat we nu eigenlijk leven in een feodaal internettijdperk waarin de macht is komen te liggen bij de grote internetbedrijven en overheden. De gebruikers, die in de begintijd van het internet zo vrij en machtig leken, zijn voor veiligheid, privacy en andere rechten online afhankelijk van de feodale heren, zonder daar zelf nog veel invloed op te hebben. De grote internetbedrijven en overheden zijn tot op zekere hoogte tot elkaar veroordeeld, waarbij de machtsbalans soms naar de ene en soms naar de andere partij doorslaat. Het beheer van big data en de mogelijkheid tot verregaande surveillance – commercieel, door overheden of in combinatie – heeft echter ook gevolgen voor internationale machtsverhoudingen en relaties tussen staten onderling.

1.4 NEDERLANDS BUITENLANDS BELEID EN HET INTERNET

De focus van dit rapport ligt op de toekomst van de internationale governance van het internet en op de bijdrage die Nederland daaraan kan leveren, zelfstandig en in het verband van het lidmaatschap van de EU en andere internationale fora. Dat betekent dat dit rapport niet of nauwelijks ingaat op het eveneens zeer belangrijke thema van de nationale governance van cybersecurity en het internet 'binnen' Nederland. Hoewel de organisatie, samenwerking en afstemming van de vele Nederlandse publieke en private actoren op het gebied van het internet van groot belang is, wordt dit in beginsel alleen meegenomen wanneer Nederlandse activiteiten of Nederlands beleid uitstralingseffecten heeft naar het internationale domein. Deze uitstralingseffecten kunnen, zoals eerder gezegd, zowel positief als negatief zijn.

De komende jaren zullen lijnen in het zand worden getrokken die bepalen hoe het net zich verder zal ontwikkelen. De belangen van een open land als Nederland zijn daarbij anders dan de belangen van sommige andere landen die zich in toenemende mate roeren. Het is dus van belang om Nederlandse belangen scherp te definiëren en te behartigen in internationale internetgovernance-fora, zeker op het Europese niveau om het gewicht van de EU waar mogelijk te benutten. Nederland heeft uitstekende 'internetpapieren' en is in de wereld van centrale internetorganisaties als de Internet Engineering Taskforce (IETF), Internet Architecture Board (IAB) en de Internet Research Taskforce (IRTF) altijd goed vertegenwoordigd geweest, ook op kaderposities. Ons land was als een van de eerste landen op het internet aangesloten; de Amsterdam Internet Exchange (AMS-IX) is een van de allergrootste internetknooppunten in de wereld; en Nederland heeft de verklaarde ambitie om de *Digital Gateway to Europe* te zijn. In termen van beleidsaandacht voor het internet en internationale oriëntatie is Nederland een van de voorlopers. Op het internationale vlak is Nederland actief als initiatiefnemer van de *Freedom Online Coalition*, een mondiale coalitie die internationale internetvrijheid voorstaat en uitdraagt. Nederland is binnen de EU lid van de G5, vijf lidstaten van de EU[8] die op internetgebied nauw samenwerken om ambitieus Europees beleid te vormen en de internationale agenda te beïnvloeden. Nederland is ook actief lid van NAVO-netwerken op het gebied van cyberactiviteiten.

De kern van wat dit rapport wil bereiken is het formuleren van een agenda voor het buitenlandbeleid inzake internetgovernance. In die agenda moet een balans worden gevonden tussen enerzijds het waarborgen en beschermen van het internet als een mondiaal publiek goed en anderzijds het normaliseren van het internet als onderdeel van internationale betrekkingen. Internetaangelegenheden zullen, gezien het grote belang van het wereldwijde internet, meer dan nu het geval is een integraal onderdeel van het buitenlands beleid moeten worden.

1.5 OPZET VAN DIT RAPPORT

In hoofdstuk 2 wordt internetgovernance verder uitgewerkt door een analytisch onderscheid te maken tussen 'governance *van* de internetarchitectuur' en 'governance die *gebruikmaakt van* de internetarchitectuur'. Het internet als een publiek goed valt daarbij hoofdzakelijk onder de eerste noemer, maar kan ook in gevaar worden gebracht als staten nationaal beleid dat gebruikmaakt van de internetarchitectuur op een technisch onverstandige manier vormgeven. Hoofdstuk 2 beargumenteert dat het veiligstellen van het internet als een mondiaal publiek goed in essentie een verlengd Nederlands nationaal belang is.

De hoofdstukken 3 en 4 bouwen voort op het analytische onderscheid tussen de governance van het internet en governance die gebruikmaakt van het internet. Hoofdstuk 3 gaat dieper in op de governance van het internet en bespreekt hoe de publieke kern van het internet wordt beheerd. Bij die publieke kern gaat het om waarden als universaliteit, interoperabiliteit, toegankelijkheid, integriteit, beschikbaarheid en vertrouwelijkheid, die 'het internet' als mondiaal systeem aan zijn gebruikers moet garanderen. De vervulling van deze waarden en functies is belegd bij instituties, protocollen en standaarden. Het 'Team Internet' dat deze protocollen en functies beheert, functioneert op een aantal vlakken heel goed en effectief, maar schiet op sommige punten ook tekort. Dat laatste heeft zowel te maken met ontwerpfouten en fricties tussen wat technisch goed is voor het internet en de verdienmodellen van de beheerders van het netwerk (bijvoorbeeld de problematiek van de update van het Internet Protocol van versie 4 naar versie 6) als met politieke en economische druk en belangen en (een gebrek aan) legitimiteit. Andere problemen zijn op de agenda gekomen doordat het groeiende gewicht van het internet in economische en politieke zin ook nieuwe spelers en belangen op het toneel heeft gebracht, die zich bemoeien met het technische functioneren en het beheer van de publieke kern van het internet. Het gaat hier telkens om conflicten die spelen binnen de governance van het publieke internet en die eerder als gevolg van verschuivingen in internationale politieke en/of economische verhoudingen zijn ontstaan dan als gevolg van onvrede over het technische functioneren van het internet.

In hoofdstuk 4 gaat het om – meestal nationale – ontwikkelingen waarin wordt ingegrepen in centrale protocollen en principes. Er komen vier ontwikkelingen aan de orde. Ten eerste een reeks recente nationale wetsvoorstellen en een internationaal verdrag om auteursrecht en intellectueel eigendom op het internet te beschermen. Ten tweede een van de, vanuit het perspectief van de mensenrechtenagenda, moeilijkst oplosbare problemen op het internet: de censuur en de beperking van de vrijheid van meningsuiting. Beide ontwikkelingen illustreren de centrale rol die Internet Service Providers (ISP's) spelen als aangrijpingspunt voor de regulering van het gedrag van consumenten, burgers en bedrijven. Ten derde wordt de groeiende aanwezigheid van inlichtingendiensten en militaire actoren op

het internet besproken, die niet alleen gevolgen heeft voor de privacy, maar ook voor de integriteit van het technische functioneren van het internet. Ten slotte komen pogingen aan de orde van nationale staten om delen van het internet te nationaliseren en wat de gevolgen daarvan zijn voor het functioneren van het net als geheel. In al deze gevallen gaat het om (potentiële) inbreuken op de universaliteit, interoperabiliteit en toegankelijkheid van het internet door acties, beleid en wetgeving die specifieke nationale en/of economische belangen boven het belang van de publieke kern van het internet stellen.

Hoofdstuk 5 bevat tot slot de conclusies en aanbevelingen. De conclusie van dit rapport is dat het op technisch niveau mogelijk is om de integriteit en de betrouwbaarheid van de publieke kern van het internet te beschadigen, waarmee het functioneren van het net als geheel onbetrouwbaar kan worden. De governance van het internet heeft daarom baat bij het organiseren van private en publieke macht en tegenmacht om de integriteit van, en de vrijheid op het internet te versterken. Op basis van drie principes van machtsbinding – menging, scheiding en beteugeling – wordt een aantal aanbevelingen gedaan voor het Nederlands buitenlands internetbeleid. Het eerste streefdoel voor die agenda is de vrijwaring van de publieke kern van het internet van oneigenlijke inmenging door staten op basis van nationale belangen. Het is wenselijk een norm van non-interventie vast te leggen ten aanzien van de centrale infrastructuur van het internet. Het tweede doel richt zich erop internationale internetpolitiek uit het frame van de (nationale) veiligheid te halen, onder meer door een duidelijker onderscheid te maken tussen verschillende vormen van veiligheid en de daarbij betrokken partijen. Het derde punt voor de agenda voor internetdiplomatie richt zich op een verbreding van het diplomatieke werkveld voor buitenlands internetbeleid. Alle aanbevelingen zijn uitgewerkt in een inhoudelijke component en in een aanzet voor een operationele strategie.
De centrale aanbeveling van dit rapport is dat het internet nadrukkelijk – en vooral eigenstandig – een speerpunt dient te zijn van het buitenlands beleid van Nederland.

NOTEN

1 Zie: http://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia.

2 Omdat het technisch mogelijk is om mensen van het internet uit te sluiten is het internet strikt genomen wat economen een 'club good' noemen, omdat de baten alleen ten goede komen aan de deelnemers. De keuze om toch te spreken van een (onzuiver) mondiaal publiek goed heeft te maken met de technische en protocollaire opzet van het internet zoals hiervoor omschreven met universaliteit, interoperabiliteit en toegang als kernwaarden.

3 Alle cijfers in deze subparagraaf zijn, tenzij anders aangegeven, ontleend aan Internet World Stats: www.internetworldstats.com.

4 De schaarste aan goede data heeft te maken met het feit dat veel dreigingen zich afspelen in het private commerciële domein. Bedrijven hebben er om redenen van reputatieschade weinig belang bij dat informatie over hun kwetsbaarheid bekend wordt. Cyberbeveiligingsbedrijven (de MacAfee's van deze wereld) hebben er weer belang bij dat de dreiging als groot wordt ervaren. Verder leveren de inlichtingendiensten materiaal aan voor dreigingsbeelden: deze informatie is niet te controleren en wellicht ook gekleurd (zie ook Broeders 2014).

5 Zie bijvoorbeeld het rapport van Human Rights Watch (2012) getiteld *In the name of security*, waarin 130 landen worden geanalyseerd die in de nasleep van 9/11 antiterrorismewetgeving hebben geïntroduceerd of aangepast. Veel van deze "post-September 11 laws, when viewed as a whole, represent a broad and dangerous expansion of government powers to investigate, arrest, detain, and prosecute individuals at the expense of due process, judicial oversight, and public transparency" (p. 4).

6 Zie: http://www.wrr.nl/actueel/pers/persbericht/article/big-data-privacy-en-veiligheid.

7 Zie: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Manifesto.pdf.

8 Naast Nederland zijn dit Duitsland, het Verenigd Koninkrijk, Frankrijk en Zweden.

2 VRIJHEID, VEILIGHEID EN INTERNETGOVERNANCE

> Internetgovernance structures were originally based on familiarity, trust, and expertise and on 'rough consensus and running code'. Things have changed.
> Laura DeNardis (2014: 18)

2.1 INLEIDING: STATEN EN INTERNETGOVERNANCE

De toekomst van het internet is afhankelijk van de wijze waarop overheden in staat blijken om nationale belangen een plaats te geven in het internetdomein zonder de publieke elementen van het internet aan te tasten. Daarnaast blijft het internet afhankelijk van de inspanningen van een grote groep van actoren uit private, commerciële, technische en civil-societyorganisaties die het internet ontwikkeld hebben tot wat het nu is. In praktische zin zijn zij de ruggengraat van het internet en de motor achter de stormachtige ontwikkeling gedurende de afgelopen dertig jaar. Het feit dat staten nu een grotere rol op het toneel opeisen zal dat noch op korte termijn noch volledig veranderen. Milton Mueller (2010: 8) gebruikt de notie van 'networked governance' om dit systeem van vele actoren te duiden: het internet is technologisch gezien een netwerk van netwerken waar een groot aantal genetwerkte actoren bij betrokken is die vraagstukken van 'rechten, autoriteit en verdeling' op het internet moeten zien op te lossen. Samenwerking is daarbij echter geen gegeven: "wat vandaag een los netwerk is, kan morgen een meer geïnstitutionaliseerde – en mogelijk hiërarchische – vorm van interactie zijn" (Mueller 2010: 8).

We lijken nu op een moment aangekomen te zijn waarin over dat laatste serieus wordt nagedacht. Staten zetten met verschillende beweegredenen druk op de huidige instituties die actief zijn op het terrein van internetgovernance. Soms doen zij dat omdat ze meer ruimte willen om het internetgebruik in eigen land te controleren en het net willen 'nationaliseren'. Een voorbeeld hiervan is het huidige debat over de vraag of de Internet Corporation for Assigned Names and Numbers (ICANN) verantwoordelijk moet blijven voor het toezicht op het beheer van de IP-adressen en de domeinnamen – de zogenoemde IANA-functie (Internet Assigned Names Authority) – of dat dit bij de VN, bijvoorbeeld bij de International Telecommunication Union (ITU) of een andere partij, belegd moet worden. Daarbij speelt natuurlijk het verzet tegen de grote invloed van één nationale staat – de VS – op ICANN een voorname rol. Soms oefenen staten druk uit omdat men van mening is dat de veiligheid van het internet versterkt moet worden. Zo stelt Lewis (2013: 3) dat "het falen om het internet 'veilig' te maken de grootste ondergraving is van de legitimiteit van de bestaande multistakeholderstructuur". En soms laten staten

zich horen omdat de structuren zoals ze in de afgelopen dertig jaar ontstaan zijn weinig recht doen aan de veranderingen in de internationale politieke verhoudingen, zowel op als buiten het internet.

Met de huidige nadruk op nationale veiligheid zijn er echter wel grote zorgen over de *manier waarop* staten hun invloed uitbreiden op het internet. Zoals Ronald Deibert (2013a: 9-10) het formuleert:

> "There is an instinctive tendency in security-related discussions to default to the tradition of realism, with its accompanying state-centrism, top-down hierarchical controls and erection of defensive perimeters to outside threats. In the creation of cyber commands, in spiralling arms races among governments, in 'kill switches' on national Internets and in the rising influence of the world's most secretive agencies into positions of authority over cyberspace, we see this tradition at play."

Anderen delen deze zorg wellicht, maar zijn tegelijk van mening dat het niet meer dan logisch is dat staten nu hun plaats in internetgovernance opeisen. De transitie naar een internet waarin overheden langzaamaan de plaats innemen – of in ieder geval een stoel aan tafel opeisen – van de informele gemeenschappen die nu zo dominant zijn in internetgovernance is op de lange termijn volgens Lewis (2013: 6) zowel wenselijk als onvermijdelijk: "Het vaststellen van grenzen op het internet is net zo min een vorm van balkanisering als het bestaan van grenzen in de fysieke wereld. Alleen zij die nog geloven in een wereldwijde 'commons' kunnen dat nog op die manier interpreteren". Het grenzeloze karakter van het (bestuur van het) internet staat door zijn eigen succes onder druk. Het vertrekpunt voor dit rapport is dat er manieren gevonden moeten worden om enerzijds het belang van staten om vertegenwoordigd te zijn in internetgovernance te faciliteren en anderzijds te blijven waarborgen dat de kern van het internet naar behoren blijft functioneren.

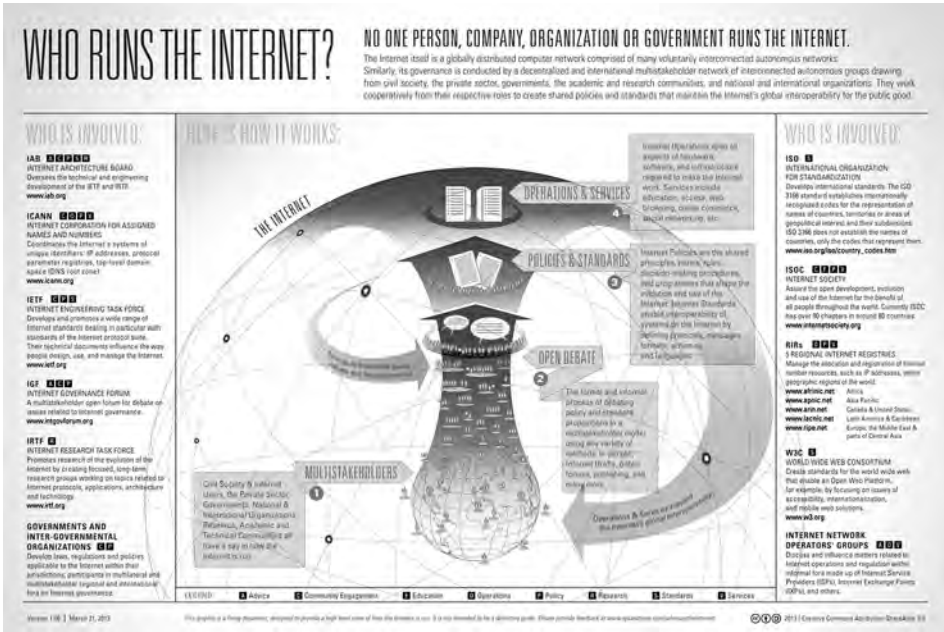
In dit hoofdstuk wordt dat vertrekpunt verder uitgewerkt in een analytisch kader. In paragraaf 2.2 wordt eerst de notie van internetgovernance uiteengezet. Vaak concentreert de literatuur zich op de bonte verzameling van organisaties die daarbij betrokken zijn. Dat kan echter soms het zicht ontnemen op *wat* er nu eigenlijk gereguleerd dient te worden en waarom. In dit rapport ligt de nadruk daarom op de governance van de verschillende technische en socio-technische lagen van het internet, en pas in tweede instantie op de organisaties. In paragraaf 2.3 wordt dit verder uitgewerkt in een onderscheid tussen de 'governance *van* de internetarchitectuur' en 'governance die *gebruikmaakt* van de internetarchitectuur'. Het internet als een mondiaal publiek goed valt daarbij hoofdzakelijk onder de eerste noemer, maar kan ook in gevaar worden gebracht als staten nationaal beleid initieren dat fundamenteel ingrijpt op de internetarchitectuur. In paragraaf 2.4 wordt het model van 'gedistribueerde veiligheid' geschetst, dat als vertrekpunt voor een buitenlandbeleid ten opzichte van het internet kan worden gebruikt. Dit model

vertrekt vanuit vrijheid als centrale waarde en formuleert drie principes – menging, scheiding en beteugeling – die bij de procedurele vormgeving van internetbeleid, met name beleid gericht op veiligheid, meegenomen moeten worden om vrijheid als waarde te borgen. Paragraaf 2.5 beargumenteert ten slotte dat het veiligstellen van het internet als een mondiaal publiek goed in essentie een verlengd Nederlands nationaal belang is.

2.2 SETTING THE SCENE: INTERNETGOVERNANCE

Het internet wordt bestuurd door een conglomeraat van meer en minder formele organisaties die zeggenschap hebben over bepaalde elementen van toegang tot het internet, verdeling van schaarse middelen (zoals IP-adressen) en transport van informatie. Veel daarvan is vastgelegd in een waaier aan protocollen en standaarden waarin de 'rules of the road' voor internetverkeer zijn vastgelegd. Dit geheel wordt vaak samengenomen onder de noemer 'internetgovernance', door Milton Mueller (2010: 9) omschreven als "the simplest, most direct and inclusive label for the ongoing set of disputes and deliberations over how the internet is coordinated, managed, and shaped to reflect policies". Omdat het toneel van internetgovernance bevolkt wordt door een grote verscheidenheid aan actoren die soms heel formeel en soms heel informeel bijdragen aan het bestuur van het internet, spreekt men van een multistakeholdermodel voor het internet. Figuur 2.1 geeft een overzicht van de vele actoren, organisaties en fora die bij internetgovernance betrokken zijn en er zijn vele van dit soort figuren in omloop. De figuur illustreert ook dat het door de bomen van het bos soms zeer moeilijk is om te zien welke beslissingen op welke plaats genomen worden en wat de rol, invloed en positie van de verschillende stakeholders binnen internetgovernance nu werkelijk is.

Figuur 2.1 Stakeholders in het internetecosysteem



Bron: ICANN

Sommigen wijzen er bovendien op dat het label 'internetgovernance' en de organisaties die doorgaans onder dat label besproken worden slechts in beperkte mate de werkelijkheid van de sturende krachten achter de ontwikkeling van het internet dekken. Van Eeten en Mueller (2013) vinden dat de aandacht in de internetgovernanceliteratuur voor formele organisaties als de Internet Corporation for Assigned Names and Numbers (ICANN), het Internetgovernance Forum (IGF) en de World Summit on the Information Society (WSIS) ten koste gaat van andere structuren die minstens evenveel en soms zelfs meer invloed hebben op de daadwerkelijke governance van het internet, zoals innovatieve gebieden als de economie van cybersecurity, netwerkneutraliteit, het filteren en reguleren van inhoud op het internet, het beschermen van auteursrecht en de (peer-to-peer) uitwisseling van bestanden en de inter-connectie afspraken tussen Internet Service Providers (ISP's). Volgens Van Eeten en Mueller (2013: 730) speelt een groot deel van de daadwerkelijke governance van het internet zich juist in deze arena's af.

Internetgovernance lijkt daarmee goed te passen bij het idee van de multi- of policentered governance, waarin er niet noodzakelijkerwijs sprake is van een duidelijke hiërarchie tussen de actoren (zie bijvoorbeeld Marks en Hooghe 2004: 21). In politieke zin is er nauwelijks een hiërarchie op het internet aan te wijzen: er is geen staat, bedrijf of organisatie die 'het internet' als geheel aanstuurt. De protocollen

en standaarden – een belangrijk resultaat van veel van de betrokken actoren – vormen in technische zin de wetten en regels voor het functioneren van het internet zelf. Daarom spreken sommige onderzoekers van "infrastructure-based forms of internetgovernance" (DeNardis 2012; 2009) of over een "regulatory shaping of 'code' – the technologies that underpin the internet – to achieve more efficient outcomes" (Brown en Marsden 2013: ix).

In dit rapport benaderen we internetgovernance niet vanuit de vele verschillende organisaties die zich met het internet bezighouden, maar in eerste instantie vanuit het technische functioneren van het internet, met een nadruk op die delen van het internet die als mondiaal publiek goed gezien kunnen worden. Wat er vanuit dit perspectief onder het begrip internetgovernance verstaan moet worden, wordt inzichtelijk wanneer we de internetarchitectuur als een gelaagde structuur in kaart brengen. In tabel 2.1 staan vier visies op het internet van verschillende onderzoekers die op de essentiële punten overeenkomen en op sommige punten verschillen of andere zaken benadrukken.

Tabel 2.1 Viermaal het internet als een gelaagde structuur

Brown en Marsden (2013: 8)	**Libicki** (2009: 12)	**Choucri** (2012: 8)	**Deibert et al.** (2012: 5)
Inhoud			
Applicaties			
Presentatie			
Sessie			
Transport (TCP)		Actoren	Niveau van ideeën
Netwerk (IP)	Semantische laag	Informatie inhoud	Niveau van regulering
Data Link	Syntactische laag	Logische bouwstenen	Niveau van de code
Fysiek	Fysieke laag	Fysieke fundering	Fysieke infrastructuur

De gelaagde indelingen in de tabel kunnen in principe tot drie lagen worden teruggebracht. De onderste laag bevat de fysieke en technische infrastructuur, die de transportfunctie mogelijk maakt, en die deel uitmaakt van het mondiale publieke goed. De bovenste laag is de sociaaleconomische laag van het internet en kan worden gezien als de laag waar het geld wordt verdiend en mensen met elkaar interacteren. Dit is het alledaagse gezicht van het web. Hier is de politieke strijd om het internet en wat er wel en niet toelaatbaar is in die 'publieke' ruimte het grootst, maar het is geen mondiaal publiek goed. Tot slot is er een middelste laag van protocollen, standaarden, codes en organisaties die de hardware en diepere laag van software van het net laten draaien en die een belangrijk aangrijpingspunt vormen voor staten om het internet te reguleren, zowel nationaal als internationaal. Sommige delen daarvan kunnen worden gezien als onderdeel van het mondiale publieke goed, andere niet of minder. Een precieze afbakening is niet eenvoudig te maken en is onderhevig aan verandering en verschillen van inzicht. In deze laag woedt een

strijd tussen ingenieurs, bedrijven, internationale organisaties en overheden over de vraag wat als publiek goed gezien moet worden, en derhalve een bijzondere bescherming zou moeten krijgen.

2.3 TWEE VORMEN VAN INTERNETGOVERNANCE

Om scherp te krijgen wat in dit licht de belangrijkste elementen van internetgovernance zijn, sluiten we aan bij een onderscheid dat Laura DeNardis (2012; 2013; 2014) heeft aangebracht. Zij maakt een vitaal en zeer nuttig onderscheid tussen 'governance *of* the internet's infrastructure' en 'governance *using* the internet's infrastructure' (DeNardis 2012: 726). De governance *van* de internetinfrastructuur gaat over het bestuur, de organisatie en de ontwikkeling van de diepere lagen van het internet; anders gezegd, het gaat hier om het internet onder de motorkap dat de ontwikkeling van het internet stuurt. Deze noemer dekt een aantal van de vitale infrastructuren en protocollen die als een mondiaal publiek goed gezien kunnen worden. In het geval van governance die *gebruikmaakt* van de internetinfrastructuur wordt het internet ingezet als een middel in de strijd om content, oftewel inhoud, op het net te controleren. Dat kan variëren van het beschermen van auteursrecht en intellectueel eigendom tot het censureren en surveilleren van burgers door overheden. Dit is een belangrijk element van internetgovernance en van internationale politiek en mensenrechten, maar raakt meestal niet direct aan het internet als een mondiaal publiek goed. Op sommige momenten, met name als staten in het kader van nationale belangen, zoals veiligheid, diep in de techniek van het internet ingrijpen, raakt het daar wel aan.

2.3.1 GOVERNANCE VAN DE INTERNETINFRASTRUCTUUR

De governance van de internetinfrastructuur gaat om het aansturen van de diepe lagen van het internet: het gaat om de essentiële technische en de logische infrastructuur. Het meest basale antwoord op de vraag 'wanneer is iemand op het internet?' is: wanneer iemand het Internet Protocol (IP) gebruikt. Het IP is een van de cruciale standaarden die maken dat het internet als een mondiaal publiek goed kan worden aangemerkt. DeNardis (2013) noemt drie gebieden van het internetgovernancesysteem die op het meest basale niveau een belangrijke rol spelen. Het gaat om (1) controle over de 'Critical Internet Resources', in het bijzonder het beheer van de domeinnamen, top-leveldomeinnamen en IP-adressen; (2) het vaststellen van internetstandaarden en -protocollen (zoals het TCP/IP-protocol); en (3) om de zogenoemde 'Interconnection agreements', die het verkeer tussen de verschillende netwerken van het internet (een netwerk van netwerken immers) regelen en beprijzen. Niet alles wat onder de vlag van deze drie gebieden tot stand komt is ook daadwerkelijk onderdeel van het mondiale publieke goed van het internet, maar als eerste, grove afbakening is het nuttig. Er worden ook veel standaarden en protocollen ontwikkeld die weliswaar van belang zijn voor het internet of het WWW maar die niet in dezelfde mate bijdragen aan het karakter van het internet als een mon-

diaal publiek goed. Bijvoorbeeld, het beruchte Bittorrent Protocol – dat in de volksmond een-op-een met internetpiraterij wordt gelijkgesteld – is niets meer dan een protocol voor het peer-to-peer delen van bestanden. Een handig protocol maar geen protocol dat de kern van het internet raakt. Het Internet Protocol daarentegen zet de standaard die het mogelijk maakt dat alle computers die het gebruiken elke vorm van informatie met elkaar uit kunnen wisselen, hetgeen bijdraagt aan het universele en non-rivale karakter van het net. Het Hypertext Transfer Protocol (HTTP) bepaalt bijvoorbeeld op welke manier webclients – zoals zoekmachines – communiceren met webservers waarop de inhoud staat en is daarmee ook een van de centrale protocollen.[1]

Het internet als een mondiaal publiek goed functioneert naar behoren als bepaalde kernwaarden of principes voor het functioneren van het internet als systeem zijn gewaarborgd. Ook zijn er bepaalde waarden toe te kennen aan de veiligheid van de informatie die op het internet circuleert, of beter, die wij als gebruikers op het internet laten circuleren. Deze verschillende waarden die in tabel 2.2 worden opgesomd, zijn vervolgens weer het fundament onder het vertrouwen dat wij – als gebruikers – wel of niet in het internet stellen.

Tabel 2.2 Waarden in relatie tot het functioneren van internet en informatieveiligheid

Kernwaarden van het internet	Architectuurprincipes van het internet	Kerndoelen van informatieveiligheid
Universaliteit Interoperabiliteit Toegankelijkheid	Openheid Interoperabiliteit Redundantie End-to-end	Vertrouwelijkheid Integriteit Beschikbaarheid
DeNardis (2013: 4)	Ziewitz en Brown (2014)	Singer en Friedman (2014: 35)

DeNardis (2013: 4) formuleert drie kernwaarden: universaliteit, interoperabiliteit en toegankelijkheid. Die waarden zorgen ervoor – ceteris paribus – dat het internet voor gebruikers in Den Haag op dezelfde manier fungeert als in New York of Bangalore. Deze waarden, die bij de ontwikkeling van het net voorop hebben gestaan, schragen het idee van het internet als een mondiaal publiek goed. Ziewitz en Brown (2014) benoemen vier architectuurprincipes die ongeveer dezelfde waarden dekken: openheid, interoperabiliteit, redundantie en 'end-to-end' (het principe dat specifieke functies voor applicaties in de eindpunten van het netwerk zijn opgenomen en niet in de tussenliggende knooppunten – het netwerk zelf is 'dom'). Een derde set van waarden vertrekt vanuit het idee van de informatieveiligheid en kent drie kerndoelen:[2] vertrouwelijkheid, integriteit en beschikbaarheid (Singer en Friedman 2014: 35). Vertrouwelijkheid houdt in dat je ervan uit moet kunnen gaan dat je informatie en data privé blijven. Integriteit houdt in dat het systeem en data in het systeem niet zonder de juiste autorisatie zijn veranderd of aangepast. Of, korter gezegd, zonder integriteit kun je het informatiesysteem

niet meer vertrouwen. In internettermen zou je hierbij kunnen denken aan routing. Het internet is technisch zo opgezet dat pakketjes informatie – zonder controle van de inhoud daarvan – altijd verstuurd en doorgeleid worden. Als de integriteit van het internet onder druk komt te staan – je weet niet meer zeker of informatie wel of niet aankomt en wel of niet veranderd is – heeft dat grote gevolgen voor het vertrouwen in het internet en voor alle sociale en economische activiteiten die we inmiddels via het internet laten verlopen. Beschikbaarheid spreekt eigenlijk nog het meest voor zich en heeft ook een directe link met betrouwbaarheid en vertrouwen.

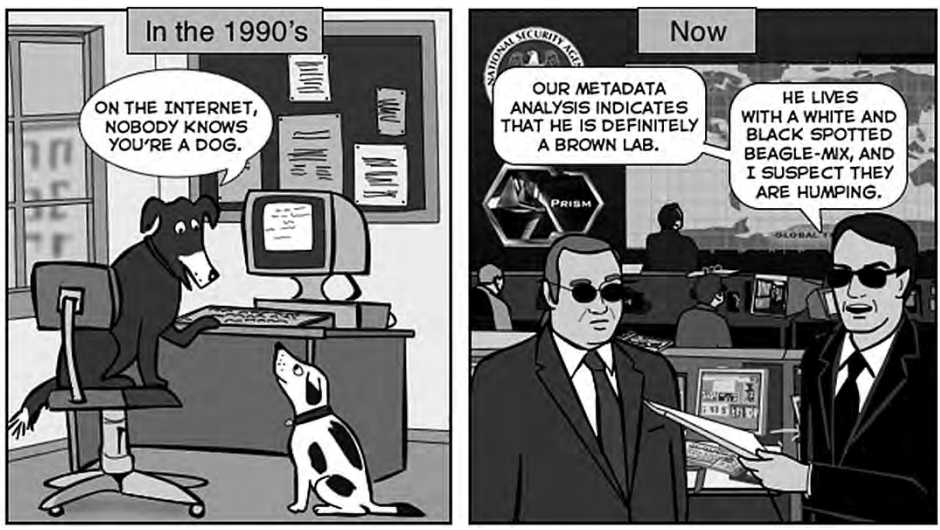
In principe sluiten deze sets van waarden en kerndoelen prima bij elkaar aan. De centrale waarden van het internet en de internetarchitectuur worden ondersteund door de kerndoelen van informatieveiligheid. Tezamen waarborgen ze de integriteit van het functioneren van het internet als een publieke infrastructuur en zijn als zodanig richtinggevend voor de governance *van* de internetinfrastructuur, opgevat als een mondiaal publiek goed. Het vertrouwen van gebruikers in het internet is gebouwd op het goed functioneren van die kern, en dus op het goed functioneren van de verantwoordelijke governancestructuren. Gebruikers wordt hier breed opgevat, variërend van individuele gebruikers tot kleine en zeer grote publieke en private gebruikers. Het probleem is echter dat deze waarden niet specifiek belegd zijn bij deze of gene partij of organisatie: in principe zijn alle bij de governance van het internet betrokken organisaties ervoor verantwoordelijk. Dat is uiteraard geen eenvoudig uitgangspunt, zeker niet in een tijd waarin ook andere politieke en economische belangen steeds zwaarder mee gaan wegen, of dat vanuit het perspectief van de governance van het internet nu als legitiem kan worden gezien of niet. Het belang van de waarden moet daarom ondersteund worden met het meer procedurele perspectief van de 'gedistribueerde veiligheid' dat in paragraaf 2.4 wordt uitgewerkt.

2.3.2 GOVERNANCE DIE GEBRUIKMAAKT VAN DE INTERNETINFRASTRUCTUUR

De tweede vorm van governance is gericht op het reguleren van het gedrag van mensen, groepen en bedrijven ('the governed'), waarbij gebruik wordt gemaakt van (technische aspecten) van het internet. Vaak gaat het om nationaal beleid – ideeën over de grenzen van de vrijheid van meningsuiting, bescherming van intellectueel eigendom en copyright, en veiligheid en opsporing – en wordt de internetinfrastructuur als instrument van regulering gebruikt. Reguleren wat wel en niet mag in de publieke ruimte van het internet is ingewikkeld omdat het internet in essentie een mondiaal systeem is. Tegelijkertijd is die mondiale publieke ruimte ook weer deels herkenbaar als een nationale ruimte, bijvoorbeeld vanwege de taal (Nederlandstalige websites), domeinnamen (.nl) en links met personen, organisaties en bedrijven die in Nederland actief zijn. Hetzelfde geldt voor de regulering van die internationale en tegelijkertijd nationale publieke ruimte. De gedachte dat die publieke ruimte en de personen en organisaties die zich daarin

ophouden niet te reguleren zijn, wordt niet vaak meer gehoord. Zoals al in hoofdstuk 1 is aangeven: de Chinezen (en vele landen met hen) hebben Bill Clintons Jell-O inmiddels stevig aan de muur gespijkerd. De anonimiteit van gebruikers, die zo kenmerkend was voor het vroege internet, is in rap tempo afgebroken door bedrijven en overheden. Alleen diegenen die de extra moeite nemen om zich af te schermen met encryptie en programma's als TOR (The Onion Router) en PGP (Pretty Good Privacy) zijn online veel moeilijker traceerbaar en identificeerbaar. In onze huidige wereld van big data, cloud computing, de opkomst van the Internet of Things en mobiel internet zijn we steeds transparanter en traceerbaarder geworden. De beroemde anonieme hond op het internet die in 1993 in de *New Yorker* stond, ziet er anno 2014 heel anders uit.

