

Wendy Hoogeboom

SWING STATES

De positie van India en
Brazilië in het debat over
cyber governance

Swing states

De serie Working Papers omvat studies die in het kader van de werkzaamheden van de WRR tot stand zijn gekomen. De verantwoordelijkheid voor de inhoud en de ingenomen standpunten berust bij de auteurs. Een overzicht van alle webpublicaties is te vinden op deze website.

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

Swing states

DE POSITIE VAN INDIA EN BRAZILIË
IN HET DEBAT OVER CYBER
GOVERNANCE

Rapporten aan de Regering nrs. 68 t/m 94 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

Omslagafbeelding: Textcetera, Den Haag

Working Paper nummer 2

e-ISBN 978 94 90186 07 4 (pdf)

WRR, Den Haag 2015

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Voor zover het maken van kopieën uit deze uitgave is toegestaan op grond van artikel 16B Auteurswet 1912 j^o het Besluit van 20 juni 1974, Stb. 351, zoals gewijzigd bij het Besluit van 23 augustus 1985, Stb. 471 en artikel 17 Auteurswet 1912, dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht (Postbus 3051, 2130 KB Hoofddorp). Voor het overnemen van gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (artikel 16 Auteurswet 1912) dient men zich tot de uitgever te wenden.

INHOUDSOPGAVE

1.	Inleiding	7
2.	Het internet in de swing states	9
2.1	Internet in Brazilië	9
2.2	Internet in India	9
3.	Beleid en internetvrijheid	11
3.1	Nationaal beleid van Brazilië	11
3.2	Internetvrijheid in Brazilië	13
3.3	Nationaal beleid van India	14
3.4	Internetvrijheid in India	16
4.	WCIT Dubai 2012	19
4.1	Positie van Brazilië op het WCIT 2012	21
4.2	Positie van India op het WCIT 2012	22
5.	NSA-onthullingen	25
5.1	De reactie vanuit Brazilië op de NSA-onthullingen	26
5.2	De reactie vanuit India op de NSA-onthullingen	28
6.	Conclusie	31
	Noten	33
	Literatuur	37

1. INLEIDING

Het internet heeft zich historisch gezien vooral ontwikkeld in de Verenigde Staten en andere westerse geïndustrialiseerde landen. Hierdoor geeft het internationale internet-governancesysteem voornamelijk de normen en waarden van deze landen weer (Ebert & Maurer 2013a; Deibert & Rohozinski 2011:25). Het huidige internet-governancemodel wordt beschreven als een multistakeholder-governancesysteem. Het bestaat uit overheden, private partijen en niet-gouvernementele organisaties. De leidende rol van de Verenigde Staten in internet-governance vormt volgens sommigen een anomalie van het multistakeholder-model (Eber & Maurer 2013a).

Het internet is sinds zijn ontstaan enorm gegroeid en heeft er steeds meer gebruikers bij gekregen. Momenteel komen de nieuwe gebruikers voornamelijk uit niet-westerse landen. Er is een demografische verschuiving in *cyberspace* gaande: steeds meer internetgebruikers komen uit het Zuiden en Oosten en niet zoals eerst uit het Noorden en Westen (Deiber & Rohozinski 2011:25).

De BRIC-landen, Brazilië, Rusland, India en China, zijn landen in het Zuiden en Oosten die een enorme groei doormaken (Wilson & Purushothaman 2006). Ebert en Maurer (2013a) beargumenteren dat deze opkomende machten in het wereldsysteem in toenemende mate het heersende internet-governancemodel betwisten. Volgens Deibert en Rohozinski (2011) is er momenteel een gezagscrisis in het cyberdomein. Er is in feite onenigheid over bijna alles, van wat aanvaardbaar gedrag is in *cyberspace* tot aan de formele en informele regels en praktijken die de basis vormen waarop het netwerk zelf is gestructureerd en wordt bestuurd.

China en Rusland nemen in dit internationale debat een duidelijke positie in en het is onwaarschijnlijk dat zij die snel zullen wijzigen. Volgens Ebert en Maurer (2013a) betwisten China en Rusland de macht van de Verenigde Staten over het internet met een *sovereignist*-benadering, waarin ze trachten een meer traditionele territoriale controle over *cyberspace* te bewerkstelligen. Deze landen streven naar een internet-governancemodel waarin staten de leiding hebben, om op die manier veiligheidskwesties op te lossen. Deze territoriale controle over het internet willen zij bereiken door middel van intergouvernementele organisaties zoals de VN en de ITU. In 2011 namen China en Rusland bijvoorbeeld het voortouw bij het indienen van een gezamenlijk voorstel over een internationale gedragscode voor informatiebeveiliging bij de Verenigde Naties. Hiermee hebben ze de huidige situatie in internet-governance betwist en vroegen ze eigenlijk om een heroverweging van de internationale waarden die ontwikkeld zijn door het Westen (Lewis 2013).

Lewis beargumenteert dat het vergroten van soevereine controle in *cyberspace* mogelijk leidt tot beperking van mensenrechten zoals de toegang tot informatie of de vrijheid van meningsuiting. De wrijving tussen het vergroten van soevereine controle op het internet en de universele mensenrechten is één van de belangrijke twistpunten in het debat over internationale internet-governance.

India en Brazilië betwisten de leidende rol van de Verenigde Staten op het internet anders dan China en Rusland. Zij hebben bijvoorbeeld een veel sterkere binding met de vrijheid van meningsuiting. Toch wijken ze op een interessante manier af van het internetbeleid van de Verenigde Staten en Europa (Faris & Gasser 2013). Volgens Ebert en Maurer (2013a) worden India en Brazilië in toenemende mate gezien als *swing states* in het internationale debat. Ze hebben de wil om bij te dragen aan de wereldwijde normen van de 21e eeuw, maar ze zijn voorzichtig om in het debat al een positie in te nemen. Ze kijken welke benadering het meest aansluit bij hun nationale belangen. Volgens Clemente (2013) moeten voorstanders van het multistakeholder- (of open) internet-governancemodel de politieke en economische motivaties en beperkingen van de *swing states* erkennen en begrijpen. Nu het huidige model van de westerse landen onder druk komt te staan, is het voor landen zoals Nederland belangrijk om een argument te formuleren waarmee ze de *swing states* kunnen overtuigen om samen een breed gesteund internationaal internet-governancemodel te creëren (Lewis 2013).

De nog onbesliste positie van Brazilië en India in het internationale debat over het cyberdomein wordt in dit paper nader besproken. In het eerste deel wordt een algemeen beeld geschetst van het internet, het nationale internetbeleid en de internetvrijheid in India en Brazilië. In het tweede deel wordt gekeken welke internationale positie de twee landen innamen bij twee gebeurtenissen, namelijk het WCIT in Dubai in 2012 en de onthullingen over de NSA van Snowden sinds de zomer van 2013.

