ARTIKEL

Cyber Westfalen en het mondiale internet

Dennis Broeders

De diepe infrastructuur van het internet is te beschouwen als een mondiaal publiek goed. Alle staten hebben hun digitale economie, samenleving en bestuur gebouwd op deze 'publieke kern van het internet'. Toch gaan korte termijn-voordelen in de internationale politiek soms boven die van de lange termijn en veroorloven staten zich in het kader van nationale veiligheid steeds grotere vrijheden als het gaat om de publieke kern van het internet. Nationale veiligheid en internet-veiligheid – de veiligheid van het internet als infrastructuur – staan steeds vaker als waarden tegenover elkaar. Daarom is het van groot belang dat er gewerkt wordt aan het vastleggen en verspreiden van een internationale norm van non-interventie waarin de publieke kern van het internet aangemerkt wordt als een neutrale zone.

Twee cyber-gebeurtenissen van dit najaar illustreren dat het internet steeds meer een omstreden domein is geworden. De hacks van de DNC (Democratic National Committee) en de e-mail-account van John Podesta – de campagneleider van Hillary Clinton – brachten onder meer via Wikileaks veel ongecensureerde informatie uit het hart van de democratische presidentscampagne in de openbaarheid. Deze informatie heeft zonder twijfel het verloop van de Amerikaanse presidentsverkiezingen beïnvloed. Velen nemen aan dat Russische hackers – op instigatie van het Kremlin – achter deze openbaringen zaten.[1] Een nieuwe vorm van informatieoorlog die alleen in het digitale tijdperk mogelijk is, net zoals de omvang van de Snowden-lekken in een analoog tijdperk onmogelijk was geweest. De wereld is veranderd.

© Flickr / Nordiske Mediedager

'De omvang van de Snowden-lekken was in een analoog tijdperk onmogelijk geweest.'

In oktober 2016 werd de server van Dyn het slachtoffer van één van de grootste DDoS-aanvallen ooit. Vooral in de Verenigde Staten viel een groot deel van het internetverkeer uit en waren grote internetplatforms lange tijd niet bereikbaar. Een novum was dat het botnet dat de aanval uitvoerde voor een belangrijk deel bestond uit gehackte camera's, printers en zelf babyfoons die met het internet verbonden waren – het zogenaamde *Internet of Things* (IoT).

Wat minder werd gerapporteerd, was dat het doel van deze aanval een zogenaamde DNS-server was. Een DNS-server is onderdeel van de vitale infrastructuur van het internet en zorgt ervoor dat vragen in mensentaal – via een zoekmachine bijvoorbeeld – worden vertaald naar de IP-adressen waarmee het internet zelf verbindingen legt tussen gebruikers. De DNS-infrastructuur behoort tot wat de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) in 2015 heeft omschreven als de "publieke kern van het internet", die in toenemende mate behoefte heeft aan internationale bescherming.[2]

'Westfalisering' van het internet

Een hack en een cyber-aanval. Twee cyber-incidenten die geopolitiek gezien op hele verschillende problemen duiden. De DNC-hacks duiden op een politiek probleem, op inmenging van de ene staat in de politieke zaken van een andere staat. Op zichzelf niets nieuws, maar de nieuwe technologische mogelijkheden – en de *plausible deniability* die internetaanvallen vaak kenmerken – tellen wellicht op tot een kwalitatieve sprong. De Dyn-aanval raakt aan iets anders. Omdat deze aanval was gericht op de diepe infrastructuur van het internet, is de *fall out* breed en ongericht. Wie aan de fundamenten trekt, kan niet bij voorbaat volledig inschatten wat er omvalt.