Figuur 2.2 Anonimiteit en het internet, toen en nu



Bron: The Joy of Tech

Tegelijkertijd is het grootste deel van het internet – het zogeheten 'deep web' – nog steeds onontgonnen terrein voor de meeste gebruikers; het onttrekt zich voor een groot deel aan regulering. Ook allerhande zwarte markten – zoals het beruchte en inmiddels 'gesloten' Silk Road waar alles te krijgen was van een online DDOS-aanval tot een offline huurmoordenaar – bevolken het deep web (Ablon et al. 2014). Overheden hebben de grootste moeite om cybercrime en cyberaanvallen die vaak vanuit andere landen en/of uit de diepe lagen van het web komen effectief aan te pakken.

Vanwege een brede waaier aan nationale belangen proberen staten te interveniëren in het gedrag van burgers, consumenten en internetgebruikers. Als het gaat om onlinegedrag doen ze dat soms door in te grijpen in, of aan te haken bij de techni-

sche infrastructuur van het internet, of bij de centrale intermediaire spelers van het internet die de eindgebruikers faciliteren om op het net te komen (internetaanbieders) en daarop te navigeren (zoals zoekmachines). Politie, justitie en inlichtingendiensten vragen bijvoorbeeld in het kader van opsporingsonderzoek gegevens van internetgebruikers op bij internetbedrijven als Google en Facebook. Die bedrijven publiceren daar overigens weer transparantierapporten[3] over die inzicht bieden in welke autoriteiten dat doen en hoe vaak ze dat doen. Wat inlichtingendiensten opvragen mag in die rapporten meestal niet vermeld worden en bovendien is inmiddels overduidelijk dat deze ook lang niet altijd om toestemming vragen. Overheden richten zich vaak tot de intermediaire actoren op het internet om het gedrag van internetgebruikers te reguleren, zoals het tegengaan van illegaal downloaden of belediging en laster, en in vele landen ook de surveillance en censuur van allerlei activiteiten die hier legaal en door mensenrechten beschermd zijn. Internet Service Providers zijn bijvoorbeeld vitale verdeelpunten op het internet. Voor overheden zijn zij in veel gevallen de ideale kandidaten om regulering uit te voeren, variërend van het blokkeren van kinderporno tot de censuur van politieke meningen. Hier raakt deze vorm van internetgovernance, zeker in de internationale betrekkingen, aan het vitale terrein van internetvrijheid en verdediging van de internationale mensenrechten in het internetdomein. Deze strijd staat echter niet centraal in dit rapport.

Als het gaat om de governance die gebruikmaakt van de internetarchitectuur kan het ook zo zijn dat een beleidsingreep rechtstreeks gevolgen heeft voor het functioneren van het internet als systeem. Dat kan gebeuren wanneer nationaal beleid eisen stelt of ingrepen doet in de centrale protocollen en mechanismen waar het internet op draait. Dan raakt nationaal beleid dat zich richt op het reguleren van gedrag van actoren *op* het internet ook aan de kern *van* het internet. Het raakt aan het mondiale publieke goed. Een goed voorbeeld zijn de twee Amerikaanse wetsvoorstellen die online piraterij moesten bestrijden en copyright beschermen: SOPA en PIPA.[4] De uitvoering van deze wetsvoorstellen zou diep ingegrepen hebben in het Domain Name System (DNS), dat webadressen zoals wij ze gebruiken (www.wrr.nl) 'vertaalt' naar IP-adressen (80.95.169.156) zoals het Internet Protocol ze kent. Door de ingrepen voorzien in deze wetten zouden sites die malafide bevonden waren door de Amerikaanse overheid de facto onbereikbaar worden, maar zou ook de stabiliteit van het DNS-systeem als geheel in gevaar komen. Of, in de woorden van DeNardis (2014: 8) "The SOPA/PIPA legislation would have required modifications to internetgovernance technologies, changes with direct implications for security and freedom". Dergelijk beleid gaat ten koste van kernwaarden van het internet als universaliteit en integriteit. In dit rapport staan, als het gaat om de governance die gebruikmaakt van internetarchitectuur, met name die ontwikkelingen centraal die ook raken aan het functioneren van het internet als een mondiaal publiek goed.

2.4 VRIJHEID ALS VERTREKPUNT: GEDISTRIBUEERDE VEILIGHEID

Het is duidelijk dat het internet als een internationaal netwerk het beste gedijt bij voldoende vrijheid (voor communicatie en innovatie) en bij voldoende veiligheid (het voorkomen van schade en behoud van vertrouwen in het internet). Hoe dat vanuit een beleidsperspectief vormgegeven en ondersteund moet worden – met name in het internationale domein – is echter nog niet zo eenvoudig. Nederland heeft zowel de vrijheid als de veiligheid van en op het internet hoog in het vaandel staan (Ministerie van VenJ 2011; 2013a; 2013b; Ministerie van Buitenlandse Zaken 2011; 2013; Ministerie van Defensie 2012; 2013). Dergelijke vitale, maar ook abstracte, waarden zijn echter vaak weinig sturend voor het beleid in de praktijk. Ze zijn eerder inspirerend dan dat ze richtinggevend zijn en uit de meeste waarden op dit abstractieniveau vallen vele verschillende en soms tegenstrijdige normen af te leiden (WRR 2003). Interpretaties van vrijheid en veiligheid lopen sterk uiteen van land tot land en dat geldt ook op het internet. Hetzelfde geldt in mindere mate voor de waarden en architectuurprincipes van het internet en de kerndoelen van informatieveiligheid die in paragraaf 2.3.1 werden geïnventariseerd. Hoewel deze waarden en principes al een slag concreter zijn dan vrijheid en veiligheid – en van groot belang zijn voor het vertrouwen in het functioneren van het internet – zijn ze alleen sturend als verschillende partijen binnen de governancestructuren van het internet ze actief ondersteunen. Ook hier geldt dat belangen en interpretaties uiteen kunnen lopen. Waarden – zowel op het hoogste niveau als op een meer operationeel niveau – worden daarom in de onderstaande uitwerking ondersteund door een procedureel perspectief dat uitgaat van 'checks and balances' en als doel heeft de publieke kern van het internet te beschermen.

Zonder de inspiratie van deze fundamentele kernwaarden te verliezen, verleggen we in dit rapport de aandacht naar een meer *procedurele* opvatting van veiligheid, die erop gericht is veiligheid te vergroten maar in dat proces bovenal de vrijheid te waarborgen. Hier sluiten we aan bij de ideeën van Ronald Deibert over *gedistribueerde veiligheid* (2012; 2013a; 2013b; 2014). Dit model gaat ervan uit dat het vergroten van veiligheid samen moet gaan met het instellen van checks and balances op en tussen de actoren die belast zijn met de veiligheid van de staat. De grondslag van de liberale staat is vrijheid, en veiligheid mag slechts in zeer beperkte mate ten koste van die vrijheid gaan.[5] "Gedistribueerde veiligheid benadrukt checks and balances op de macht, toezicht en autoriteit en bescherming voor rechten en vrijheden. Het is onderdeel van een traditie van de inperking van macht en geweld die in het hart van liberaal-republikeinse theorievorming over veiligheid staat en terug gaat tot het oude Griekenland" (Deibert 2012: 16).

Deibert stelt dat het model van gedistribueerde veiligheid vooral van belang is in een wereld waarin staten het internet in toenemende mate bekijken door de bril van nationale veiligheid. De natuurlijke neiging tot geheimhouding, het uitbreiden

van invloed en bevoegdheden van overheidsdiensten verantwoordelijk voor de nationale veiligheid en het vaak beperkte juridisch en democratisch toezicht op deze bevoegdheden, moeten worden ingebed in een model dat deze macht bindt en tegenmacht organiseert en verankert op het nationale niveau, en waar mogelijk op het internationale niveau. Op die manier kunnen fundamentele vrijheden en rechten beter worden beschermd en worden liberale staten gedwongen om nationaal een consistente visie op veiligheid en vrijheid op te bouwen en deze internationaal uit te dragen. De structuren die de politieke macht ten aanzien van het internet moeten binden en controleren, moeten worden gebouwd op drie principes (Deibert 2013a: 11-12):

- *menging:* het intentioneel bijeenbrengen van meerdere partijen met eigen rollen en verantwoordelijkheden in een domein van governance;
- *scheiding:* een ontwerpprincipe waarbij geen van deze partijen in staat is het domein te beheersen zonder de medewerking en/of instemming van andere partijen;
- *beteugeling:* het inperken van macht met checks and balances tussen de verschillende betrokken partijen.

Deze principes, herkenbaar als de klassieke beginselen van de rechtsstaat, grijpen terug op oude tradities van machtenscheiding en machtenspreiding, zoals die bijvoorbeeld vorm werden gegeven in het Romeinse rijk en in de traditie van de Amerikaanse *founding fathers*. Deze principes zijn binnen een nationale context vrij herkenbaar. De machtenscheiding of machtenspreiding tussen de uitvoerende, de wetgevende en de rechtsprekende macht is het klassieke – maar ook op nationaal niveau zelden volledig doorgevoerde – ideaalbeeld. Ook verschillende vormen van toezicht, accountability en gedeelde verantwoordelijkheden op beleidsterreinen zijn voorbeelden van *scheiding, menging en beteugeling*. Het internationale domein is echter geen gesloten politiek systeem met een verdeling van machten, noch is het een democratisch en rechtsstatelijk staatssysteem met een afgebakende bevolking, volksvertegenwoordiging, regering en rechterlijke macht. Dat wil niet zeggen dat er geen wet- en regelgeving in het internationale domein geldt. Er zijn verdragen, er is internationaal recht en er zijn (regionale) gerechtshoven met een bindend gezag. Maar het punt is dat er geen autoriteiten zijn die consequent en systematisch toezien op naleving, hoewel ad-hoc-coalities, al dan niet met politieke steun en legitimiteit van de VN, sommige regels soms afdwingen of daar toezicht op houden. Het internationale systeem is gebouwd op het fundament van de territoriale integriteit van soevereine nationale staten. Het horizontale en mondiale internet staat daar tot op zekere hoogte haaks op.

Interessant is echter dat de huidige opzet van internetgovernance al een aantal elementen heeft van het model van gedistribueerde veiligheid gebouwd op de principes van scheiding, menging en beteugeling. Met name het meer technische deel van het bestuur van het internet functioneert tot op zekere hoogte langs lijnen van

de drie principes. Mueller et al. (2013) stellen dat de technische gemeenschap op een non-hiërarchische en vrijwillige manier samenwerkt om internetproblemen op te lossen. Daarbij gaat het om serieuze problemen zoals cybersecuritydreigingen, denk aan botnets en malware, en zelfs ook om centrale processen als routing. De technische gemeenschap fungeert daarbij als wat Haas (1992) als 'epistemic communities' beschreef: "een netwerk van professionals met een erkende expertise en competentie in een gegeven terrein en een gezaghebbende claim op beleidsrelevante kennis in dat domein". Volgens Deibert is de opgave dan ook om deze peer-to-peer gemeenschappen juist te versterken en beter in te bedden in waarborgen langs lijnen van de drie principes. Dat gaat echter tegen de huidige stroom in: de algemene trend is in de richting van meer inmenging door staten, hybride vormen van netwerken en hiërarchieën, toenemende geheimhouding en de politisering van standaarden (Deibert 2014: 50).

Het model van gedistribueerde veiligheid verbindt ook het nationale met het internationale, omdat een gebrek aan verankering van deze principes in nationaal (veiligheids)beleid ook de kracht van het buitenlands beleid ondermijnt: "a country cannot lament the loss of rights and freedoms internationally when those very rights and freedoms are being eroded at home" (Deibert 2012: 17). Het meest voor de hand liggende voorbeeld is het verlies aan moreel leiderschap van de VS op het gebied van internetgovernance, als gevolg van de onthullingen over de surveillanceprogramma's van de NSA (Greenwald 2014). Nederland en de VS liggen op veel dossiers binnen het internetdomein op een lijn, maar de onthullingen hebben de VS geen goed gedaan. De onthullingen stralen internationaal uit naar het 'kamp' waartoe de VS en Nederland beide behoren en binnen dat kamp is het vertrouwen in een gedeelde opvatting van vrijheid en veiligheid beschadigd. Naast het probleem van de surveillance en spionage zelf, heeft dat dus ook gevolgen voor de internationale inzet en positie van Nederland op het belangrijke moment dat veel landen keuzes zullen gaan maken op het gebied van internetgovernance. Maar de verbinding tussen het nationale en het internationale kan ook een heel andere gedaante aannemen. Het veiligheidsdenken rondom internet leent zich uitstekend voor een moderne digitale versie van een oud probleem binnen de internationale politiek: het veiligheidsdilemma. Jervis (1978: 169) omschreef het dilemma als volgt: "many of the means by which a state tries to increase its security decrease the security of other". En de reactie op die toegenomen onveiligheid van de ander kan op zijn beurt weer de onveiligheid van de eerste staat vergroten. Een digitale wapenwedloop kan uiteindelijk de veiligheid van allen – om nog maar te zwijgen van het internet zelf – sterk verkleinen. Het principe van beteugeling staat volgens Deibert dan ook het sterkst onder druk en zou in een buitenlands beleid de meeste aandacht moeten krijgen.

2.5 CONCLUSIE: INTERNETGOVERNANCE EN DE VERLENGDE NATIONALE BELANGEN VAN NEDERLAND

Nederland heeft een groot belang bij een vrij, open en veilig internet. Bovendien wil Nederland graag als de digitale poort tot Europa fungeren (Ministerie van ELI 2011; Ministerie van VenJ 2013a). Het is daarbij van belang dat een aantal kenmerken van het internet die dragend zijn geweest voor het succes en de groei van het internet ook in de toekomst worden gewaarborgd en waar nodig beschermd. Een aantal kerndelen van het internet kan, zoals hiervoor is omschreven, aangemerkt worden als een mondiaal publiek goed. Voor Nederland, met zijn open economie en internationale oriëntatie, levert het publieke goed van een open internet zoveel voordeel op, dat het ook als een verlengd nationaal belang kan worden gezien. De WRR (2010) gebruikte deze term om aan te geven waar de nationale belangen van Nederland raken aan strategische mondiale vraagstukken die als mondiaal publiek goed gedefinieerd kunnen worden. De opdracht voor de Nederlandse overheid is daarbij: (a) om te bezien op welke wijze deze publieke goederen zich verhouden tot Nederland en tot de belangen van Nederlandse burgers; (b) na te gaan waar de meest tastbare aanhechtingspunten tussen die mondiale publieke goederen en de Nederlandse belangen zitten; en (c) te onderzoeken op welke wijze en in welke mate Nederland kan en wil bijdragen aan het veiligstellen daarvan (WRR 2010: 61).

De manier om deze opdracht vorm te geven is door allereerst een analytisch onderscheid te maken in het brede terrein van internetgovernance. Het onderscheid tussen de governance *van* de internetinfrastructuur en de governance *die gebruikmaakt* van de internetinfrastructuur geeft een eerste houvast. Het publieke goed van het internet moet met name gewaarborgd worden in de governance *van* het internet, dat in de regulering van de diepe technologische en logische lagen van het internet moet voorzien. Tegelijkertijd moet voorkomen worden dat staten die hun nationale belangen op het internet willen veiligstellen, dit op een manier doen die raakt aan de vitale protocollen en infrastructuren van het internet. Door de toegenomen *securitisation* van het internet en de steeds grotere rol die staten in internetgovernance opeisen, neemt de kwetsbaarheid van de diepe lagen die het collectieve karakter van het internet belichamen toe. Door nationaal beleid kunnen verstoringen optreden waardoor de universaliteit, interoperabiliteit en toegankelijkheid van het internet als geheel (DeNardis 2014) of de vertrouwelijkheid, integriteit en beschikbaarheid van het internet als een informatiesysteem (Singer en Friedman 2014) onder druk komen te staan. Dat brengt schade toe aan het publieke goed dat het internet is en waarop een groot deel van onze economie en samenleving is gebouwd. De voornoemde waarden en principes moeten worden gekoppeld aan een procedureel perspectief dat kan helpen bij de vormgeving van toekomstige internetgovernance. De inzet zou moeten zijn om internetgovernance te benaderen aan de hand van het model van de gedistribueerde veiligheid. Dit model

gaat uit van het principe dat het vergroten van veiligheid samen moet gaan met het instellen van checks and balances op en tussen de actoren die belast zijn met de veiligheid van de staat. Om de vrijheid – de grondslag van de liberale traditie waaruit gedistribueerde veiligheid is afgeleid – te waarborgen, moet in de ontwikkeling van internetgovernance zoveel mogelijk gewerkt worden met de principes menging, scheiding en beteugeling, die macht scheiden, inperken, transparant maken en onder toezicht stellen.

NOTEN

1 Soms worden de centrale protocollen samengenomen onder de noemer van TCP/IP en omvatten dan ook de volgende protocollen: het e-mailprotocol SMTP (Simple Mail Transfer Protocol), het protocol dat het delen van bestanden mogelijk maakt (FTP, File Transfer Protocol) en HTTP (Hypertext Transfer Protocol) (DeNardis 2014: 67).

2 Deze waarden worden ook wel de CIA-triade genoemd: vertrouwelijkheid (Confidentiality), integriteit (Integrity) en beschikbaarheid (Availability).

3 Zie bijvoorbeeld: http://www.google.com/transparencyreport/ en https://www.facebook.com/about/government_requests.

4 SOPA staat voor Stop Online Piracy Act en PIPA staat voor Protect Intellectual Property Act. Beide wetten zijn inmiddels, waarschijnlijk definitief, ingetrokken.

5 Of zoals Bauman et al. (2014: 139) het formuleren: "The liberal example is one of security through liberty, not security at the expense of liberty".

3 DE GOVERNANCE VAN HET PUBLIEKE INTERNET

> Internetgovernance functions have been around for far longer than the term internetgovernance.
> Laura DeNardis (2009: 13)

3.1 HET INTERNET ALS EEN PUBLIEK GOED

De publieke kern van het internet wordt in essentie belichaamd door een aantal abstracte waarden. Deze waarden, zoals universaliteit, interoperabiliteit, toegankelijkheid, integriteit, beschikbaarheid en vertrouwelijkheid, zijn de kernwaarden die 'het internet' als mondiaal systeem aan zijn gebruikers moet garanderen. Het gaat in essentie om functionaliteiten. Deze wat etherisch geformuleerde kern heeft op sommige punten een heel praktische uitwerking. Het praktische zit hem erin dat de vervulling van dergelijke waarden en functies belegd is bij instituties, protocollen en standaarden. Dit hoofdstuk gaat over deze instituties, protocollen en standaarden die de publieke kern van het internet ondersteunen en waarborgen en over de nieuwe problemen die daarbij zijn ontstaan als gevolg van technologische, economische en politieke ontwikkelingen.

Zoals DeNardis (2009: 13) stelt, is internetgovernance veel ouder dan de term zelf. Die governance is in de korte geschiedenis van het internet echter wel sterk veranderd en geprofessionaliseerd. Het schrift waarin internetpionier Jon Postel in de begindagen van het net bijhield wie welk IP-adres had gekregen is al lang geleden vervangen door een professionele organisatie die de nu bijna vier miljard uitgegeven IP-adressen beheert. De organisatie – ICANN – die deze zogeheten IANA-functie beheert (Internet Assigned Numbers Authority), is omstreden en er woedt een discussie over de vraag of deze *organisatie* nu wel de beste kandidaat is om deze kern*functie* van het internet vorm te geven. Met andere woorden, het feit dat ooit voor een bepaalde oplossing is gekozen is geen voldoende argument om een bepaalde oplossing voort te laten bestaan. Wíe een functie vervult is van minder belang dan dát die functie vervuld wordt, zolang de waarden van het internet maar gewaarborgd zijn. De groei van het internet heeft voor meer governanceproblemen gezorgd dan alleen de noodzaak om het schrift van Jon Postel te vervangen. Sommige van die problemen zijn van technische aard en hangen samen met de groei van het netwerk zelf (bijvoorbeeld de noodzaak van een update van het Internet Protocol van versie 4 naar versie 6). Andere problemen zijn op de agenda gekomen omdat het groeiende gewicht van het internet in economische en politieke zin ook nieuwe actoren en belangen op het toneel heeft gebracht. Sommige nieuwe actoren bemoeien zich met het technische functioneren en het beheer van de publieke kern van het internet. De blik van de ingenieur krijgt gezelschap van een economische en een (geo)politieke invalshoek op het functioneren van het net en dat levert op sommige dossiers spanningen op.

Als het gaat om de kern van het internet als een publiek goed dan spreken we – in de terminologie van hoofdstuk 2 – van de governance *van* de internetinfrastructuur. Hoewel de afbakening van wat tot die kern behoort niet volledig scherp te trekken is, behoort een aantal protocollen en functies ontegenzeggelijk tot het publieke goed van het internet. Die protocollen en functies zijn in handen van een aantal organisaties. Tezamen functioneert dit Team Internet – waartoe we zowel de organisaties als de protocollen zelf rekenen – op veel vlakken heel goed en effectief, maar schiet op sommige punten ook tekort. Dat laatste kan zowel met ontwerpfouten en technisch onvermogen te maken hebben als met politieke en economische druk en belangen en (een gebrek aan) legitimiteit. In paragraaf 3.2 wordt eerst Team Internet uiteengezet: dat wat tot de kern van het publieke goed van het internet gerekend kan worden en welke organisaties dat beheren en uitvoeren. De paragraaf geeft bovendien een kort overzicht van de grootse prestaties van dit Team Internet in termen van de groei van het netwerk en haar gebruikers en de sociaaleconomische rijkdom die daarop gebouwd is. Paragraaf 3.3 gaat in op een aantal van de grotere conflicten die spelen *binnen* de governance van het publieke internet die eerder als gevolg van verschuivingen in internationale politieke en/of economische verhoudingen zijn ontstaan dan als gevolg van onvrede over het technische functioneren van het internet. Paragraaf 3.4 vat het hoofdstuk samen en trekt conclusies.

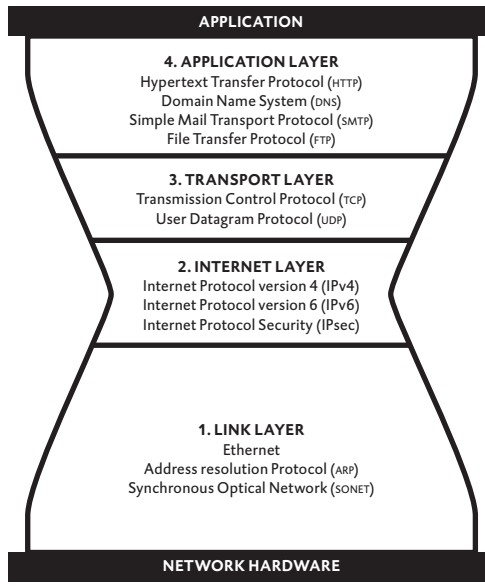
3.2 TEAM INTERNET: WIE 'STUURT' DE KERN VAN HET INTERNET AAN?

Er zijn verscheidene manieren om naar de governance van het internet als publiek goed te kijken. In termen van mensen en organisaties zijn er de bedenkers, de beheerders en de uitvoerders. In termen van technologie zijn met name de protocollen en de standaarden van belang en in sommige gevallen ook de harde infrastructuur. Uiteraard lopen deze functies en rollen op sommige punten door elkaar. Team Internet bestaat derhalve uit een groot aantal personen en organisaties – het merendeel actief in de private sector en/of civil society en een minderheid in de overheidssfeer – en uit technische standaarden en protocollen. Deze laatste mogen dan technisch zijn, maar dat wil nog niet zeggen dat in die protocollen geen belangen, politiek en macht besloten liggen (DeNardis 2009; 2014; Mueller 2010; 2002; Brown en Marsden 2013). Voor elk protocol dat het tot standaard geschopt heeft, waren ook alternatieven voorhanden die het – om wat voor reden dan ook – niet gered hebben. De regulerende werking van software en protocollen is groot: 'code is law' zoals Lessig (1999; 2006) het formuleerde. Politiek en andere vormen van macht doen er wel degelijk toe en zitten soms in de code en de protocollen ingebakken.[1]

De bedenkers zijn de – veelal vrij informeel georganiseerde – personen en organisaties die de softwareprotocollen en standaarden uitdenken, bediscussiëren en uiteindelijk tot standaard 'verheffen'. Dit laatste tussen aanhalingstekens, aangezien het uiteindelijk het wereldwijde gebruik van de standaard is die het tot een echte standaard maakt. De belangrijkste bedenkers zijn organisaties als de Internet Engineering Task Force (IETF), de Internet Society (ISOC) en het World Wide Web Consortium (W3C). Binnen deze organisaties zijn bekende en onafhankelijke 'netheads' als Vint Cerf en Tim Berners-Lee de oorspronkelijke smaakmakers (Brown en Marsden 2013: 12). Uit deze organisaties komen de ideeën voor protocollen en standaarden voort die het transport van informatie, de overgangen tussen netwerken (interoperabiliteit, interconnectie en routing) en het format van informatie die over het internet verzonden wordt, bepalen. Zo komen centrale protocollen als het Internet Protocol en webstandaarden als HTTP en HTML uit de koker van het IETF en deze zijn later overgenomen door het W3C dat intensief met het IETF samenwerkt. Deze organisaties – en enkele andere – vormen een belangrijke kern van wat in internetterminologie wel de 'technische gemeenschap' wordt genoemd. Ze hebben een relatief open structuur: deelname aan de beraadslagingen van de IETF staat in principe open voor iedereen; ze zijn overduidelijk meer privaat dan publiek; en ze hebben een grote impact op de protocollen en standaarden die de kern van het internet uitmaken.

Uit het werk van de bedenkers vloeien de logische bouwstenen van het internet zelf voort: de protocollen en standaarden die ervoor zorgen dat het internet draait, informatie zijn weg vindt en in alle hoeken van de wereld aankomt. De belangrijkste van deze protocollen worden samengenomen onder de naam 'TCP/IP Protocol Suite'. Het Transmission Control Protocol (TCP) en het Internet Protocol (IP) zijn het hart van de groep protocollen die deel uitmaken van het TCP/IP Suite. Zonder deze protocollen functioneert het net niet. Het TCP/IP Protocol Suite groepeert een aantal protocollen in vier lagen: de 'link'-laag, de internetlaag, de transportlaag en de applicatielaag. In figuur 3.1 zijn de voornaamste protocollen per laag opgenomen.

Figuur 3.1 Een weergave van de TCP/IP Protocol Suite



Bron: DeNardis 2009: 8

Iedere laag in het model vervult een cruciale rol in de communicatie over het internet. In de bovenste laag van de applicaties hebben de digitale gegevens een voor ('gewone') mensen leesbare vorm, zoals tekst en getallen. De twee lagen daaronder – transport en internet – regelen de manier waarop informatie wordt omgezet in bits en bytes, opgebroken wordt in pakketjes die over de netwerken van het internet verstuurd worden. De linklaag ten slotte zorgt ervoor dat informatie zich over het hele net kan bewegen ongeacht hoe de hardware aan het net verbonden is, bijvoorbeeld via de ether of via de kabel. Van al deze protocollen is het Internet Protocol – de naam zegt het al – het meest dragende protocol voor het functioneren van het internet. Het bovenstaande lagenmodel wordt soms als een zandloper voorgesteld met IP als het smalste deel. Op de andere lagen zijn protocollen alternatieven voor elkaar (transport kan zowel via TCP als via UDP) maar de internetlaag functioneert – momenteel – alleen via IP (DeNardis 2009: 9). Al deze protocollen zijn op hun eigen manier van vitaal belang voor het functioneren van het internet, maar in het kader van deze studie springen er enkele uit. Dat komt omdat ze (a) belichamingen zijn van bepaalde waarden van het internet als publiek goed en/of (b) sterk in beeld zijn bij private partijen, maar met name bij staten, als aangrijpingspunt om het internet te reguleren dan wel zaken *via* het internet te reguleren. De hoofdrolspelers zijn TCP/IP en DNS omdat deze protocollen tezamen de voornaamste hulpbronnen van het internet opleveren: de internetadressen die communicatie

mogelijk maken en de domeinnamen waarop websites gebouwd kunnen worden. Deze 'Critical Internet Resources' (CIR) zijn de unieke namen en adressen van het internet en zijn ook daadwerkelijk 'van' het net: "CIRs are virtual, internet specific, globally unique resources rather than physical architecture or virtual resources not specific to the internet" (DeNardis 2014: 36).

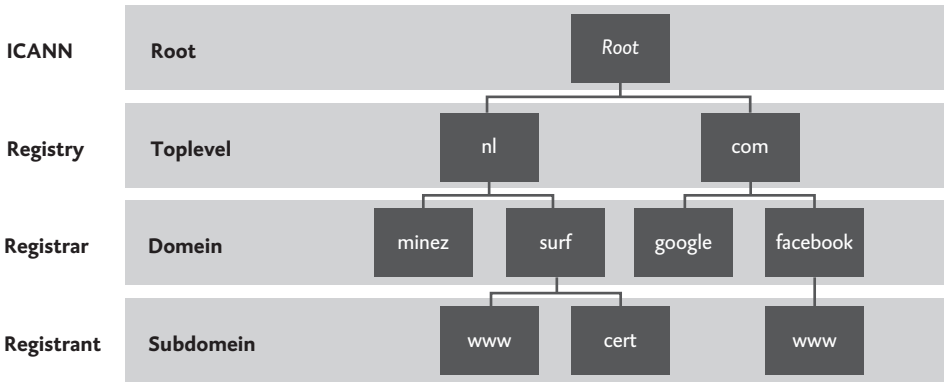
Voordat TCP/IP tot standaard verheven werd, konden de apparaten van de ene fabrikant, zeg IBM, niet communiceren met die van een andere fabrikant als Apple. Het protocol legde de standaard vast voor het transport van informatie en bepaalde dat elk apparaat dat via het internet informatie verstuurt en/of ontvangt een IP-adres (een uniek nummer) heeft dat vastzit aan het apparaat of de sessie zolang die duurt. Zonder adres kan de informatie niet verstuurd of ontvangen worden. Informatie die wordt verstuurd, wordt opgeknipt in kleine pakketjes (packets) en wordt voorzien van informatie over de afzender (IP-adres), de geadresseerde (IP-adres) en de juiste volgorde van de informatiepakketjes. Verschillende pakketjes nemen verschillende routes over het internet en worden pas op het eindpunt weer in de juiste volgorde gezet. Het netwerk (de routers, de Internet Service Providers) kijkt niet naar de inhoud van de pakketjes maar let alleen op de meest effectieve route op basis van de belasting van het netwerk. Dit wordt ook wel het end-to-endprincipe genoemd, dat in extreme vorm uitgaat van een 'dom netwerk' dat alleen informatie doorstuurt en de bewerking en inhoud van de informatie volledig overlaat aan de eindpunten (de computers van de verzender en ontvanger). Of, zoals de technische gemeenschap het vastlegde in het document 'The Architectural Principles of the Internet': "the goal is interconnectivity, the tool is the Internet Protocol, and the intelligence is end to end rather than hidden in the network" (geciteerd in Ziewitz en Brown 2014).

Critical Internet Resources

IP-adressen zijn daarmee een vitale hulpbron van het internet omdat ze de communicatie tussen twee unieke gebruikers mogelijk maken. Aangezien IP-adressen voor mensen niet te begrijpen of onthouden zijn, zijn domeinnamen geïntroduceerd. Een domeinnaam, zoals www.wrr.nl, wordt onzichtbaar voor de gebruiker vertaald naar het bijbehorende IP-adres. Daaruit volgt dat ook domeinnamen uniek moeten zijn en derhalve slechts eenmalig aan een enkele persoon of organisatie uitgegeven worden. Het spreekt voor zich dat bepaalde domeinnamen veel geld waard zijn. The Coca Cola Company heeft er een zeer groot belang bij het bezit van domeinnamen als www.cocacola.com en www.cocacola.nl omdat het de logische plaatsen zijn waar mensen op zoek gaan naar informatie over dat bedrijf. Het uitgeven van zulke domeinnamen gebeurt in een hiërarchische structuur van over het algemeen private organisaties met aan de top het Californische bedrijf ICANN, een zogenoemde 'nonprofit public benefit corporation'. Deze organisatie geeft de topleveldomeinen uit, de meest brede noemer waaronder websites op het internet verschijnen, oftewel het laatste deel van het webadres van een internetsite. Dit kan

een generiek topleveldomein (TLD) zijn, zoals .com of .org, of een landen-TLD zoals .nl. Die grote domeinen worden vervolgens weer door zogeheten 'registries' beheerd. Zo beheert het Amerikaanse bedrijf Verisign het generieke TLD '.com' en beheert het Nederlandse bedrijf SIDN het country TLD '.nl'. Daaronder zitten weer allerlei organisaties en bedrijven ('registrars') die namen binnen een specifiek domein verkopen aan klanten. Die opbouw is in figuur 3.2 weergegeven.

Figuur 3.2 De hiërachie van internetdomeinen en domeinnamen



Milton Mueller (2002: 2-6) geeft in zijn boek *Ruling the root* het dubbele belang van IP-adressen en domeinnamen duidelijk aan: als het beheer van deze beide hulpbronnen slecht is georganiseerd kan het internet 'breken' en tegelijkertijd zijn IP-adressen en domeinnamen sterk gecommodificeerd, verhandelbaar en soms veel geld waard. Met andere woorden, ze zijn van vitaal belang voor het functioneren van het internet als publiek goed, maar hebben ook economische en politieke waarde en dus spelen er ook economische en politieke belangen mee. Deze Critical Internet Resources (DeNardis 2009) worden uitgegeven door middel van het creëren van nieuwe domeinnamen en de uitgifte van IP-adressen. Het beheer ervan bestaat uit het registreren van IP-adressen en domeinnamen en het up-to-date houden en publiek maken van dat register. Voor beide activiteiten, uitgifte en beheer, staat ICANN aan de top: het bedrijf kan als enige nieuwe topdomeinnamen creëren (zoals .apple, .shop en .xxx) en heeft een hiërarchische relatie ten opzichte van het beheer van de domeinen. Ook is ICANN – samen met het Amerikaanse Department of Commerce – verantwoordelijk voor de uitgifte van IP-adressen (de IANA-functie) die in grote blokken verdeeld worden over vijf grote regionale organisaties (de Regional Internet Registries, RIR's), zie figuur 3.3. De RIR's wijzen de IP-adressen vervolgens weer in kleinere blokken toe aan lokale registries. En deze registries wijzen weer adressen toe aan Internet Service Providers en uiteindelijk aan eindgebruikers. In sommige regio's heerst inmiddels grote schaarste aan IP-adressen. Om dat te adresseren is Team Internet in 1995 al begonnen met de ontwikkeling en introductie van een nieuwe versie van het Internet Protocol (IP ver-

sie 6, IPv6) dat over nagenoeg oneindig veel adressen beschikt. De invoering van IPv6 gaat echter langzaam, omdat het een verandering vergt die diep in de kern van het internet en overal ter wereld moet worden doorgevoerd.

Figuur 3.3 De verdeling van internetadressen door RIR's

Bron: ARIN

Domeinnamen moeten volledig uniek zijn om ervoor te zorgen dat het internetverkeer op de juiste plaats terechtkomt en ze moeten zijn gekoppeld aan een IP-adres. Het Domain Name System (DNS) legt dit vast. Het DNS is in essentie een database waarin de hiërarchie van domeinnamen is vastgelegd en die geraadpleegd wordt om domeinnamen te vertalen naar IP-adressen: "The DNS is a look-up system that handles billions upon billions of queries per day locating requested internet resources. It is an enormous database management system (DBMS) distributed internationally across numerous servers with the purpose of providing the locations of resources such as a website, email address, or file" (DeNardis 2014: 41). Inmiddels is er een internationaal netwerk van DNS-servers – met een sterke oververtegenwoordiging in de VS en Europa – dat ervoor moet zorgen dat internetverkeer op de juiste plek aankomt. Deze DNS-database moet consistent en accuraat zijn om het internet te laten functioneren.