2. HET INTERNET IN DE SWING STATES

2.1 INTERNET IN BRAZILIË

Brazilië werd in 1990 voor het eerst verbonden aan het internet en sindsdien maken steeds meer Brazillianen er gebruik van. Het internetgebruik nam de afgelopen jaren vooral toe door de opkomst van mobiele technologie (Freedom House 2013a). In 2012 maakte bijna de helft, 49,9 procent¹, van de bevolking gebruik van het internet: 99 miljoen mensen van een bevolking van 198,7 miljoen.² In 2000 maakte 2,9 procent¹ van de bevolking gebruik van het internet en in 2006 28,2 procent.¹

Brazilië maakt een soortgelijke ontwikkeling door als China en Rusland. In 2000 maakte in zowel Rusland als China minder dan twee procent¹ van de bevolking gebruik van het internet. In 2012 was dit gestegen tot 53,3 procent¹ voor Rusland en 42,3 procent¹ voor China. Net als in Brazilië is dit percentage gestegen tot rond de helft van de bevolking. De internetpenetratie ligt nog steeds achter bij het gemiddelde van de westerse landen, maar Brazilië is wel aan het inlopen op landen zoals de Verenigde Staten.

In Zuid-Amerika is Brazilië één van de landen met een relatief hoge internetpenetratie. In drie andere landen maken er relatief meer mensen gebruik van het internet. Chili heeft met 61 procent³ de hoogste internetpenetratie. In Paraguay maakte in 2012 27 procent³ van de bevolking gebruik van het internet, het laagste aantal in Zuid-Amerika.

Door haar vele inwoners heeft Brazilië de grootste internetpopulatie van Zuid-Amerika (Varon Ferraz & Maciel 2012). Met de aanleg van intercontinentale kabels die Brazilië met de Verenigde Staten, Europa en Afrika verbindt en kabels over land naar de andere Zuid-Amerikaanse landen, probeert Brazilië zijn internationale internetverbindingen te verbeteren. Vooral de landen die niet aan zee liggen, zoals Paraguay en Bolivia, zijn afhankelijk van de internationale kabelsystemen via de landen aan de kust en met name via Brazilië.⁴

2.2 INTERNET IN INDIA

De informatietechnologie-industrie in India, waaronder ook IT-diensten vallen, is zeer uitgebreid (Shih, et al. 2013). Toch maakte in India in 2012 slechts 12,6 procent³ van de bevolking gebruik van het internet. Het is een relatief laag percentage vergeleken met andere landen, maar met 1,237 miljard⁵ inwoners zijn dat nog altijd 155,6 miljoen internetgebruikers. In 2000 maakte 0,5 procent³ van de inwoners gebruik van het internet; in 2006 was de internetpenetratie gestegen tot

2,8 procent.³ In India maken meer mensen gebruik van het internet dan in Rusland en Brazilië. India is het derde land, na China en de Verenigde Staten, qua absolute aantal internetgebruikers.

Wat betreft internetpenetratie komt de regio Azië op de zesde plek. Azië heeft een potentiële internetpopulatie van 42 procent, het hoogste aantal per regio. In de komende jaren zullen er hoogstwaarschijnlijk veel nieuwe gebruikers van het internet uit India komen (Deibert & Rohozinski 2011:27). India is niet de enige potentiële grote speler in Azië; China heeft nu al 571 miljoen internetgebruikers en is daarmee de andere grote reus in de regio. De Verenigde Staten ziet India soms als het eventuele tegenwicht van China in de regio.⁶

3. BELEID EN INTERNETVRIJHEID

In het artikel “*Contested Cyberspace and Rising Powers*” beargumenteren Ebert en Maurer (2013) dat de internationale positie van landen in het cyberdomein voor een aanzienlijk deel worden bepaald door het politieke stelsel, het binnenlandse beleid en de binnenlandse actoren. Om de internationale positie van Brazilië en India bij het WCIT in 2012 en na de onthullingen over de NSA te kunnen doorgronden, is het van belang om de institutionele verhoudingen in de landen zelf te beschrijven. Dit hoofdstuk gaat daarom over de status van het nationale beleid over het cyberdomein en beschrijft welke departementen en organisaties een aandeel hebben in het maken en uitvoeren van het beleid. Ook wordt besproken wat de status is van internetvrijheid en welke binnenlandse discussies er plaatsvinden over internetvrijheid. De nadruk ligt hierbij op de debatten rondom internetvrijheid, om op die manier inzicht te geven in de binnenlandse verhoudingen.

3.1 NATIONAAL BELEID VAN BRAZILIË

De internetpenetratie van Brazilië blijft nog achter bij die van de westerse landen door onder andere een gebrekkige infrastructuur, sociale ongelijkheid en gebrek aan onderwijs. De afgelopen jaren is de Braziliaanse overheid een aantal projecten gestart om meer Brazilianen met het internet te verbinden. Het *National Broadband Plan* is bijvoorbeeld begonnen in 2010 met als streven om de toegang tot breedband-internet te verdrievoudigen in 2014. Daarnaast kondigde de overheid in 2012 een reeks investeringen en belastingprijkkels aan om diverse ICT- en technologische capaciteiten in het hele land uit te breiden. Door de vernieuwing van het *One Laptop per Child*-programma wordt er aandacht besteed aan het gebrekkige onderwijs, wordt geprobeerd de computervaardigheden van kinderen te verbeteren en om onderwijs in het algemeen toegankelijker te maken voor kinderen. Mede door dit beleid is het gebruik van sociale media en de maatschappelijke participatie door middel van het internet gestegen (*Freedom House* 2013a).

Nu Brazilië dichterbij het niveau van westerse landen komt en steeds meer een genetwerkte samenleving wordt, komen kwesties zoals *cybercrime*, DDoS-aanvallen en toegang tot publieke informatie steeds meer onder de aandacht van de Braziliaanse overheid. De overheid heeft de toegankelijkheid van institutionele websites en de kwaliteit van informatie op deze websites verbeterd (*Freedom House* 2013a). De verhoogde aandacht voor cyberdreigingen heeft ertoe geleid dat er een aantal wetsvoorstellen is ontworpen om het internet beter te kunnen reguleren, voornamelijk voor wat betreft internetcriminaliteit. Een bekend wetsvoorstel is de wet 84/99 waarin onder andere de politie meer bevoegdheden krijgt.

De wet leidde echter tot veel kritiek vanuit de samenleving. Volgens sommigen worden gedragingen gecriminaliseerd die eigenlijk onbeduidend zijn (*Observatório da internet.br* 2011: 13-18).