Het eerste voorval hoort dan ook bij wat wel de 'Westfalisering'[3] van het internet wordt genoemd: het mondiale internet wordt onderdeel van de traditionele machtspolitiek van soevereine staten. De gedachte dat het internet een 'global commons' is – een gedachte die in de begindagen van het internet vaak als ideaal werd gehuldigd - is niet meer houdbaar in een wereld waarin het internet economisch, politiek en militair verknoopt is geraakt met nationale belangen en internationale veiligheid. Het feit dat het internet niet meer gezien kan worden als een ruimte die buiten het bereik en de invloed van staten floreert, wil echter nog niet zeggen dat er geen collectief internet meer bestaat. Delen van het internet kunnen en moeten als een mondiaal publiek goed gezien en behandeld worden, zowel om economische als om veiligheidsredenen.

Het internet als een onzuiver 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 decennia van zijn geschiedenis miljarden gebruikers en nieuwe toepassingen te accommoderen. Of zoals Vint Cerf – een van de 'vaders van het internet' – het formuleert: "de hulpbronnen van het internet, hoewel eindig, worden uitsluitend beperkt door ons vermogen meer hulpbronnen te creëren om de gedeelde virtuele ruimte van het internet en de bijbehorende applicaties te doen groeien."[4]

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 verwezenlijken 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.[5]

© Flickr / Tech.Co

'In de kern is het internet gemaakt om internationaal, zonder aanzien des persoons of nationaliteit, te functioneren.'

Deze redenering kan men toepassen op het internet als een netwerk en infrastructuur. Het collectieve is dan niet zozeer de inhoud van het www – waarover veel strijd is – maar juist het functioneren van het internet als systeem dat toepassingen als het www en inhoud daarvan mogelijk maakt. Laura DeNardis, hoogleraar Internet Governance aan de American University, 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".[6]

Non-exclusiviteit en non-rivaliteit

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, wat op zichzelf al uitsluitend is. Sommige overheden, zoals Egypte in 2011, hebben het internet in tijden van onrust en crisis zelfs een paar dagen uitgezet, door de netwerken buiten werking te stellen.

> De kracht van het internet is zijn groei geweest en het indrukwekkende vermogen in de eerste decennia van zijn bestaan miljarden gebruikers en nieuwe toepassingen te accommoderen

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 te citeren: “met uitzondering van repressieve politieke contexten van censuur, zijn de kernwaarden van het internet universaliteit, interoperabiliteit en toegankelijkheid”.[7] 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 is in die zin dus een onzuiver mondiaal publiek goed– zoals infrastructuur dat bijvoorbeeld ook is.

Het beschermen van de publieke kern van het internet

Gezien het belang van de internet-infrastructuur voor alle staten – alle staten hebben hun digitale economie, overheid en samenleving gebouwd op hetzelfde fundament – zou het beschermen van de publieke kern van het internet een haalbare zaak moeten zijn. Maar, zoals vaker, gaan korte termijn-voordelen in de internationale politiek soms boven die van de lange termijn. *Internet governance* is steeds sterker gepolitiseerd en in het bijzonder nationale veiligheid en internet-veiligheid – de veiligheid van het internet als infrastructuur - staan steeds vaker als waarden tegenover elkaar.

In het domein van de nationale veiligheid veroorloven staten zich steeds 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 functionerende internet-infrastructuur. Tezamen leiden deze ontwikkelingen echter wel tot een digitale variant van het *security dilemma*, 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.[8]

> Op het gebied van nationale veiligheid veroorloven staten zich steeds grotere vrijheden als het gaat om de publieke kern van het internet

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. De onthullingen over de NSA – die kwetsbaarheden in het internet-ecosysteem creëert en achterhoudt, en daarmee de veiligheid van het internet schaadt – geven een mooi voorbeeld.