Uitvoerders: internet exchanges, CERT's en ISP's

Naast deze kern van protocollen, standaarden en organisaties zijn er nog vele andere te noemen die allemaal noodzakelijk zijn om internetverkeer zoals wij dat kennen mogelijk te maken. Zonder de internet exchanges, zoals het Nederlandse AMS-IX en de onderzeekabels die de continenten met elkaar verbinden, is wereldwijde communicatie onmogelijk. Routingovereenkomsten tussen de verschil-

lende netwerken die samen het internet vormen bepalen hoe informatie over de wereld beweegt. En de verschillende publieke, private en gemengde Computer Emergency Response Teams (CERT's) proberen het internet – lokaal, regionaal en internationaal – gezond te houden in de strijd tegen Distributed Denial of Service (DDOS) aanvallen, virussen en malware. De Internet Service Providers vormen meestal de directe link tussen gebruikers en het internet: zij maken de toegang tot het internet mogelijk (access) en leveren vaak ook diensten als een eigen domeinnaam, e-mailservice of de mogelijkheid om een website op te zetten (hosting). Omdat ze in het sociaaleconomische domein van het internet een vitale schakel zijn, komen de ISP's nogal eens in beeld als het gaat om het ingrijpen in de virtuele wereld om redenen van politieke (opsporing, censuur, veiligheid) en economische belangen (copyright).

3.2.1 HET GROTE SUCCES VAN TEAM INTERNET

Team Internet heeft een geweldig trackrecord op het punt van de groei van het internet. Het is een vitaal en nog steeds verder groeiend onderdeel van onze economie en samenleving, waarbij 'onze' digitale samenleving inmiddels al net zo verweven is met de rest van de wereld als het internet zelf. De verwevenheid van ons dagelijks leven met het internet zal in de komende jaren alleen maar verder toenemen, zeker als tendensen als cloud computing en 'the internet of things' zich verder doorzetten. De cloud maakt onze data tot op grote hoogte los van territorium en plaats en het internet of things zal onze huizen, auto's, gebruiksvoorwerpen en zelfs het lichaam koppelen aan het internet. Het internet heeft zich op vele manieren uit weten te breiden, onder meer door gebruik te maken van bestaande infrastructuren, zoals telefoonlijnen en kabel, en via nieuwe infrastructuren zoals glasvezel en draadloze netwerken. Op het niveau van infrastructuur zijn overheden vaak van vitaal belang geweest, maar verder heeft het internet zich zonder grote bemoeienis van overheden zo ontwikkeld dat het nagenoeg elke nieuwe gebruiker, applicatie en innovatie heeft kunnen accommoderen. Volgens Zittrain (2008) is het juist het open karakter van het internet – open standaarden en protocollen en dus laagdrempelige toegang voor iedereen met een goed nieuw idee – dat ten grondslag ligt aan de stormachtige ontwikkeling van het internet en alles wat daarop gebouwd is. De groeicijfers van het aantal gebruikers, het aantal websites en de interneteconomie spreken in ieder geval boekdelen over de successen van een netwerk dat zo bescheiden is begonnen.

Het internet als geheel wordt vaak omschreven als een 'best effort network': het samenspel van de verschillende netwerken en aanbieders zorgt in combinatie met de klassieke protocollen voor een zo goed mogelijke service voor het internetverkeer door de beschikbare bandbreedte zo effectief mogelijk te gebruiken, zonder daarbij vooraf een garantie te geven voor een vaststaande kwaliteit. 'Het internet' doet zijn best maar geeft geen garanties. Een van de voornaamste manieren om het internet te laten groeien is dan ook de toename van bandbreedte geweest, zeker

gezien het feit dat de groei van het internetgebruik van de laatste jaren steeds omvangrijker is geworden in termen van het aantal bits en bytes dat over het net verstuurd moet worden. Het internet van de tekst wordt nu volledig overschaduwd door het internet van foto, muziek, video en streaming. De belasting van het net is daarmee exponentieel toegenomen. Ter illustratie: op sommige piekmomenten zijn Netflix en YouTube – de twee populairste streamingwebsites op dit moment – verantwoordelijk voor bijna de helft van het totale Amerikaanse internetverkeer (Anders 2014). De enorme groei van data in het digitale tijdperk in de zeer recente geschiedenis wordt door sommigen wel de datarevolutie genoemd (Kitchin 2014). In 2012 schatte IBM dat 90 procent van de wereldwijd beschikbare data in de afgelopen twee jaar was gecreëerd. Een veelheid aan rapporten en analyses heeft dezelfde strekking: het volume van de wereldwijd gecreëerde data is en blijft exponentieel toenemen (Kitchin 2014: 69-72). Veel hiervan wordt op/door het internet gegenereerd en/of beweegt zich over het netwerk. De grootste verdienste van Team Internet is daarmee het feit dat het internet tot op heden die enorme groei heeft kunnen accommoderen zonder te imploderen of te exploderen. Het succes van het internet heeft echter ook de economische en politieke belangen bij het internet vergroot. Dat betekent ook dat de ingenieursblik op het internet gezelschap krijgt van een economische en politieke blik.

3.3 PROBLEMEN ROND DE GOVERNANCE VAN HET INTERNET ALS EEN PUBLIEK GOED

In de loop der jaren zijn er problemen ontstaan in de governance van het internet. Zo leidt de sterke groei van het internet tot de IPv6-problematiek. Daarnaast scheppen technologische ontwikkelingen zoals Deep Packet Inspection (DPI) nieuwe mogelijkheden voor controle van dataverkeer. Bovendien leiden politieke en economische belangen en conflicten tot debatten over de uitgifte en het beheer van IP-adressen en domeinnamen. Ook veranderen de opvattingen over cybersecurity. In al deze gevallen komt de technische invalshoek van Team Internet in botsing met verschillende politieke en economische belangen. Zelfs het probleem van de invoering van IPv6 – een op het oog volledig technische kwestie van updaten – loopt vast op economische belangen en politieke impasses en onmacht. Deze debatten zijn op verschillende manieren te bekijken en te framen, maar kunnen zeker ook bekeken worden vanuit het perspectief van het collectieve belang van het internet als een publiek goed versus individuele/nationale politieke of economische belangen. Vier van deze debatten worden hierna kort besproken. Doel daarvan is om de collectieve kern van het publieke goed, dat geen speelbal van nationale politieke belangen zou moeten worden, te onderscheiden van die delen van het debat die – of men dat nu wel of niet leuk vindt – een inherente politieke component hebben. Deze debatten zijn: (1) het collectieve dilemma van de update van het Internet Protocol naar de broodnodige versie 6; (2) de discussie over de verantwoordelijkheid voor de uitgifte en het beheer van IP-adressen en de omstreden rol

en positie van ICANN; (3) het debat over Deep Packet Inspection en netneutraliteit; en (4) het debat over de verschuivende opvattingen over en aanpak van internet veiligheid.

3.3.1 EEN COLLECTIEF-ACTIEPROBLEEM: DE (NON-)ADOPTIE VAN IPV6

De groei van het internet is gebouwd op een voorraad beschikbare internetadressen om nieuwe gebruikers en applicaties aan het internet te koppelen. Dat betekent wel dat er voldoende van die adressen beschikbaar moeten zijn. IPv4, het huidige protocol, loopt op zijn einde, ondanks de vooruitziende blik van de bedenkers om grofweg vier miljard unieke IP-adressen te creëren in een tijd waarin er slechts enkele duizenden gebruikers waren. Al in 2011 zijn de laatste grote blokken IPv4-adressen vanuit de IANA uitgegeven en inmiddels zijn er twee regio's, RIPE-NCC en APNIC, ofwel Europa en Azië, door hun voorraad IPv4-adressen heen (OECD 2014: 14). Hier is de schaarste acuut. Het alternatieve protocol IPv6 wordt echter nog maar zeer beperkt gebruikt. Het nieuwe protocol maakt onmiddellijk een einde aan deze schaarste wanneer het doorgevoerd zou worden, aangezien het voorziet in de creatie van 340 undecillion unieke internetadressen (een undecillion is een 1 met 36 nullen). Hoewel de technische gemeenschap al in 1990 de uitputting van de IPv4-adressen als een risico aanmerkte en de nieuwe standaard IPv6 in de jaren negentig al beschikbaar was (DeNardis 2009), is de huidige stand van zaken van de adoptie van IPv6 bedroevend. België (met 29%) en de VS (10,2%) zijn de koplopers, een handvol landen bevindt zich tussen 3 en 10 procent en de rest van de wereld scoort daar ver onder, waarbij nul procent adoptie geen uitzondering is in sommige delen van de wereld.[2] Het voornaamste probleem met het protocol is dat het niet 'backward compatible' is met IPv4. Met andere woorden, zolang niet alles en iedereen is overgestapt, heeft men twee adressen naast elkaar nodig om er zeker van te zijn dat de informatie aankomt. Dat maakt IPv6-adoptie tot een collectief-actieprobleem: zij die geen IPv4-adressen meer kunnen krijgen omdat ze in die regio op zijn, hebben belang bij adoptie van IPv6, maar zijn voor een goede mondiale communicatie afhankelijk van de adoptie van het nieuwe protocol door andere gebruikers – ook diegenen die nog IP4-adressen kunnen krijgen – om compatibel te zijn. Bovendien is overstappen kostbaar en vereist investeringen door ISP's. Het levert echter geen *first mover advantage* op voor ISP's: je kunt je eigenlijk niet van je concurrent onderscheiden door IPv6 aan te bieden omdat het de reeds aangesloten klant niets zichtbaar extra's oplevert.

De keuze voor deze onhandige constructie verklaart DeNardis (2014: 81) vanuit de cultuur en het collectieve internetgevoel van de technische gemeenschap: "Although retrospectively this seems like a design problem, at the time IPv6 was selected, the assumption was that internet users would want to upgrade for the network's overall good". Die mate van betrokkenheid bestaat echter niet meer onder de hedendaagse miljarden internetgebruikers. Anderen wijzen erop dat binnen het IPv4-format gewoonweg geen ruimte was voor een uitbreiding die compa-

tibel zou zijn.[3] De huidige situatie kenmerkt zich door een combinatie van de upgrade naar IPv6 – die zeer langzaam gaat, hoewel sommigen menen dat er een kentering aankomt (Czyz et al. 2013) – en het ontstaan van een internationale handel in IPv4-adressen die eerder uitgegeven zijn en nog niet zijn gebruikt (Mueller en Kuerbis 2013). Het uitblijven van een transitie naar IPv6, het vermarkten van IPv4-adressen en het steeds toepassen van technische trucs (middleware) om verschillende gebruikers gebruik te laten maken van één internetadres heeft uiteindelijk gevolgen voor de stabiliteit en de fragmentatie van het internet. Ook overheden beginnen nerveus te worden over het uitblijven van de transitie naar IPv6 omdat dit mogelijk grote schade aan de interneteconomie toe zal brengen, maar zij hebben eigenlijk geen instrument in handen om de overstap te versnellen of op te leggen (OECD 2014: 7). Het blijft daarom voornamelijk bij oproepen en stimulering, zoals in de ministeriële verklaring over de toekomst van de interneteconomie van Seoul: "Encourage the adoption of the new version of the Internet Protocol (IPv6), in particular through its timely adoption by governments as well as large private sector users of IPv4 addresses, in view of the ongoing IPv4 depletion."

3.3.2 DE UITGIFTE EN HET BEHEER VAN IP-ADRESSEN EN DOMEINNAMEN

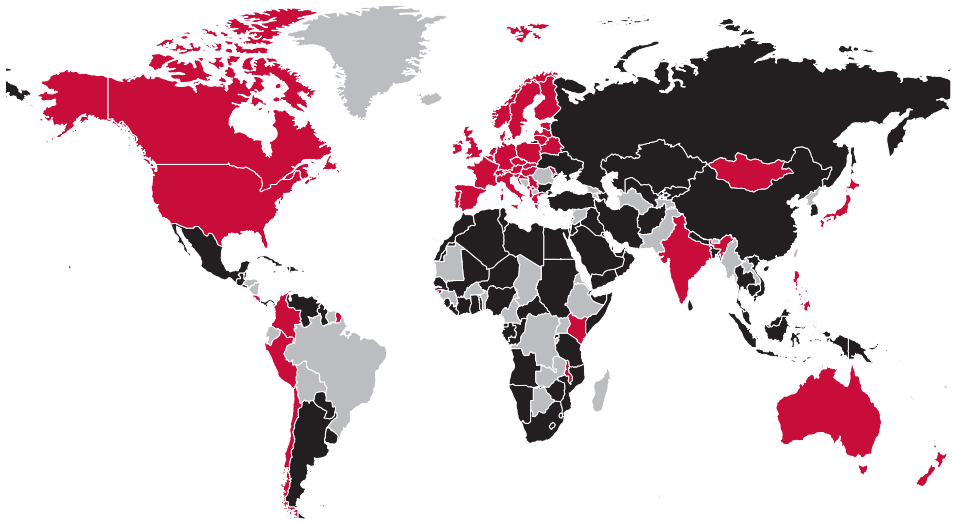
De uitgifte en het beheer van IP-adressen en domeinnamen is zoals eerder aangegeven door de Amerikaanse overheid – die de IANA-functie te vergeven had – ondergebracht bij het Amerikaanse bedrijf ICANN (Internet Corporation for Assigned Names and Numbers). Die keuze ligt al jaren onder vuur vanwege de invloed – via een contractuele relatie met het Amerikaanse Department of Commerce – van de Amerikaanse overheid op de belangrijkste grondstoffen van het internet: IP-adressen en domeinnamen. De recente onthullingen van Edward Snowden hebben de geloofwaardigheid van de Amerikaanse overheid als hoeder van het vrije internet geen goed gedaan en dit debat in een versnelling gebracht. De al veel langer klinkende roep om een verandering van het systeem waarin ICANN en de VS zo'n centrale plaats innemen is alleen maar groter geworden. De Amerikaanse overheid heeft de deur voor zo'n verandering overigens ook zelf op een kier gezet door in maart 2014 aan te kondigen dat zij op zoek gaat naar een manier om de relatie met ICANN in zijn huidige vorm te beëindigen. Het is echter niet de eerste keer dat de Verenigde Staten een dergelijke aankondiging hebben gedaan en bij een eerdere keer werd het contract met ICANN uiteindelijk gewoon verlengd en bleef alles bij het oude. De meningen over deze aankondiging zijn in de VS sterk verdeeld: sommige commentatoren menen dat president Obama hiermee het internet te grabbel gooit en de Amerikaanse nationale veiligheid in gevaar brengt, terwijl anderen menen dat het toezicht op IANA ook prima op een andere manier kan worden vormgegeven (Zittrain 2014).

De discussie loopt echter al veel langer. De onvrede met de geprivilegieerde positie van de VS in het aansturen van wat als een mondiaal publiek goed kan worden gezien, is vele landen een doorn in het oog. Grofweg gezegd zijn er twee kampen

die ICANN, of beter: het toezicht op de IANA-functie van de uitgifte en het beheer van domeinnamen en IP-adressen, willen hervormen. Het eerste kamp zijn de multilateralisten, die in de internetwereld ook wel de voorstanders van *multistakeholderism* worden genoemd. Zij zien de toekomst van het internet het best gewaarborgd als een brede coalitie van individuen, organisaties, civil society, bedrijven en overheden het beheer van deze grondstoffen in handen heeft. De andere groep zijn de nationalisten, die het beheer van het internet juist nationaler willen maken zodat staten meer grip en zeggenschap krijgen over hun 'eigen nationale internet'. In het eerste kamp bevinden zich in hoofdzaak mensen en organisaties die deel uitmaken van 'de internetgemeenschap'. Ook veel staten ondersteunen de idee van multistakeholderism, maar zelden volledig ten koste van een (groeiende) positie voor henzelf. Bij het opstellen van formele verklaringen geven staten de pen niet graag uit handen en blijft de bijdrage van ngo's indirect en daardoor beperkt (Cogburn 2010; Dutton en Peltu 2010). Het tweede kamp wordt aangevoerd door autoritaire staten die de controle die de staat offline op de eigen populatie heeft ook online willen garanderen en versterken.

In verschillende ronden is over het beheer van de 'namen en nummers' van het internet flink wat afgevochten tussen de verschillende kampen zonder dat er daadwerkelijk iets is veranderd. Dat veranderde in 2012 tijdens de World Conference on International Telecommunications (WCIT) in Dubai, waar over een nieuw Telecommunicatieverdrag werd onderhandeld onder de auspiciën van de International Telecommunication Union (ITU). Dit nieuwe verdrag, dat volgens vele analisten de deur openzet voor een nationalisering of balkanisering van het internet, liet haarfijn zien dat de wereld verdeeld is op het punt van internetgovernance: 89 staten, waaronder China, Rusland en veel Arabische staten, tekenden het nieuwe verdrag en 55 landen waaronder de VS, de lidstaten van de EU, de meeste andere OESO-landen en landen als Mongolië, India en Peru weigerden te tekenen en verzetten zich openlijk. Figuur 3.4, die is gebaseerd op data van de ITU, maakt de verdeling in de wereld op dit punt duidelijk inzichtelijk. Rood gekleurd zijn de landen die het verdrag niet tekenden en zwart zijn de landen die het verdrag wel tekenden. De stemmen van de grijze landen zijn om redenen als achterstallig lidmaatschapsgeld niet formeel geregistreerd.

Figuur 3.4 Voor- en tegenstanders van het Telecommunicatieverdrag (ITRs), 2012



Bron: Techdirt.com

Diplomatiek gezien is het van groot belang om vast te stellen dat de toekomst van dit debat niet zozeer bij de extreme stemmen in het debat ligt – die zullen hun positie nauwelijks veranderen – maar veel meer bij de staten in het 'midden'. De zogenoemde *swing states* of *fencesitters* zijn zich vaak wel bewust van het belang van deze internetvraagstukken maar hebben geen of nauwelijks capaciteit, beleid of strategie ontwikkeld, zeker niet op het internationale vlak (Maurer en Morgus 2014). Op sommige punten zullen zelfs niet alle lidstaten van de EU op een lijn zitten en zijn de verschillen tussen lidstaten in termen van kennis en strategiebepaling en zelfs beleid aanzienlijk. Dat de ideeën over internetvraagstukken uiteenlopen blijkt bijvoorbeeld uit de poging van de regering van Hongarije om dataverkeer te belasten – een wetsvoorstel dat na grootschalig protest weer is ingetrokken. Het is dus zaak voor Nederland om diplomatiek sterk in te zetten op de landen met *swing*potentieel, en daarbij in het achterhoofd te houden dat de Europese stem slechts krachtig is als er geen interne verdeeldheid is. Nederland maakt binnen de EU deel uit van de G5, een groep van vijf digitaal geavanceerde landen die vooroplopen bij de ontwikkeling van Europees cyberbeleid, en heeft daarmee een strategische positie om Europese eensgezindheid over internetvraagstukken te beïnvloeden. Nederland als lidstaat van de EU zal steeds moeten beoordelen wanneer gezamenlijk Europees optreden, bijvoorbeeld binnen het gemeenschappelijk buitenlands en veiligheidsbeleid van de EU, aansluit bij de eigen positie en wanneer eigen optreden (ook) noodzakelijk is. Dit lijkt het moment te zijn waarop nieuwe coalities gesmeed moeten worden in aanvulling op al lopende initiatieven. Zeker

gezien het feit dat de ICANN-discussie, hoewel de meest bekende en symbolische discussie over internetgovernance, beslist niet de laatste discussie over de toekomst van (delen van) het internet zal zijn.

Zoals gezegd heeft de Snowden-affaire het morele leiderschap van de VS geen goed gedaan en dat is ook in deze discussie goed te zien. Brazilië, een van de landen waar spionage door de NSA op het hoogste niveau plaatsvond, organiseerde in april 2014 de NetMundial conferentie in São Paulo. Die conferentie stond sterk in het teken van de verontwaardiging over de Snowden-onthullingen en zette in op het multistakeholdermodel voor de toekomst van internetgovernance. NetMundial was het begin van een proces waarin gezocht wordt naar een manier om de taken van ICANN daadwerkelijk te globaliseren zonder de stabiliteit van het net te bedreigen. Velen mengen zich in deze discussie. Zo formuleerde de Europese Commissie (2014) de ambitie om een 'genuine multistakeholder approach' voor het bestuur van het internet te bewerkstelligen met als expliciete wens dat contracten over domeinnamen en IP-adressen niet meer onder Californische wetgeving hoeven te worden gesloten. Soms steken bij de voorstellen klassieke staatstradities de kop op. Zo mengde de Franse senaat zich in juli 2014 in het debat met een lijvig rapport over de toekomst van internetgovernance. In het rapport staan vergaande voorstellen om ICANN te veranderen in W(orld)ICANN, deze organisatie onderhevig te maken aan internationaal recht in plaats van Californisch recht en haar verantwoording af laten leggen aan een World Internet Council, waarvan de leden benoemd worden door VN-lidstaten (Sénat Français 2014). Het voorstel was mede bedoeld om de invloed van de EU in de internationale internetgovernance te vergroten. De suggestie van het Franse rapport om de politieke invloedssfeer van één staat – de Verenigde Staten – te vervangen door een mulilateraal kader is op zichzelf een verbetering, maar het voorstel is ook kwetsbaar voor een politiek van verdeel en heers door staten die het internet de facto liever nationaliseren dan internationaliseren. Ondanks de vele verwijzingen in het rapport naar het multistakeholdermodel versterkt het Franse voorstel door de oprichting van een politieke raad vooral de positie van staten in het beheer van het internet.

Velen zien de ICANN-discussie als een symbolische discussie (zie bijvoorbeeld Zittrain 2014). ICANN heeft niet zo veel 'fout gedaan' en heeft bovendien slechts twee – weliswaar vitale – functies als het gaat om het functioneren van het internet. De eerste functie zijn de IANA-functies, grofweg gezegd het beheer van het register van domeinnamen en IP-adressen en de zorg voor het up-to-date en consistent houden van het DNS-systeem. De tweede functie is het uitbreiden en 'vermarkten' van nieuwe topleveldomeinen. Mueller en Kuerbis (2014) trekken uit dit onderscheid een belangrijke conclusie: er zou zo min mogelijk politieke bemoeienis moeten zijn met de eerste functie, aangezien die in essentie bestaat uit technische en operationele taken. De tweede taak is veel meer een 'politieke' beleidstaak: welke domeinnamen zijn acceptabel? Hoeveel IP-adressen moeten er zijn? Wie

moet ze beheren? Hoe de tweede taak in politieke zin vormgegeven moet worden, is een kwestie van voorkeur en ligt gevoelig. Maar dat de eerste taak buiten politiek getouwtrek en politieke invloed zou moeten blijven – om het technische systeem consistent en integer te houden – staat buiten kijf of zou dat moeten staan. Of zoals Mueller en Kuerbis (2014) het formuleren: "Many observers of the IANA controversy believe that root zone management is an appropriate site for public oversight and policy intervention. This is a mistake". In de transitie naar een andere manier om de namen en nummers van het internet aan te sturen is dus de nodige terughoudendheid geboden.

3.3.3 NETNEUTRALITEIT

Een derde debat dat het technische functioneren van het internet raakt, is dat over netneutraliteit. Netneutraliteit is het principe dat al het dataverkeer dat over een netwerk gaat gelijk behandeld wordt. Het hangt samen met het end-to-endprincipe dat uitgaat van een 'dom' netwerk dat gewoon doorgeeft wat er aangeboden wordt. Netwerkneutraliteit is overigens een principe – de default van IP en het internet – en geen protocol dat is vastgelegd. De centrale vraag bij netwerkneutraliteit is of een ISP (van een van de netwerken die tezamen het internet vormen) onderscheid mag maken tussen de verschillende soorten dataverkeer die zijn netwerk passeren door middel van het blokkeren, afknijpen of juist prioriteren van een deel van dat verkeer. Omdat het bij netneutraliteit voornamelijk gaat over de snelheid waarmee data bij de eindgebruiker – lees in de meeste gevallen: de klant – aankomen (*last mile access*) is het vaak een regionaal of zelfs nationaal issue. Het is wel een issue dat in vele landen speelt en heftige debatten veroorzaakt in nationale en Europese politieke arena's en van invloed is op hoe het internet gezien wordt, dataverkeer behandeld wordt en hoe er op het internet geld verdiend wordt.

Cruciaal in de discussie over netneutraliteit is of netwerkbeheerders in staat zijn om de inhoud van datapakketjes te bekijken, anders is onderscheid maken immers onmogelijk. Lang was dat niet het geval en was het technisch onmogelijk om – in real time – de inhoud van passerende pakketjes data te scannen. Met de technologische vooruitgang maken nieuwe technieken als DPI dat inmiddels zonder meer mogelijk. Netwerkbeheerders kunnen de inhoud van pakketjes scannen en kunnen – indien gewenst – het verkeer ervan vertragen of blokkeren op basis van de soort applicatie, het gebruikte protocol (denk bijvoorbeeld aan het BitTorrent-protocol dat met piraterij wordt geassocieerd), de gebruiker of de inhoud (DeNardis 2014: 135). De redenen daarvoor kunnen sterk uiteenlopen: netwerkbeheer, veiligheidsoverwegingen en allerlei politieke en economische redenen om inhoud te blokkeren of te beprijzen. Het feit dat netneutraliteit een principe is dat stamt uit de begindagen van het internet maakt het voor velen die zich in het debat mengen ook een geloofsartikel: het is vermengd met de idee van het internet als een vrijplaats. De term zelf is volgens DeNardis (2014: 149) dan ook niet echt neutraal te noemen: "net neutrality is not neutral but represents a set of values. Many of these

are historical values embedded in the design of the internet's architecture, such as engineering user choice about what information to access and creating a level playing field for the introduction of new information products".

In het debat over netneutraliteit lopen eigenlijk drie logica's door elkaar heen: een technische logica die gaat over netwerkbeheer en kwaliteit van dienstverlening (quality of service), een economische logica die gaat over verdienmodellen op het internet en over de vraag 'wat een level playing field is', en een politieke logica die eigenlijk meer gaat over het gebruik van DPI om politieke controle en censuur via de netwerken van internet providers mogelijk te maken. Onderzoek van Asghari et al. (2013) naar het gebruik van DPI door ISP's over de gehele wereld[4] laat zien dat het gebruik ervan wijdverbreid is, maar dat DPI ook gevoelig is voor regulering. In landen met sterke opvattingen over en regulering van privacy is het gebruik van DPI veel beperkter en in landen met een traditie van censuur is het toepassen ervan veel sterker. Het gebruik van DPI voor netwerkbeheer is minder omstreden, maar ook niet nauw omschreven.[5] Er zijn goede en legitieme redenen om verschillende datastromen te ordenen en ervoor te zorgen dat het netwerk maximale kwaliteit levert voor de meeste gebruikers. De precieze afbakening tussen legitiem netwerkbeheer en schendingen van netneutraliteit – dat geen scherp gedefinieerde afbakening heeft – is lastig te trekken maar begint snel te vervagen als economische of politieke motieven een rol gaan spelen.

Aangezien het internet in overgrote meerderheid een netwerk van private netwerken (ISP's) is, spelen er verschillende economische belangen. Het scherpst tegenover elkaar staan de ISP's en de aanbieders van digitale diensten. Soms is dat omdat nieuwe diensten concurreren met de eigen kerntaken van de ISP's, die vaak activiteiten uit vele bedrijfstakken in een enkel bedrijf geïntegreerd hebben: KPN, als ISP, is niet zo enthousiast over het doorgeven van het dataverkeer van Skype, dat direct concurreert met de telefonietak van het bedrijf. Aan de andere kant staan de internetdiensten en bedrijven. De succesvolste aanbieders van digitale diensten – of het nou Netflix of Facebook is – zijn grootverbruikers van data. Het uploaden van foto's en filmpjes en het streamen van video's legt een groot beslag op de bandbreedte van de netwerkbeheerders, die de kwaliteit van de verbinding voor al hun gebruikers moeten 'garanderen'. De netwerkbeheerders willen de rekening graag indienen bij bijvoorbeeld Netflix, die in ruil dan een gegarandeerde en geprivilegieerde behandeling van zijn datastromen krijgt. Zowel gebruikers als internetondernemingen verzetten zich hiertegen. Gebruikers zijn bang dat deze prioritering betekent dat de rest van het internet vertraagt. Bedrijven zijn van mening dat het internet – lees de ISP's – gewoon hun werk moeten doen en alle data optimaal door moeten geven. Bovendien betalen de gebruikers voor het datagebruik en niet de platforms en internetdiensten.[6] In het verlengde hiervan ligt het vaak gebezigde argument van innovatie en level playing field: als het internet grotendeels bestaat uit de privaat betaalde snelwegen van de Google's, Netflixen en Facebook's van

deze wereld, hoe kan een innovatief nieuw bedrijf dan groeien op de trage B-wegen van het internet die overblijven? Een start-up nu heeft dan niet meer dezelfde kansen als Google had toen het aan de weg timmerde. De ISP's willen echter meer incentives en compensatie om dure investeringen te doen die nodig zijn om aan de almaar groeiende vraag naar bandbreedte te voldoen. Die wentelen ze liever af op grote bedrijven dan op de eigen klanten die eenvoudig met de voeten kunnen stemmen.

De politiek schaart zich soms aan de kant van netneutraliteit. Nederland en Slovenië hebben het netneutraliteitsbeginsel in de wet vastgelegd. In de EU wordt gediscussieerd over een nieuwe verordening voor de Europese interne markt voor telecommunicatie[7] waarin het beginsel al dan niet verder wordt ingevuld. Het Europees Parlement heeft in april 2014 op het nippertje netneutraliteit opgenomen in deze ontwerpverordening, maar de ministers uit de EU-lidstaten zijn nog verdeeld over het onderwerp. Vanwege het dwingende karakter van een Europese verordening, die nationale wetgeving zal vervangen, vormen de vergaderingen tussen EU-lidstaten de komende tijd het toneel voor de strijd om het principe van netneutraliteit in Europa. Ook een aantal Latijns-Amerikaanse landen, zoals Peru, Chili en Brazilië heeft netneutraliteit vastgelegd in wet- of regelgeving (De Filippi en Belli 2014). Het blijft echter een politiek en economisch zeer omstreden veld. Met name economische belangen spelen een grote rol en grote gevestigde belangen als die van de kabelmaatschappijen en de telecom verzetten zich heftig tegen meer regulering omdat die de mogelijkheden voor een andere beprijzing van dataverkeer onmogelijk maken. De recente voorstellen van president Obama voor het reguleren van netneutraliteit in de VS werden onmiddellijk in stevige bewoordingen door kabelaars en breedbandaanbieders weggezet ('a 1930s regulation').[8] Ze willen ruimte behouden om tot nieuwe verdienmodellen te komen.

Omdat netneutraliteit een negatieve regulering is – het regelt wat een ISP niet mag doen – komt het nogal nauw om te bepalen waar de grens ligt. De grens tussen welk dataverkeer ISP's mogen beïnvloeden in het kader van netwerkmanagement en quality of service (veelal als legitiem en nuttig beoordeeld) en waar dat overgaat in discriminatie en/of zelfs censuur is niet scherp te trekken en is al helemaal niet eenvoudig voor toezichthouders (DeNardis 2014; Brown en Marsden 2014). Ook in dit debat staat de positie van de ISP centraal: deze (steeds meer) centrale speler in het internetveld heeft – dankzij DPI-technologie – de mogelijkheid om in te grijpen in de datastromen die over zijn netwerk lopen. De reden om dat te doen varieert van technisch onderhoud, via economische gewin (centraal in het net neutraliteitsdebat) tot censuur, hetzij vanwege economische belangen (blokkeren van copyright protected inhoud) of politieke belangen (blokkeren van politiek onwelgevallige inhoud). De laatste twee vormen van wat wel 'intermediary censorship' (Zuckerman 2010; Brown en Marsden 2014) wordt genoemd, worden in hoofdstuk 4 verder besproken.

3.3.4 INTERNETVEILIGHEID

Met de centrale plaats die het internet nu inneemt, is het internet ook een kwetsbaarheid geworden. Het internet is een 'backbone of backbones' (Choucri 2012) geworden, met alle (potentiële) gevolgen en risico's van dien. Daarmee is ook het concept van wat de veiligheid van het internet is door de jaren heen veranderd. Veiligheid was echter geen kernoverweging bij de opzet van de centrale mechanismen van het internet: het end-to-endprincipe en het feit dat het netwerk zelf vrij 'dom' is, houdt ook in dat veiligheid een verantwoordelijkheid is van de eindpunten van het internet. Dat virussen zich soms als een veenbrand kunnen verspreiden heeft alles te maken met het gegeven dat het internet informatie zo effectief mogelijk verstuurt – ongeacht de inhoud – als de gebruikers daartoe de opdracht geven. Dat geldt ook als die opdracht verstopt zit in een attachment waar de gebruiker op moet klikken (denk aan het I LOVE YOU virus) of wordt opgepikt op een dubieuze website (zogeheten 'drive by downloads'). De kracht van het internet – snelle verspreiding van informatie – is soms dus ook zijn zwakte. Security in de zin van beveiliging tegen kwaadwillende individuen die de kracht van het internet voor eigen gewin inzetten, was geen echte overweging bij het ontwerp van de centrale protocollen die in de begindagen van het internet werden geschreven. De relatief kleine, homogene en afgesloten gemeenschap die aan de wieg van het internet stond, had gebruik met goede intenties op het netvlies staan en niet zozeer misbruik. Met de groei van het gebruik van het internet is de onlinewereld steeds meer op de offlinewereld gaan lijken, inclusief criminaliteit, vandalisme, politieke verschillen van mening en andere veiligheidsvraagstukken. Cyberaanvallen, phishing, malware, digitale spionage, massasurveillance en DDoS-aanvallen zijn inmiddels onderdeel geworden van onze dagelijkse nieuwsconsumptie. Daarmee zijn deze vormen van onveiligheid centraler komen te staan dan de meer technische benadering van het netwerk, die denkt in termen van het risico van overbelasting en redundantie.

Op het internet is veiligheid van oudsher een verantwoordelijkheid van de eindgebruiker: die is ervoor verantwoordelijk dat hij of zij de juiste software heeft geïnstalleerd om virussen en andere aanvallen te weerstaan. In de afgelopen decennia is dat uiteraard wel verder opgeschaald: bedrijven beveiligen hun eigen netwerken, netwerkbeheerders doen aan beveiliging en grote internetaanbieders en ISP's geven veel geld uit aan security. Ook is er Europese regelgeving in de maak om een aantal sectoren vanwege hun vitale belang voor de maatschappij te verplichten een hoog niveau van netwerkbeveiliging te garanderen. Op een hoger collectief niveau opereren binnen veel landen de zogenoemde Computer Emergency Response Teams (CERT's). Voorbeelden in Nederland zijn het voormalige GovCERT, dat inmiddels in het Nationaal Cyber Security Centrum (NCSC) is opgegaan, en de CERT's van een aantal grote bedrijven en universiteiten. De meeste digitaal geavanceerde landen hebben inmiddels een of meer nationale CERT's, hoewel de kwaliteit hiervan sterk verschilt tussen landen. Internationaal werken deze CERT's ook met

elkaar samen, waarbij internationale overeenkomsten vaak van minder groot belang zijn dan het vertrouwen tussen de technici onderling. Tezamen werken deze organisaties – en vele andere organisaties en individuen – aan cybersecurity, in de zin van internetveiligheid. Wat we onder cybersecurity verstaan is echter aan verandering onderhevig. Zowel de dreigingen zijn pluriformer geworden als de interpretatie daarvan en de middelen die daarbij ingezet (kunnen) worden. De toename van DDoS-aanvallen, waarbij websites door een botnet zo sterk overvraagd worden dat ze uit de lucht gaan, ziet er anders uit vanuit het perspectief van een politieagent van de High Tech Crime Unit dan vanuit het perspectief van een CERT-techneut. De eerste ziet een misdaad (cybercrime), zoekt naar motief en middelen en wil de dader oppakken en via het strafrecht berechten. De tweede ziet een overbelasting van een website en het netwerk en wil die wegnemen. De eenvoudigste manier om dat te doen is de bandbreedte te vergroten. Beiden zien het botnet graag verdwijnen, maar de gedachte van schuld en boete is geen primaire ingenieursgedachte. Het punt is dat er meerdere opvattingen van veiligheid op het internet zijn die elkaar beïnvloeden en niet altijd ten goede.