In Brazilië zijn er verschillende overheidspartijen die zich bezighouden met het nationale cyberbeleid. Eén van deze partijen is het *Brazilian Internet Steering Committee (CGI.br)*, een multistakeholder-model voor internet-governance met 21 vertegenwoordigers uit de private sector, de technologische en wetenschappelijke gemeenschap, de overheid en de *civil society*. CGI.br is opgericht in 1995 en heeft een vrij grote rol in het internetbeleid. Het heeft onder andere een mandaat om strategische richtlijnen voor het gebruik en de ontwikkeling van internet vast te stellen. De CGI.br werkt samen met de *Division on Information Society* van het ministerie van Buitenlandse Zaken. Deze afdeling speelt een rol in de Braziliaanse vertegenwoordiging in internationale internet-governance, bijvoorbeeld bij het *Internet Governance Forum (Global Partners Digital 2013)*.

Anatel, de *Brazilian Telecommunications Regulatory Agency*, is samen met het ministerie van Communicatie tevens een invloedrijke partij in het Braziliaanse cyberbeleid. Het is een onafhankelijke organisatie voor de ontwikkeling van telecommunicatie en telecommunicatie-infrastructuur. Anatel vertegenwoordigt Brazilië ook in internationale telecommunicatiebijeenkomsten zoals het ITU. Het is opgericht door het ministerie van Communicatie en werkt nog altijd veel samen met dit ministerie (*Global Partners Digital 2013*).

Het *Department of Information and Communication Security* is de 'cybersecurity-afdeling' van de overheid, opgericht door *The Institutional Security Cabinet of the President's Office*. Het departement is verantwoordelijk voor de planning en coördinatie van cyberveiligheid, informatie- en communicatieveiligheid van Brazilië. In 2010 bracht dit departement twee publicaties uit, één over de beveiliging van kritieke informatie-infrastructuren en de *Green Book on Brazil's Cybersecurity*, over de uitdagingen die Brazilië moet aangaan op het gebied van *cybersecurity*. De *Green Book* is geschreven om de Brazilianen bewust te maken van het belang van *cybersecurity*. Met die kennis kunnen de Brazilianen volgens het departement actief participeren in het debat over het *Nationaal Cybersecurity Beleid*, dat waarschijnlijk in de nabije toekomst wordt vastgesteld (Canabarro & Borne 2013:7).

Het ministerie van Defensie heeft ook een rol in *cybersecurity*. Sinds de *Nationale Strategie Defensie* van 2008 is *cyber* een strategisch gebied voor het Braziliaanse leger. In 2010 is hierin een kerngroep opgericht die het *Cyber Defence Centre (CDCiber)* is gestart. De begroting van dit centrum was afgelopen jaar ongeveer 90 miljoen Braziliaanse Real, ongeveer 28 miljoen euro.⁷ In 2012 verscheen nog een beleidsstuk waarin de defensie-cybermaatregelen nader worden toegelicht. Al die

acties tezamen zijn het *Cyber Defense Project*, waarin tot 2031 bijna 840 miljoen Braziliaanse Real, ongeveer 261,4 miljoen euro, wordt geïnvesteerd (Canabarro & Borne 2013).

3.2 INTERNETVRIJHEID IN BRAZILIË

In Brazilië wordt het internet niet systematisch gefilterd: het is grotendeels vrij (*Freedom House* 2013a; Deibert et al. 2008). Bij regulatie van het internet gaat het in Brazilië meestal om kwesties zoals kinderporno of het beperken van de toegang voor kinderen tot voor hun leeftijd ongeschikt materiaal (Deibert et al. 2008). Wel verzoekt de overheid geregeld socialmediabedrijven zoals Google en Twitter om inhoud te verwijderen. Voorafgaand aan de gemeenteraadsverkiezingen in 2012 waren er bijvoorbeeld veel verzoeken om inhoud te verwijderen die inbreuk maakte op de verkiezingswet. De wet verbiedt elke inhoud die een verkiezingskandidaat belachelijk maakt of beledigt. Hiermee wordt de vrijheid van meningsuiting *online* direct beïnvloed. De afgelopen jaren laten een stijgende trend zien in de hoeveelheid bedreigingen, intimidatie en geweld tegen online-journalisten en bloggers, wat kan leiden tot zelfcensuur (*Freedom House* 2013a).

Brazilië is al enige tijd in de ban van een nationaal debat, het debat over *Marco Civil*, een wetsvoorstel met als onderwerp het internetbeleid. Allereerst volgt hier de ontstaanswijze van het voorstel. Brazilië heeft tien principes voor de *governance* en het gebruik van het internet in Brazilië opgesteld, als een reactie op de eerdere *cybersecurity*-wetten. Dit initiatief is uitgegroeid tot een kans om een positieve agenda voor internetbeleid in Brazilië te ontwikkelen (*Global Partners Digital* 2013). CGI.br heeft het voortouw genomen bij het opstellen van deze principes en het proces is mede gesponsord door vijf ministeries. De principes zijn tot standgekomen door een twee jaar lang durend *online* publiek raadplegingsproces. Internetgebruikers konden rechtstreeks via de website commentaar leveren op elke paragraaf in de conceptversie. Er werden meer dan 2000 bijdragen ontvangen, die in latere versies werden verwerkt. Tijdens het consultatieproces vonden er verhitte discussies plaats over de balans tussen het recht op *privacy* voor gebruikers en de belangen van de overheid om de veiligheid te verhogen, en over de rechten van individuen en de ambities van de private sector (Ebert & Maurer 2013a:1064; *Global Partners Digital* 2013). Uiteindelijk zijn er tien progressieve principes opgesteld en goedgekeurd over de vrijheid van meningsuiting, privacy en mensenrechten, innovatie, democratisch en collaboratief bestuur, universele toegang, stabiliteit, veiligheid en functionaliteit van het web, en netneutraliteit (*Observatório da internet.br* 2011: 19-35).