De aanval op Dyn is een goede illustratie van het feit dat een gerichte aanval op de kerninfrastructuur van het internet niet louter meer een theoretische optie is. Internet security-expert Bruce Schneier waarschuwde in september jl. al dat iemand aan het verkennen was hoe de kerninfrastructuur van het internet met een aanval onderuit gehaald kan worden. Exact vaststellen wie is lastig, maar Schneier vermoedt dat het om statelijke actoren gaat en hij was niet te beroerd om China en Rusland als zijn beste gok aan de lezer mee te geven.[9]

Naar een norm van non-interventie

Tegen deze achtergrond is het van groot belang dat er gewerkt wordt aan het vastleggen van een internationale norm waarin de centrale protocollen van het internet– de publieke kern van het internet – aangemerkt worden als een neutrale zone, waarin overheidsbemoeienis omwille van nationale belangen niet geoorloofd is, zoals de WRR in 2015 betoogde. Gezien de grote internationale verdeeldheid en de geopolitieke onzekerheid over en binnen het cyberdomein, ligt het voor de hand te beginnen bij het formuleren van internationale normen en niet bij het inzetten op internationale verdragen.[10]

In het cyberdomein wordt al over normen gesproken in vele fora en conferenties, bijvoorbeeld ook in een serie van zogenoemde *Groups of Governmental Experts* (GGE's), die onder auspiciën van de VN, maar los van een verdrag, proberen vooruitgang te boeken en normen, principes en vertrouwenwekkende maatregelen vast te leggen op het terrein van het internet en internationale veiligheid.[11]

© Flickr / Fort George G. Meade Public Affairs Office

'Nationale veiligheid en internet-veiligheid staan steeds vaker als waarden tegenover elkaar.'

Het formuleren van de norm en het afbakenen van de publieke kern van het internet is in principe op twee manieren mogelijk: met een gelaagde of een functionele benadering. In de gelaagde benadering moet op minimaal drie niveaus vastgesteld worden wat tot de publieke kern behoort:

- De logische infrastructuur (bijvoorbeeld protocollen als TCP/IP, DNS, BGP, etc.)
- De fysieke infrastructuur (bijvoorbeeld DNS-servers, zeekabels, etc.)
- Vitale organisatie van het internet-ecosysteem (bijvoorbeeld CERT's, Internet Exchanges, etc.)

Een alternatief is de norm – en de publieke kern – functioneel te benaderen en in de norm niet zozeer de bestanddelen, maar de *functies* van de publieke kern te benoemen. Een werkbare formulering wordt dan bijvoorbeeld dat de norm de "algehele beschikbaarheid en integriteit van de kern 'forwarding and naming'-functies van het mondiale internet moet beschermen".[12] Deze formulering legt de kernfuncties van de publieke kern vast, waaruit vervolgens afgeleid kan worden welke onderdelen onder de norm vallen: te weten alles wat vitaal is voor de beschikbaarheid en integriteit van de 'forwarding and naming'-functies. Aangezien het proces van het uitwerken van internationale normen zich in diverse fora afspeelt, is het niet bij voorbaat nodig één benadering of één formulering van het idee van de publieke kern tot de norm te verheffen.

De weg voorwaarts

Sinds 2015 zijn er steeds meer stemmen opgegaan die de publieke kern van het internet – of vergelijkbare concepten – centraal stellen en willen beschermen. In juni 2016 publiceerde de Internet society een beta-versie van zijn *Policy Framework for an open and trusted Internet*; daarin staat dat de technische gemeenschap "a sense of collective stewardship towards the public core of the Internet and the open standards on which its technologies and networks are based" met elkaar deelt.[13] In dezelfde maand publiceerde de Global Commission on Internet Governance zijn langverwachte eindrapport genaamd *One Internet*. Een van de beleidsaanbevelingen gaat in essentie over de publieke kern van het internet: "Consistent with the recognition that parts of the Internet constitute a global public good, the commission urges member states of the United Nations to agree not to use cyber weapons against core infrastructure of the Internet."[14]

In Nederland publiceerde de regering in mei 2016 zijn officiële reactie op het WRR-rapport en nam daarin de bescherming van de publieke kern van het internet op als onderdeel van het buitenlands cyberbeleid.[15] De eerste gelegenheid waar de Nederlandse regering deze norm kan uitwerken en verspreiden, is de huidige ronde (2016-2017) van de UN GGE waarin Nederland één van de 25 deelnemende lidstaten is. Deze eerste stap wordt de komende jaren hopelijk vervolgd in andere VN-fora en relevante diplomatieke fora zoals de EU en de OVSE.