Die verschillende opvattingen over veiligheid van het net komen met elkaar op gespannen voet te staan – overigens niet voor het eerst – en het is de traditionele ingenieursopvatting van internetveiligheid die de druk het sterkst voelt. De grootste uitdager is de opkomende dominantie van nationale veiligheid als bril om naar het internet te kijken. Inlichtingen- en veiligheidsdiensten, militaire cybercommando's en in mindere mate politie en justitie spelen een steeds dominantere rol in het publieke en politieke debat over het internet. De internationale technische gemeenschap, en meer in het bijzonder de wereld van de CERT's, waarin private partijen en overheden op veelal informele manieren informatie over problemen en oplossingen met elkaar uitwisselen, werkt echter voor een groot deel op basis van onderling vertrouwen dat door de jaren heen is opgebouwd. Op het Internetgovernance Forum op Bali in 2013 waarschuwde Yurie Ito van de Japanse CERT (JPCERT) ervoor dat de steeds grotere rol van overheden en overheidsdiensten op het gebied van nationale veiligheid, inlichtingen en defensie begint te interfereren met het werk van de internationale technische gemeenschap om het internet als infrastructuur veilig en stabiel te houden:

> The involvement of the national security organisations can potentially break down in trust, in CERT and technical communities if we were seen as an instrument of state focused competition. (…) So the result may be a significant rise in cybersecurity risk level because of the lack of transparency and the collaboration at the technical and, you know, CERT level, operational level.[9]

Verscheidene auteurs hebben gewezen op de spanning tussen nationale veiligheid – per definitie beredeneerd vanuit de belangen van een staat – en de collectieve veiligheid van het internet als een publiek goed. Dunn Cavelty (2014) heeft het bij-

voorbeeld over het doorbreken van het cybersecurity-dilemma, waarbij het najagen van nationale veiligheid negatieve gevolgen heeft voor het mondiale collectieve niveau van cybersecurity (zie verder paragraaf 4.4).

Nationale veiligheid laat echter weinig ruimte voor vergissingen en dat vertaalt zich in de manier waarop politici met het onderwerp omgaan. Van Eeten en Bauer (2009) zetten in dat kader de *precluded event security* en de *marginal security cost* tegenover elkaar. De eerste hanteert een absolute norm van veiligheid waarin (bijna) alles moet wijken, terwijl in de tweede ook een afweging tussen veiligheid enerzijds en maatschappelijke kosten anderzijds meegenomen worden. Daarbij gaat het vaak om financiële kosten – veiligheid is duur – maar het kan ook gaan om immateriële kosten zoals de waarden van de rechtsstaat (AIV 2014) of een andere opvatting van internetveiligheid en het vitale onderlinge vertrouwen van de organisaties en personen die daarbij betrokken zijn. De eerste logica lijkt echter steeds dominanter te worden als het over internetveiligheid gaat.

Om deze manier van denken – en vooral de gevolgen daarvan – tegen te gaan, komen er ook nieuwe initiatieven op vanuit de technische en CERT-gemeenschap om internetveiligheid anders te framen en te organiseren. Interessant is bijvoorbeeld het *Cyber Green Initiative*, dat mondiale cybersecurity vanuit het perspectief van gezondheid(szorg) bekijkt in plaats van vanuit het perspectief van nationale veiligheid (JPCERT/CC 2014). Bouwend op het idee van het internet als een ecosysteem wordt internetveiligheid voorgesteld als het bestrijden en voorkomen van botnets en allerlei vormen van malware om dat ecosysteem gezond te houden. Een belangrijke eerste stap in deze benadering is om informatie over cyberdreigingen, DDoS-aanvallen en andere trends internationaal te standaardiseren en uit te wisselen en openbaar te maken. Dit moet resulteren in betere en meer realistische inschattingen van dreigingen op het internet en in een evenwichtiger level playing field in termen van informatie voor beleidsmakers en professionals op het gebied van cybersecurity. Een beter inzicht in daadwerkelijke ontwikkelingen op het gebied van cyberonveiligheid kan zeer nuttig zijn in een tijd van dreigingsinflatie en kan de zorg voor de veiligheid van het netwerk uit de sfeer van nationale veiligheid halen.

3.4 CONCLUSIE

De publieke kern van het internet is enerzijds in goede gezondheid en in goede handen maar anderzijds begint zich vanuit verschillende kanten druk op te bouwen. In sommige gevallen heeft dat te maken met het overweldigende succes van het internet zelf. De groei van het net heeft ervoor gezorgd dat de huidige IPv4-adressen in sommige delen van de wereld op zijn geraakt en daardoor is de internetgemeenschap nu zo groot (miljarden gebruikers) dat een overstap naar IPv6 geen zaak meer kan zijn van 'doen wat goed is voor het net'. Zo heeft het succes een

collectief-actieprobleem gecreëerd waarbij het wellicht eerst fout moet gaan voor het probleem opgelost wordt. Het gebrek aan daadkracht en actie bij zowel de industrie als bij overheden suggereert dat er een schok nodig is om in actie te komen.

Voor een aantal van de hiervoor besproken problemen geldt dat de druk van buiten de kern van het internet komt. Politieke en economische belangen en verschillen van inzicht – soms in combinatie met nieuwe technologische mogelijkheden – maken dat het collectieve karakter van het internet uitgedaagd wordt. Grote economische belangen – zoals de bescherming van copyright en verdienmodellen voor datatransport – voeren de druk op de politiek op om netneutraliteit, dat voorheen een default van het internet was, op te heffen of juist met wetgeving te beschermen. Sommige landen hebben daarin een duidelijke keuze gemaakt, maar ook daar blijft toezicht op het handelen van ISP's een punt van aandacht. Uit deze ontwikkelingen blijkt dat het internet er bij uitstek goed in is om afbakeningen te vervagen: wat de juiste verhouding is tussen 'netwerkbeheer' enerzijds en het remmen of blokkeren van dataverkeer om 'oneigenlijke redenen' anderzijds is niet zo eenvoudig vast te leggen en te controleren. ISP's zijn sleutelactoren en poortwachters van het internationale dataverkeer geworden. Het is een positie waar ook staten ze in manoeuvreren, maar die ook vanuit een oogpunt van legitimiteit ingewikkelder aan het worden is.

De politieke druk op Team Internet heeft alles te maken met veranderingen in internationale politieke verhoudingen en de opkomst van nationale veiligheid als een centraal paradigma voor de overheidsblik op het internet. Die beide ontwikkelingen moeten worden geplaatst tegen de achtergrond van het feit dat het internet in steeds meer landen onlosmakelijk verweven is geraakt met nationale economieën en samenlevingen en de internationalisering daarvan. Met andere woorden, er staat voor staten veel op het spel en het feit dat ze 'er niet over gaan' maakt dat sommige bestaande arrangementen van het beheer van het internet ter discussie komen te staan. Het vraagstuk van het beheer van de namen en nummers van het internet is een goed voorbeeld van hoe de politisering van een technische functie kan doorschieten. De transitie van dat beheer uit de directe invloedssfeer van de VS is vanuit internationale politieke verhoudingen een logische stap – het net is immers inmiddels van vitaal belang voor vrijwel alle landen en niet alleen voor de VS. Maar daarmee is nog niet evident wat de nieuwe vorm moet worden en hoe en of belangen van nationale staten hier belegd moeten worden. Twee zaken zijn daarbij van het grootste belang. In de eerste plaats moeten in de transitie de beheerstaken van de meer politieke taken gescheiden worden, waarbij het evident zou moeten zijn dat in het eerste geval de technische gemeenschap aan het roer staat en er in het tweede geval meer mogelijkheden zijn om politieke en economische belangen te accommoderen. Nederland heeft er een groot belang bij dat het technische beheer zo 'agnostisch' mogelijk vormgegeven wordt. Dit vanwege de ver-

klaarde ambities om een *digital gateway to Europe* te zijn en om redenen van het functioneren van het internet als een collectieve infrastructuur op de lange termijn. Nederland heeft dus alle reden om dit standpunt internationaal actief uit te dragen. In de tweede plaats is de discussie over ICANN weliswaar deels symbolisch, maar daarmee misschien wel juist van vitaal belang. Het is de meest zichtbare en tot op zekere hoogte meest tastbare discussie over het toch relatief vage idee van 'internetgovernance', waarover in de toekomst nog veel meer debatten te verwachten zijn. Maar in die debatten kunnen ogenschijnlijk kleine wijzingen in de technische onderlaag soms grote gevolgen hebben. Daarmee is het ook een belangrijke testcase voor de Nederlandse en Europese internetdiplomatie om coalitievorming vorm te geven op een manier die zich niet beperkt tot 'the usual suspects' van de trans-Atlantische as. Van veel landen weten we grofweg aan welke kant van het debat ze zich zullen opstellen en die extremen zullen niet veel veranderen. Van een grote andere groep weten we dat niet zo precies en in die groep bevinden zich veel landen waar het groeipotentieel van het internet nog zeer groot is. Hun belang bij het internet zal alleen maar toenemen en het denken over internetgovernance in die landen heeft zich nog niet vastgezet. Nederland heeft zich op het gebied van de digitale mensenrechten opgeworpen als een voorloper toen het de *Freedom Online Coalition* oprichtte. Nu zou Nederland voor kunnen gaan in een nieuwe diplomatieke inspanning die het waarborgen van de publieke kern van het internet voor de langere termijn als centrale inzet heeft.

Het nationale veiligheidsdenken op het internet is sterk in opkomst en dat heeft gevolgen voor de manier waarop het net wordt gezien en vooral ook voor welke actoren staten in stelling brengen om internetveiligheid te bevorderen. De meer traditionele ingenieursbenadering van de CERT's en de internationale samenwerking die daarin door de jaren heen is opgebouwd, begint last te krijgen van de vele nieuwe actoren in het cyberdomein die meer op nationale veiligheid gericht zijn, zoals inlichtingendiensten en politieagenten. Een vermenging van de aan die twee verbonden logica's is om twee redenen ongewenst. In de eerste plaats is nationale veiligheid altijd een partieel belang terwijl internetveiligheid – de veiligheid van het netwerk als geheel – een collectief belang is. Vermenging van de twee logica's, of dominantie van de eerste, kan het vertrouwen dat in de technische gemeenschap in lange jaren is opgebouwd serieuze schade toebrengen. Het duidelijk onderscheiden van taken (*scheiding*) is dus van groot belang. In de tweede plaats brengt de logica van nationale veiligheid een veel lagere risicotolerantie met zich mee. Nationale veiligheid laat weinig (politieke) ruimte voor restrisico's en trial and error: een enkele fout kan fataal zijn. Die logica verdringt andere opvattingen van veiligheid die voor de stabiliteit en betrouwbaarheid van het internet als publiek goed minimaal even groot of van groter belang zijn. Juist als het gaat om nationale veiligheid en de belangen van het collectieve internet geldt dat beteugeling en terughoudendheid van groot belang zijn om de stabiliteit van het net op de langere termijn te garanderen. In de praktijk hebben actoren op het gebied van

nationale veiligheid echter eerder de neiging om uit te breiden dan om zich te beperken. Het is daarom van belang om de discussie over internetveiligheid versus nationale veiligheid internationaal te agenderen en te pogen verschillende opvattingen van veiligheid in relatie tot het internet te ontvlechten. Hiervoor wordt in hoofdstuk 5 een aanzet uitgewerkt. Ook hier geldt dat Nederland in een unieke positie is om dat te doen: een internationale reputatie als een technologische hoogstaande natie, een *early adapter* als het gaat om het internet en een groeiende reputatie als centrum van internationaal recht en diplomatieke denkkracht.

NOTEN

1 Zelfs het meest centrale protocol – IP – kreeg in 1982 een stevige steun in de rug toen Vint Cerf en collega's internetgebruikers van het toen nog zeer kleine internet met uitsluiting dreigden: "If you don't implement TCP/IP, you're off the net" (geciteerd in Wu 2011: 202).

2 Zie de statistieken op: http://www.google.com/intl/nl/ipv6/statistics.html#tab=per-country-ipv6-adoption, bezocht op 5 november 2014.

3 Gesprek met prof. dr. Erik Huizer, 21 januari 2015.

4 Dit onderzoek is overigens wel beperkt tot het meten van het gebruik van DPI voor het terugdringen (*throtteling*) van P2P-dataverkeer.

5 Netwerkbeheer gaat over effectief gebruik van bandbreedte en heeft minimaal twee aspecten. Moeten meerdere gebruikers 'boeten' – in termen van toegang en snelheid – als enkele gebruikers enorm data-intensief gebruik hebben? Of moet dan de snelheid van de enkeling teruggebracht worden? Daaraan gerelateerd is het zo dat bepaalde toepassingen zoals digitaal telefoneren (Voice over IP, VoIP), online gaming en het streamen van muziek en video veel data-intensiever en veel gevoeliger zijn voor verlies aan bandbreedte. Niemand heeft er last van als de pakketjes van een e-mail schokkerig bij de eindgebruiker aankomen of dat een download iets langer duurt maar de minste vertraging in een digitale telefoonverbinding maken een gesprek nagenoeg onmogelijk. Beide gevallen zijn legitieme redenen om verschillende datastromen te ordenen en ervoor te zorgen dat het netwerk maximale kwaliteit levert voor de meeste gebruikers.

6 Dat betekent overigens nog niet dat grote internetbedrijven als Netflix en Google geen grote investeringen doen om hun bereikbaarheid te verbeteren en te garanderen. Integendeel.

7 Voorstel voor een verordening tot vaststelling van maatregelen inzake de Europese interne markt voor elektronische communicatie en om een connectief continent tot stand te brengen, zie http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013PC0627.

8 Dominic Rushe (2014) 'Net neutrality: cable companies 'stunned' by Obama's 'extreme' proposals', *The Guardian*, 11 November 2014. Zie: http://www.theguardian.com/technology/2014/nov/10/cable-companies-obama-net-neutrality-proposals-fcc-fight.

9 8th Internet Governance Forum, Bali, Indonesia. Session number 143, 22 October 2013. Zie: http://www.intgovforum.org/cms/igf-2013-transcripts/1501-ws-143-emerging-cyber-security-threats-, geraadpleegd 13 December 2013.

4 NATIONALE BELANGEN EN HET INTERNET ALS MONDIAAL PUBLIEK GOED

> Invite states in, and along with them comes their fragmentation and their stifling political constraints; shut them out entirely, and there is a risk that accountability will disappear and rights will be lost.
> Milton Mueller (2010: 240)

4.1 INLEIDING: WAAR NATIONALE BELANGEN RAKEN AAN DE PUBLIEKE KERN VAN HET INTERNET

In dit hoofdstuk staat een aantal ontwikkelingen centraal waarbij inbreuk wordt gemaakt op de publieke kern van het internet of waarbij dat dreigt te gebeuren. Hierbij komen de centrale waarden van het internet als publiek goed in het geding hetgeen serieuze gevolgen kan hebben voor het technisch en sociaaleconomisch functioneren van het net. Wie bijvoorbeeld rommelt in het DNS rommelt met het hele internet. Met andere woorden, het gaat om inbreuken op waarden als universaliteit, interoperabiliteit en toegankelijkheid van het internet die het gevolg zijn van acties, beleid en wetgeving die specifieke nationale en/of economische belangen boven het belang van de collectieve kern van het internet stellen. De gevolgen van dergelijke ingrepen zijn potentieel zeer groot. Op technisch niveau is het mogelijk om het internet 'kapot' te maken, zeker in de zin van het beschadigen van de integriteit en de betrouwbaarheid van de centrale protocollen en dus van het functioneren van het net.

In dit hoofdstuk worden vier beleidsontwikkelingen bekeken waarbij er in de uitwerking en implementatie voor gekozen is om de publieke kern van het internet te 'gebruiken'. Dat dreigde bijvoorbeeld te gebeuren met een aantal recente voorstellen voor wetgeving en verdragen waarmee auteursrecht en intellectueel eigendom op het internet beschermd dienden te worden. Paragraaf 4.2 gaat in op de drijvende krachten achter dergelijke wetgeving – vaak een klassiek geval van wat economen 'regulatory capture' noemen waarbij de industrie feitelijk de wetten schrijft – en op de gevolgen voor het internet van sommige van deze voorstellen. Een aantal voorstellen met bekende acroniemen zoals SOPA, PIPA en ACTA zijn inmiddels in hun huidige vorm van de agenda afgevoerd, maar noch de problematiek noch de krachten achter deze ontwikkelingen zijn weggenomen. Ook het politieke gebrek aan inzicht in de gevolgen van bepaalde technische keuzes blijft vruchtbare grond voor nieuwe wetgeving die potentieel schadelijk is voor de publieke kern van het internet. Paragraaf 4.3 gaat in op een van de, vanuit het perspectief van de mensenrechtenagenda, grootste problemen op het internet: censuur en de beperking van de vrijheid van meningsuiting. De nadruk in dit rapport ligt daarbij meer op de gevolgen van technische maatregelen die raken aan het functioneren van de kern van het publieke internet dan op de schendingen van mensenrechten in de mondiale digi-

tale sfeer zelf (zie voor een uitgebreide analyse vanuit dit laatste perspectief het recente AIV-rapport (2014) *Het internet. Een wereldwijde vrije ruimte met begrensde staatsmacht*). Zowel paragraaf 4.2 als 4.3 onderstreept bovendien de centrale rol die ISP's spelen als de favoriete laag van het internet voor de regulering van het gedrag van consumenten, burgers en bedrijven. Overheden en bedrijven kloppen bij ISP's aan om hun belangen te behartigen. Daaraan zijn uiteraard de nodige risico's verbonden, met name het probleem dat controle en censuur verdwijnen in de backoffice van het internet en zich onttrekken aan toezicht en democratische controle. Paragraaf 4.4 richt zich op de groeiende invloed van actoren uit het domein van de nationale veiligheid. De groeiende aanwezigheid van inlichtingendiensten en militaire actoren op het internet heeft niet alleen gevolgen voor privacy, maar ook gevolgen voor de integriteit van het technische functioneren van het internet. Paragraaf 4.5 ten slotte behandelt pogingen van nationale staten om delen van het internet te nationaliseren en wat de gevolgen daarvan zijn voor het functioneren van het net als geheel. Langer lopende ambities van autoritaire regimes – zoals the great firewall van China of het halalinternet van Iran – krijgen daarbij gezelschap van democratische staten als Duitsland en Brazilië die in reactie op de onthullingen van Snowden over NSA-surveillance ook plannen hebben om dataverkeer, clouds en hardware (zeekabels) te nationaliseren. Een nationalisering van het net met strikt doorgevoerde voorgeschreven routes voor datastromen staat echter haaks op de manier waarop het internet normaal gesproken informatie verstuurt.

4.2 IP VERSUS IP[1]

Het internet is een gigantisch, wereldwijd verspreid kopieerapparaat dat altijd aanstaat (Mueller 2010: 131). Gebruikers kunnen waar dan ook ter wereld content raadplegen, downloaden en delen met anderen. Sinds de opkomst van P2P-software gaat het steeds vaker om illegale uitwisseling van met auteursrecht beschermde muziek, films, games en boeken. Dit gegeven staat uiteraard op gespannen voet met de bescherming van intellectueel eigendom. De georganiseerde entertainmentindustrie – met een machtige lobby en een leger advocaten – zet zich al jaren in voor striktere nationale en internationale wet- en regelgeving om het ongeautoriseerd delen en downloaden van auteursrechtelijk beschermde content via het internet te bestrijden (Breindl en Briatte 2010). Daarbij wordt in toenemende mate gebruikgemaakt van regimes en maatregelen die ingrijpen op de vitale technische infrastructuur van het internet, zoals IP-adressen of het DNS. Deze strategie, waarbij het internet zelf wordt gebruikt om intellectueel eigendom te beschermen, stuit echter op steeds groter verzet van gebruikers, internetbedrijven, civil society en internetorganisaties. Zij betogen dat de voorgestelde maatregelen ineffectief zijn, voorbijgaan aan elementaire rechtstatelijke beginselen en, niet in de laatste plaats, schadelijk zijn voor het functioneren van het internet. De bescherming van intellectueel eigendom heeft zich ontwikkeld tot een van de centrale kwesties van

de strijd om de governance van het internet, door Mueller (2010) kernachtig samengevat als 'IP versus IP', oftewel Intellectual Property versus Internet Protocol.

De clash tussen internet en intellectueel eigendom komt voort uit twee diametraal tegenovergestelde processen, die elkaar in eerste instantie nauwelijks raakten. Aan de ene kant was er de liberalisering van de telecommunicatie-industrie, waar het internet enorm van profiteerde en waardoor een decentraal, competitief mondiaal internet ontstond. Aan de andere kant waren er de pogingen om de bescherming van intellectuele-eigendomsrechten mondiaal te reguleren, hetgeen resulteerde in een aantal internationale verdragen als TRIPS (WTO 1994), WCT en WPPT (WIPO 1996) en de Europese Auteursrechtrichtlijn (2001). De sterke groei van het internet maakte dat deze twee ontwikkelingen hard met elkaar in botsing kwamen, waarbij de aandacht al snel verschoof van de bescherming van softwarepatenten naar de aanpak van 'piraterij'.

De bescherming van intellectuele eigendom op het mondiale internet is echter lastig: intellectueel eigendom moet afgebakend worden om eraan te kunnen verdienen. Digitale content valt echter nauwelijks te beschermen omdat die oneindig te reproduceren is, tegen marginale kosten over de gehele wereld verspreid kan worden en dat alles zonder dat de eigenaar daar iets van merkt en zijn bezit uit handen hoeft te geven (Boyle 1997). De digitalisering destabiliseerde eerdere wetgeving en beleid ten aanzien van auteursrecht. Voor gebruikers namen de mogelijkheden en het gemak voor het delen van door auteursrecht beschermd materiaal enorm toe, in het bijzonder door de opkomst van peer-to-peer file sharing (P2P) die via websites als Napster, LimeWire, Torrentz en Pirate Bay snel groeide. Tegen georganiseerde vormen van P2P file sharing vonden rond de eeuwwisseling in verschillende landen rechtszaken plaats, zoals die tegen *Napster* in de Verenigde Staten (2001) en *MMO* in Japan (2002). In Nederland werd *Pirate Bay* onlangs nog verboden. Dit soort maatregelen blijkt in de praktijk echter geen structureel effect te hebben (Poort et al. 2014; Danaher et al. 2013), omdat er steeds nieuwe en slimmere P2P-tools worden ontwikkeld. Ook blijkt downloaden uit illegale bron allang geen uitzondering meer te zijn maar een wijdverspreide praktijk. Illegaal downloaden lijkt daarmee behoorlijk te 'democratiseren': in Nederland doet inmiddels ruim een kwart van de bevolking tussen 18 en 65 jaar eraan mee (Poort en Leenheer 2012). Omdat rechtszaken kostbaar en tijdrovend zijn en soms grote pr-risico's met zich meebrengen ('rijke entertainment industrie ruïneert downloadende tiener') concentreert de entertainmentindustrie zich al jaren op de politieke lobby. Zij probeert zo nieuwe wetgeving van de grond te krijgen die zich richt op (a) internetintermediairs en (b) regels die via de internetarchitectuur uitgevoerd moeten worden. Een aantal daarvan is inmiddels doorgevoerd en staande praktijk.

Een belangrijk kenmerk van deze maatregelen is de inschakeling van private internetbedrijven. De maatregelen zijn er in twee soorten. Het meest gangbaar is het 'notice and take down'-regime waarbij internetbedrijven bepaalde content ontoegankelijk maken. Zij doen dit meestal in ruil voor verminderde aansprakelijkheid voor het hosten of doorgeven van illegale content. Zo stelt de Amerikaanse *Digital Millennium Copyright Act* (1998) ISP's vrij van aansprakelijkheid in ruil voor de verplichting om content te verwijderen wanneer rechtshouders daarom vragen. In de EU trad in 2000 de Richtlijn inzake elektronische handel (e-commerce) in werking.[2] Om een beeld te geven van de omvang van deze praktijk: Google ontving in 2012 in een maand tijd ruim 6,5 miljoen verzoeken om door auteursrecht beschermd materiaal te verwijderen (DeNardis 2014: 178). Hier ontstaat het risico dat controle op inhoud – en in het verlengde daarvan censuur – verschuift naar de anonieme laag van de ISP's en andere internetintermediairs. Zuckerman (2010) heeft het in dat verband over de opkomst van 'intermediary censorship'. Wanneer overheden – in dit geval met een grote industrie op de achtergrond – erin slagen om internetbedrijven deze regels te laten volgen en af te dwingen onder de eigen gebruikers zijn implementatie en censuur "effectively outsourced to private industry" (MacKinnon 2011: 197). Nog een stap verder gaat het als deze bedrijven preventief inhoud van het netwerk gaan weren om conflicten met overheden of schadeclaims en rechtszaken voor te zijn. Dan is niet alleen de letter van de wet aan private partijen uitbesteed, maar in toenemende mate ook de geest van de wet. De vraag is uiteraard of dit een wenselijke ontwikkeling is.

Een radicalere aanpak vormen de zogenoemde 'graduated response'-mechanismen, bij wet geïmplementeerd in landen als Frankrijk, Zuid-Korea, Chili en Taiwan of als product van private overeenkomsten tussen ISP's en de entertainmentindustrie toegepast in het Verenigd Koninkrijk, de Verenigde Staten en Ierland (Brown en Marsden 2013; DeNardis 2014; Van Eeten et al. 2014). Daarbij wordt – na enkele waarschuwingen – de internetverbinding van de gebruiker beëindigd of de snelheid van de verbinding zo sterk teruggeschroefd dat het downloaden van grote bestanden onmogelijk wordt; ook kan de toegang tot bepaalde diensten domweg worden geblokkeerd. Deze maatregelen worden in de praktijk meestal uitgevoerd door internetbedrijven, die strategisch het beste gepositioneerd zijn om (hun) gebruikers aan te pakken en daarvoor ook de technische knowhow bezitten. Hun rol is in veel landen wettelijk vastgelegd en/of gecodificeerd in gebruikersovereenkomsten. Nu zij door de ontwikkeling van DPI in staat zijn het internetverkeer te analyseren, gaan er ook stemmen op om ze te verplichten het verkeer actief te monitoren ten behoeve van rechtshouders. Het Europees Hof heeft voor deze ontwikkeling een stokje gestoken met zijn uitspraak in de zaak Scarlet vs. SABAM (C-70/10) in november 2011.[3] Ook hier is dus de tendens dat controle en de uitvoering van beleid verschuift naar de private backoffice van het internet, en daarmee ook steeds meer uit het publieke zicht verdwijnt.

De meeste voorstellen voor de regulering van auteursrecht op het internet zijn tot stand gekomen onder sterke druk van de media- en entertainmentindustrie en vormen een klassiek voorbeeld van *regulatory capture*, de situatie waarin wet- en regelgeving sterk onder invloed staat van een bepaalde groep belanghebbenden. Hierin is enkele jaren geleden verandering gekomen toen een grootschalig, mondiaal protest ontstond tegen twee nieuwe Amerikaanse wetsvoorstellen, SOPA (Stop Online Piracy Act) en PIPA (Protect IP Act), en tegen het internationale verdrag ACTA (Anti-Counterfeiting Trade Agreement). Na grootschalige protesten kwam de ratificatie van de ACTA door de Europese lidstaten stil te liggen nadat het Europees Parlement besloot de overeenkomst te verwerpen. De nieuwe Europese Commissie heeft het wetsvoorstel inmiddels op de lijst van in te trekken voorstellen gezet. De protesten tegen SOPA, PIPA en ACTA worden gezien als een keerpunt in de geschiedenis van de totstandkoming van auteursrechtwetgeving (Benkler 2012; Hofmann 2012; Dubuisson 2012). Omdat het de eerste keer was dat de onlinegemeenschap zich collectief organiseerde en in actie kwam, wordt dit keerpunt ook wel beschreven als een strijd tussen de 'oude' en de 'nieuwe' economie: "PIPA and SOPA became nothing less than a referendum on who controlled the evolution of digital life" (Downes 2012, geciteerd in Hofmann 2012: 74-75). Beide Amerikaanse wetsvoorstellen zouden het 'notice and take down system' van de eerdere Digital Millennium Copyright Act (1998) uitbreiden naar betalingsnetwerken en advertentienetwerken. Bovendien boden de wetsvoorstellen private partijen ook immuniteit voor de schade die ze mogelijk veroorzaakten wanneer ze bepaalde content en betalingen ten onrechte blokkeerden (Hofmann 2012). De werking van SOPA en PIPA beperkt zich daarbij niet alleen tot de Verenigde Staten, ook websites in het buitenland of sites waarvan de toegang via in het buitenland geregistreerde domeinnamen plaatsvond, vielen eronder. Dit gegeven was een belangrijke oorzaak van de mondiale aandacht voor beide wetsvoorstellen. Deze aandacht werd in niet onbelangrijke mate veroorzaakt doordat websites als Wikipedia, Reddit en WordPress op 18 januari 2012 uit protest een dag 'op zwart gingen' waardoor delen van het internet onbereikbaar werden. Wikipedia deed dat onder de slogan 'imagine a world without free knowledge' en Google plaatste een zwarte censuurbalk over zijn logo: vrijheid van meningsuiting en informatievrijheid werden zo in stelling gebracht tegen het excessief beschermen van auteursrecht.

Een andere belangrijke kritiek op SOPA en PIPA, die vooral door technische experts naar voren werd gebracht, was dat deze wetsvoorstellen het functioneren van het internet ondermijnden, door te diep in te grijpen in de technische architectuur van het internet. Omdat ze aangrijpen op het niveau van de meest basale internetprotocollen als DNS en IP, werd 'don't break the internet' een andere belangrijke slogan van het verzet. Wederom klom een groot aantal van de internetpioniers in de pen en richtte zich op de gekozen vertegenwoordigers in het Amerikaanse Congres: "Regardless of recent amendments to SOPA, both bills will risk fragmenting the internet's global domain name system (DNS) and have other capricious techni-

cal consequences".[4] Ook wetenschappers lieten zich niet onbetuigd: "Directing the remedial power of the courts towards the internet's core technical infrastructure in this sledgehammer fashion has impact far beyond intellectual property rights enforcement – it threatens the fundamental principle of interconnectivity that is at the very heart of the internet" (Lemley et al. 2011). Kort gezegd: de invoering van beide wetten zou mogelijk grote schade aan het internet toebrengen. Het DNS is een van de centrale bouwstenen van het internet en vormt te samen met enkele andere protocollen de basis voor vrijwel alle andere protocollen en talloze applicaties die het internet goed en betrouwbaar doen werken (Lemley et al. 2011). Door blokkades in het kader van de bescherming van intellectueel eigendom en auteursrecht kunnen gebruikers er niet langer van uitgaan dat DNS-servers betrouwbare zoekresultaten opleveren. Door in te grijpen in kernprotocollen dreigt het internet behalve minder betrouwbaar en universeel ook minder veilig te worden.

Hier komt bij dat er grote twijfels zijn over de effectiviteit van dergelijke maatregelen, omdat blokkades door triviale veranderingen kunnen worden ontlopen (bijvoorbeeld door het intikken van het IP-adres, waardoor de DNS-server niet geraadpleegd hoeft te worden) en door gemakkelijk toegankelijke en installeerbare software plug-ins die gebruikers automatisch met niet-geblokkeerde DNS-servers verbinden (Crocker et al. 2011). Dergelijke trucs verspreiden zich snel onder verstokte up- en downloaders. Illegale content duikt na een blokkade bovendien al snel weer op, zoals steevast blijkt bij het verbod op P2P-netwerken, waarbij de ondergang van het ene platform de opkomst van het andere betekent. Daarnaast treedt door 'overblocking' vaak aanzienlijke nevenschade op. Door de grote interdependentie op het internet, bijvoorbeeld door virtual hosting of een website met diensten en e-mailverkeer gerund door andere domeinen, wordt al snel een veel groter deel van het DNS geblokkeerd dan wettelijk de bedoeling is. Dat dit een reëel probleem is, blijkt uit gevallen waarbij vele tienduizenden subdomeinen per ongeluk werden geblokkeerd. Yu (2012; 2014) noemt dit soort maatregelen dan ook 'highly disproportional'.

Het gevaar dat diep wordt ingegrepen op het internet ligt echter nog altijd op de loer. Er doen inmiddels nieuwe, soortgelijke voorstellen opgeld om auteursrecht te handhaven (Masnick 2014). En hoewel technisch filteren imperfect is en onvermijdelijk leidt tot het blokkeren van te veel of te weinig content (Zittrain en Palfrey 2008) is filteren gemeengoed geworden om intellectueel eigendom te beschermen (Sellars 2014; Breindl 2013). Dit is allereerst een gevolg van de eenzijdige en onevenwichtige betrokkenheid van stakeholders bij de besluitvorming over de regulering van intellectueel eigendom. Een tweede tekortkoming is het gebrek aan kennis over de technische aspecten van het internet bij degenen die de wetgeving maken dan wel goedkeuren. In de strijd rondom SOPA en PIPA verschenen steeds vaker artikelen met de strekking dat het 'no longer ok' is dat leden van het Congres

niet weten hoe het internet werkt (McDiarmid en Sohn 2013). Die boodschap is beslist niet alleen van toepassing op de Amerikaanse politiek. Het gevolg is echter geweest dat de economische belangen van de entertainmentindustrie boven het belang van de collectieve kern van het internet komen te staan, met als consequentie dat het publieke internet onder druk staat.

4.3 CENSUUR EN SURVEILLANCE

Omdat het internet – als het de vrije loop krijgt – van nature een vrijplaats is voor de meest uiteenlopende ideeën, is het van meet af aan met argwaan bekeken door regimes die de informatie die hun bevolking bereikt strikt onder controle proberen te houden. Met name autoritaire regimes zien surveillance en censuur als een noodzakelijke randvoorwaarde voor de internettoegang van hun bevolking. Het oorspronkelijke westerse optimisme dat internet en censuur onverenigbaar zouden blijken en dat vrijheid van meningsuiting zich eenvoudigweg op de rug van de techniek zou verspreiden, is inmiddels verlaten. De digitale vrijheid van meningsuiting – en andere digitale manifestaties van traditionele mensenrechten – staan in vele westerse landen als een prominent aandachtspunt op de diplomatieke agenda. In de VS zette Hillary Clinton in 2010 'internet freedom' op de agenda van Buitenlandse Zaken en Nederland nam in 2011 het voortouw in het opzetten van de 'Freedom Online Coalition', een coalitie van staten die internationaal samenwerken om vrijheid van meningsuiting in het digitale domein te versterken en beschermen. De Amerikaanse agenda voor internetvrijheid was met het vertrek van Clinton als minister van Buitenlandse Zaken al enigszins in het slop geraakt en sinds de Snowden-onthullingen is het leiderschap van de VS op dit punt weinig geloofwaardig.

Over de gehele wereld worden overheden steeds actiever in het monitoren en controleren van het internetverkeer (Howard et al. 2011; zie voor overzichten Deibert et al. 2008; 2010; 2011). Autoritaire regimes gaan daarin het verst, maar ook liberale democratieën laten zich niet onbetuigd. In China is de aansluiting op het wereldwijde internet van meet af aan opgezet met controle van de eigen bevolking in het achterhoofd. Het Chinese internet draait op "state-owned hardware servers, state-owned fibre optics via state-owned switches, boiling down to the idea that 'China is not on the internet, it's basically an intranet'" (Herold 2011: 5). China heeft een muur om 'zijn' internet gebouwd, met slechts enkele poorten naar buiten, installeert filtersoftware op pc's (Groene Dam project) en legt regelmatig bepaalde diensten, zoals Wikipedia, plat om ze van filters te voorzien die op basis van woordkenmerken automatisch content kunnen blokkeren (Zuckerman 2010). Ook in Saoedi-Arabië passeert al het in- en uitgaande internetverkeer een enkele toegangspoort, waar de staat een filtermechanisme heeft aangebracht (Zittrain en Palfrey 2008). De plannen voor een Iraans nationaal internet bouwen op dezelfde logica voort.[5]

De reikwijdte van de censuur, de digitale middelen die daarvoor beschikbaar zijn en de strategieën die staten gebruiken om hun bevolking te controleren hebben bovendien ook niet stilgestaan. In de begindagen van het internet was de gedachte nog vaak dat trage autoritaire overheden geen grip zouden krijgen op de jonge, snelle wereld van het internet. De reuzen op lemen voeten bleken echter al snel digitaal vaardiger dan gedacht en daarmee werd de censuur ook verfijnder en intelligenter. Blokkeren van inhoud gebeurt nog steeds als de nood acuut en hoog is, maar in veel landen is het onder toezicht toestaan en monitoren van het internetgebruik vaak een belangrijke informatiebron voor politie en inlichtingendiensten geworden. Hoewel het internet als geheel niet 'uitgezet' kan worden, zijn er wel vele *kill-switches* (DeNardis 2014: 207-213). Deze kill-switches variëren van het blokkeren van specifieke content tot DNS-blokkades, en van het uitvoeren van DDoS-aanvallen op specifieke websites tot het platleggen van delen van het internet door ISP's te dwingen om gebruikers de toegang tot hun netwerken te blokkeren. Dit gebeurde in 2011 in Egypte, toen het internet gedurende enige dagen tijdens de opstand tegen het regime van Mubarak werd platgelegd, maar daarvoor ook al in Libië, Birma, Nepal en Iran (DeNardis 2014). Budish en Kumar (2013) noemen dergelijke strategische blokkades 'Just in time censorship', dat bijvoorbeeld tijdens verkiezingen kan worden ingezet om de informatievoorziening rond de oppositie te blokkeren.