Op basis van de tien principes hebben het ministerie van Justitie en het *Center for Technology and Society (CTS/FGV)*, een Braziliaanse denktank over internetbeleid, een wetsvoorstel ontwikkeld, *Marco Civil da Internet*, oftewel *Marco Civil*. Er deed

zich echter een politieke verandering voor: na zijn tweede termijn werd President Lula opgevolgd door Dilma Rousseff, die een iets conservatiever, links georiënteerd beleid begon. ICT bleef een strategische prioriteit, maar het aantal initiatieven zoals open online-consultaties of andere innovatieve en progressieve internet-initiatieven nam af. Daarnaast klonk de mening van de telecommunicatiebedrijven bij het ministerie van Communicatie en Anatel weer sterker door in de besluitvorming (*Global Partners Digital* 2013). In 2012 stond Brazilië op het punt om de wet aan te nemen, maar zij werd uiteindelijk tegengehouden door de lobby van de telecommunicatiebedrijven. De bedrijven ageerden onder andere tegen de bepalingen over netneutraliteit (Ebert & Maurer 2013a:1064). Zij waren van mening dat de regulatie van netneutraliteit bij Anatel moest komen te liggen en niet bij CGI.br. Brazilië is een sterk voorstander van de vrijheid van meningsuiting. Een uitspraak van het hoogerechtshof in 2009, die de vrijheid van meningsuiting en een actieve *civil society* versterkt, onderstreept dit (Ebert & Maurer 2013:1064). De *civil society* is in Brazilië actief betrokken in het debat rondom *Marco Civil*. De *Marco Civil* en de tien principes worden door de Braziliaanse overheid als voorbeeld gebruikt bij internationale bijeenkomsten zoals het *Internet Governance Forum* of regionale bijeenkomsten.

Het is nog afwachten of, en in welke vorm, de *Marco Civil* wordt aangenomen, maar de wet in zijn originele vorm wordt door de internationale *civil society* gezien als een innovatief en positief voorbeeld van internetbeleid (*Global Partners Digital* 2013).

3.3 NATIONAAL BELEID VAN INDIA

India is bekend om zijn IT-diensten en is in de software-industrie een grote wereldwijde speler (Shih et al. 2013). De overheid hecht veel belang aan de IT-industrie en aan het gebruik van IT voor sociaal-economische ontwikkeling (*Global Partners Digital* 2013:16). In het nationale cybersecurity-beleid van 2013 wordt de IT genoemd als één van de meest significante groeikatalysatoren van de Indiase economie (*Department of Electronics and Information Technology* 2013). De overheid benadrukt daarom het belang van nationaal beleid voor de IT-industrie. Het beleid voor de IT-industrie is goed ontwikkeld op nationaal niveau (*Global Partners Digital* 2013:16). Beleidsvoorbeelden waarmee de Indiase overheid de IT-industrie probeert te stimuleren zijn belastingvoordelen voor de IT-industrie en het verbeteren van de infrastructuur door middel van IT-investeringsregio's.⁸

In India houden verschillende overheidspartijen zich bezig met beleid op het gebied van *cyber*. Een grote partij is het ministerie van Communicatie en Informatie Technologie, dat uiteenvalt in het *Department of Electronics and Information Technology* (DeitY), het *Department of Telecommunications* en het *Department of Posts*. Het eerste departement (DeitY) is de centrale speler in internet-governance in India (*Global Partners Digital* 2013:17). De CERT-IN, India's CERT, valt bijvoor-

beeld onder dit departement. Het DeitY heeft in de zomer van 2013 een nationaal cybersecurity-beleid gepubliceerd (*Department of Electronics and Information Technology* 2013). Het betreft actief verschillende *stakeholders*, zoals de *civil society* en het bedrijfsleven, bij het opstellen van internetbeleid. Het tweede departement, het departement van Telecommunicatie, heeft een meer traditioneel technisch telecomperspectief en vertegenwoordigt India bijvoorbeeld op bijeenkomsten van de ITU (*Global Partners Digital* 2013:18).

In 2013 heeft DeitY een nationaal cybersecurity-beleid bekendgemaakt om een veilige en veerkrachtige *cyberspace* te maken voor burgers, bedrijven en de overheid. De belangrijkste doelen ervan zijn om informatie en de informatie-infrastructuur te beschermen, om de vaardigheden te vergroten voor het reageren op cyberdreigingen of om dreigingen te voorkomen, om kwetsbaarheden te verkleinen en schade van incidenten te verminderen door middel van een combinatie van institutionele structuren, mensen, processen, technologie en samenwerking. De komende vijf jaar worden hiertoe 500.000 mensen in *cybersecurity* opgeleid en wordt een effectieve publiek-private samenwerking ontwikkeld. Ook wordt een nationale instantie aangewezen die alle zaken met betrekking tot *cybersecurity* coördineert, met duidelijk omschreven taken en verantwoordelijkheden (*Department of Electronics and Information Technology* 2013).

Het *Centre for Internet and Society* geeft aan dat het nationale cybersecurity-beleid een stap in de goede richting is: het omvat veel van de meest dringende onderwerpen in *cybersecurity* en heeft ambitieuze doelstellingen. Er is echter een gebrek aan diepgang in het beleid: om de beleidsdoelen te vertalen in een effectieve strategie moet er een veel gedetailleerder stappenplan komen. En er wordt niet beschreven welke taken en verantwoordelijkheden de nationale instantie die alle zaken rondom *cybersecurity* zou moeten coördineren, krijgt. Bij het ontwikkelen van publiek-private samenwerking wordt verder niet vermeld hoe dat in zijn werk moet gaan. Het *Centre for Internet and Society* is wel positief over de inzet om de *privacy* van burgers te waarborgen, hoewel het beleid niet specifiek genoeg de reikwijdte van deze waarborgen beschrijft.⁹

De NIB, de *National Information Board*, is het hoogste nationale beleidsorgaan belast met informatiebeveiliging en de coördinatie van alle aspecten rondom informatiebeveiliging in India. De NIB bestaat uit vertegenwoordigers van relevante departementen en instanties (*Department of Information Technology* 2011). Door deze samenstelling komt de NIB alleen weinig bijeen en is daardoor niet altijd even effectief (*IDS Task Force Report* 2012:27). De *National Security Council Secretariat* (NSCS) fungeert als het secretariaat van de NIB. Het kijkt naar de politieke, economische, energie en strategische veiligheidsbelangen van India (*Department of Information Technology* 2011).

Sinds 2005 wordt er meer aandacht aan *cyberwarfare* besteed, doordat India bezorgd was over de groeiende militaire cyber-capaciteiten van Pakistan en China (Ebert & Maurer 2013a:1061). In augustus 2010 heeft de Indiase regering overheidsinstanties opgedragen om hun vaardigheden in *cyberwarfare* te vergroten. De overheidsinstanties kregen de opdracht om vaardigheden te ontwikkelen waarmee zij konden inbreken in netwerken van vijandige landen, om laboratoria op te zetten om cyber-aanvallen na te bootsen, om testfaciliteiten op te zetten, om tegenmaatregelen te ontwikkelen en om verschillende CERTs (*Computer Emergency Response Teams*, red.) op te zetten, waaronder een defensie-CERT. De overheidsinstanties die zich vooral bezighouden met het uitvoeren van de strategie van 2010 zijn de *National Technical Research Organization*, de *Defense Intelligence Agency*, en de *Defense Research and Development Organization*. De verhoogde aandacht voor *cybersecurity* op militair gebied in India is versterkt door een aantal incidenten: de vondst van een Chinese variant van de Stuxnet-worm in Indiase installaties en hackincidenten vanuit Pakistan zoals het onleesbaar maken van de website van *India's Central Bureau of Investigation* (Carr 2012:250).