Noten

[1]
Zie bijv. de *long read* (http://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/) van Thomas Rid, hoogleraar Security Studies aan het King's College in Londen, op *Esquire*

[2]

Zie WRR (http://www.wrr.nl/fileadmin/nl/publicaties/PDF-Rapporten/De_publieke_kern_van_het_internet_def.pdf), *De Publieke kern van het internet. Naar een buitenlands internetbeleid*, Amsterdam: Amsterdam University Press, 2015.

[3]
Zie bijv.: C. Demchack & P. Dombrowksi, 'Rise of a cybered Westphalian age', *Strategic Studies Quarterly*, Spring 2011, pp. 32-61; en: D. Broeders. Westfalen 2.0? Internetvrijheid en buitenlands beleid. *Internationale Spectator*, jrg. 66 (2012), pp. 79-83.

[4]
V. Cerf, 'Revisiting the tragedy of the commons', *Communications of the ACM*, jrg. 56 (2013), nr. 10, p. 7.

[5]
WRR, *Minder pretentie, meer ambitie*, WRR rapporten aan de Regering, nr. 84, Amsterdam: Amsterdam University Press, 2010, pp. 196-197.

[6]
L. DeNardis, *The global war for internet governance*, New Haven: Yale University Press, 2014, p. 17.

[7]
L. DeNardis, *Internet points of control as global governance*, CIGI Internet Governance Papers nr. 2, augustus 2013, p. 4.

[8]
M. Dunn Cavelty, 'Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities', *Science and Engineering Ethics*, jrg. 20 (2014), nr. 3, pp. 701-715.

[9]
Bruce Schneier, 'Someone Is Learning How to Take Down the Internet (https://www.lawfareblog.com/someone-learning-how-take-down-internet)', 13 september 2016.

[10]
Zie voor een bespreking van normen-initiatieven in cyberspace: M. Finnemore & D. Hollis, 'Constructing Norms for Global Cybersecurity', *The American Journal of International Law,* jrg. 110 (2016), nr. 3, pp. 425-479.

[11]

A. Kane, '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*, jrg. 36 (2014), nr. 5, pp. 314-321; R. Hurwitz, 'The play of states: Norms and security in cyberspace', *American Foreign Policy Interests*, jrg. 36 (2014), nr. 5, pp. 322-331.

[12]
Een dergelijke formulering werd uitgewerkt in een internationale workshop over 'The Public Core of the Internet', georganiseerd door het Ministerie van Buitenlandse Zaken in Den Haag op 11 juli 2016.

[13]
Internet Society (http://www.internetsociety.org/sites/default/files/bp-Trust-20160621-en.pdf), *A policy framework for an open and trusted Internet An approach for reinforcing trust in an open environment*, 2016, p.7. (http://www.internetsociety.org/sites/default/files/bp-Trust-20160621-en.pdf)

[14]
Global Commission on Internet Governance, *One Internet* (https://www.ourinternet.org/sites/default/files/inline-files/GCIG_Final%20Report%20-%20USB.pdf), Centre for International Governance Innovation and Chatham House, 2016, p.75.

[15]
Minister van Buitenlandse Zaken (2016) Kamerbrief kabinetsreactie advies (https://www.rijksoverheid.nl/documenten/kamerstukken/2016/05/19/kabinetsreactie-op-aiv-advies-het-internet-een-wereldwijde-vrije-ruimtemet-begrensde-staatsmacht-enwrr-advies-de-publieke-kern-van-het-internet-naar-een-buitenlands-internetbeleid) 'Het internet: een wereldwijde vrije ruimte met begrensde staatsmacht' en advies 'De publieke kern van het internet: naar een buitenlands internetbeleid'.

Auteurs

Dennis Broeders
Senior wetenschappelijk medewerker bij de WRR en hoogleraar aan de Erasmus Universiteit Rotterdam ▸
(http://www.wrr.nl/bureau/staf/article/dennis-broeders/)