Soms hebben acties om content te blokkeren echter grote gevolgen voor het bredere internet omdat men ingrijpt in centrale protocollen als het DNS en routingprotocollen. Het bekendste voorbeeld is dat van de Pakistaanse blokkade van YouTube, dat wereldwijde gevolgen kreeg. In 2008 besloot het Pakistaanse ministerie van Informatie YouTube in Pakistan te blokkeren omdat er blasfemisch materiaal op te vinden was. De uitvoering door Pakistan Telecom was echter nogal ondoordacht: de door hen aangebrachte wijziging in de routingprotocollen beperkte zich niet tot alleen Pakistaanse ISP's maar werd mondiaal verspreid en overgenomen waardoor YouTube op het gehele internet onvindbaar werd (DeNardis 2014: 96; Deibert 2013b: 40). Hoewel de fout vrij snel werd teruggedraaid, is het een indicatie van de verwevenheid van het internet door de centrale protocollen en de kwetsbaarheid daarvan voor nationale acties, ingegeven door een specifieke opvatting van wat wel en niet op het internet toelaatbaar is.
Ook westerse staten laten zich niet onbetuigd: filteren is inmiddels gemeengoed, bijvoorbeeld om extremistische uitlatingen te bestrijden. De aanslag op Charlie Hebdo in Parijs heeft geleid tot hernieuwde aandacht voor het verwijderen van extremisme op het net in samenwerking met de private sector. Overigens wordt in het kielzog van het tegengaan van extremisme ook het opsporen en verwijderen van illegale content in zijn algemeenheid genoemd.[6] Wel zijn er wereldwijd verschillen in de – politieke, religieuze en sociale – redenen waarom het internet geblokkeerd wordt en de middelen die daarvoor worden ingezet (Zittrain en Palfrey 2008). Filteren wordt in westerse democratieën voornamelijk ingezet

(a) om een reeks van uitingen op het vlak van genocide en racisme te bestrijden, hoewel landen daar ook vaak heel verschillende opvattingen over hebben (Breindl 2013) en (b) om inbreuken op intellectueel-eigendomsrecht te voorkomen. Daarnaast proberen ook liberale democratieën om het internet en de activiteiten die daarop plaatsvinden aan nationale wetgeving te onderwerpen. Zo is de aanpak van cybercriminaliteit en de bestrijding van de verspreiding van kinderporno in veel landen hoog op de agenda geplaatst. Een ouder en bekend voorbeeld is de rechtszaak van de Franse regering tegen Yahoo om Nazi-parafernalia van een veilingsite te verwijderen. Een meer recent voorbeeld is Wikileaks, waarbij een reeks van private (internet)bedrijven zoals EveryDNS, Amazon, MasterCard, Visa en Paypal na het uitbreken van 'Cablegate' hun diensten aan Wikileaks beëindigden, waardoor Wikileaks onvindbaar werd en geen inkomsten meer kon genereren (Brown en Marsden 2013). Benkler (2011) trekt een directe lijn tussen deze 'spontane' acties van grote private bedrijven en de oproepen van prominente Amerikaanse politici als Senator Joseph Liebermann om Wikileaks uit de lucht te halen. De acties van deze bedrijven waren volgens de bedrijven zelf geen reactie op deze politieke oproepen, maar waren zeker ook geen uitvoer van een officieel verzoek van een regering of rechtbank. Deze ontwikkeling roept vragen op over de rol van private partijen bij de bescherming en/of de inperking van de vrije meningsuiting.

Internetbedrijven bevinden zich in toenemende mate in een spagaat als het gaat om de vrijheid van meningsuiting. Enerzijds worden zij – in het kader van de mensenrechtenagenda – geacht om ethisch te handelen in hun pogingen om marktaandeel te vergaren op de internationale groeimarkt van het internet. Toenmalig Amerikaans minister van Buitenlandse Zaken Clinton (2010) verwachtte veel van Silicon Valley als het ging om de strijd tegen censuur en voor de rechten van de mens: "American companies need to make a principled stand. This needs to be part of our national brand. I'm confident that consumers worldwide will reward companies that follow those principles." Anderzijds zijn deze bedrijven de eerste aanspreekpunten als overheden zelf willen ingrijpen op het internet om redenen van wat binnen de eigen nationale context als legitiem is gedefinieerd. Daarbij gaat het tegenwoordig vaak om redenen van veiligheid en nationale veiligheid (zie paragraaf 4.4). De verzoeken om informatie nemen sterk toe. Nederland heeft eind 2012 bijvoorbeeld Clean IT opgezet, een Europees project met België, Groot-Brittannië, Duitsland en Spanje om internet te schonen van terrorisme – zonder bindende overheidsvoorschriften, dus op basis van informele samenwerking met ISP's. Dit project is inmiddels afgerond, maar de recent geuite voornemens van EU-ministers in Riga wijzen op voortzetting ervan. De centrale rol van internetbedrijven in het mondiale internet roept vragen op over hun verantwoordelijkheid en autonomie. Het internationaal recht is echter nog steeds in hoofdzaak van toepassing op het gedrag van staten en de gedachte om dit direct van toepassing te laten zijn op internationale bedrijven is nog relatief nieuw (Scherer en Palazzo 2011: 911). Ook Ruggie, Harvard-hoogleraar en tussen 2005 en 2011 speciaal VN-vertegen-

woordiger voor Business and Human Rights, zag in hoofdzaak vormen van zelfregulering waarbij het taalgebruik soms 'zo elastisch is dat het elke betekenis verliest' (Ruggie 2007: 836). De zogenoemde Ruggie-principes die hij voor de VN heeft opgesteld en die zijn geaccepteerd in 2011 zijn een startpunt geweest voor de discussie over de rol van bedrijven bij de naleving van mensenrechten. Deze principes zouden in het digitale domein meer aandacht verdienen, waarvoor zou kunnen worden aangesloten bij het besluit uit 2014 van de Mensenrechtenraad van de VN om een werkgroep op te richten die de mogelijkheid van wettelijk bindende voorschriften onderzoekt.

Internetbedrijven geven niet klakkeloos gevolg aan alle verzoeken om content te blokkeren en hebben ruimte om afwegingen te maken. Tegelijkertijd geldt dat bedrijven op veel punten wel – soms meer en soms minder vrijwillig – meewerken aan allerlei verzoeken van de bevoegde instanties. Uit de transparantieverslagen die bedrijven als Google,[7] Twitter[8] en Microsoft[9] publiceren om zich te verantwoorden tegenover de internetgemeenschap, blijkt dat het vooral liberale democratische regimes zijn die – openlijk – de meeste data opvragen (Deibert 2013b). Veel van deze opvragingen en 'blocklists' van websites zijn niet openbaar en daarom niet of nauwelijks aan democratische controle onderhevig (Zittrain en Palfrey 2008; Brown en Marsden 2013). Hetzelfde geldt voor de blokkades die voortvloeien uit afspraken tussen private partijen (Van Eeten et al. 2014). De uitvoering van de meeste censuur komt dus op het bordje te liggen van internetbedrijven die daarin deels de autoriteiten te volgen hebben, deels mogelijkheden zien tot verzet tegen de wensen van overheden – met name die bedrijven die leven van hun publieke profiel – en deels juist voor de troepen uitlopen en preventief ingrijpen, zoals in de casus van Wikileaks het geval lijkt te zijn geweest. DeNardis (2014: 158-159) heeft het in deze context over 'discretionairy censorship'; het is echter niet duidelijk hoe ver die discretie strekt en welke keuzes verschillende bedrijven daarin maken. Het is in ieder geval onderdeel van een bredere beweging naar wat Zuckerman (2010) 'intermediairy censorship' noemt, waarbij private bedrijven publieke taken uitvoeren, maar dan wel buiten het zicht van het publiek.

Een dergelijke aanpak heeft in potentie een negatief uitstralingseffect, en maakt het voor westerse landen lastig om op het mondiale toneel op geloofwaardige wijze de censuur van autoritair geregeerde staten te veroordelen (Yu 2012; 2014). De kosten van filteren, de bijkomende schade als gevolg van overblocking, het gebrek aan transparantie en potentieel voor misbruik van dit type technische interventie wegen volgens Mueller (2010: 209-211) niet op tegen de voordelen van de vrije en open communicatie waarmee het internet groot geworden is.

4.4 VEILIGHEID BOVEN VEILIGHEID

De opkomst van het veiligheidsdenken op het internet werd al aangestipt in hoofdstuk 3. Cybersecurity is door de jaren heen steeds meer een kwestie van nationale veiligheid geworden. Nederland is daarin geen uitzondering. Vijf jaar geleden was internetbeleid in hoofdzaak een kwestie voor het ministerie van Economische Zaken en ging het over e-commerce en de kaders voor telecom en internet. Anno 2014 is het zwaartepunt verschoven naar het thema cybersecurity dat onder het ministerie van Veiligheid en Justitie valt, om precies te zijn de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Het ministerie van Defensie is een goede tweede met een operationeel Cyber Commando en een officiële bevoegdheid om defensieve en offensieve militaire operaties op het internet uit te voeren. Een vergelijkbare verschuiving van het primaat van economie naar veiligheid heeft op Europees niveau plaatsgevonden. Binnen de Europese Commissie heeft lang niet alleen het directoraat-generaal (DG) CONNECT aandacht voor internet. Ook de DG's voor Justitie en Binnenlandse Zaken en de diplomatieke dienst van de Commissie hebben cyberbeleid inmiddels hoog op de veiligheidsagenda staan.

Nu is het internet in de afgelopen jaren in absolute zin ontegenzeggelijk onveiliger geworden maar hoe groot de dreiging is, en voor wie precies, is moeilijk vast te stellen. Bovendien is het de vraag of staten de juiste organisaties in stelling brengen om de juiste dreigingen tegen te gaan (Dunn Cavelty 2014). Vele onderzoekers vinden dat er sprake is van dreigingsinflatie en dat de taal van nationale veiligheid en oorlog niet helpt (Brito en Watkins 2011; Betz en Stevens 2011; Libicki 2012; Rid 2013; Lawson 2013). Daarmee is nog niet gezegd dat het (Nederlandse) internet is gesecuritariseerd of gemilitariseerd, maar de beleidsblik op het internet is wel degelijk aan het schuiven. Het internet van de economische kansen is nu (ook) het internet van de bedreigingen, de kwetsbare vitale infrastructuren en de nationale veiligheid. Misschien zelfs meer.

Dat dit gevolgen heeft, werd pijnlijk duidelijk door de Snowden-onthullingen, waaruit bleek dat – onder meer – de Amerikaanse NSA en het Britse GCHQ onder de vlag van nationale veiligheid grote delen van het mondiale internetverkeer bleken te traceren en op te slaan (Greenwald 2014). De verschillende surveillanceprogramma's die publiek geworden zijn, zoals PRISM, MUSCULAR en BULLRUN,[10] laten een beeld zien van veiligheidsdiensten met een enorme verzameldrift, een gebrekkige werking van de juridische kaders, tekortschietend juridisch en democratisch toezicht en massale privacyschendingen, afgezet tegen wat een zeer beperkte opbrengst lijkt in termen van nationale veiligheid (Landau 2013; Glennon 2014; Van Hoboken en Rubinstein 2014; Mueller en Stewart 2014). De technologische

mogelijkheden en de ruime budgetten hebben de werkelijkheid van deze veiligheidsdiensten losgezongen van een meer traditionele visie op nationale veiligheid en hun eigen rol daarin.

> "In prior generations, the cost of surveillance and data acquisition constituted a useful buffer between state surveillance and privacy; resource constraints forced law enforcement to focus on a limited number of targets on a scale where judicial oversight was a practical— if imperfect— deterrent against overreach."
> (Faris en Gasser 2013: 21)

Naast de massaliteit van de privacyschendingen, die de nodige tegenreacties hebben opgeroepen, bleek uit de onthullingen dat uit naam van nationale veiligheid ook diep is ingegrepen in de technische infrastructuur van het internet die wij dagelijks gebruiken. Tim Berners-Lee, de uitvinder van het WWW, noemde de beslissing van NSA en GCHQ om de encryptiesoftware van internetbedrijven te kraken 'appalling and foolish' en in directe tegenspraak met de Amerikaanse en Britse strijd tegen cybercriminaliteit en de bestrijding van cyberconflicten, die als prioriteiten voor de nationale veiligheid zijn aangemerkt. Hij beschouwde deze acties bovendien als verraad aan de technologische industrie.[11] Een grote groep Amerikaanse crypto- en internetveiligheidsexperts schreef in januari 2014 een open brief aan de Amerikaanse regering met dezelfde strekking: "The choice is not whether to allow the NSA to spy. The choice is between a communications infrastructure that is vulnerable to attack at its core and one that, by default, is intrinsically secure for its users".[12]

De spanning tussen de 'noden' van de inlichtingendiensten en de belangen van de IT- en internetindustrie kwam al eerder aan de oppervlakte tijdens de zogenoemde 'cryptowars' van de jaren negentig. Onderwerp van deze oorlogen was de cryptografische beveiliging van Amerikaanse softwareproducten en vooral de export daarvan. Het ging om software die bestemd was voor de overgrote meerderheid van de computer- en internetgebruikers. De IT-industrie wilde producten met een sterke beveiliging kunnen exporteren, maar de Amerikaanse inlichtingendiensten waren daar mordicus tegen omdat ze de toegang tot systemen (wereldwijd) niet wilden bemoeilijken (Van Hoboken en Rubinstein 2014; Landau 2010; 2014). Met andere woorden: de diensten wilden toegang voor zichzelf garanderen door de cryptografische standaarden laag te houden, door het bezit van sleutels tot cryptografie of door het invoegen van geheime achterdeuren in de software die aan gebruikers wereldwijd werd geleverd. Na een lange strijd tussen de veiligheidsdiensten en de industrie werd de export uiteindelijk vrij gegeven. Inmiddels weten we echter dat de diensten sindsdien niet stil hebben gezeten. In het huidige post-Snowdentijdperk reageren de grote internetbedrijven en cloudservices die – deels bewust en deels onbewust – de data aan de NSA 'leverden', door het dataverkeer met klanten en tussen de eigen datacentra cryptografisch beter te beveiligen. Dit in

de hoop het beschadigde vertrouwen van Amerikaanse, maar ook niet-Amerikaanse, klanten terug te winnen. Het protest van diensten als de FBI en NSA tegen nieuwe beveiliging met encryptie en de roep om wettelijke bevoegdheden om cryptologische beveiliging te breken, zijn zowel in de VS als in Europa aangezwollen na de aanslag tegen Charlie Hebdo in Parijs. Apple en Google, die de beveiliging van smartphones recentelijk hebben opgewaardeerd, worden openlijk bekritiseerd door bijvoorbeeld de FBI.[13] Ook beschuldigde de directeur van het Britse GCHQ de Amerikaanse technologiebedrijven – vanwege het opschroeven van encryptie – ervan de "Command-and-control networks of choice for terrorists and criminals" te zijn (geciteerd in Faris en Heacock Jones 2014: 34).

De ambitie van veiligheidsdiensten om toegang tot data en communicatie te verkrijgen en zelfs te garanderen gaat echter verder. Uit de Snowden-onthullingen blijkt namelijk dat de NSA zich ingespannen heeft om de cryptografie niet alleen te breken, maar die ook op het niveau van de officiële standaardisatie door het National Institute of Standards and Technology (NIST) doelbewust te verzwakken. De dienst probeert zwakheden in cryptografische standaarden in te bouwen om zo een permanente achterdeur te verkrijgen. Dit is uiteraard niet alleen schadelijk voor de reputatie van NIST, maar ook voor de algemene veiligheid op het internet en voor de internationale politieke verhoudingen: "It appears that the NSA's SIGINT division viewed corrupting cryptography standards as a goal. If other goverments had done such a thing, the US would have been outraged" (Landau 2014: vii). Het ingrijpen op het niveau van de standaarden heeft uiteraard een olievlekwerking: omdat een protocol gecertificeerd is als een standaard is de verspreiding ervan groot. Dat maakt het bereik van de NSA – in termen van toegang – zeer groot, maar maakt ook het bereik van internetkwetsbaarheid zelf en het risico voor de gebruiker zeer groot. Of, zoals internetbeveiligingsexpert Bruce Schneier het zegt: "You can't build a back door that only the good guys can walk through".[14]

Dat laatste geldt nog veel sterker voor een internationale markt in *cyberonveiligheid* die in de afgelopen jaren tot wasdom is gekomen. Elke cyberaanval, of het nu gaat om criminaliteit, spionage, cybervandalisme of een militaire cyberaanval, heeft een of meer kwetsbaarheden nodig in de software van het doelwit om toegang tot diens systemen te krijgen. Die kwetsbaarheden worden ook wel 'zero-day vulnerabilties' genoemd: een fout in software die onbekend is voor zowel de gebruiker als de producent van de software en waarvoor dus geen reparatie beschikbaar is. De softwarefabrikant heeft 'nul dagen' om de kwetsbaarheid te repareren als een hacker deze ontdekt en gebruikt. Van deze kwetsbaarheden kun je cyberwapens maken door code te schrijven die de kwetsbaarheid uitbuit en schade toebrengt aan systemen of via de systemen (iets laten ontploffen, sluizen openzetten enz.): dan spreken we van 'cyber exploits'. Cyberwapens komen in vele vormen voor: van heel simpel en met een beperkt potentieel – zoals een DDOS-aanval – tot zeer specifiek met een groot potentieel (Rid en McBurney 2012:

6). Het beroemde voorbeeld van de Stuxnet-aanval op Iran, waarbij een schadelijk computervirus het Iraanse nucleaire programma op substantiële achterstand zette, was naar alle waarschijnlijkheid een langdurige militaire operatie van de VS en Israël, vereiste een minutieuze voorbereiding in termen van inlichtingen en maakte gebruik van ten minste vier tot dan toe onbekende zero days (Sanger 2012; Singer en Friedman 2014). Die zero days hebben de Amerikaanse en Israëlische militairen en inlichtingendiensten wellicht zelf ontdekt, maar even waarschijnlijk is dat ze deze gekocht hebben op de internationale groeimarkt voor zero days. Deze markt kent drie 'kleuren' – wit, grijs en zwart – en is de afgelopen jaren dramatisch gegroeid (Fidler 2014; Ablon et al. 2013). In de begindagen van groei van het WWW was het vaak nog een sport voor hackers om kwetsbaarheden in software op te sporen en deze onder de aandacht van fabrikanten te brengen. De kick en de erkenning van de prestatie waren vaak voldoende. Tegenwoordig worden hackers voor het opsporen van kwetsbaarheden steeds vaker en beter betaald door die bedrijven. Dat is de witte markt. Maar het echte geld is op de grijze en de zwarte markt te verdienen. De zwarte markt werkt online via websites als Silk Road en zijn opvolgers en levert in principe alles wat verboden is aan iedereen. De grijze markt wordt voornamelijk gebruikt door nationale veiligheids- en inlichtingendiensten en door militaire cybereenheden, hoewel sommige van hen zich waarschijnlijk ook op de zwarte markt begeven (Fidler 2014). De grijze markt is een open en legale – of in ieder geval ongereguleerde – markt waarin de bedrijven websites hebben waarop producten worden aangeprezen en waarop benoemd wordt wat zij als legitieme klanten zien.[15] Zo verkoopt het Franse VUPEN niet aan alle partijen maar alleen aan "approved government agencies (Intelligence, Law Enforcement, and Defense) in approved countries".[16] Uitgesloten zijn landen die het onderwerp zijn van een internationaal wapenembargo van de VN, de VS of de EU (zie ook Stockton en Golabek-Goldman 2013). Echter, aangezien veel van deze bedrijven waarschijnlijk ook leveren aan de wapenindustrie is de verspreiding wellicht veel groter (Fidler 2014).

Het probleem is dat deze overheden in naam van de nationale veiligheid kwetsbaarheden in de software die wij gebruiken – en onze vitale infrastructuren, banken en clouds – opkopen en geheim houden, zodat ze op een later moment kunnen worden ingezet voor een militaire of inlichtingentaak. Het achterhouden van deze kwetsbaarheden is echter niet zonder risico's omdat 'hun' veiligheid en 'onze' veiligheid op het internet nu eenmaal onlosmakelijk verbonden zijn. Wederom verwoordt Bruce Schneier (2014) het scherp in zijn kritiek op het verzamelen ('stockpiling') van kwetsbaarheden door de Amerikaanse diensten en strijdkrachten: "There is no way to simultaneously defend U.S. networks while leaving foreign networks open to attack. Everyone uses the same software, so fixing us means fixing them, and leaving them vulnerable means leaving us vulnerable".

Ook de levendige handel in zero days wijst dus op de groeiende spanning tussen *nationale* veiligheid in het cyberdomein en de veiligheid van het cyberdomein zelf. Myriam Dunn Cavelty (2014) vertaalde het securitydilemma van Jervis (1978) naar de huidige ontwikkelingen in het cyberdomein: "Paradoxically, the use of cyber space as a tool for national security, both in the dimension of war fighting and the dimension of mass surveillance, has detrimental effects on the level of cyber security globally". De inspanningen van de ene staat om zichzelf te beveiligen, roepen een tegenreactie op van een andere staat en dat maakt de eerste staat weer onveiliger. En bijgevolg wordt het hele cyberdomein onveiliger. Deibert en Rohozinksi (2011) wijzen erop dat China zijn militaire cybercapaciteit heeft opgezet in reactie op de Amerikaanse beslissing een militair Cyber Command in te stellen. Op een recente conferentie over civiel-militaire samenwerking in cyberspace stelde een expert op het gebied van militaire cyberstrategie dat de voornaamste fall-out van de NSA-onthullingen was dat andere staten nu de opbouw van dezelfde capaciteiten nastreven.[17] Een cyber-Westfalen waarin staten hun eigen nationale veiligheid vooropstellen heeft daarmee grote gevolgen voor de collectieve infrastructuur waarop al die staten de cyberversie van hun land, economie en samenleving hebben gebouwd. Op het fundamentele niveau van standaarden, encryptie en kwetsbaarheden in software is de verwevenheid tussen staten zo groot dat 'wij' en 'zij' tot op zekere hoogte lege begrippen worden.

Het voorgaande betekent dat een zekere mate van terughoudendheid (beteugeling) zeker in het cyberwardomein van groot belang is en daar ligt meteen een flink probleem. Nationale veiligheid is verankerd in het principe van nationale soevereiniteit en daarmee gegrond in nationale wetgeving en slechts in zeer beperkte mate in internationaal recht. Veiligheids- en inlichtingendiensten zijn nauwelijks onderwerp van internationaal recht, maar worden alleen op nationaal niveau met wet- en regelgeving ingekaderd. Nagenoeg elk land heeft ze en ze doen allemaal ongeveer hetzelfde binnen de restricties die de wet, maar met name hun budget, aan ze oplegt. Dat maakt de discussie over de rol van deze diensten zo lastig, zeker tegen de achtergrond van nieuwe technologische mogelijkheden en onverwachte afwegingen tussen nationale veiligheid en internetveiligheid (en daarmee uiteindelijk ook weer nationale veiligheid). Op deelgebieden wordt over oplossingen nagedacht. Zo zijn er pleidooien om het Verdrag van Wassenaar, dat de export van dual-usetechnologie reguleert, te verbreden naar cyberwapens en de handel in zero days (Stockton en Golabek-Goldman 2013; Fidler 2014). Dat zou de internationale markt iets kunnen reguleren maar laat het dieper liggende cybersecurity-dilemma grotendeels ongemoeid.

4.5 TECHNOLOGISCHE SOEVEREINITEIT

Het afschermen van een 'nationaal' deel van het internet was tot voor kort voornamelijk een wens van autoritaire regimes, met the great firewall of China en het halalinternet van Iran als de meest tot de verbeelding sprekende voorbeelden. In het post-Snowdentijdperk lijken echter meer landen op zoek naar een betere bescherming van 'eigen' internet, dataverkeer en -opslag. De kwestie van soevereiniteit speelt al heel lang op het internet en ook westerse landen laten zich niet onbetuigd als het gaat om het handhaven van wet- en regelgeving in het digitale domein. Maar enkele recente proefballonnen en initiatieven gaan een stap verder dan pogingen om offline verboden zaken – zoals kinderporno, criminaliteit en schendingen van auteursrecht – ook op het internet tegen te gaan.

De onthullingen over de activiteiten van inlichtingendiensten als de NSA en GCHQ zijn door vele burgers en overheden niet alleen ervaren als een massale schending van privacy maar ook als een aantasting van de soevereiniteit. Dit ondanks het feit dat ook de staten die zich aangetast voelen in de regel eigen inlichtingen- en veiligheidsdiensten hebben met grofweg dezelfde opdracht en bevoegdheden. Het verschil tussen staten lijkt tot op zekere hoogte meer te gaan om budget en technische capaciteiten dan om de opdracht en bevoegdheden van de diensten zelf. Toch hebben de schaal en massaliteit van de NSA-surveillance, de politieke doelwitten (bevriende staatshoofden en regeringsleiders zoals Rousseff van Brazilië en Merkel van Duitsland), de intermediaire doelwitten (van Google tot Belgacom) en de economische doelwitten (in sommige gevallen leek nationale veiligheid toch wel heel sterk op economische spionage) in veel landen kwaad bloed gezet. Aangezien inlichtingendiensten in essentie internationaal ongereguleerd zijn en internationale regulering weinig kans lijkt te maken, kijken getroffen landen naar andere mogelijkheden om zich tegen grootschalige surveillance te beschermen. Gezien het feit dat de VS door velen als de grootste digitale indringer wordt gezien en gegeven het feit dat de informatierijkdom voor het overgrote deel is afgetapt van de websites, diensten, servers en clouds van Amerikaanse bedrijven, zijn er verschillende initiatieven opgekomen om het dataverkeer om (Amerika heen) te leiden of – als het via Amerikaanse platforms loopt – lokaal te maken waar dat kan. 'Technologische soevereiniteit', 'datasoevereiniteit', 'datalokalisering' en 'nationale clouds' zijn eigenlijk allemaal varianten van de wens om privacyschendingen te voorkomen en politiek een vuist te maken tegen buitenlandse surveillance van burgers, bedrijven en overheden.

Er zijn sinds de onthullingen die in juni 2013 begonnen in verschillende delen van de wereld initiatieven ontplooid die onder de noemer technologische soevereiniteit en/of datalokalisering vallen (zie bijvoorbeeld Chander en Le 2014; Maurer et al. 2014; Polatin-Reuben en Wright 2014 voor overzichten). Een bekend voorbeeld is het voornemen van Brazilië om een nieuwe zeekabel aan te leggen die het land

direct met Europa verbindt zodat het Braziliaanse dataverkeer niet via de Amerikaanse kabels – en de 'prying eyes' van de NSA – hoeft te lopen. Maar ook Europa heeft zich niet onbetuigd gelaten, hoewel sommige initiatieven en voorstellen met de tijd ook weer geruisloos van de agenda afgevoerd lijken te zijn (Maurer et al. 2014). Sommige van deze initiatieven zijn gebaseerd op ideeën over verplichte lokale opslag van data en verplichte lokale routing van data. Met name dat laatste is een principe dat op gespannen voet kan staan met de basale werking van het Internet Protocol, dat ervan uitgaat dat data de route neemt die het netwerk – op basis van lokale belasting – op dat moment het meest effectief lijkt. Bovendien geldt dat in een tijdperk van cloud computing dat routing en opslag onlosmakelijk met elkaar verbonden zijn. De clou van de cloud is immers dat de plaats van de gevraagde opslag of rekencapaciteit bepaald wordt door waar het cloudnetwerk op dat moment het minste belast is: clouddata zijn dus altijd in beweging en lokalisering staat daar haaks op. Duitsland is het meest uitgesproken geweest in zijn ambities om zijn technologische soevereiniteit te vergroten met voorstellen voor nationale cloudservices en het uitsluiten van buitenlandse bedrijven die niet kunnen garanderen dat data niet met andere overheden gedeeld worden. Het 'terugwinnen van technologische soevereiniteit' is zelfs letterlijk als opdracht in het regeerakkoord van de huidige coalitie terug te vinden (CDU, CSU en SPD 2013: 103). In februari 2014 bespraken de Franse president Hollande en de Duitse bondskanselier Merkel een 'Europees communicatienetwerk' waarin data zoveel mogelijk binnen een netwerk van Europese servers wordt gehouden (Maurer et al. 2014: 5). In de pers werd wel gesproken van een EU-cloud of een Schengencloud.[18] Maar ook verder in Europa en wereldwijd zijn er vele voorbeelden te vinden van opkomend datanationalisme.

In de VS is er door politiek en bedrijfsleven weinig enthousiast gereageerd op dergelijke Europese voorstellen. Het verzet heeft enerzijds politieke en economische motieven (slecht voor de mondiale zaken van Silicon Valley en concurrentievervalsing door uitsluiting van Amerikaanse bedrijven) en bevat anderzijds overwegingen die ingegeven zijn door zorgen over het functioneren van het internet als een mondiaal netwerk. Uiteraard worden de beide soorten argumentatie soms naar het eigen optimum met elkaar gemengd. Het technische argument komt erop neer dat het daadwerkelijk doorvoeren van datasoevereiniteit mogelijk uitdraait op 'breaking the web' (Chander en Le 2014) of 'the end of the internet' (Goldstein 2014). Dat is veel te sterk aangezet: lokale routing is wel degelijk mogelijk zonder de internetinfrastructuur geweld aan te doen. Er ontstaan pas problemen als gebruikers gedwongen worden lokale services te gebruiken door routering naar andere diensten te blokkeren. Dan tast lokalisering de werking aan van het gedistribueerde netwerk dat het internet is, hetgeen zich niet verhoudt tot de 'blinde' werking van het Internet Protocol. Als iedereen zijn data en dataverkeer zoveel mogelijk achter zijn eigen digitale muren wil laten circuleren, verandert het karakter van het internet. Google's Richard Salgado (Directeur Law Enforcement and

Information Security) spiegelde de Amerikaanse Senaat in 2013 in deze context het volgende scenario voor: "the creation of a 'splinternet' broken up into smaller national and regional pieces with barriers around each of the splintered internets to replace the global internet we know today".[19] De vraag is of het middel erger is dan de kwaal en – minstens zo belangrijk – of het middel wel een oplossing voor de kwaal is.

Verschillende auteurs (Maurer et al. 2014; Chander en Le 2014) wijzen er namelijk op dat lokale dataopslag en routing de data nog niet per definitie vrijwaren van spionage, niet in de laatste plaats vanwege het feit dat inlichtingendiensten veel informatie met elkaar delen. In het voornaamste samenwerkingsverband van de 'five eyes' zit bijvoorbeeld al een EU-lidstaat, het VK, waardoor vele data al snel voor de VS toegankelijk zijn. Het willen afsluiten van de voordeur door middel van datalokalisatie heeft weinig zin als er niet tegelijkertijd kritisch gekeken wordt naar de internationale uitwisseling van bulkdata tussen de verschillende diensten. De AIV (2014: 61) adviseerde onlangs al dat bij de aanstaande herziening van de Nederlandse Wet op de inlichtingen- en veiligheidsdiensten (WIV 2002) bijzondere aandacht uit moet gaan naar het verbeteren van de waarborgen voor burgers als het gaat om internationale uitwisseling van data tussen diensten. Het louter lokaal opslaan van vitale data kan uiteraard een belangrijke veiligheidsmaatregel zijn. Voor sommige vitale data is het een boerenwijsheid dat ze buiten de cloud gehouden moeten worden. Maar volgens auteurs als Maurer et al. (2014) en Chander en Le (2014) ligt een andere oplossing als antwoord op massasurveillance meer voor de hand. *Encryptie* van het dataverkeer – zowel van data in transit als van opgeslagen data – zou de grootschalige onderschepping van data door inlichtingen- en veiligheidsdiensten zowel veel moeilijker als veel duurder maken. Dat zou de diensten dwingen om keuzes te maken en zich te beperken, iets wat nu nauwelijks nodig lijkt gegeven de grote technologische mogelijkheden. Een toename van de kosten zou, in termen van de eerder in dit hoofdstuk geciteerde Faris en Gasser (2013: 21), financiële overwegingen weer als buffer tussen staatssurveillance en privacy laten fungeren. Het zou inlichtingendiensten dwingen om hun activiteiten veel scherper en doelgerichter op te zetten in plaats van in te zetten op massale dataverzameling en andere vormen van 'sleepnet surveillance' (Lyon 2014).

Een laatste politiek argument om zeer voorzichtig om te gaan met ideeën over technologische en datasoevereiniteit is van diplomatieke aard. In de komende jaren zal de internetpopulatie hand over hand groeien, waarbij de meeste gebruikers in niet-westerse landen online zullen komen. In veel van die landen spelen soevereiniteit, argwaan tegen het internet en de internationalisering van de populatie die dat met zich meebrengt een veel grotere rol dan in Nederland en Europa. Als Europa al muren op het internet optrekt die zich niet verhouden met de werking

van de kern van het internet slaat het zichzelf de argumenten uit handen om andere landen – nieuw in het veld van internetgovernance – te overtuigen van het gedeelde belang van een goed werkende publieke kern van het internet.

4.6 CONCLUSIE

In dit hoofdstuk stonden wetten en maatregelen centraal waarbij staten gebruikmaken van de infrastructuur van het internet om het gedrag van personen, groepen, bedrijven en andere staten te beïnvloeden en reguleren. Het centrale punt bij de verschillende ontwikkelingen die hiervoor zijn uitgewerkt, is dat staten daarbij de eigen nationale, of andere particuliere belangen zwaarder laten wegen dan het collectieve belang van een betrouwbare werking van het internet. Voor alle beschreven ontwikkelingen geldt dat de schade die aan de publieke kern van het internet wordt toegebracht nu nog vaak incidenteel is. Maar een toenemend gebruik en wijdere verspreiding van beleid dat ingrijpt op de centrale protocollen van het internet – zoals routing, DNS en IP – heeft uiteindelijk een zeer schadelijke uitwerking op de universaliteit, interoperabiliteit en toegankelijkheid van het internet. Als de geest eenmaal volledig uit de fles is, is het ondoenlijk om hem er weer terug in te krijgen.