3.4 INTERNETVRIJHEID IN INDIA

Over het algemeen respecteert de Indiase overheid de vrijheid van meningsuiting en geeft zij verschillende politieke, sociale en economische overtuigingen de ruimte. Op het internet maakt de overheid echter gebruik van selectief filteren. Bij bepaalde politieke en sociale conflicten vindt er censuur plaats bij *online* media, discussies, blogs en andere inhoud. Dit gebeurt met name bij sociale onrust en bij conflicten tussen kasten of religieuze groepen. In het conflict met Pakistan wordt er materiaal gecensureerd waarvan de overheid inschat dat het aanzet tot geweld. Soms worden journalisten en bloggers bedreigd, maar dat doen vooral politieke, religieuze of etnisch-nationalistische groepen en niet de overheid (*OpenNet Initiative* 2012; Freedom House 2013b).

De gewijzigde IT-wet van 2008 heeft de overheid de macht gegeven om elke inhoud *online* te blokkeren in het belang van defensie, nationale veiligheid, soevereiniteit, vriendschappelijke relaties met andere staten, en openbare orde. In 2007 rapporteerde het *OpenNet Initiative* dat politieke en sociale inhoud op het internet in India niet werd gefilterd, maar sindsdien is het filteren toegenomen (Freedom House 2013b). CERT-IN is door het departement van informatietechnologie in de gewijzigde IT-wet opgericht om het filteren uit te voeren (*OpenNet Initiative* 2012). De *state surveillance* is toegenomen in schaal en in geavanceerdheid, maar er is nog een ontoereikend privacy-wetgevingskader. In 2013 is India begonnen met de overgang naar een nationaal surveillance-project, het *Central Monitoring System* (CMS), dat verschillende overheidsinstanties toestaat om elektronische verkeer

te monitoren zonder de medewerking van de *serviceproviders* en zonder gerechtelijk toezicht. Er is weinig transparantie rondom het opzetten van het CMS en het systeem is nooit door het parlement beoordeeld (*Freedom House* 2013b).

Momenteel vindt er in India geen *systematisch* filteren plaats op het internet (*Freedom House* 2013b). Ook het selectieve filteren door de overheid is niet altijd effectief, omdat de overheid een slecht begrip heeft van de techniek. Gebruikers hebben daardoor manieren gevonden om aan het filteren te ontkomen (*OpenNet Initiative* 2012: 305). Daarnaast steunt India in het internationale debat het belang van internetvrijheid (*Global Partners Digital* 2013:16).¹⁰

Het selectieve filteren van inhoud op het internet heeft ook geleid tot weerstand. Er is een sterke *civil society* in India die betrokken is bij de debatten en pleit voor internetvrijheid (Ebert & Maurer 2013:1064-1065; *OpenNet Initiative* 2012; *Freedom House* 2013b). De *civil society* raakte vooral gemobiliseerd en betrokken in het debat over internet-governance vanaf 2011, toen India een voorstel indiende bij de Verenigde Naties over een *UN Committee on Internet Related Policy (CIRP)*. Zij waren tegen het voorstel van de overheid om een wereldwijd VN-comité aan te stellen dat de inhoud op het internet reguleerde. Volgens de *civil society* heeft de overheid een unilaterale beslissing genomen over internet-governance zonder dit te bespreken met afgevaardigden van de *civil society*, de industrie en academici. Deze kritiek leidde ertoe dat de overheid in gesprek ging met de *civil society* en andere partijen. In New Delhi vond bijvoorbeeld in oktober 2012 de eerste multi-stakeholder-*India Internet Governance-Conferentie* plaats (Ebert & Maurer 2013:1065).

4. WCIT DUBAI 2012

In december 2012 kwamen vertegenwoordigers van 139 landen bijeen in Dubai op de *World Conference on International Telecommunication* (WCIT). Tijdens deze conferentie onderhandelden diplomaten over een herziene versie van de *International Telecommunication Regulations* (ITRs). De ITRs zijn aangenomen in 1988 als een internationaal verdrag met een bindend effect onder internationaal recht op de landen die de ITRs ondertekenen en ratificeren. In de regelgeving staan algemene principes over de levering en werking van internationale telecommunicatiediensten en over de onderliggende internationale telecommunicatietransportmiddelen die gebruikt worden om de diensten te leveren. Deze principes zijn opgesteld om de doelstellingen van de ITU te bewerkstelligen, om de ontwikkeling van telecomdiensten en hun meest efficiënte werking te bevorderen en de ontwikkeling van faciliteiten voor wereldwijde telecommunicatiediensten te harmoniseren voor verschillende staten (Hill 2013:314). Het verdrag vereist dat lidstaten ervoor zorgen dat telecommunicatiebedrijven, vaak staatseigendom, zich houden aan de ITRs (Maurer 2012).

In 2012 werd door de lidstaten van de ITU besloten dat het noodzakelijk was om de ITRs te herzien, omdat er sinds 1988 structurele en technologische veranderingen hadden plaatsgevonden. Specifieke veranderingen waren de privatisering en liberalisering van telecommunicatiebedrijven en de groei van mobiele en IP-gebaseerde netwerken (Hill 2013:313-314).

In 1988 stond het internet nog in zijn kinderschoenen en is daarom niet vermeld in het verdrag. Hierdoor bleef het buiten de regelgeving met betrekking tot telecommunicatie, hoewel het groeide en verbonden raakte met commerciële netwerken. In plaats daarvan is er een multistakeholder-governancesysteem ontstaan dat bestaat uit de *civil society*, de private sector en overheden (Maurer 2012). Het multistakeholder-model wordt gezien als een mogelijkheid voor 'stakeholders' om toegang te krijgen tot statelijke internationale organisaties. Het multistakeholder-model wordt echter in de praktijk gekenmerkt door de leidende rol van de Verenigde Staten in internet-governance en de relatie tussen ICANN en de Verenigde Staten (Ebert en Maurer 2013a:1057).

Alle lidstaten van de ITU dienden voorafgaand aan Dubai 2012 hun voorstellen voor de herziening van de ITRs in. De voorstellen vormden de basis voor de onderhandelingen tijdens het WCIT (Maurer 2012). Een groot deel van de ITRs van 1988 werd behouden, alleen werden er enkele wijzigingen aangebracht om ze aan te passen aan de huidige tijd. Artikel 8 over *charging* en *accounting* werd gemoderiseerd: er werden bijvoorbeeld bepalingen toegevoegd over commerciële overeenkomsten of om investeringen aan te moedigen. Er werden ook nieuwe bepalingen toegevoegd om misbruik van telefoonnummers te voorkomen, om de

overdracht van nummerweergave te garanderen, om transparantie van internationale roamingtarieven te garanderen, om de veiligheid van netwerken te verbeteren, om spam te bestrijden, om energie-efficiëntie te verbeteren en e-afval te verminderen, en om het gebruik van telecommunicatie voor mensen met een handicap te vergemakkelijken (Hill 2013).

Tijdens de onderhandelingen werd duidelijk dat bepaalde landen fundamenteel van standpunt verschilden. Een groep landen, waaronder de Verenigde Staten en de gehele Europese Unie, was van mening dat er met de vernieuwde ITRs een nieuw internationaal regelgevingsregime voor het internet ontstond en dat de ITRs nieuwe bevoegdheden aan de ITU gaven. De nieuwe ITRs bedreigden volgens de groep het huidige multistakeholder-model, de economische groei en de vrijheid van meningsuiting wereldwijd. Een bepaling in de preambule van de ITRs zou tot nieuwe rechten voor staten leiden en daardoor een bedreiging voor individuele rechten zijn. Nieuwe artikelen in de ITRs over veiligheid en spam zouden een uitnodiging voor overheden zijn om inhoud-gebaseerde actie te ondernemen, hetgeen zou kunnen leiden tot beperking van vrijheid van meningsuiting op het internet. Tijdens de onderhandelingen zijn daarom bepaalde bepalingen verplaatst uit de tekst van de ITRs naar een aparte, niet-bindende resolutie, resolutie 3. De bepalingen in resolutie 3 zorgden volgens deze landen voor een uitbreiding van de rol van de ITU in internet-governance. Doordat de ITU een intergouvernementele organisatie is, geeft de resolutie meer macht aan staten en minder aan de *stakeholders* (Hill 2013).

Er ontstond een tweedeling, doordat een andere groep landen, onder andere China en Rusland, zich wel sterk maakte voor de genoemde kwesties. China en Rusland zijn meer gefocust op veiligheidsissues, zoals het beperken van spam, en minder op individuele rechten. Ze zijn meer *sovereignist* ten opzichte van internet-governance en willen meer nationale controle over het cyberdomein. Deze territoriale controle willen zij bewerkstelligen door middel van intergouvernementele organisaties zoals de ITU (Ebert & Maurer 2013). Op de WCIT ontstond een discussie over de internationale governance van het internet, waardoor een aantal landen weigerde de nieuwe ITRs te ondertekenen. Er was een brede consensus over ongeveer negentig procent van het verdrag, maar tien procent van het verdrag werd gezien als controversieel (Hill 2013:315).

Op het WCIT waren ook landen aanwezig die tussen de hiervoor genoemde uitersten instonden. Sommige landen waren er bijvoorbeeld een voorstander van om een intergouvernementele organisatie zoals de ITU nieuwe bevoegdheden te geven om daarmee de leidende rol van de Verenigde Staten te beperken (Ebert & Maurer 2013:1060). Uiteindelijk ondertekenden 89 landen de vernieuwde versie van de ITRs; 55 landen weigerden (Hill 2013:314).

4.1 POSITIE VAN BRAZILIË OP HET WCIT 2012

Brazilië heeft de vernieuwde versie van de ITRs wel ondertekend tijdens het WCIT in 2012 en had geen bezwaar tegen resolutie 3. Brazilië steunde het idee van een actualisatie van de ITRs. De ITRs moesten gebaseerd worden op beginselen van hoog niveau, die afgeleid werden van de traditionele aspecten van telecommunicatie. De meeste voorstellen van Brazilië waren gericht op beoordeling en tariefbepaling, in het bijzonder bij mobiele *roaming*. Van tevoren gaf de Braziliaanse overheid aan dat er in het debat onderscheid moest worden gemaakt tussen telecommunicatie en de inhoudslaag van het internet. Brazilië steunde de bepalingen over het tegengaan van spam en het verbeteren van netwerkveiligheid, hoewel dit volgens velen kan leiden tot controle over de inhoudslaag van het internet (Varon Ferraz & Maciel 2012). Voorafgaand aan het WCIT gaf de leider van de Braziliaanse delegatie, Paulo Bernardo, aan geen voorstander van ICANN te zijn. ICANN zou niet open genoeg zijn en te veel gecontroleerd worden door de Verenigde Staten.¹¹

Volgens de Algemene Wet Telecommunicatie in Brazilië moet de *Brazilian Telecommunications Regulatory Agency* (Anatel) het land vertegenwoordigen in internationale telecommunicatieorganisaties zoals het ITU (Varon Ferraz & Maciel 2012). In de Braziliaanse delegatie bij het WCIT waren er weinig andere vertegenwoordigers vanuit bijvoorbeeld het ministerie van Buitenlandse Zaken, CGI.br-leden en *civil society* (*Global Partners Digital* 2013). Varon Ferraz, de enige vertegenwoordiger van de Braziliaanse *civil society* tijdens het WCIT, gaf aan dat de *civil society* in Brazilië geen formele uitnodiging van Anatel had ontvangen om zich aan te sluiten bij de Braziliaanse delegatie. Wel merkte zij op dat het eenvoudig was om Anatel te benaderen en zelf om een uitnodiging te vragen, waarna het geen probleem was om zich aan te sluiten bij de delegatie (Varon Ferraz & Maciel 2012).

De Braziliaanse *civil society* was weinig betrokken bij zowel de voorbereiding als ook de conferentie in Dubai zelf. De *civil society* participeerde nauwelijks in de publieke bijeenkomsten die Anatel organiseerde voorafgaand aan het WCIT, ook al waren deze bijeenkomsten vrij toegankelijk voor geïnteresseerde organisaties. Er waren wel enkele obstakels, zoals het ontbreken van een reiskostenvergoeding en verlate publicatie van de notulen van voorgaande vergaderingen, waardoor het lastig was om door te gaan op de discussies (Varon Ferraz & Maciel 2012). De *civil society* was vooral minder gefocust op het WCIT doordat ze in beslag werd genomen door de cruciale debatten die op dat moment op nationaal niveau plaatsvonden (Ebert & Maurer 2013a; Varon Ferraz & Maciel 2012; *Global Partners Digital* 2013). In 2012 had Brazilië namelijk de *Marco Civil*, het wetsvoorstel voor nationaal internetbeleid en internet governance, bijna aangenomen. Het mislukte door de lobby van telecommunicatiebedrijven tegen de bepalingen over onder andere netneutraliteit bij het ministerie van Communicatie en Anatel. Door deze nationale discussie stond de positie van Brazilië tijdens het WCIT vast.