Vanuit verschillende belangen – auteursrecht, nationale veiligheid – richten staten zich op de technische en logische kern van het internet. Soms raken ze daarbij aan centrale protocollen en soms worden vitale kwetsbaarheden in software en protocollen met een potentieel groot effect 'geheim gehouden' voor later gebruik. Deze praktijken leiden er (potentieel) toe dat het functioneren van het internet als geheel minder betrouwbaar wordt. In de eerste plaats in technische zin, maar in het verlengde daarvan ook in economische en sociaal-culturele zin: als de we de integriteit, de beschikbaarheid en de vertrouwelijkheid van het internet niet meer kunnen vertrouwen, heeft dat gevolgen voor de manier waarop we ermee willen en kunnen omgaan. En dat heeft gevolgen voor het sociaaleconomische bouwwerk dat we op die infrastructuur hebben geconstrueerd: van online bankieren tot communicatie. Sommige van deze praktijken leiden er ook simpelweg toe dat het internet onveiliger wordt. Kwetsbaarheden die worden 'bewaard' om cyberaanvallen mogelijk te maken en het doelbewust inbouwen van zwakheden in standaarden en software die wij allemaal gebruiken om een betere toegang tot dataverkeer te garanderen voor inlichtingendiensten, verslechteren de algehele veiligheid van het gehele internet en van al zijn gebruikers. Zoals Bruce Schneier al schreef: er zijn geen achterdeurtjes waar alleen de 'good guys' gebruik van kunnen maken.

De voornaamste conclusie die hieruit te trekken valt, is dat overheden uiterst terughoudend moeten zijn met beleid, wetgeving en operationele activiteiten die ingrijpen in de kernprotocollen van het internet. Tegelijkertijd moet ook voorkomen worden dat private partijen zich vrijheden veroorloven met deze publieke

kern van het internet. Beteugeling en terughoudendheid zijn op dit punt de voornaamste opgaven: ideaal gezien zou non-interventie de internationale norm moeten zijn voor de kernprotocollen en dragende technologie van het publieke internet. Deze gedachte wordt in hoofdstuk 5 verder uitgewerkt in een diplomatieke opgave. Die terughoudendheid is echter uitermate ingewikkeld omdat de baten van veel van dit beleid direct zijn te relateren aan nationale belangen, terwijl de kosten in eerste instantie collectief zijn. Echter, alles wat de integriteit en de veiligheid van de mondiale architectuur van het internet aantast, komt uiteindelijk als een boemerang terug bij *alle* nationale staten. Het heeft dus belangrijke kenmerken van een collectief-actieprobleem. De mogelijkheden voor staten om terughoudendheid aan de dag te leggen wordt bovendien moeilijker naarmate het beleid in kwestie meer in het kader van de nationale veiligheid staat. Een aantal wetsvoorstellen om auteursrecht op het internet te beschermen ging ten onder omdat de economische belangen – voor het eerst – publiekelijk werden afgezet tegen het belang van het functioneren van het internet als geheel en de vrijheid van meningsuiting. Als het gaat om nationale veiligheid is een dergelijke afweging traditioneel veel lastiger omdat dit beleid omgeven is met geheimhouding, er nauwelijks internationaal recht van toepassing is en omdat beleid ten behoeve van nationale veiligheid al snel voorrang krijgt op andere overwegingen. Ook op het internet is het hemd bovendien vaak nader dan de rok. Toch geldt hier onverkort een digitale variant van het securitydilemma: de cumulatie van nationaal gemotiveerde interventies om de eigen veiligheid te beschermen leidt uiteindelijk tot een veel grotere onveiligheid van het internet en de daarop aangesloten staten en gebruikers.

Als het gaat om deze grensconflicten tussen nationale belangen en het publieke internet geldt dat terughoudendheid (beteugeling) niet of nauwelijks van de grond zal komen zonder voldoende tegendruk. In termen van Deiberts model van gedistribueerde veiligheid ontbreekt het aan menging en scheiding – meerdere betrokken actoren met een rol, macht en verantwoordelijkheid. Zeker als het gaat om nationale veiligheid is dat een probleem. Het multistakeholdermodel wordt vaak naar voren geschoven als een manier om meerdere relevante actoren een rol te geven in internetgovernance. Met een rol alleen is echter nog geen tegendruk gecreëerd omdat macht en verantwoordelijkheid vaak ontbreken. Dat is zelfs in toenemende mate het geval omdat staten een grotere verantwoordelijkheid voor zichzelf opeisen of eigen beleid doordrukken. SOPA, PIPA en ACTA waren waarschijnlijk wet geworden als er geen breed verzet tegen was aangetekend, waaraan sleutelfiguren uit de technische gemeenschap en grote internetbedrijven en sites deelnamen die politici direct op hun verantwoordelijkheid voor het beheer van het internet aanspraken. Als het gaat om nationale veiligheid en de nasleep van de Snowden-onthullingen is er weliswaar sprake van internationale verontwaardiging, maar nauwelijks van (georganiseerde) tegenmacht. Dat is deels goed te verklaren vanuit het ontbreken van internationale regelgeving en vanuit het feit dat

eigenlijk alle staten dezelfde bevoegdheden aan de eigen diensten toekennen. Het is echter zeer de vraag of het democratisch en juridisch toezicht op deze diensten in het tijdperk van high technology en big data nog wel toereikend is. In Nederland wordt nu opnieuw gekeken naar het kader van de Wet op de inlichtingen- en veiligheidsdiensten (WIV). In de VS sneuvelde in de Senaat onlangs een herziening van de wetgeving voor inlichtingendiensten – die het toezicht op de diensten moest versterken en de bevoegdheden van die diensten (iets) zou inperken – waardoor alles vooralsnog bij het oude blijft.[20]

Er komt wel tegendruk vanuit een aantal grote internetbedrijven die door de Snowden-onthullingen te kijk zijn gezet: zij waren bewust en/of onbewust de grootleveranciers van de datamassa voor inlichtingendiensten. Zij reageren met transparantierapporten – voor zover wettelijk toegestaan – om de gebruiker inzicht te geven in wat overheden opvragen. Ook schroeven ze de encryptie van het dataverkeer van hun gebruikers op. Op beide punten worden ze tegengewerkt door de veiligheidsdiensten. Toch is dit een eerste aanzet tot tegenmacht: encryptie verhoogt de kosten van massasurveillance en dwingt de diensten om hun surveillance specifiek te maken en te houden. Een ander voorbeeld is dat de VS en Microsoft momenteel tegenover elkaar staan in de rechtbank omdat de Amerikaanse overheid eist dat Microsoft data overdraagt die is opgeslagen op een server in Ierland. Microsoft weigert omdat de data onder Iers recht vallen, terwijl de VS redeneert dat de data van een Amerikaans bedrijf zijn en dus zonder meer opgevraagd kunnen worden.[21] Gek genoeg zijn het nu dus de grote bedrijven die de externe privacy van hun klanten verdedigen tegen overheden, terwijl zij de grenzen van privacy zo ver mogelijk oprekken als het om de interne datahuishouding van hun klanten gaat. Gezien de grote macht van deze informatiegiganten en hun vitale rol in de manier waarop het leven van hele bevolkingen gedigitaliseerd is, kunnen overheden deze actoren in diplomatieke zin niet meer negeren. Deze bedrijven zijn meer dan mogelijke investeerders die aangetrokken moeten worden of juist privacyschenders die aangepakt moeten worden: het zijn actoren die serieuze diplomatieke aandacht behoeven vanwege hun vitale rol in het digitale leven, met alle tegenstrijdigheden die eigen zijn aan de diplomatie.

In het verlengde hiervan zou er meer helderheid moeten komen over wat overheden verwachten van de vele internetintermediairs die het digitale leven faciliteren: in de eerste plaats de ISP's, maar ook zoekmachines, clouddiensten enz. Deze organisaties moeten een eigen koers volgen tussen soms tegenstrijdige wensen van overheden. Zij worden geacht zich ethisch en verantwoordelijk te gedragen ten opzichte van hun klanten maar worden ook geacht zich te conformeren aan de eisen van het bevoegd gezag. Internationaal betekent dat soms dat Google wordt geacht niet mee te werken met de censuur van de Chinese overheid en wel met de Amerikaanse verzoeken om data van hun gebruikers ter beschikking te stellen. Hoewel daar vanuit een perspectief van mensenrechten en de democratische

rechtsstaat uiteraard iets voor te zeggen valt, begint het zich te wreken dat er noch nationaal, noch internationaal, een doordachte strategie, beleid of zelfs maar een gestructureerde discussie is waarin verkend wordt wat intermediairs wel en niet moeten doen en wat overheden wel en niet mogen vragen. Intermediairs hebben nu drie opties ten opzichte van de – al dan niet geheime – verzoeken van overheden: volgzaamheid, verzet en preventief enthousiasme, waarbij ze op verzoeken vooruitlopen. De laatste is vanuit een rechtsstatelijk perspectief ongewenst, en de eerste twee zijn vanuit een perspectief van een machtenscheiding wellicht beide nodig. Alleen volgzaamheid of alleen verzet is problematisch. Een gestructureerde discussie – zeker op het internationale niveau – hierover moet echter nog beginnen.

NOTEN

1 Deze mooie titel is 'geleend' van Milton Mueller (2010).

2 Richtlijn 2000/31/EG betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ("Richtlijn inzake elektronische handel"), zie: http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32000L0031&qid=1424093839470.

3 De uitspraak in zaak C-70/10 Scarlet vs. SABAM houdt in dat de Europese richtlijnen 2000/31, 2001/29, 2004/48, 95/46 en 2002/58 een nationale rechter niet toestaan een internetprovider op te leggen een filtersysteem in te voeren om het verkeer van auteursrechtelijk beschermde elektronische bestanden op het netwerk te blokkeren. Een dergelijk filtersysteem vereist actieve observatie van alle elektronische communicatie op het netwerk van de betrokken internetprovider en daarmee is het evenwicht tussen enerzijds het intellectueleeigendomsrecht en anderzijds de vrijheid van ondernemerschap, het recht op bescherming van persoonsgegevens en de vrijheid om informatie te ontvangen of te verstrekken niet verzekerd.

4 Zie: https://www.eff.org/deeplinks/2011/12/internet-inventors-warn-against-sopa-and-pipa.

5 Christopher Rhoads and Farnaz Fassihi, 'Iran Vows to Unplug Internet', *Wall Street Journal*, 28 mei 2011, http://www.wsj.com/articles/SB10001424052748704889404576277391449002016.

6 Zie de Riga Joint Statement van Europese ministers van Binnenlandse Zaken van 29 januari 2015, https://eu2015.lv/images/Kalendars/IeM/2015_01_29_jointstatement_JHA.pdf.

7 Zie: http://www.google.com/transparencyreport.

8 Zie: https://transparency.twitter.com.

9 Zie: http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency.

10 PRISM is een digitaal spionageprogramma dat de NSA gebruikt om op grote schaal communicatieverkeer te verzamelen van negen Amerikaanse technologiebedrijven, namelijk Microsoft, Yahoo, Google, Facebook, Paltalk, Youtube, Skype, AOL en Apple. MUSCULAR is een programma van de NSA en GCHQ dat gegevens verzamelt van Yahoo en Google door onder meer de kabels die de servers van deze internetbedrijven verbinden heimelijk af te tappen. BULLRUN is een programma van de NSA en de GCHQ waarmee op verschillende manieren versleutelde internetcommunicatie wordt ontcijferd door bijvoorbeeld de keuzes van encryptiestandaarden te beïnvloeden zodat deze zwaktes en achterdeuren hebben.

11 'Tim Berners-Lee: encryption cracking by spy agencies 'appalling and foolish'', *The Guardian*, 7 november 2013.

12 Zie: http://masssurveillance.info/openletter.pdf, geraadpleegd op 10 december 2014.

13 Rob Lever, 'Crypto Wars 2.0 Have Begun After Privacy Moves By Apple And Google', *Business Insider*, 1 oktober 2014. Zie: http://www.businessinsider.com/afp-new-privacy-battle-looms-after-moves-by-apple-google-2014-9#ixzz3LhSogz1B, geraadpleegd

12 december 2014. Zie ook: http://www.theguardian.com/technology/2014/oct/09/crypto-wars-redux-why-the-fbis-desire-to-unlock-your-private-life-must-be-resisted, geraadpleegd 12 december 2014.

14 Zie: https://www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html.

15 Zie bijvoorbeeld de websites van VUPEN (http://www.vupen.com/english), Endgame (https://www.endgame.com), Revuln (http://revuln.com/index.htm), en Exodus Intelligence (https://www.exodusintel.com).

16 Zie: http://www.vupen.com/english/services/solutions-gov.php.

17 RSIS-Leiden, CTC Roundtable on civil-military relations in cyberspace, Singapore, 18-19 November 2014.

18 Zie: http://www.welt.de/politik/deutschland/article126343060/So-wuerde-Europas-Schengen-Internet-funktionieren.html.

19 Zie: http://www.judiciary.senate.gov/imo/media/doc/11-13-13SalgadoTestimony.pdf.

20 Zie: http://www.theguardian.com/us-news/2014/nov/18/usa-freedom-act-republicans-block-bill.

21 Zie bijvoorbeeld: http://www.theguardian.com/technology/2014/dec/14/privacy-is-not-dead-microsoft-lawyer-brad-smith-us-government.

5 NAAR EEN NEDERLANDSE AGENDA VOOR INTERNETDIPLOMATIE

5.1 INLEIDING: INTERNETGOVERNANCE OP EEN KRUISPUNT

Het internet is niet meer weg te denken uit ons dagelijks leven. Het is vervlochten met ons sociale leven, onze consumptie, ons werk en onze relatie met de overheid, en in toenemende mate met objecten die we dagelijks gebruiken, van de slimme meter tot de auto waarin we rijden en de ophaalbrug die we onderweg tegenkomen. Het beheer van het internet was lange tijd het exclusieve domein van wat in internetkringen wel de 'technische gemeenschap' wordt genoemd. Die gemeenschap legde het fundament voor de huidige sociaaleconomische vervlechting van het fysieke leven en het digitale leven. Dat fundament, met het Internet Protocol als meest prominent onderdeel, is nog steeds de vitale onderbouw van ons digitale bestaan. Maar het beheer daarvan is omstreden geraakt. Vanwege de vele belangen, kansen en kwetsbaarheden die aan het internet zijn verbonden, zijn overheden zich met het reilen en zeilen van het internet gaan bemoeien. Daarbij is het beleidsmatige zwaartepunt aan het verschuiven van een primair economische blik op het internet (de interneteconomie, telecommunicatie en netwerken) naar een blik die meer door (nationale) veiligheid wordt bepaald: het internet van de cybercrime, kwetsbare vitale infrastructuren, digitale spionage en cyberaanvallen. Steeds meer landen willen bovendien om uiteenlopende redenen het gedrag van burgers op het internet reguleren: dat loopt van het beschermen van auteursrecht, via de aanpak van cybercrime tot censuur en controle op de eigen bevolking via het internet.

Steeds vaker worden de infrastructuur en de centrale protocollen van het internet zelf daarbij gezien als een legitiem instrument om beleidsdoelen te verwezenlijken. Waar voorheen internetgovernance voornamelijk de governance *van* het internet was, is er nu steeds frequenter sprake van governance die *gebruikmaakt* van de architectuur van het internet (DeNardis 2012). Staten gebruiken bijvoorbeeld centrale protocollen als DNS of IP om websites te blokkeren of onvindbaar te maken. Dergelijke ingrepen hebben potentieel grote gevolgen voor de kern van infrastructuren en protocollen van het internet die – zo is in dit rapport betoogd – als een mondiaal publiek goed beschouwd moet worden. Deze publieke kern van het internet zou gevrijwaard moeten blijven van interventies van staten die alleen het eigen nationale belang dienen, schade toebrengen aan dat mondiale publieke goed en het vertrouwen in het internet eroderen. Internetgovernance staat in dit opzicht op een kruispunt: het internet is simpelweg zo belangrijk geworden dat staten het niet langer meer willen en kunnen bezien met de *benign neglect* die heel lang voor de meeste landen de norm is geweest. Tegelijkertijd geldt dat staten nu eenmaal andere nationale belangen hebben dan (alleen) het goede beheer van het internet als een collectieve infrastructuur. Het komt er dus op aan om binnen het

veld van de internetgovernance af te bakenen wat als een mondiaal publiek goed gezien moet worden – en gevrijwaard moet blijven van alle oneigenlijke inmengingen – en wat als een legitiem werkterrein van nationale staten, waarbij zij hun plek en rol kunnen opeisen zonder schade toe te brengen aan de infrastructuur van het internet zelf. Het vereist een specifieke politieke benadering en een bijzondere diplomatieke inspanning om dit op de internationale agenda te krijgen en het gedrag van staten te beïnvloeden. Het cliché wil dat het internet bij uitstek grensoverschrijdend is en daarom alleen internationaal valt te reguleren. Hoewel daar een kern van waarheid in zit, hebben recente jaren ook juist laten zien dat (ondoordacht) nationaal beleid een grote invloed kan hebben op het functioneren van dat internationale internet. Daarmee is nationaal beleid de facto óók een vorm van internetgovernance geworden.

De internationale opdracht zal zijn om (de kernprotocollen en infrastructuur van) het internet te beschermen tegen bepaalde vormen van nationaal beleid en de externe effecten daarvan. De invalshoek die in dit rapport gekozen is, stelt dus internetveiligheid – het beschermen van het (goed functioneren van het) internet als een infrastructuur – centraal in de redenering en gebruikt deze als startpunt voor het formuleren van een agenda voor het Nederlandse buitenlands internetbeleid. Het zwaartepunt in de aanbevelingen valt daardoor anders uit dan wanneer het rapport was opgesteld vanuit de invalshoek van bijvoorbeeld de nationale veiligheid, de bescherming van de mensenrechten of het versterken van de digitale economie. Uiteraard wordt de agenda die hierna wordt uiteengezet wel verbonden met deze beleidsterreinen die ook allemaal onderdeel zijn van, of raken aan, het vraagstuk van internetgovernance. Dit rapport is echter gericht op een uitwerking van het belang van het waarborgen van de publieke kern van het internet en de diplomatieke inspanningen die daarvoor nodig zijn.

5.2 NAAR EEN BUITENLANDS INTERNETBELEID

5.2.1 NUT EN NOODZAAK VAN INTERNETDIPLOMATIE

Als het internet niet meer functioneert staan er vele processen stil: van triviaal – onze Facebookstatus – tot vitaal – het functioneren van het betalingsverkeer. Als de kernprotocollen van het internet worden gecorrumpeerd, wordt het internet onbetrouwbaar. Wie durft er dan nog te internetbankieren? Als we er niet van uit kunnen gaan dat informatie verzonden wordt en aankomt, heeft dat gevolgen voor welke economische en sociale processen we wel en niet via het internet willen laten verlopen. Kunnen we onze private en werk gerelateerde communicatie dan nog wel aan het internet overlaten? Als we weten dat er doelbewust gaten worden geïnstalleerd in internetstandaarden, -protocollen, en hard- en software om de toegang te garanderen voor buitenlandse inlichtingen- en veiligheidsdiensten, dan erodeert dat op termijn ons vertrouwen in het internet. Als steeds meer landen zich terugtrekken achter digitale grenzen heeft dat consequenties voor het functio-

neren van het internet als internationale infrastructuur. En in de zwartste scenario's kan het uitbuiten van kwetsbaarheden in de kernprotocollen en infrastructuren leiden tot een ontwrichting van samenleving en economie. Als alles met het internet verbonden is, is de uitval daarvan vernietigend.

Het overkoepelende belang van internetveiligheid veronderstelt een diplomatieke benadering waarin het internet tot een speerpunt verheven wordt. Het internet staat reeds prominent op de agenda van een handvol ministeries, die verschillende nationale en internationale dossiers behartigen. Ook is de Nederlandse overheid in vele internationale fora vertegenwoordigd. Toch is er vooralsnog geen sprake van een samenhangende diplomatieke inspanning, met als vertrekpunt het functioneren van het internet als mondiaal publiek goed. Wel zijn onder de vlag van cybersecurity in de *Cyber Security Strategie 2* (Ministerie van VenJ 2013) prioriteiten gesteld en de activiteiten van verschillende departementen op elkaar betrokken. Nederland heeft bovendien een bestuurlijke en ambtelijke cultuur waarbij de verschillende partijen op het gebied van cyber- en internetbeleid elkaar – en relevante private partijen – weten te vinden. Dat is een uitstekende uitgangspositie om de bescherming van de publieke kern van het internet uit te werken als speerpunt en dit vervolgens via de EU en op eigen gezag internationaal uit te dragen in de verscheidene fora die Nederland ter beschikking staan.

De integriteit van die publieke kern van het internet is een *conditio sine qua non* voor het functioneren van het internet zelf. Internetveiligheid is dus een zeer fundamenteel beginsel. Het nastreven van een digitale economie heeft immers alleen zin als het internet zelf naar behoren functioneert. Ook de nationale en economische veiligheid zijn mede gebouwd op een robuuste internetinfrastructuur. Het waarborgen van de publieke kern van het internet vergt een veel grotere coherentie en politieke prioritering dan de huidige inspanningen, in het bijzonder waar het de internationale agenda betreft. Het internet dient nadrukkelijk – en vooral eigenstandig – een speerpunt te zijn van het buitenlands beleid van Nederland. Naast traditionele speerpunten als handel, mensenrechten en vrede en veiligheid zou de regering een buitenlands internetbeleid moeten prioriteren en uitwerken. In het internationale domein zou Nederland met een diplomatieke benadering die het beschermen van de publieke kern van het internet voorop zet, een voorloper kunnen zijn. De publieke kern van de infrastructuur vraagt behalve om politiek optreden van staten tegelijkertijd ook om een grote terughoudendheid van diezelfde staten. De hier voorgestelde diplomatieke inspanning kan alleen slagen wanneer Nederland zijn eigen huis op orde heeft.

5.2.2 NEDERLAND IN DE VOORHOEDE

Nederland is een klein land, maar heeft zich in het verleden al vaker bewezen als een land met een internationale oriëntatie en een eigen diplomatiek geluid. Waar grote staten zich vaak verlaten op de 'hard power' van economische en militaire

macht, moeten kleine staten het meestal hebben van wat Nye (2011: 20-21) 'soft power' noemt: de mogelijkheid om andere staten te beïnvloeden door middel van het formuleren en framen van de agenda, het overtuigen van de ander en het genereren van positieve aandacht voor geprefereerde uitkomsten (het goede voorbeeld). En waar grote en machtige staten nog wel eens baat kunnen hebben bij 'strategische ambivalentie', waarbij het feit dat normen niet helemaal uitgekristalliseerd zijn juist handelingsruimte biedt, hebben kleinere staten er vaak juist belang bij om de discussie in de richting van normering te kanaliseren.

Het beschermen van de publieke kern van het internet is bovendien voor Nederland een verlengd nationaal belang. Een dergelijk belang ligt op een lijn met strategische mondiale vraagstukken die als internationaal publiek goed gedefinieerd kunnen worden, zoals het mitigeren van klimaatverandering of de stabiliteit van het financiële systeem (WRR 2010b). Voor Nederland is het betrouwbaar functioneren van het internet van vitaal belang voor zijn economie, economische groei en het functioneren van de (digitale) samenleving. Nederland scoort zeer hoog op internationale ranglijsten over internettoegang en breedbandverbindingen en bevindt zich in de top van OECD-landen met het hoogste percentage van de bevolking dat online aankopen doet (OECD 2014; CBS 2014). Nederland heeft een levendige internetindustrie en de AMS-IX is een van de grootste Internet Exchange Points ter wereld (Deloitte 2014). De omvang van de totale interneteconomie is echter lastig te meten, vanwege de zich snel ontwikkelende nieuwe technologieën en de sterke verwevenheid van economische online- en offlineactiviteiten (OECD 2014). Een recente schatting (Deloitte 2014) komt uit op 5,3 procent van het BBP. The Boston Consultancy Group (2014; 2011) komt met ruim 4 procent op een wat lager percentage uit, maar plaatst Nederland in de toptien van landen wereldwijd waar de interneteconomie verhoudingsgewijs het grootst is.[1]

Nederland heeft niet alleen veel mee in termen van een levendige internetindustrie en -cultuur en politiek leiderschap op een aantal dossiers als netneutraliteit, maar kent ook een traditie van idealisme en pragmatisme. Deze traditie zorgde in eerdere tijden voor een relatief vrije informatiecultuur en bloeiende economie in Nederland.[2] Dat kleine staten aan de wieg van internationale normen of diplomatieke doorbraken staan, is bovendien geen uitzondering. Voor Nederland is het uitwerken en uitdragen van een nieuwe agenda voor internetdiplomatie, met als uitgangspunt het waarborgen van de kern van het internet als een mondiaal publiek goed, een passende nieuwe ambitie. Dat het waarborgen van de publieke kern van het internet ook voor andere staten een verlengd nationaal belang is, kan als frame voor de internationale agenda dienen.

5.3 NAAR EEN INHOUDELIJKE AGENDA VOOR INTERNETDIPLOMATIE

De hier voorgestelde agenda voor internetdiplomatie kan vorm krijgen aan de hand van de ideeën van Ronald Deibert over gedistribueerde veiligheid (zie hoofdstuk 2). Binnen deze conceptie van veiligheid wordt het organiseren van macht en tegenmacht in het internationale domein van de internetgovernance benadrukt, met als doel vrijheid te waarborgen. Deibert onderscheidt drie principes van machtsbinding die zijn ontleend aan de context en traditie van de nationale liberale democratische rechtsstaat en die naar de internationale context vertaald zouden moeten worden. Deze principes zijn *menging*, *scheiding* en *beteugeling*. Bij menging gaat het erom verschillende partijen een rol en verantwoordelijkheid te geven. Scheiding is een ontwerpprincipe dat ervan uitgaat dat geen van de betrokken partijen het systeem kan controleren zonder de medewerking of goedkeuring van andere partijen. Het principe van beteugeling gaat uit van het inperken van macht door middel van het organiseren van checks and balances, zoals toezicht. Beteugeling kan zowel intrinsiek vormgegeven worden – als partijen zich terughoudend opstellen – als extrinsiek afgedwongen of gecontroleerd worden door externe partijen of door bestuurlijke en juridische arrangementen.

Deze drie principes zijn niet direct verplaatsbaar naar de internationale arena. Omdat instituties – met regels, procedures en verantwoordelijkheden – internationaal een beperktere rol spelen dan op nationaal niveau, vereisen de principes van menging, scheiding en beteugeling de betrokkenheid van partijen die daadwerkelijk bevoegdheden en/of macht hebben. In het private cyberdomein zijn dat vaak ook private partijen. Dit wil niet zeggen dat er geen formele en informele mechanismen van kracht zijn die de soevereiniteit van staten inperken. In de afgelopen eeuwen, met een grote versnelling in de periode na de Tweede Wereldoorlog, is een netwerk van internationale en regionale organisaties, zoals de VN, de EU en de Raad van Europa, ontstaan die het gedrag van staten inkaderen. Over dezelfde periode van eeuwen is, deels binnen en deels buiten deze organisaties, internationaal recht ontstaan dat staten aan normen en regels bindt en hen verplichtingen oplegt. Maar ook informele normen, onderlinge verwachtingen, waarschuwingen en dreigementen spelen een rol in de internationale betrekkingen. Internetgovernance moet uiteindelijk binnen deze internationale context vorm krijgen. Soms kan dat in aansluiting op lopende internationale initiatieven en binnen bestaande internationaal juridische en organisatorische kaders en soms moet daar nieuwe diplomatieke grond voor gebroken worden.

Deze paragraaf werkt twee inhoudelijke hoofdpunten voor een agenda voor internetdiplomatie uit, waarin de principes van Deibert op verschillende manieren impliciet doorklinken. Het eerste agendapunt is de vrijwaring van de publieke kern van het internet van oneigenlijke inmenging door staten op basis van natio-

nale belangen. Het is wenselijk een norm van non-interventie vast te leggen ten aanzien van de centrale infrastructuur van het internet. Het tweede agendapunt is gericht op het de-securitiseren van de internationale internetpolitiek, onder meer door een duidelijker onderscheid te maken tussen verschillende vormen van veiligheid en de daarbij betrokken partijen.

5.3.1 DE PUBLIEKE KERN VAN HET INTERNET VEILIGSTELLEN

In deze studie is uiteengezet dat er een kern van centrale protocollen en technologie aan te wijzen is die als een *mondiaal publiek goed* kan worden aangemerkt. Als centrale protocollen zoals TCP/IP, DNS en routingprotocollen niet naar behoren functioneren, staat het functioneren van het internet zelf onder druk. Iedereen verliest als deze protocollen gecorrumpeerd worden. Het internet kan 'kapot' gaan als we er niet meer van uit kunnen gaan dat de informatie die we verzenden aankomt, dat we bij de sites uitkomen waar we naar op zoek zijn en dat deze toegankelijk zijn. Het internet als publiek goed functioneert alleen als het de kernwaarden universaliteit, interoperabiliteit en toegankelijkheid garandeert en als het de kerndoelen van informatieveiligheid, te weten vertrouwelijkheid, integriteit en beschikbaarheid ondersteunt. In Duitsland heeft het Federale Constitutionele Hof in 2008 een nieuw grondrecht geformuleerd op de 'vertrouwelijkheid en integriteit' van IT-systemen, waar een aantal van deze waarden duidelijk in doorklinkt.[3] Het is essentieel dat we – de gebruikers – op de werking van de meest fundamentele protocollen van het internet kunnen vertrouwen omdat daar ook het vertrouwen van afhangt dat we hebben in het sociaaleconomische bouwwerk dat daarbovenop gebouwd is.

Het lijkt evident dat er wereldwijd overeenstemming zou moeten zijn over het belang van het goed functioneren van deze protocollen omdat ze de betrouwbaarheid van het mondiale internet garanderen. De huidige internationale ontwikkelingen op het gebied van beleid en regelgeving voor de bescherming van auteursrechten, defensie en nationale veiligheid, spionage en inlichtingen en verschillende vormen van censuur laten echter een heel ander beeld zien. DNS, routingprotocollen, standaarden en het inbouwen, geheim houden en benutten van kwetsbaarheden in software, hardware en protocollen worden door sommige staten als een ideaal aangrijpingspunt gezien voor nationaal beleid om het gedrag van mensen, groepen en bedrijven te monitoren, te beïnvloeden en te blokkeren. De effecten van dergelijke ingrepen in de kern van het publieke internet worden echter collectief gevoeld en tasten de kernwaarden en het functioneren van het internet aan.

In het domein van het auteursrecht kon een bonte coalitie van internetingenieurs, internetbedrijven en websites, ngo's en gebruikers een tweetal Amerikaanse wetsvoorstellen (SOPA en PIPA) en een verdrag (ACTA) van tafel krijgen die vitale internetprotocollen zouden gebruiken om content te reguleren en blokkeren. Politici kregen als gevolg van het protest door dat men met dergelijke ingrepen met het

internet zelf aan het rommelen was. De gedachte en de techniek achter dit soort wetgeving is met het sneuvelen van deze wetsvoorstellen echter nog niet van de baan.

In het domein van de nationale veiligheid veroorloven staten zich nog veel grotere vrijheden als het gaat om de publieke kern van het internet. Militaire cybereenheden, inlichtingen- en veiligheidsdiensten en soms ook politie en justitie stellen het belang van nationale veiligheid in toenemende mate boven het collectieve belang van een goed functionerend internet. Omdat het gaat om nationale veiligheid – of het in ieder geval als zodanig wordt 'geframed' – is de neiging in veel nationale parlementen groot om zulk beleid te ondersteunen. Als het gaat om inlichtingendiensten geldt bovendien dat deze uitsluitend op nationaal niveau zijn gereguleerd omdat nagenoeg elke internationale wetgeving ontbreekt. Bij elkaar opgeteld leiden deze ontwikkelingen echter wel tot een digitale variant van het securitydilemma van Jervis (1978) waarin het gebruik van cyberspace als een instrument voor nationale veiligheid, zowel in de zin van oorlogsvoering als in de zin van massale surveillance door inlichtingendiensten, schadelijke gevolgen heeft voor het algemene niveau van cybersecurity op een mondiale schaal (Dunn Cavelty 2014). Het risico is levensgroot dat het cumulatieve effect van nationale maatregelen – waarbij staten in toenemende mate tegen elkaar opbieden – resulteert in grote kwetsbaarheden van de kern van het internet als een publieke infrastructuur. In aanvulling hierop ontstaat op nationaal niveau de paradox dat sommige delen van de overheid dagelijks proberen een betrouwbaar en veilig internet te waarborgen terwijl andere delen van de overheid op dit gebied de risico's juist vergroten.

Tot op zekere hoogte staan we nog aan het begin van deze ontwikkeling. Een aantal machtige staten heeft een aanzienlijke cybercapaciteit opgebouwd en gaat het verst voorop in deze ontwikkeling, die vanuit het perspectief van het internet als publiek goed en mondiale cybersecurity gezien uiterst dubieus is. Maar veel landen zitten nog volop in het proces van digitalisering van staat, economie en samenleving en zijn hun cybercapaciteiten nog aan het opbouwen. De komende jaren, als de volgende miljard(en) gebruikers het internet opgaan, zullen ook deze opkomende staten nationaal beleid van de offlinewereld naar de onlinewereld willen vertalen en komen ze voor de vraag te staan of ze de publieke kern van het internet daarbij wel of niet instrumenteel gaan gebruiken. Een groot deel van die landen heeft autoritaire regimes met een geschiedenis van controle op, en soms onderdrukking van, de eigen bevolking, en zet daartoe moderne technologische middelen in. Het is zeker geen gegeven dat deze landen de publieke kern van het internet zullen ontzien wanneer de digitalisering van hun samenleving doorzet. Bovendien zal het niveau van de technische cybercapaciteiten van vele landen over een aantal jaren veel hoger liggen dan nu het geval is. Een veel grotere groep landen heeft dan de capaciteiten die nu slechts in handen van enkele grootmachten liggen. Wat nu *cutting edge* is, is over vijf jaar gemeengoed. Als intussen tevens de norm postvat

dat nationale staten vrijelijk kunnen bepalen of ze wel of niet willen ingrijpen in de centrale protocollen van het internet om de eigen belangen veilig te stellen, heeft dat waarschijnlijk een uiterst schadelijk effect op het internet als een publiek goed. Het is daarom zaak om haast te maken met de borging van de publieke kern van het internet.

Aanbeveling: bevorder het vastleggen en internationaal verspreiden van de norm dat de publieke kern van het internet – de centrale protocollen en infrastructuur die een mondiaal publiek goed zijn – gevrijwaard moet zijn van bemoeienis van overheden.

Tegen deze achtergrond is een centrale aanbeveling van dit rapport dat er gewerkt wordt aan het vastleggen van een internationale norm waarin de centrale protocollen van het internet aangemerkt worden als een neutrale zone, waarin overheidsbemoeienis omwille van nationale belangen niet geoorloofd is. In termen van gedistribueerde veiligheid is op dit vlak de voornaamste opgave het organiseren van inperking en terughoudendheid op het internationale vlak. Terughoudendheid geldt daarbij als de intrinsieke opdracht aan staten – restricties opleggen aan jezelf – en inperking geldt als opdracht aan het collectief: hoe kan de norm worden vastgelegd en worden gecontroleerd? Het uitwerken van een dergelijke norm zal eerst op de internationale politieke agenda moeten worden gezet, wat vereist dat het collectieve belang van deze neutrale zone voor alle overheden duidelijk gemaakt wordt. Dat zal gezien de grote verschillen tussen landen in termen van internettoegang, algehele digitalisering en technologische kennis in diplomatieke en politieke kringen om een grote inspanning vragen. Nederland zou bij deze diplomatieke inspanning voorop kunnen gaan. Uiteraard is de opdracht van terughoudendheid veel breder dan alleen een dergelijke norm, maar het vastleggen van een dergelijke norm kan helpen als een belangrijk referentiepunt.