Wanneer in Brazilië over het WCIT werd bericht, kwamen vaak kwesties aan de orde die belangrijk waren voor het nationale debat, zoals netneutraliteit. In een krantenartikel stond bijvoorbeeld dat er nog geen consensus was over het voorstel voor netneutraliteit in Brazilië, maar dat de minister toch garandeerde dat hij documenten in strijd met de netneutraliteit niet zou tekenen op het WCIT.¹²

De positie die Brazilië innam tijdens het WCIT werd grotendeels bepaald door de samenstelling van de delegatie en door de nationale debatten over dit onderwerp, waardoor er minder aandacht was voor de onderhandelingen op het WCIT (*Global Partners Digital* 2013). Hierdoor was de positie die Brazilië op het WCIT innam vooral de positie van Anatel, dat gesteund werd door het ministerie van Communicatie en beïnvloed werd door de lobby van de telecommunicatiebedrijven, en minder de positie van de *civil society*, CGI.br en het ministerie van Buitenlandse Zaken. Anatel was wel een voorstander van de ambities van het ITU om een legitieme institutie te worden om internet-governanceproblemen zoals spam en cybercriminaliteit aan te pakken. De tien internetprincipes van Brazilië en het multistakeholder-model van CGI.br werden daardoor weinig onder de aandacht gebracht op het WCIT.

4.2 POSITIE VAN INDIA OP HET WCIT 2012

India heeft de *International Telecommunication Regulations* niet ondertekend in Dubai tijdens het WCIT en heeft zich het recht voorbehouden om later te ondertekenen. Traditioneel vertegenwoordigt het departement van Telecommunicatie India op bijeenkomsten van de ITU. In eerste instantie hield daardoor met name het departement van Telecommunicatie zich bezig met de voorbereidingen van het WCIT. De betrokkenheid van het departement gebeurde vooral vanuit een telecommunicatieperspectief en doordat internet-governance geen onderdeel is van het departement, werd dit niet meegenomen. Vooraf werden in eerste instantie alleen de telecommunicatiebedrijven geraadpleegd, doordat zij van oudsher betrokken werden bij ITU-bijeenkomsten door het departement van Telecommunicatie (*Global Partners Digital* 2013:18).

Het eerste voorstel van India voor de conferentie in Dubai was vooral een weergave van het perspectief van het departement van Telecommunicatie. Het bevatte een voorstel om de definitie van telecommunicatie te verbreden en informatie-technologie eraan toe te voegen. Het departement beargumenteerde daarbij dat IT-systemen tegenwoordig onlosmakelijk verbonden zijn met de basistelecommunicatie-infrastructuur. Het departement was daarnaast bezorgd over netwerkbeveiligingsvraagstukken, vooral over de internationale dimensie ervan. De conceptversie bevatte daardoor een geheel nieuw deel over de veiligheid van netwerken.¹³ Dit was echter geen poging van het departement om de inhoud van het internet te controleren. Dat de telecommunicatiebedrijven intensief betrokken

zijn geweest bij de voorbereiding bleek bijvoorbeeld uit de eis dat er voldoende rendement moest zijn op de investeringen van netwerk-providers (*Global Partners Digital* 2013:18).

Het voorstel dat het departement van Telecommunicatie indiende bij de ITU zorgde voor veel kritiek van de *civil society* en delen van de industrie in India. Beide partijen vreesden dat het voorstel van India tot meer controle van de ITU over het internet zou leiden en meer mogelijkheden gaf om de inhoud van het internet te controleren.¹⁴ Daarnaast vonden zij dat ze te weinig betrokken waren bij het voorbereidingsproces.¹⁵ De *civil society* raakte tijdens het debat over het CIRP-voorstel van India bij de Verenigde Naties gemobiliseerd. Dit debat viel samen met de voorbereidingen voor het WCIT (Ebert & Maurer 2013a:1064). *Civil society*-organisaties, zoals het *Internet Democracy Project* en het *Center for Internet and Society*, mobiliseerden zich ook in het debat rondom de voorbereidingen voor het WCIT en dienden bijvoorbeeld een gezamenlijke inzending in bij de ITU over de toekomst van de ITRs en gerelateerde kwesties.¹⁶ In de inzending verzochten ze onder andere om meer transparantie bij de voorbereidingen van de ITU en stelden voor om de ITRs te beperken tot de fysieke laag van het internet en hen niet uit te breiden naar de inhoudslaag. Een deel van de industrie vormde een soort bondgenootschap met de *civil society* en gaf ook kritiek op het voorstel van India voor de ITRs. Zo liet de *National Association of Software and Services Companies* (NASSCOM) weten dat zij er geen voorstander van was om een bestaande VN-organisatie zoals de ITU meer toezicht te laten houden.¹⁷ En de *Cellular Operators Association of India* (COAI), India's grootste mobiele aanbieder, was tegen elke rol die de ITU zou kunnen hebben op het gebied van internationale *roaming* en internet-governance.¹⁸

Het departement van Telecommunicatie en het departement van Elektronica en Informatietechnologie (DeitY) vallen onder hetzelfde ministerie en delen daardoor hun minister, Kapil Sibal. Sibal was aanwezig op het *Internet Governance Forum* in Baku en werd zich daar bewust van de aankomende internet-governance discussies op het WCIT in Dubai. Samen met de houding van de *civil society* en de industrie zorgde dit ervoor dat de minister op het laatste moment nog bijeenkomsten organiseerde waarbij ook de *civil society* en de private sector werden betrokken, en niet meer alleen de telecommunicatiebedrijven. Door deze bijeenkomsten veranderde India's positie voorafgaand aan het WCIT. Sibal gaf na de stakeholder-bijeenkomsten de toezegging dat hij de tekst van het voorstel zou heroverwegen om ervoor te zorgen dat het overeenkwam met het voornemen van de overheid dat zowel het internet, het internetverkeer en de inhoud niet onder toezicht van de ITU zou komen te vallen.¹⁹ Hij deed daarnaast ook de toezegging om expliciet te refereren aan de mensenrechten in de *International Telecommunication Regulations* (*Global Partners Digital* 2013:18).