Operationele strategie

Een belangrijke vraag is of een dergelijke norm meteen in de vorm van een verdrag moet worden gegoten, een gedachte die wel vaker wordt geuit (zie bijvoorbeeld Hughes 2010). Daarmee kan het onderwerp echter onderdeel worden van een multilateraal onderhandelingsspel waar de kleinste gemene deler vaak de uitkomst is. Het heeft voordelen om het streven in kleinere stukken te hakken in plaats van in te zetten op een verdrag voor het internet of een verdrag dat internetconflicten en digitale oorlogsvoering reguleert. In het cyberdomein wordt al over normen gesproken in vele conferenties, maar ook in een serie van zogenoemde GGE's (Groups of Government Experts) die onder auspiciën van de VN, maar los van een verdrag, proberen vooruitgang te boeken en normen, principes en vertrouwenwekkende maatregelen (CBM's) vast te leggen op het terrein van het internet en internationale veiligheid (Kane 2014; Hurwitz 2014). Het verspreiden van een internationale norm waarin de centrale protocollen van het internet worden aan-

gemerkt als een neutrale zone zou een breder en aanvullend bereik hebben op de route van de GGE, die zich richt op nationale veiligheid en op het voorkomen van escalatie van (cyber)conflicten. Het voordeel van de formulering van deze norm in termen van een mondiaal publiek goed van het internet is bovendien dat het geen rechtstreekse poging is om inlichtingen- en veiligheidsdiensten internationaal te reguleren. Dat moet om redenen van soevereiniteit immers kansloos worden geacht. Op regionaal Europees niveau hebben bijvoorbeeld uitspraken van de hoven in Luxemburg en Straatsburg – zoals de uitspraak over dataretentie – in principe wel een (direct) effect op de inkadering van de diensten. De norm van non-interventie heeft een indirect effect omdat die grenzen stelt aan wat in het kader van nationale veiligheid wel en niet is toegestaan op het internet. De naleving hiervan valt dan onder nationaal democratisch en juridisch toezicht. Hoewel het verspreiden van deze norm op zichzelf geen garantie biedt voor naleving, creëert het wel een benchmark waaraan het gedrag van staten – ook die staten die de norm niet formeel onderschrijven – afgemeten en beoordeeld kan worden.

Het startpunt is het formuleren van de norm en deze internationaal uit te dragen in de verscheidene internationale fora die Nederland daarbij ter beschikking staan. Het agenderen van deze norm binnen de verschillende overlegfora van de EU ligt voor de hand. Nederland is een voorloper in de club van Europese cyberattachés en kan invloed uitoefenen daar waar de besluiten worden genomen over Europese wetgeving en beleid inzake internet en cyber security. Het uitdragen van de norm richting Europese Commissie is eveneens een logische stap omdat de Europese Commissie alle EU-lidstaten vertegenwoordigt in (cyber)dialogen met strategische partners van de EU (Renard 2014). Bovendien onderhandelt de Commissie namens Nederland en de andere lidstaten over bilaterale handelsverdragen zoals TTIP[4] en in het kader van de Wereldhandelsorganisatie, waar kan worden gepleit voor het opnemen van de norm voor non-interventie naar analogie met de mensenrechtenclausules. Andere organisaties waar de norm geagendeerd kan worden zijn de Raad van Europa, de OESO, de OVSE en relevante fora binnen de VN. Hiermee kan een kiem worden geplant die op termijn uit kan groeien tot een breder regime. Daarvan geeft de diplomatieke geschiedenis een interessant voorbeeld. Het regime van de non-proliferatie van nucleaire wapens had zijn startpunt in de discussie over de Ierse resoluties over dit onderwerp binnen de VN. Een kleine staat zonder nucleaire capaciteit nam dus het initiatief in het formuleren van de eerste principes waar vervolgens een belangrijke internationale norm van terughoudendheid op gebouwd is.

5.3.2 ONTVLECHTEN VAN VEILIGHEID EN INTERNETPOLITIEK

Een tweede inhoudelijk punt voor de diplomatieke agenda is de noodzaak om het debat over internetgovernance waar mogelijk los te koppelen van (nationale) veiligheid en om verschillende vormen van veiligheid te ontvlechten. De grote nadruk op nationale veiligheid heeft een negatieve uitwerking op het debat over

internetveiligheid, want daarbij komen zaken al snel in een contraproductieve sleutel te staan. Veel media duidden de ophef over de film *The interview* en de hack van Sony als een cyberoorlog tussen de VS en Noord-Korea. Het is echter weinig productief om deze hack onder de noemer van oorlog te bespreken. Hoewel er zeker schade is toegebracht, ligt die ver onder het niveau dat de taal van oorlog rechtvaardigt, laat staan dat er sprake is van menselijke slachtoffers. Eerste aanzetten om het oorlogsrecht te doordenken in het cyberdomein, zoals het Tallinn manual (Schmitt 2013; AIV/CAVV 2011), laten zien dat geen enkel incident tot nu toe aan de juridische definities van 'oorlog' voldoet.

De nadruk op nationale veiligheid gaat ten koste van een breder spectrum van opvattingen van veiligheid op het internet – en de afbakeningen daartussen – die de veiligheid van het internet juist kan verhogen.

Aanbeveling: Bevorder dat verschillende vormen van veiligheid in relatie tot het internet op nationaal en internationaal niveau beter van elkaar onderscheiden worden en door aparte actoren worden geadresseerd.

Er zijn verschillende opvattingen van veiligheid in relatie tot het internet. Aan de ene kant van het spectrum staat de notie van internetveiligheid, waarin de veiligheid van het netwerk zelf centraal staat. Aan de andere kant staat de notie van nationale veiligheid, waarin de veiligheid van een staat centraal staat en het internet wordt gezien als bron van de dreiging én als potentieel beleidsinstrument. Tussen deze polen staat een veiligheidsopvatting die meer is geënt op criminaliteit en politie en justitie als voornaamste nationale en internationale actoren heeft. Op alle posities in het spectrum spelen ook private partijen een rol: als ontwikkelaars en toeleveranciers van technologische oplossingen, als bedrijven die hun eigen netwerken beschermen en als consultants die 'veiligheid' op of via het internet ten uitvoer brengen: voor opdrachtgevers uiteenlopend van Shell tot de NSA.

De meer traditionele technologische benadering van de CERT's richt zich meer op een public health-achtige benadering van de veiligheid van het netwerk als geheel. Het gaat hier om het gezond houden van het internet als netwerk, ten bate van alle gebruikers. Vertrouwen en een gedeelde opvatting van veiligheid op het niveau van het gehele netwerk en informatie-uitwisseling zijn belangrijke ingrediënten van de internationale samenwerking die door de jaren heen tussen de CERT's gegroeid is. Het is van belang om deze logica niet te vermengen met die van de nationale veiligheid, waarin nationale belangen boven de belangen van het netwerk gaan. Er moet een strikte scheiding zijn en blijven tussen enerzijds actoren die verantwoordelijk zijn voor nationale veiligheid, zoals de strijdkrachten en inlichtingen- en veiligheidsdiensten, en anderzijds partijen als CERT's die internetveiligheid bevorderen. Scheiding is hier als principe van groot belang. Vermenging

van de twee logica's, of dominantie van de tweede, kan het vertrouwen dat in de technische gemeenschap in lange jaren is opgebouwd serieuze schade toebrengen. Het is zaak dat ook politie en justitie zich niet laten verleiden om aan te sluiten bij benaderingen van veiligheids- en inlichtingendiensten die raken aan de publieke kern van het internet. Deze twee vormen van veiligheid moeten – ook in onveilige tijden in de online- en de offlinewereld – uit elkaar gehouden worden.

Het duidelijk onderscheiden en afbakenen van taken (scheiding) is ook van belang omdat de logica van nationale veiligheid een veel lagere risicotolerantie met zich meebrengt en daarmee de kans op escalatie vergroot. Nationale veiligheid laat weinig (politieke) ruimte voor restrisico's en 'trial and error': op het hoogste veiligheidsniveau kan een enkele fout fataal zijn. Die logica verdringt andere opvattingen van veiligheid die voor de stabiliteit en betrouwbaarheid van het internet als publiek goed minimaal even groot of van groter belang zijn. Van Eeten en Bauer (2009) zetten in dat kader de *precluded event security* en de *marginal security cost* tegenover elkaar. De eerste hanteert een absolute norm van veiligheid waarvoor (bijna) alles moet wijken, terwijl in de tweede een afweging plaatsvindt tussen veiligheid en maatschappelijke kosten. Daarbij gaat het behalve om financiële kosten – veiligheid is duur – ook om immateriële kosten, zoals de waarden van de rechtsstaat (AIV 2014) en het onderlinge vertrouwen van de betrokken organisaties en personen. Het is zaak om de logica van het restrisico centraler te stellen en de logica van nationale veiligheid sterker af te bakenen en exclusiever te maken om escalatie te voorkomen en beperken.

Operationele strategie

De discussie over de hoogste regionen van de nationale veiligheid – militaire cybereenheden en inlichtingen- en veiligheidsdiensten – is vanuit een perspectief van beteugeling zowel het meest noodzakelijk als het meest gecompliceerd. Internationale regulering van deze actoren is zeer ingewikkeld vanwege overwegingen van soevereiniteit. Tegelijkertijd geldt dat dit een nieuw veld is waarin sommige zaken bij het oude blijven – en de offline-regels 'gewoon' vertaald moeten worden naar online-regels – maar sommige zaken wel degelijk veranderen. 'Cyber' als vijfde domein van oorlogsvoering is bijvoorbeeld niet alleen een door mensen gemaakt domein, het is ook nog eens een grotendeels privaat domein. Dat roept nieuwe vragen op over wat wel en niet toegestaan is en hoe diep staten bijvoorbeeld mogen ingrijpen in private soft- en hardware. De levendige handel in 'zero-day vulnerabilities' – kwetsbaarheden in de hard- en software die wij allen dagelijks gebruiken om aldus inlichtingendiensten en militaire cybereenheden toegang te verschaffen tot systemen en informatie – vindt plaats in een grijs gebied. Een serieus nationaal en internationaal politiek debat over de vraag wat landen wel en niet acceptabel vinden en hoe de afweging wordt gemaakt ten opzichte van andere opvattingen van internetveiligheid kan helpen om dit domein beter te reguleren, hoe ingewikkeld dat ook zal zijn. Maar dit vraagstuk heeft het waarschijnlijk maar

in een zeer beperkt aantal hoofdsteden tot de regeringstafel en het parlement geschopt. De afgelopen jaren is internetbeveiliging in het bedrijfsleven steeds vaker een zaak van het bestuur geworden: een 'Chefsache'. Ook bij de overheid zou moeten gelden dat internetveiligheid – en de externe effecten van de ene vorm van veiligheid op de andere vorm van veiligheid – aan de tafel van de ministerraad en in het parlement besproken wordt.

In het internationale domein staan we nog aan het begin van dit traject, dit ondanks staande internationale overeenkomsten om te werken aan 'norms, rules and principles of responsible behaviour of states' in het cyberdomein, zoals bijvoorbeeld neergelegd in het 'Seoul Framework for and Commitment to Open and Secure Cyberspace'.[5] Er lopen uiteraard wel initiatieven om te komen tot gedeelde normen maar die vinden nu nog vooral plaats *binnen* de context van de internationale veiligheid en zijn bedoeld om escalatie tussen staten te voorkomen. Initiatieven als de VN Groups of Government Experts leggen daarbij de nadruk op gedragscodes en Confidence Building Measures, die ervoor moeten zorgen dat staten elkaars gedrag op het internet niet verkeerd interpreteren. Deze maatregelen monden uit in uitwisseling van informatie over nationale cyberstrategieën, dialogen tussen verschillende staten en internationale hulp bij het opbouwen van cybercapaciteit – voor verdediging – bij zwakkere staten (Kane 2014; Hurwitz 2014). In deze lopende internationale gesprekken over normen in cyberspace – en in regionale varianten daarvan, zoals de NAVO en OVSE in Europa en ASEAN in Azië bijvoorbeeld – zou het inbrengen van een duidelijke scheiding tussen verschillende vormen van veiligheid en het afbakenen van werkterreinen tussen de verschillende betrokken actoren winst kunnen betekenen. Zeker als deze worden beargumenteerd vanuit de gedachte van het buiten de orde verklaren van oneigenlijke ingrepen in de publieke kern van het internet. Deze norm kan ook helpen bij het ontvlechten van verschillende vormen van veiligheid, aangezien sommige opvattingen van veiligheid de integriteit van de publieke kern van het internet juist ondersteunen – internetveiligheid – terwijl andere vormen van (nationale) veiligheid, in de keuze van het instrumentarium, die integriteit soms juist schaden. Verder kan ook worden nagedacht over vormen van acceptabele transparantie over de werkzaamheden van de verschillende partijen. Op het niveau van internetveiligheid zoals de CERT's die zien, zijn daar al lopende initiatieven voor, zoals het Cyber Green Initiative (zie hoofdstuk 3). Op het niveau van de nationale veiligheid komt transparantie tot op heden alleen tot stand door klokkenluiders als Chelsea Manning en Edward Snowden. Transparantie op een – noodzakelijkerwijs – hoog niveau zou kunnen helpen om nut en noodzaak van bepaalde programma's van de diensten op nationaal niveau te beoordelen en kunnen internationaal een aanzet zijn als vertrouwenwekkende maatregel.

5.4 VERBREDING VAN HET DIPLOMATIEKE WERKVELD

Het derde punt voor de agenda voor internetdiplomatie is meer procedureel van aard en is gericht op de partijen die betrokken moeten worden bij de diplomatieke inspanningen en/of daar onderwerp van zouden moeten zijn.

Aanbeveling: maak de verbreding van het diplomatieke werkveld onderdeel van de agenda voor internetdiplomatie.

Deze verbreding bestaat uit (een heroverweging van) aandacht voor drie verschillende groepen van actoren: staten, bedrijven en ngo's (vgl. WRR 2010b). In de eerste plaats gaat het om een diplomatiek offensief om die staten die nu nog relatief nieuw en/of inactief in het debat over internetgovernance zijn – de zogeheten swing states – sterker te betrekken. In de tweede plaats zouden de grote internetbedrijven expliciet onderwerp van internetdiplomatie moeten zijn; en in de derde plaats moet een realistische benadering van ngo's worden uitgewerkt.

5.4.1 AANDACHT VOOR DE SWING STATES

Het agenderen van terughoudendheid in het internationale veld van internetgovernance vereist dat er gewerkt wordt aan nieuwe brede coalities die deze norm willen ondersteunen. Het is daarbij van belang dat er ook voorbij de *usual suspects* van de trans-Atlantische as, de EU en de OECD gedacht wordt. Binnen deze diplomatieke fora is voor Nederland nog genoeg werk te verzetten. Het Europese geluid wint aan kracht wanneer er binnen de EU overeenstemming is over de boodschap. Echter, de grootste uitdaging ligt elders. Het gesprek tussen 'like minded' bondgenoten is van belang om de normen die men nastreeft scherp te krijgen, maar de echte impact komt in dit veld van het gesprek met staten buiten die cirkel (Hurwitz 2014: 330). Dat valt onder meer af te lezen aan de stemming over het nieuwe Telecommunicatieverdrag tijdens de World Conference on International Telecommunications in Dubai in 2012. Hierbij bevonden Nederland en zijn traditionele medestanders zich in het kamp van de minderheid door te stemmen tegen grotere invloed van nationale staten. Naast landen die er een tegengesteld beeld van het internet en internetgovernance op nahouden, is er een grote groep van landen zonder uitgewerkt idee over de eigen positie inzake internetgovernance. Deze zogenoemde *swing states* of *fence sitters* zitten als staten wel degelijk aan tafel als het gaat om bepaalde dossiers, zoals de IANA-transitie en ITU-verdragen. Bovendien geldt dat de digitale grootmachten – zeker in termen van aantallen internetgebruikers – van vandaag niet per se gelijk zijn aan die van morgen. Er speelt zich een demografische verschuiving op het internet af: weg van Noord en West in de richting van Oost en Zuid. Andere stemmen dan de Europese en Amerikaanse zullen in de nabije toekomst harder spreken en daar zullen ook andere economische en politieke ideeën in doorklinken. Het is daarom zaak om een brede diplomatieke

inspanning te plegen om met name de *swing states* ervan te overtuigen dat het ongemoeid laten van de publieke kern van het internet een belang van *alle* staten is.

Inhoudelijk zijn er verscheidene dossiers waar het principe van beteugeling aan de oppervlakte ligt, bijvoorbeeld in de discussie over de transitie van het toezicht op het beheer van de namen en nummers van het internet. Daar ligt de vraag voor hoe het toezicht op dat beheer, dat nu bij ICANN (en de Amerikaanse overheid) is ondergebracht, moet worden vormgegeven. Een goed uitgangspunt in de discussie is om de beheerstaken (de IANA-functie) duidelijk te onderscheiden van ICANN's meer politiek omstreden taken, zoals het creëren van nieuwe domeinnamen. Het toezicht op de IANA-functie moet dan los worden gemaakt van ICANN en/of aan meerdere spelers worden toebedeeld. Nederland heeft er als sterk genetwerkt land en als digitaal knooppunt een groot belang bij dat het technische beheer zo 'agnostisch' mogelijk vormgegeven wordt. Het beheer van de internetnamen en -nummers – het kloppend houden van de adresfunctie – moet zoveel mogelijk buiten de politiek gehouden worden. In het belang van het goed functioneren van het internet als een collectieve infrastructuur op de lange termijn, heeft Nederland er dan ook alle reden voor om dit standpunt internationaal actief uit te dragen en andere landen ervan te overtuigen dat dit ook voor hen een verlengd nationaal belang is.

Operationale strategie

Nederland heeft zich met de oprichting van *Freedom Online Coalition* opgeworpen als een voorloper op het gebied van de digitale mensenrechten. Nederland zou ook het voortouw kunnen nemen bij een diplomatieke inspanning die het waarborgen van de publieke kern van het internet als centrale inzet heeft. Een eerste focus kunnen de swing states zijn. Maurer en Morgus (2014) selecteerden een top-dertig van swing states,[6] verspreid over alle werelddelen, door de stemuitslagen over het Telecommunicatieverdrag te combineren met een brede waaier aan criteria, zoals het lidmaatschap van internationale organisaties en de mate van democratie. Ook de mate van internetpenetratie, de aanwezigheid van een actieve internetgemeenschap en de grootte van de digitale economie werden meegenomen. De swing states zijn niet de 'like minded' staten van 'het eigen kamp' en ook niet de 'other minded' staten van de onvrije en dictatoriale regimes. Het zijn ook niet heel kleine staten en/of landen met heel weinig middelen die verondersteld worden weinig impact te hebben. De notie van swing states en deze eerste invulling daarvan kan een nuttig startpunt zijn voor het opbouwen van nieuwe coalities. Nederland zal het daadwerkelijke swingpotentieel van deze landen verder kunnen onderzoeken door de overwegingen te achterhalen die hebben meegespeeld bij de stemming in 2012. Het lijkt ook logisch zich te concentreren op landen die een potentieel invloedrijke rol op zich kunnen nemen in de eigen regio.

Daarnaast heeft de EU een aantal geïnstitutionaliseerde strategische partnerschappen met belangrijke landen van buiten de Unie, waarmee op regelmatige basis dialogen plaatsvinden. Met de Verenigde Staten, Brazilië, China en India kan zelfs al worden gesproken van ontwikkelde cyberdialogen, met overigens zeer grote verschillen als het gaat om het karakter van deze gesprekken. Met andere landen zoals Japan, Mexico, Rusland, Zuid-Afrika en Zuid-Korea wordt gewerkt aan het bespreekbaar maken van internetvraagstukken (Renard 2014).[7] Een aantal van de strategische partners van de EU, te weten Brazilië, Mexico, India, Zuid-Afrika en Zuid-Korea, overlapt overigens met de lijst van swing states. Begin 2015 hebben de Europese lidstaten besloten om tot een 'gemeenschappelijke totaalaanpak van de EU voor cyberdiplomatie op mondiaal niveau' te komen.[8] Ook de ontwikkeling van normen voor verantwoordelijk gedrag van staten in cyberspace maakt hier deel van uit. Het is voor Nederland zaak om bij deze dialogen en EU-cyberdiplomatie aan te sluiten waar dit meerwaarde heeft en daar waar nodig of nuttig zelf dialogen aan te gaan en initiatieven te ontplooien.

5.4.2 BETREK DE PRIVATE GIGANTEN

In de overwegend private wereld van het internet zijn private grootmachten zoals Apple, Google en Microsoft machtsfactoren van belang. Ze bepalen voor een groot deel hoe ons onlineleven eruitziet en welke nieuwe richtingen de informatiesamenleving inslaat. Dat betekent ook dat deze partijen veel meer dan voorheen met een diplomatieke en rechtsstatelijke bril bekeken moeten worden. Het gaat daarbij om macht en tegenmacht en – net zoals bij diplomatieke relaties met staten – zullen de belangen en agenda's soms op een lijn liggen met die van een land als Nederland en soms tegengesteld zijn.

Zo constateerde de Adviesraad Internationale Vraagstukken onlangs in het kader van de mensenrechtenagenda op het internet: "Niet goed valt in te zien waarom Nederland met autoritair geregeerde landen een mensenrechtendialoog onderhoudt, maar niet met bedrijven die voor de handhaving van privacy en vrijheid van communicatie in de wereld essentieel zijn" (AIV 2014). Die gedachte is veel breder te trekken omdat deze partijen bij uitstek een machtsfactor vormen voor vraagstukken van internetgovernance die – vanuit het perspectief van gebruikers en nationale belangen – soms productief en soms negatief aangewend wordt. Daarbij gaat het bijvoorbeeld om vraagstukken van privacy en databescherming, marktmacht, veiligheid van hard- en software en beveiliging van data met encryptie. Overheden staan vaak niet sterk ten opzichte van deze private giganten, hoewel zij gezamenlijk via de EU op sommige terreinen wel een vuist kunnen maken. Op het gebied van databescherming wordt in het kader van de onderhandelingen over de nieuwe EU-verordening ter bescherming van persoonsgegevens bijvoorbeeld een veel ruimere boetebevoegdheid toegekend aan databeschermingsorganisaties als het College Bescherming Persoonsgegevens. Ondanks het grote politieke gewicht van de EU moet wel bedacht worden dat EU-molens relatief traag zijn in vergelij-

king met de snelle wereld van de interneteconomie, zoals bleek in de beroemde zaak van de EU tegen Microsoft onder het mededingingsrecht. Hoewel de boete hoog en proportioneel was (860 miljoen dollar) duurde het proces zo lang dat het neerkwam op "solving the antitrust problem long after the competitors have died" (Brown en Marsden 2013: 40). Toch vergroot de aanwezigheid van serieuze sancties uiteraard het gewicht dat de EU en zijn lidstaten in de schaal leggen in de dialoog met deze bedrijven. De 'shadow of hierarchy' kan een belangrijk incentive zijn voor private partijen om een serieuze dialoog met staten aan te gaan (Börzel en Risse 2010).

Op een informele manier geven deze bedrijven momenteel wel tegendruk tegen overheden – in het bijzonder de Amerikaanse overheid – omdat de recente Snowden-onthullingen zeer schadelijk zijn voor hun reputatie bij internetgebruikers. Een aantal grote internetbedrijven is door de Snowden-onthullingen te kijk gezet: zij waren bewust en/of onbewust de grootleveranciers van de datamassa die de inlichtingendiensten verzamelden. Zij reageren nu met transparantierapporten – voor zover wettelijk toegestaan – om de gebruiker inzicht te geven in wat overheden opvragen en met het opschroeven van de encryptie van het dataverkeer van hun gebruikers. Hoewel dit grotendeels te verklaren is vanuit opportunistische motieven om klanten te behouden en/of terug te winnen, is het in termen van macht en tegenmacht een interessante ontwikkeling. Op beide punten worden ze tegengewerkt door veiligheidsdiensten. Toch is dit een eerste aanzet tot tegenmacht: encryptie verhoogt de kosten van massasurveillance en dwingt de diensten om hun surveillance specifiek te maken en te houden. Ook voeren bedrijven als Microsoft nu processen om de opvatting van de Amerikaanse overheid aan te vechten dat alle data in het beheer van een Amerikaans bedrijf – ook al staat die data op servers in Ierland – door de overheid te vorderen is. Gezien de grote macht van deze informatiegiganten en hun vitale rol in de manier waarop het leven van hele bevolkingen gedigitaliseerd is, kunnen overheden deze partijen in diplomatieke zin niet meer negeren. Deze bedrijven zijn meer dan mogelijke investeerders die aangetrokken moeten worden of juist privacyschenders die aangepakt moeten worden: het zijn partijen die serieuze diplomatieke aandacht behoeven vanwege hun vitale rol in het digitale leven, met alle tegenstrijdigheden die eigen zijn aan de diplomatie.

In het verlengde hiervan zou er meer helderheid moeten komen over wat overheden verwachten van de vele internetintermediairs die het digitale leven faciliteren: zoals ISP's, zoekmachines en clouddiensten. Deze organisaties moeten in zekere zin laveren tussen Scylla en Charybdis. Zij worden geacht zich ethisch en verantwoordelijk te gedragen ten opzichte van hun klanten, maar worden ook geacht zich te conformeren aan de eisen van het bevoegd gezag. Internationaal betekent dat soms dat Google wordt geacht niet mee te werken met de Chinese overheid en wel met de Amerikaanse. Hoewel daar vanuit een perspectief van

mensenrechten en de democratische rechtsstaat uiteraard iets voor te zeggen valt, begint het zich te wreken dat er noch nationaal noch internationaal een doordachte strategie, een voornemen voor beleid of zelfs maar een gestructureerde discussie is waarin verkend wordt wat intermediairs wel en niet moeten doen en wat overheden wel en niet mogen vragen. Intermediairs hebben nu drie opties ten opzichte van de – al dan niet geheime – verzoeken van overheden: volgzaamheid, verzet en preventief enthousiasme, waarbij ze op verzoeken vooruitlopen. De laatste is vanuit een rechtsstatelijk perspectief ongewenst, en de eerste twee zijn vanuit een perspectief van een machtenscheiding wellicht beide nodig. Alleen volgzaamheid of alleen verzet is problematisch. Een gestructureerde discussie – zeker op het internationale niveau – hierover moet echter nog beginnen.

Operationele strategie

Een eerste aanzet is te vinden in het werk van John Ruggie, de voormalig Speciaal gezant van de Secretaris-Generaal van de VN voor bedrijfsleven en mensenrechten. Zijn werk resulteerde onder meer in 2011 in de publicatie van de UN Guiding Principles on Business and Human Rights,[9] waarin de plichten van bedrijven – en staten in relatie tot die bedrijven – voor mensenrechten werden geschetst. Dit raamwerk zou verder vertaald moeten worden naar de rol en verantwoordelijkheid van internetbedrijven die de facto – en soms gedwongen door nationale wet- en regelgeving – een grote rol spelen in de online- en offline-mensenrechtensituatie in bepaalde landen. In juni 2014 is via een resolutie besloten tot de oprichting van een intergouvernementele werkgroep die een juridisch bindend instrument voor multinationals gaat uitwerken.[10] Er zou kunnen worden bekeken in hoeverre aangesloten kan worden bij de werkzaamheden van deze werkgroep. Het raamwerk zou hun rol en verantwoordelijkheden duidelijker moeten maken en ervoor kunnen zorgen dat overheden en bedrijven elkaar wederzijds kunnen aanspreken op – de grenzen van – hun verantwoordelijkheden en plichten. Een vergelijkbaar traject zou gestart kunnen worden als het gaat om de wederzijdse verplichtingen van bedrijven en overheden in hun zorg voor de bescherming van de publieke kern van het internet.

5.4.3 REALISME IN DE RELATIE MET NGO'S

De formele omarming van het multistakeholdermodel voor internetgovernance dat Nederland en zijn bondgenoten voorstaan, staat op gespannen voet met de steeds grotere rol die nationale staten in dit veld voor zichzelf opeisen. Het beheer van het internet is de facto in handen van een amalgaam van private en semi-private partijen, maar door toenemende regulering – zowel nationaal als internationaal – worden de kaders steeds meer door overheden geschetst. Tegelijkertijd is er een grote verscheidenheid aan ngo's die op nationaal en internationaal niveau opereren om het karakter, het gebruik en de toekomst van het internet – in hun eigen visie – te waarborgen. De onderwerpen en interesses zijn daarbij zeer divers: van het beschermen van mensenrechten en dissidenten online tot het beheer van

het technische deel van het internet. Soms kunnen bonte coalities van ngo's, bezorgde internetgebruikers, internetbedrijven en organisaties en personen van de technische gemeenschap het verschil maken in de ontwikkeling van beleid, zoals gebeurde bij SOPA/PIPA en het ACTA-verdrag. Op het internationale niveau is de aanwezigheid van ngo's overwegend groot, maar is er vaak geen plaats voor ze ingeruimd op het moment dat er afspraken worden gemaakt en conclusies worden getrokken op formele conferenties over de regulering en de toekomst van het internet. Op de twee grote internetconferenties die door de VN werden georganiseerd, de World Summit on the Information Society in Genève in 2003 en in Tunis in 2005, waren vele ngo's aanwezig. Bij het opstellen van de slotverklaring waren het echter vooral de staten die het woord konden voeren en de pen vasthielden. De bijdrage van ngo's aan de eindteksten en de verklaringen van de conferenties was zeer beperkt (Dutton en Peltu 2010; Cogburn 2010) hetgeen de frustratie voedt. Op dit ogenblik, zeker in het kader van de nasleep van de NETmundial-bijeenkomst in Brazilië waar het multistakeholdermodel wederom op het schild is gehesen, is het zaak om de bijdrage van ngo's productief te maken, maar geen valse verwachtingen te wekken. Nu internetgovernance politieker en statelijker is geworden, zal de bijdrage aan het formele proces eerder afnemen dan toenemen. Om de bijdrage van ngo's en andere stakeholders productief aan te wenden – in aanvulling op de publieke strategieën die ngo's nationaal en internationaal gebruiken om invloed uit te oefenen – zullen nationale staten nieuwe strategieën moeten ontwikkelen (vgl. WRR 2010a).

Operationele strategie

De Nederlandse overheid zou bij het vormgeven van haar beleid op nationaal, maar zeker op internationaal niveau veel sterker gebruik kunnen maken van de in Nederland aanwezige kennis bij ngo's – bijvoorbeeld over de mensenrechtensituatie in bepaalde landen – en de kennis bij de technische gemeenschap – bijvoorbeeld over de technische gevolgen van beleidsvoornemens. Zeker waar het gaat om het doordenken van de gevolgen van internetgovernance voor het technisch functioneren van het internet als geheel, valt hier een wereld te winnen. Op dit terrein is een verbinding tussen enerzijds diplomatieke kennis en kunde en anderzijds technische kennis en kunde van vitaal belang.

5.5 PRACTICE WHAT YOU PREACH

Voor Nederland, dat een kleine, maar potentieel invloedrijke diplomatieke speler in dit veld genoemd mag worden, geldt dat 'practice what you preach' de meest solide basis is om als een aanjager te kunnen fungeren. Nederland heeft goede ideeën en beleidsinitiatieven, die zich lenen voor verdere verspreiding. Zo is de Nederlandse wetgeving op het gebied van netneutraliteit een voorbeeld van een vorm van beteugeling – van bedrijven – die door de overheid wordt afgedwongen. Ook is de strategievorming binnen de overheid snel op een hoog en ambitieus

niveau gebracht en is er veel interdepartementaal contact tussen de verschillende betrokken ministeries. Ook internationaal bevindt Nederland zich in de voorhoede als een van de vijf landen in de G5 die samen de Europese cyberhygiëne en bijbehorend beleid naar een hoog niveau proberen te tillen.

Tegelijkertijd moet Nederland ervoor waken niet buiten bepaalde kaders te treden. Het Wetsvoorstel computercriminaliteit III geeft de politie een omstreden hackbevoegdheid die ook buiten het Nederlandse grondgebied mag worden ingezet. Dit staat op gespannen voet met het beginsel van nationale soevereiniteit en een aantal internationale verdragen.[11] Bovendien ondergraaft het de positie van Nederland in het internationale diplomatieke debat om te pleiten voor terughoudendheid en internetvrijheid. Het is ingewikkeld om andere landen op hun verantwoordelijkheid aan te spreken als je jezelf bevoegdheden toekent die het soevereiniteitsbeginsel niet respecteren. Ook op andere dossiers zoekt Nederland de grenzen op, bijvoorbeeld bij de interpretatie van uitspraken van het Europees Hof van Justitie over dataretentie.[12] 'Do as I say, don't do as I do' is een strategie waar alleen de heel machtige landen mee wegkomen, maar die nooit als rechtvaardig wordt ervaren. Bij nieuwe wetgeving moet de vraag of Nederland hiermee internationaal voor de dag kan komen een belangrijke overweging zijn (AIV 2014: 70). Op het gebied van de fundamentele rechten moet Nederland eigenlijk consequent een acht scoren om een voortrekkersrol te kunnen claimen.[13]

In dat licht zijn er ook kansen. Nederland is waarschijnlijk een van de eerste landen die in het post-Snowdentijdperk een herziening van de Wet op de inlichtingen- en veiligheidsdiensten (WIV 2002) heeft geagendeerd. De WIV 2002 staat op de agenda omdat de Nederlandse diensten formeel geen bevoegdheden hebben om data te onderscheppen die via de kabel worden verstuurd. Oftewel, de dataverzameling via het internet die in de Snowden-onthullingen centraal staan, zijn in Nederland helemaal nog niet toegestaan. De regering wil de inlichtingen- en veiligheidsdiensten in het digitale tijdperk niet de handen op de rug binden en hen deze bevoegdheden toestaan. Gezien de taak waarvoor zij staan is dat niet meer dan logisch. Echter, de Snowden-onthullingen hebben ook duidelijk laten zien dat de mogelijkheden en bevoegdheden van de Amerikaanse diensten niet in verhouding stonden tot het juridische en het politiek-democratische toezicht op het functioneren van deze diensten, dat duidelijk tekort is geschoten (Landau 2013; Glennon 2014). Ook in Nederland is het toezicht, zowel in de Tweede Kamer als door de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD), voor verbetering vatbaar. Zowel het parlementaire toezicht als het toezicht door de CTIVD kenmerkt zich door een grote afstand tussen toezichthouder en onder toezicht gestelde in termen van expertise en met name technologische kennis. De Nederlandse overheid kan de uitbreiding van de bevoegdheid van de inlichtingen- en veiligheidsdiensten combineren met het opnieuw doordenken en inrichten van het toezicht dat daar in het digitale tijdperk bij hoort.

Met andere woorden, nationale wetgeving kan een belangrijk internationaal uitstralingseffect hebben, zowel positief als negatief, en van grote invloed zijn op wat een land op diplomatiek vlak kan uitdragen en bereiken.

5.6 SAMENVATTING VAN DE AANBEVELINGEN

De centrale aanbeveling van dit rapport is dat het internet nadrukkelijk – en vooral eigenstandig – een speerpunt dient te zijn van het buitenlands beleid van Nederland. Naast traditionele speerpunten als handel, mensenrechten en vrede en veiligheid zou de regering een buitenlands internetbeleid moeten prioriteren en uitwerken. Verschillende ministeries zijn verantwoordelijk voor nationaal internetbeleid dat de toets van een internationale voorbeeldfunctie kan doorstaan. Daarnaast zijn ook verschillende ministeries verantwoordelijk voor de uitvoering van de diplomatieke agenda, zoals blijkt uit de intensieve interdepartementale contacten op het gebied van internetbeleid. De twee inhoudelijke aanbevelingen voor dit gezamenlijke beleid zijn:

> **Aanbeveling**: bevorder het vastleggen en internationaal verspreiden van de norm dat de publieke kern van het internet – de centrale protocollen en infrastructuur die een mondiaal publiek goed zijn – gevrijwaard moet zijn van bemoeienis van overheden.

> **Aanbeveling**: bevorder dat verschillende vormen van veiligheid in relatie tot het internet op nationaal en internationaal niveau beter van elkaar onderscheiden worden en door aparte actoren worden geadresseerd.

Voor het vastleggen en verspreiden van deze norm staan Nederland een aantal belangrijke fora ter beschikking. In de eerste plaats de EU en via de EU ook handelsverdragen waarin een dergelijke clausule opgenomen kan worden. Ook fora als de Raad van Europa, de OESO, de OVSE en de VN bieden mogelijkheden om deze norm te verankeren. Het onderscheiden van verschillende vormen van veiligheid in relatie tot het internet vergt een duidelijke afbakening en scheiding van taken en organisaties en vooral ook een beteugeling van de neiging van staten om nationale veiligheid de dominante visie op het internet te laten worden.

In aanvulling op deze twee inhoudelijke prioriteiten bevat dit rapport tevens een operationele aanbeveling:

> **Aanbeveling**: maak de verbreding van het diplomatieke werkveld onderdeel van de agenda voor internetdiplomatie.

Bij deze verbreding gaat het in de eerste plaats om een inspanning om de zogenoemde *swing states* ervan te overtuigen dat het ongemoeid laten van de publieke kern van het internet een (verlengd nationaal) belang van alle staten is. In de tweede plaats gaat het erom private partijen expliciet onderdeel van de diplomatieke inspanning op het gebied van internetgovernance te maken. En in de derde

plaats gaat het om het productief maken van de expertise van ngo's en andere private betrokkenen, zonder valse verwachtingen te scheppen over hun rol in het beheer van het internet.

NOTEN

1 De gebruikte indicatoren zijn: infrastructure, industry, individual en information. Voor de verdere operationalisering zie Boston Consultancy Group 2014a: 13. Voor de scores van Nederland zie Boston Consultancy Group 2014b: 45.

2 Dit punt werd bijvoorbeeld mooi gemaakt door Axel Arnbak in zijn bijdrage aan de Expertsessie Cyberintelligence en publiek belang in de Eerste Kamer: https://www.axelarnbak.nl/2014/05/21/opinie-fd-en-lezing-eerste-kamer-nederland-als-internetdokter-tussen-cybergrootmachten/.

3 Zie: https://www.axelarnbak.nl/2014/05/21/opinie-fd-en-lezing-eerste-kamer-nederland-als-internetdokter-tussen-cybergrootmachten en http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.

4 Het Transatlantic Trade and Investment Partnership (TTIP) is een bilateraal vrijhandelsverdrag waarover momenteel wordt onderhandeld tussen de EU en de VS.

5 Zie: https://www.gccs2015.com/sites/default/files/Seoul%20Framework.pdf.

6 De dertig swing states zoals Maurer en Morgus (2014) ze identificeren zijn: Albanië, Argentinië, Armenië, Botswana, Brazilië, Colombia, Costa Rica, Dominicaanse Republiek, Filippijnen, Georgië, Ghana, India, Indonesië, Jamaica, Kenya, Maleisië, Mexico, Moldavië, Mongolië, Namibia, Panama, Peru, Servië, Singapore, Tunesië, Turkije, Uruguay, Wit-Rusland, Zuid-Afrika en Zuid-Korea.

7 Zie ook de Outline for European Cyber Diplomacy Engagement, http://data.consilium.europa.eu/doc/document/ST-9967-2014-INIT/en/pdf.

8 Zie: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

9 Zie: http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

10 Zie: http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G14/064/48/PDF/G1406448.pdf?OpenElement.

11 Zie bijvoorbeeld de brief die Bits of Freedom op 28 juni 2013 aan de minister van VenJ stuurde in het kader van de consultatie Wetsvoorstel computercriminaliteit III, https://www.bof.nl/live/wp-content/uploads/20130628-BOFreactie-op-wetsvoorstel-computercriminaliteit.pdf.

12 Zo bracht het College Bescherming Persoonsgegevens op 10 februari 2015 een negatief advies uit over de wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met het aanbieden van openbare elektronische telecommunicatiediensten, die de uitspraak van het Hof voor de Nederlandse wet moest verwerken. Zie: https://cbpweb.nl/sites/default/files/atoms/files/z2014-00885_bewaarplicht.pdf.

13 Deze formulering is ontleend aan het commentaar dat Nico van Eijk op een eerdere versie van dit rapport gaf.

LITERATUURLIJST

Ablon, L., M. Libicki en A. Golay (2014) *Markets for cybercrime tools and stolen data. hackers' bazaar,* RAND National Security Research Division, Santa Monica: RAND.

AIV (2014) *Het internet: Een wereldwijde vrije ruimte met begrensde staatsmacht*, Den Haag: Adviesraad voor Internationale Vraagstukken.

AIV/CAVV (2011) *Digitale oorlogsvoering*, nr. 77, AIV/ nr. 22, CAVV, Den Haag.

Anders, G. (2014) 'The right way to fix the internet. Letting go of an obsession with net neutrality could free technologists to make online services even better', *MIT Technology Review*, 14 October 2014.

Ashgari, H., M. van Eeten, J. Bauer en M. Mueller (2013) 'Deep packet inspection: Effects of regulation and its deployment by internet providers', Paper presented at TPRC 2013, 25 September 2013.

Bauman, Z. et al. (2014) 'After Snowden: Rethinking the impact of surveillance', *International Political Sociology*, 8 (2): 121-144.

Benkler, Y. (2011) 'A free irresponsible press: Wikileaks and the battle over the soul of the networked fourth estate', *Harvard Civil Rights-Civil Liberties Law Review*, 46 (2): 311-396.

Benkler, Y. (2012) 'Seven lessons from SOPA/PIPA/Mega upload and four proposals on where we go from here', available at http://techpresident.com/news/21680/seven-lessons-sopapipamegauplaod-and-four-proposals-where-we-go-here, 25 januari 2012.

Betz, D. en T. Stevens (2011) *Cyberspace and the state. Towards a strategy for cyber-power*, Londen: Routledge.

Börzel, T. en T. Risse (2010) 'Governance without a state: Can it work?', *Regulation & Governance*, 4 (2): 113–134.

Boston Consultancy Group (2011) *Interned. Hoe het internet de Nederlandse economie verandert*, Amsterdam: The Boston Consultancy Group.

Boston Consultancy Group (2014) *Connecting the world. Greasing the wheels of the internet economy*, study commissioned by ICANN, The Boston Consultancy Group.

Boyle, J. (1997) 'A politics of intellectual property: Environmentalism for the net?', *Duke Law Journal,* 47: 87-116.

Bradford, A. (2012) 'The Brussels effect', *Northwestern University Law Review*, 107 (1): 1-68.

Breindl, Y. (2013) 'Internet content regulation in liberal democracies. A literature review', *DH Forschungsverbund – Working Papers zu Digital Humanities*, 2.

Breindl, Y. en F. Briatte (2010) 'Digital network repertoires and the contentious politics of digital copyright in France and the European Union', *Internet, Politics, Policy 2010: An Impact Assessment*, Sep 2010, Oxford, United Kingdom

Brito, J. en T. Watkins (2011) 'Loving the cyber bomb? The dangers of threat inflation in cyber security policy', *Harvard National Security Journal*, 3 (1): 41-84.

Broeders, D. (2014) *Investigating the place and role of the armed forces in Dutch cyber security governance*, Breda: The Netherlands Defence Academy.

Brown, I. en C. Marsden (2013) *Regulating code: Good governance and better regulation in the information age*, Cambridge (Mass.): MIT Press.

Budish, R. en P. Kuman (2013) 'Just in time censorship: Targeted internet filtering during Iran's 2013 elections', blz. 32-33 in U. Gasser, R. Faris en R. Heacock (red.) *Internet monitor 2013: Reflections on a digital world*, Cambridge (Mass): The Berkman Center for Internet and Society.

CBS (2014) *ICT, kennis en economie 2014*.Den Haag: CBS.

CDU, CSU en SPD (2013) 'Deutschlands zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD', https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf.

Cerf, V. (2013) 'Revisiting the tragedy of the commons', *Communications of the ACM*, 56 (10): 7.

Chander, A. en U. Le (2014) 'Breaking the Web: Data localization vs. the global internet', *Emory Law Journal* (forthcoming), available online at: http://ssrn.com/abstract=2407858.

Choucri, N. (2012) *Cyberpolitics in international relations*, Cambridge (Mass.): MIT Press.

Clarke, R. en R. Knake (2010) *Cyber war: The next threat to national security and what to do about it,* New York: Harper Collins.

Clemente, D. (2013) *Adaptive internet governance: Persuading the swing states*, CIGI Internet Governance Papers nr. 5 (October 2013).

Clinton, H. (2010) *Remarks on internet freedom*. Speech at the Newseum, Washington D.C., 21 January 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm.

Cogburn, D. (2010) 'Enabling effective multi-stakeholder participation in global internet governance through accessible cyber-infrastructure', blz. 401-423 in A. Chadwick en P. Howard (red.) *The Routledge handbook of internet politics*, London: Routledge.

Council on Foreign Relations (2013) *Defending an open, global, secure and resilient internet,* New York: Council on Foreign Relations.

Crocker, S., D. Dagon, D. Kaminsky, D. McPherson en P. Vixie (2011) 'Security and other technical concerns raised by the DNS filtering requirements in the Protect IP Bill', http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf.

Czyz, J., M. Allman, J. Zhang, S. Iekel-Johnson, E. Osterweil en M. Bailey (2013) *Measuring IPv6 Adoption*, ICSI Technical Report TR-13-004, August 2013.

Danaher, B., M.D. Smith en R. Telang (2013) 'Piracy and copyright enforcement mechanisms', *Innovation Policy and the Economy*, 14.

Degli Esposito, S. (2014) 'When Big Data meets dataveillance: the hidden side of analytics', *Surveillance and Society*, 12 (2): 209-225.

Deibert, R. (2012) *Distributed security as cyber strategy: Outlining a comprehensive approach for Canada in cyber space*, Calgary: Canadian Defense & Foreign Affairs Institute.

Deibert, R. (2013a) *Bounding cyber power: Escalation and restraint in global cyberspace*, CIGI Internet Governance Papers nr. 6 (October 2013).

Deibert, R. (2013b) *Black code. Inside the battle for cyber space*, Toronto: Signal.

Deibert, R. (2014) 'Divide and rule. Republican security theory as civil society cyber Strategy', *The Georgetown Journal of International Affairs*, 20: 45-56.

Deibert, R. en R. Rohozinski (2011) 'Liberation versus control: the future of cyberspace', *Journal of Democracy*, 21 (4): 43-57.

Deibert, R., J. Palfrey, R. Rohozinski en J. Zittrain (2008, red.) *Access denied: The practice and policy of global internet filtering*, Cambridge (Mass.): MIT Press.

Deibert, R., J. Palfrey, R. Rohozinski en J. Zittrain (2010, red.) *Access controlled: The shaping of power, rights, and rule in cyberspace*, Cambridge (Mass.): MIT Press.

Deibert, R., J. Palfrey, R. Rohozinski en J. Zittrain (2011, red.) *Access contested. Security, identity, and resistance in Asian cyberspace*, Cambridge (Mass.): MIT Press.

Deloitte (2014) *Digital infrastructure in the Netherlands. Driver for the online ecosystem.*

Demchack, C. en P. Dombrowksi (2011) 'Rise of a cybered Westphalian age', *Strategic Studies Quarterly*, Spring 2011: 32-61.

Demchack, C. en P. Dombrowski (2014) 'Cyber Westphalia. Asserting state prerogatives in cyberspace', *The Georgetown Journal of International Affairs*. International Engagement on Cyber III. State Building on a New Frontier, 20: 29-38.

DeNardis, L. (2009) *Protocol politics. The globalization of internet governance*, Cambridge (Mass.): MIT Press.

DeNardis, L. (2012) 'Hidden levers of internet control. An infrastructure-based theory of internet governance', *Information, Communication and Society*, 15 (5): 720-738.

DeNardis, L. (2013) *Internet points of control as global governance*, CIGI Internet Governance Papers nr. 2 (August 2013).

DeNardis, L. (2014) *The global war for internet governance*, New Haven: Yale University Press.

Dijck, J. van (2014) 'Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology', *Surveillance and Society*, 12 (2): 197-208.

Dubuisson, T. (2012) 'When the World Wide Web becomes the World Wild Web; PIPA, SOPA, OPEN Act, CISPA and the "Internet Revolution", file:///C:/Users/wrr45/Downloads/SSRN-id2373906.pdf

Dunn Cavelty, M. (2012) 'The militarisation of cyberspace: Why less may be better', blz. 141-153 in C. Czossceck, R. Ottis en K. Ziolkowski (red.) *2012 4th International Conference on Cyber Conflict*, Talinn: NATO CCD COE Publications.

Dunn Cavelty, M. (2013) 'From Cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse', *International Studies Review*, 15 (1): 105-122.

Dunn Cavelty, M. (2014) 'Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities', *Science and Engineering Ethics*, 20 (3): 701-715.

Dutton, W. en M. Peltu (2010) 'The new politics of the internet. Multi-stakeholder policy-making and the internet technocracy', blz. 384-200 in A. Chadwick en P. Howard (red.) *The Routledge handbook of internet politics*, London: Routledge.

Eeten, M. van, en J. Bauer (2009) 'Emerging threats to internet security: Incentives, externalities and policy implications, *Journal of Contingencies and Crisis Management*, 17 (4): 221-232.

Eeten, M. van, en M. Mueller (2013) 'Where is the governance in Internet governance?', *New Media & Society*, 15 (5): 720-736.

Eeten, M. van, en J. Bauer (2009) 'Emerging threats to internet security: Incentives, externalities and policy implications, *Journal of Contingencies and Crisis Management*, 17 (4): 221-232.

Eeten, M. van, M. Mueller en N. van Eijk (2014) *The internet and the state: A survey of key developments*, Den Haag: Raad voor Maatschappelijke Ontwikkeling.

Europese Commissie (2014) *Internet policy and governance. Europe's role in shaping the future of internet governance* (COM(2014) 72).

Faris, R. en R. Heacock Jones (2014) 'Platforms and policy', blz. 28-35 in U. Gasser, J. Zittrain, R. Faris en R. Heacock Jomes (red.) *Internet Monitor 2014: Reflections on the digital world: Platforms, policy, privacy, and public discourse*, Cambridge (Mass.): The Berkman Center for Internet and Society at Harvard University.

Faris, R. en U. Gasser (2013) 'Governments as actors', blz. 19-24 in U. Gasser, R. Faris en R. Heacock (red.) *Internet monitor 2013: Reflections on the digital world*, Cambridge (Mass.): The Berkman Center for Internet and Society at Harvard University.

Fidler, M. (2014) *Anarchy or regulation? Controlling the global trade in zero-day vulnerabilities*, Honors thesis in International Security Studies, Stanford University.

Fillipini, P. de, en L. Belli (2014) 'Introduction. Network neutrality: an unfinished debate', blz. 3-16 in L. Belli en P. De Fillipini (red.) *Network neutrality: an ongoing regulatory debate*. 2nd report of the Dynamic Coalition on Network Neutrality.

Garton-Ash, T. (2013) 'If Big Brother came back, he'd be a public-private partnership', *The Guardian*, 27 June 2013.

Glennon, M. (2014) 'National security and double government', *Harvard National Security Journal*, 5 (1): 1-114.

Goldsmith, J. en T. Wu (2008) *Who controls the Internet? Illusions of a borderless world*, Oxford: Oxford University Press.

Goldstein, G. (2014) 'The end of the internet? How regional networks may replace the World Wide Web', *The Atlantic*, July/August, http://www.theatlantic.com/magazine/archive/2014/07/the-end-of-the-internet/372301

Graham, M. (2014) 'Internet geographies: Data shadows and digital divisions of labour', blz. 99-116 in M. Graham en W. Dutton (red.) *Society and the internet: How networks of information and communication are changing our lives*, Oxford: Oxford University Press.

Greenwald, G. (2014) *No place to hide. Edward Snowden, the NSA and the US Surveillance State*, New York: Metropolitan Books.

Guitton, C. (2013) 'Cyber insecurity as a national threat: Overreaction from Germany, France and the UK?', *European Security*, 22 (1): 21-35.

Haas, P. (1992) 'Introduction: Epistemic communities and international policy coordination', *International Organization*, 46 (1): 1-35.

Hansen, L. en H. Nissenbaum (2009) 'Digital disaster, cyber security and the Copenhagen School', *International Studies Quarterly*, 53: 1155-1175.

Herold, D. (2011) 'An inter-nation-al internet: China's contribution to global internet governance?', paper presented at symposium 'A decade in internet time', 22 September 2011, Oxford: Oxford Internet Institute.

Hoboken J. van, en I. Rubinstein (2014) 'Privacy and security in the cloud: Some realism about technical solutions to transnational surveillance in the post-Snowden era', *Maine Law Review*, 66 (2): 487-534.

Hofmann, J. (2012) 'Narratives of copyright enforcement: The upward ratchet and the sleeping giant', *Revue francaise d'études Américaines*, 43: 4.

Howard, P., S. Agarwal en M.Hussain (2011)'When do states disconnect their digital networks? Regime responses to the political uses of social media', *The Communication Review*, 14: 216-232.

Hughes, R. (2010) 'A treaty for cyberspace', *International Affairs*, 86 (2): 523-541.

Human Rights Watch (2012) *In the name of security. Counterterrorism laws worldwide since September 11*, http://www.hrw.org/sites/default/files/reports/global0612ForUpload_1.pdf, geraadpleegd 1 augustus 2012.

Hurwitz, R. (2014) 'The play of states: Norms and security in cyberspace', *American Foreign Policy Interests*, 36 (5): 322-331.

Jervis, R. (1978) 'Cooperation under the security dilemma', *World Politics*, 30 (2): 167-214.

JPCERT/CC (2014) *The cyber green initiative: Improving health through measurement and mitigation*, JPCERT/CC Concept Paper, 10 August 2014.

Kane, A. (2014) 'The rocky road to consensus: The work of UN groups of governmental experts in the field of ICTs and in the context of international security, 1998-2013', *American Foreign Policy Interests*, 36 (5): 314-321.

Kitchin, R. (2014) *The data revolution. Big data, open data, data infrastrcutures and their consequences*, Londen: Sage.

Landau, S. (2010) *Surveillance or security? The risks posed by new wiretapping technologies*, Cambridge (Mass.): MIT Press.

Landau, S. (2013) 'Making sense of Snowden: What's significant in the NSA revelations', *IEEE Security & Privacy*, 11 (4): 54–63.

Lawson, S. (2013) 'Beyond cyber-doom: Assessing the limits of hypothetical scenario's in the framing of cyber-threats', *Journal of Information Technology and Politics*, 10: 86-103.

Lemley, M., D.S. Levine en D.G. Post (2011) 'Don't break the internet', *Stanford Law Review Online*, 34, 19 december 2011.

Lessig, L. (1999) *Code and other laws of cyber space*, New York: Basic Books.

Lessig, L. (2006) *Code. Version 2.0*, New York: Basic Books.

Lewis, J. (2013) *Internet governance: Inevitable transitions*, CIGI Internet Governance Papers nr. 4 (October 2013).

Libicki, M. (2012) 'Cyberspace is not a warfighting domain', *I/S: A Journal of Law and Policyfor the Information Society*, 8 (2): 321-336.

Lin, H. (2012) 'Thoughts on threat assessment in cyberspace', *I/S: A Journal of Law and Policy for the Information Society*, 8 (2): 337-355.

Lyon, D. (2014) 'Surveillance, Snowden, and Big Data: Capacities, consequences, critique', *Big Data & Society*, July-September 2014: 1-13.

MacKinnon, R. (2011) 'Corporate accountability in networked Asia', blz. 195-215 in R. Deibert, J. Palfrey, R. Rohozinski en J. Zittrain (red.) *Access contested. Security, identity, and resistance in Asian cyberspace*, Cambridge (Mass.): MIT Press.

Maher, K. (2013) 'The new Westphalian web', *Foreign Policy Magazine Online*, 25 February 2013.

Marks, G. en L. Hooghe (2004) 'Contrasting visions of multi-level governance', blz. 15-30 in Bache, I. en M. Flinders (red.) *Multi-level governance*, Oxford: Oxford University Press.

Masnick, M. (2014) 'The rebranding of SOPA: now called "Notice and staydown"', *Techdirt*, 14 maart 2014. Beschikbaar op: https://www.techdirt.com/articles/20140313/17470826574/rebranding-sopa-now-called-notice-staydown.shtml.

Maurer, T. en R. Morgus (2014) *Tipping the scale: An analysis of global swing states in the internet governance debate*, CIGI Internet Governance papers nr. 7 (May 2014).

Maurer, T., R. Morgus, I. Skierka en M. Hohmann (2014) *Technological sovereignty: Missing the point? An analysis of European proposals after June 5, 2013*. Report for Transatlantic Dialogues on security and freedom in the digital age.

Mayer-Schönberger, V. en K. Cukier (2013) *Big Data. A revolution that will transform how we live, work and think*, Londen: John Murray Publishers.

McDiarmid, A. en D. Sohn (2013) 'Bring in the nerds: The importance of technical experts in defeating SOPA and PIPA', blz. 133-139 in D. Moon, P. Ruffini en D. Segal (red.) *Hacking politics. How geeks, progressives, the Tea Party, gamers, anarchists and suits teamed up to defeat SOPA and save the internet*, New York: OR Books.

Ministerie van Buitenlandse Zaken (2011) *Verantwoordelijk voor vrijheid. Mensenrechten in het buitenlands beleid*, Den Haag, 5 april 2011.

Ministerie van Buitenlandse Zaken (2013) *Veilige wereld, veilig Nederland. Internationale veiligheidsstrategie*, Den Haag, 21 juni 2013.

Ministerie van Defensie (2012) *Defensie cyber strategie*, Den Haag, 27 juni 2012.

Ministerie van Defensie (2013) *In het belang van Nederland*, Den Haag, 25 oktober 2013.

Ministerie van Economische Zaken, Landbouw en Innovatie (2011) *Digitale Agenda.nl. ICT voor innovatie en economische groei*, Den Haag, 17 mei 2011.

Ministerie van Veiligheid en Justitie (2011) *De Nationale Cyber Security Strategie*, Den Haag, 28 februari 2011.

Ministerie van Veiligheid en Justitie (2013a) *De nationale cyber security strategie 2. Van bewust naar bekwaam*, Den Haag.

Ministerie van Veiligheid en Justitie (2013b) *Vrijheid en veiligheid in de digitale samenleving. Een agenda voor de toekomst*, Den Haag.

Mueller, J. en M. Stewart (2014) 'Secret without reason and costly without accomplishment: Questioning the National Security Agency's metadata program', *I/S: A Journal of Law and Policy for the Information Society*, 10 (2): 407-432.

Mueller, M. (2002) *Ruling the root. Internet governance and the taming of cyberspace*, Cambridge (Mass.): MIT Press.

Mueller, M. (2010) *Networks and states. The global politics of internet governance*, Cambridge (Mass.): MIT Press.

Mueller, M. en B. Kuerbis (2014) 'Towards global internet governance: How to end U.S. control of ICANN without sacrificing stability, freedom or accountability', TPRC Conference Paper, available at SSRN: http://ssrn.com/abstract=2408226.

Mueller, M., A. Schmidt en B. Kuerbis (2013) 'Internet security and networked governance in international relations', *International Studies Review*, 15 (1): 86-104.

NCTV (2014) *Tussen naïviteit en paranoia. Nationale veiligheidsbelangen bij buitenlandse overnames en investeringen in vitale sectoren.* Rapportage Werkgroep Economische Veiligheid, April 2014

Nye, J. (2011) *The future of power*, New York: Public Affairs.

Nye, J. Jr. (2011) 'Nuclear lessons for cyber security?', *Strategic Studies Quarterly*, 5 (4): 8-38.

OECD (2012) *OECD Internet economy outlook 2012*, Parijs: OECD Publishing.

OECD (2014) 'The internet in transition: The state of the transition to IPv6 in today's internet and measures to support the continued use of IPv4', *OECD Digital Economy Papers*, No. 234, available at http://dx.doi.org/10.1787/5jz5sq5d7cq2-en.

OECD (2014) *Measuring the digital economy: A new perspective*, Parijs: OECD Publishing.

Polatin-Reuben, D. en J. Wright (2014) 'An internet with BRICS characteristics: Data sovereignty and the balkanisation of the internet', paper presented at the 4th USENIX workshop on free and open communications on the internet, August 18.

Poort, J. en J. Leenheer (2014) *Filesharing 2@12. Downloading from illegal sources in the Netherlands*, Tilburg: IViR.

Poort, J., J. Leenheer, J. van der Ham en C. Dumitru (2014) 'Baywatch: Two approaches to measure the effects of blocking access to The Pirate Bay', *Telecommunications Policy*, http://dx.doi.org/10.1016/j.telpol.2013.12.008i.

Raymond, M. (2014) 'Puncturing the myth of the internet as a commons', *The Georgetown Journal of International Affairs*. International Engagement on Cyber III. State Building on a New Frontier, 20: 53-64.

Renard, T. (2014) *The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security*, European Strategic Partnerships Observatory, Working Paper 7, available at http://strategicpartnerships.eu/publications/the-rise-of-cyber-diplomacy-the-eu-its-strategic-partners-and-cyber-security.

Rid, T. (2013) *Cyber war will not take place*, Londen: Hurst and Company.

Rid, T. en P. McBurney (2012) 'Cyber weapons', *The RUSI Journal*, 157 (1): 6-13.

Ruggie, J.G. (2007) 'Current developments. Business and human rights: the evolving international agenda', *The American Journal of International Law*, 101 (4): 819-840.

Sanger, D. (2012) *Confront and conceal: Obama's Secret Wars and Surprising Use of American Power*, New York: Broadway Books.

Scherer, A. en G. Palazzo (2011) 'The new political role of business in a globalized world: Review of a new perspective on CSR and its implications for the firm, governance, and democracy', *Journal of Management Studies*, 48 (4): 899-931.

Schmitt, M. (2013, ed.) *Talinn Manual on the international law applicable to Cyber Warfare*, Cambridge: Cambridge University Press.

Schneier, B. (2013) 'Power in age of the feudal internet', blz. 10-14 in U. Gasser, R. Faris en R. Heacock (red.) *Internet monitor 2013: Reflections on the digital world*, Cambridge (Mass.): The Berkman Center for Internet and Society.

Schneier, B. (2014) 'Should US hackers fix cybersecurity holes or exploit them?', *The Atlantic*, http://www.theatlantic.com/technology/archive/2014/05/should-hackers-fix-cybersecurity-holes-or-exploit-them/371197/, accessed 9 July 2014.

Sellars, A. (2014) 'SOPA lives: copyright's existing power to block websites and "Break the Internet"', blz. 36-39 in U. Gasser, J., Zittrain, R. Faris en R. Heacock Jomes (red.) *Internet monitor 2014: Reflections on the digital world: platforms, policy, privacy, and public discourse*, Cambridge (Mass.): The Berkman Center for Internet and Society at Harvard University.

Sénat Francaise (2014) Rapport d´information fait au nom de la mission commune d'information «Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet». Session extraordinaire de 2013-2014, 8 juillet 2014.

Severs, H. (2013) *The cyber-industrial complex: What does the militarisation of the 'fifth domain' entail and what are the consequences?*, http://theriskyshift.com/2013/03/the-cyber-industrial-complex-2, geraadpleegd 8 juli 2014.

Singer, P. en A. Friedman (2014) *Cyber security and cyberwar. What everyone needs to know*, Oxford: Oxford University Press.

Stockton, P. en M. Golabek-Goldman (2013) 'Curbing the market for cyber weapons', *Yale Law and Policy Review*, 32 (1): 101-128.

Went, R. (2010) *Internationale publieke goederen: Karakteristieken en typologie*, WRR webpublicatie 41, Den Haag: WRR.

World Economic Forum (2014) *Global Risks 2014*, Ninth Edition, Insight Report, Geneva: World Economic Forum.

WRR (2003) *Waarden, normen en de last van het gedrag*, WRR rapporten aan de regering nr. 68, Amsterdam: Amsterdam University Press.

WRR (2010a) *Minder pretentie, meer ambitie*, WRR rapporten aan de Regering, nr. 84, Amsterdam: Amsterdam University Press.

WRR (2010b) *Aan het buitenland gehecht. Over verankering en strategie van Nederlands buitenlandbeleid*, Amsterdam: Amsterdam University Press.

Wu, T. (2010) 'Is internet exceptionalism dead?', blz. 179-188 in B. Zsoka en A. Marcus (red.) *The next digital decade. Essays on the future of the internet*, Washington DC: Techfreedom.

Wu, T. (2011) *The master switch. The rise and fall of information empires*, New York: Vintage Books.

Yu, P.K. (2012) 'The alphabet soup of transborder intellectual property enforcement', *Legal studies research Paper series*.

Yu, P.K. (2014) 'Digital copyright enforcement measures and their human rights threats', in C. Geiger (ed.) *Research Handbook on Human Rights and Intellectual Property*, Edward Elgar (te verschijnen).

Ziewitz, M. en I. Brown (2014) 'A prehistory of internet governance', blz. 3-26 in I. Brown (ed.) *Research handbook on governance of the internet*, Cheltenham: Edward Elgar.

Zittrain, J. (2008) *The future of the internet. And how to stop it*, Londen: Penguin Books.

Zittrain, J. (2014) 'No, Barack Obama isn't handing control of the internet over to China. The misguided freakout over ICANN', *New Republic*, 14 March 2014.

Zittrain, J. en Palfrey (2008) 'Internet filtering: The politics and mechanisms of control', blz. 29-56 in R. Deibert, J. Palfrey, R. Rohozinski en J. Zittrain (ed.) *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge (Mass.): MIT Press.

Zuckerman, E. (2010) 'Intermediairy censorship', blz. 71-85 in R. Deibert, J. Palfrey, R. Rohozinski en J. Zittrain (red.) *Access controlled: The shaping of power, rights, and rule in cyberspace*, Cambridge (Mass.): MIT Press.

BEGRIPPENLIJST

ACTA	Anti-Counterfeiting Trade Agreement
AIV	Adviesraad Internationale Vraagstukken
AMS-IX	Amsterdam Internet Exchange
APNIC	Asia Pacific Network Information Centre
ARPANET	Advances Research Projects Agency Network
CERT	Computer Emergengy Response Teams
CIA-triade	Confidentiality, Integrity, Availability triade
CIR	Critical Internet Resources
CBP	College bescherming persoonsgegevens
CTIVD	Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten
DBMS	Database Management System
DDoS	Distributed Denial–of-Service
DG	Directoraat-Generaal
DNS	Domain Name System
DPI	Deep Packet Inspection
GCHQ	Government Communications Headquarters
HTML	Hyper Tekst Markup Language
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IP	Internet Protocol
IPv4	Internet Protocol versie 4
IPv6	Internet Protocol versie 6
ISOC	Internet Society
ISP	Internet Service Providers
ITU	International Telecommunication Union
ELI	Ministerie van Economische Zaken, Landbouw en Innovatie
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NGO	Non-Governmental Organization
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
P2P	Peer-to-Peer network
PGP	Pretty Good Privacy
PIPA	Protect Intellectual Propery Act
RIPE-NCC	RIPE Network Coordination Centre
RIRs	Regional Internet Registries

SABAM	Société d'Auteurs Belge
SIDN	Stichting Internet Domeinregistratie Nederland
SIGINT	Signals Intelligence
SOPA	Stop Online Piracy Act
TCP/IP	Transmission Control Protocol/Internet Protocol
TLD	Top Level Domein
TOR	The Onion Router
TRIPs	Agreement on Trade Related Aspects of Intellectual Property Rights
UDP	User Datagram Protocol
VoIP	Voice over IP
W3C	World Wide Web Consortium
WCIT	World Conference on International Telecommunications
WCT	WIPO Copyright Treaty
WIPO	World Intellectual Property Organization
WIV	Wet Inlichtingen- en Veiligheidsdiensten
WPPT	WIPO Performances and Phonograms Treaty
WRR	Wetenschappelijke Raad voor het Regeringsbeleid
WSIS	World Summit on the Information Society
WTO	World Trade Organization

GESPROKEN PERSONEN

Functieaanduidingen ten tijde van het interview

Erik Akerboom, Secretaris-generaal, Ministerie van Defensie
Caspar Bowden, Zelfstandig onderzoeker privacy
Sergio Carrera, Head of Justice and Home Affairs programme, Centre for European Policy Studies (CEPS)
Nicola Dubois, Policy advisor/ data protection, European Commission, DG Justice
Kol. Paul Duchein, UHD Cyber Operations, Nederlandse Defensie Academie, Ministerie van Defensie
David van Duren, Coördinator Internationale Cybersecurity Strategie, Ministerie van Veiligheid en Justitie
Michel van Eeten, Hoogleraar Governance van Cybersecurity, TU Delft
Kol. Hans Folmer, Commandant Task Force Cyber, Ministerie van Defensie
Wil van Gemert, Directeur Cybersecurity, Dienst Nationale Coördinator Terrorismebestrijding en Veiligheid, Ministerie van Veiligheid en Justitie
Bruno Gencarelli, Head of Unit Data Protection, European Commission, DG Justice
Rickey Gevers, Digital Forensic investigator, Digital Investigation
Patrick de Graaf, Principal Consultant/ teamlead Security & Privacy, Cap Gemini
Wim Hafkamp, Chief Information Security Officer, Rabobank
Stan Hegt, Manager Information Protection Services, KPMG
Hielke Hijmans, Head of Unit Policy and Consultations, European Data Protection Supervisor
Peter Hustinx, European Data Protection Supervisor, European Data Protection Supervisor
Bart Jacobs, Hoogleraar security en correctheid van software
Wouter Jurgens, Hoofd Terrorismebestrijding en Nationale Veiligheid, Ministerie van Buitenlandse Zaken
Geran Kaai, Hoofd Veiligheid, Justitie en Binnenlandse Zaken, Permanente Vertegenwoordiging van het Koninkrijk der Nederlanden bij de EU
Gerben Klein Baltink, Secretaris Cyber Security Raad
Joe MacNamee, Directeur, European Digital Rights (EDRi)
Nicole Mallens, Beleidsadviseur, cybersecurity en vitale infastructuur,VNO-NCW
René Marchal, Senior manager bedrijfsveiligheid en security, TenneT
Karin Mössenlechner, Adjunct-directeur veiligheidsbeleid, Ministerie van Buitenlandse Zaken
Hans Oosters, Dijkgraaf; Bestuurslid met portefeuille crisisbeheersing, management en IT, Unie van Waterschappen
Constantijn van Oranje-Nassau, Kabinetschef Commissaris Kroes, Europese Commissie
Ronald Prins, Directeur, Fox-IT

Mieneke de Ruiter, Senior Policy Advisor, Permanent Representation the Netherlands at the EU
Marietje Schaake, Lid van het Europees Parlement (D66)
Claudia Selli, Director European Government Affairs, AT&T, Brussels and American Chamber of Commerce EU
Willem van Sluis, Senior beleidsadviseur, Permanente Vertegenwoordiging van het Koninkrijk der Nederlanden bij de EU
Heli Tiirma-Klaar, Head of Cyber Policy Coordination, European External Action Service
Gen. Marc van Uhm, Plaatsvervangend Commandant Landstrijdkrachten, Ministerie van Defensie
Mathijs Veenendaal, Senior beleidsadviseur Cybersecurity, Ministerie van Veiligheid en Justitie
Michel Verhagen, Plaatsvervangend directeur Telecommarkt, Ministerie van Economische Zaken
Hein Verweij, Strategisch adviseur (Cyber) security en Terrorismebestrijding, Ministerie van Veiligheid en Justitie
Ben Voorhorst, Operationeel directeur, TenneT
Lodewijk van Zwieten, Landelijk Officier van Justitie cybercrime & rechtmatig onderscheppen, Openbaar Ministerie

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

De publieke kern van het internet

Het internet is een internationaal succesverhaal van groei en innovatie. De basisinfrastructuur van het internet maakt de incorporatie van steeds nieuwe ideeën en toepassingen mogelijk, waardoor het online- en het offline-leven van steeds meer mensen versmolten raken. Maar daardoor doen zich ook nieuwe risico's voor. De toename van cybercrime, de kwetsbaarheid van vitale infrastructuren en de opkomst van veiligheidsvraagstukken in de digitale wereld maken dat staten hun terughoudendheid ten opzichte van het internet laten varen.

De WRR beargumenteert in dit rapport dat de protocollen en standaarden die tezamen de basisinfrastructuur van het internet vormen als een mondiaal publiek goed zijn te beschouwen. Voor Nederland heeft het internet grote sociaaleconomische betekenis. Het is daarom van groot belang het functioneren en de integriteit van de publieke kern van het internet veilig te stellen en die te beschermen tegen oneigenlijke interventies door staten en andere partijen. De WRR bepleit om het internet tot speerpunt van het buitenlands beleid te verheffen en formuleert aanbevelingen voor een diplomatieke agenda.

ISBN 978 90 4853 004 5

9 789048 530045

AUP.nl