Tijdens de WCIT was de positie van India veel genuanceerder dan bij het eerste voorstel. De delegatie hield effectief rekening met de vele zorgen van de *civil society* en de industrie, ook al waren er volgens de *civil society* nog steeds knelpunten.²⁰ India steunde uiteindelijk de kern van de nieuwe *International Telecommunication Regulations*, maar besloot niet te ondertekenen, omdat ze eerst verdere consultaties wilde houden met de relevante *stakeholders* om de potentiële impact van het internet-governance-deel van de ITRs te doorgronden.²¹

5. NSA-ONTHULLINGEN

Op 5 juni 2013 kwam *the Guardian* met een eerste onthulling over de surveillance-programma's van de *National Security Agency* (NSA), de veiligheidsdienst van de Verenigde Staten. Hierna volgden er vele onthullingen waaruit bleek dat de NSA massaal metadata had verzameld in binnen- en buitenland. Via bijvoorbeeld het programma PRISM verkreeg de NSA informatie over gebruikers van bedrijven zoals Microsoft, Yahoo, Google, Facebook, Apple en Skype. Op 9 juni 2013 maakte Edward Snowden, een voormalig medewerker van de CIA, bekend dat de onthullingen over het verzamelen van data door de Amerikaanse geheime diensten bij hem vandaan kwamen. Er had ook politieke spionage plaatsgevonden: de NSA had onder meer het hoofdkantoor van de Verenigde Naties in New York bespioneerd en regeringsleiders zoals Angela Merkel van Duitsland en Dilma Rousseff van Brazilië afgeluisterd.²²

De Verenigde Staten beweerde dat het verzamelen van data gebeurde om terrorisme tegen te gaan. President Obama verdedigde de surveillance: volgens hem waren minstens vijftig dreigingen van terrorisme afgewend door informatie uit de data, niet alleen dreigingen in de Verenigde Staten, ook erbuiten (Bergen et al 2014). In oktober 2013 gaf Keith Alexander, de directeur van de NSA, toe dat dit misleidende informatie was en dat het daadwerkelijke aantal van aanslagen die voorkomen waren door het af luisterwerk veel lager was.

De Verenigde Staten vormt samen met Canada, Groot-Brittannië, Nieuw Zeeland en Australië de zogenoemde '*five eyes*': de vijf landen werken intensief samen en delen bijna alle informatie die vergaard is door hun inlichtingendiensten.²³

Andere landen reageren wisselend op de activiteiten van de Verenigde Staten en andere landen uit de '*five eyes*'. Merkel reageerde bijvoorbeeld fel op de onthullingen. Duitsland en Frankrijk besloten in oktober 2013 om de Verenigde Staten om opheldering te vragen over het af luisteren en om met hen voor het einde van 2013 tot afspraken te komen. In september 2013 stelde een commissie van het Europees Parlement dat Europa een eigen *cloud* moet ontwikkelen in plaats van alleen gebruik te maken van Amerikaanse *clouds*.²⁴ Een commissie van het Europees Parlement hield ook een reeks hoorzittingen om informatie te verzamelen over de impact van de *surveillance* (Morales 2014). Volgens Mueller en Wagner (2014) destabiliseerden de onthullingen over de NSA-surveillance de grondslagen van internationale internet-governance. Men vreesde bijvoorbeeld dat westers georiënteerde internet-governance-instituties (mede)verantwoordelijk werden gehouden voor de gebeurtenissen rondom de NSA, en dat samenwerking en vertrouwen op het internet zouden afkalven tot een nationaal afgebakend internet (Mueller & Wagner 2014).

5.1 DE REACTIE VANUIT BRAZILIË OP DE NSA-ONTHULLINGEN

Begin september 2013 kwamen gelekte NSA-documenten naar buiten waaruit bleek dat de Braziliaanse president, Dilma Rousseff, was bespioneerd door de *National Security Agency* (NSA), de veiligheidsdienst van de Verenigde Staten. Kort daarna werd onthuld dat er naast politieke spionage ook economische spionage had plaatsgevonden: de Verenigde Staten hadden de grote nationale oliemaatschappij Petrobras bespioneerd. Uit de NSA-documenten bleek tevens dat Brazilië in Zuid-Amerika het meest door de NSA bespioneerde land was.²⁵

In haar eerste reactie vroeg Rousseff vooral om een verklaring van de Verenigde Staten over de nieuwsberichten over spionage.²⁶ Al snel werd haar reactie feller en zegde ze haar geplande staatsbezoek aan Washington af. Het was de eerste keer sinds 1995 dat een Braziliaans staatshoofd een staatsbezoek aan de Verenigde Staten zou brengen.²⁷ Rousseff kondigde daarnaast ook een aantal nationale maatregelen aan om de *privacy* van de Braziliaanse burgers, de overheid en bedrijven beter te beschermen tegen spionage. Brazilië nam maatregelen om de internationale connecties te verbeteren, met minder tussenkomst van de Verenigde Staten. Er zijn bijvoorbeeld plannen om Brazilië te verbinden met Europa en Afrika door intercontinentale kabels aan te leggen. De Braziliaanse overheid tracht daarnaast de binnenlandse bandbreedteproductie te verhogen en het gebruik van binnenlands geproduceerde netwerkapparatuur te stimuleren.²⁸ Door satellieten te bouwen voor militair en civiel gebruik probeert Brazilië belangrijke communicatie veiliger te stellen en de overheid heeft een nationaal e-mailsysteem besteld bij de Braziliaanse postdienst. Het nieuwe e-mailsysteem is bedoeld als een alternatief voor Gmail en Hotmail en gaat gebruikers de mogelijkheid geven versleutelde mails te versturen.²⁹

Op de aangekondigde maatregelen van Brazilië om het internet meer te 'nationaliseren' kwam kritiek. Volgens sommigen hadden de maatregelen weinig effect op het tegengaan van buitenlandse digitale spionage. Anderen beweerden dat Brazilië zich hierdoor richting meer autoritaire landen zoals China en Iran beweegt. De Braziliaanse overheid zelf betoogde dat ze simpelweg haar burgers wil beschermen tegen een uit de hand gelopen surveillance-machine van de Verenigde Staten en tegelijkertijd de ontwikkeling van een lokale internet industrie wil bevorderen.³⁰ Ian Brown, onderzoeker aan het *Oxford Internet Institute*, beargumenteerde in *the Guardian* dat er een groot verschil is tussen de plannen van China en Brazilië. Chinese burgers worden door de Chinese overheid opzettelijk afgesneden van het debat over controversiële politieke kwesties, terwijl Braziliaanse burgers nieuwe opties krijgen om hun *privacy* te beschermen. Zonder aanzienlijke hervormingen in de Amerikaanse en internationale wetgeving zijn er volgens Brown weinig andere opties voor landen die niet tot de 'five eyes' behoren. Staten zullen daarom waarschijnlijk het pad van Brazilië volgen door soortgelijke maatregelen te nemen.

Dit is een dure optie die waarschijnlijk de snelle innovatie afremt die de ontwikkeling van het internet tot dusver heeft aangedreven.³¹ De eventuele impact van dit systeem op de economische ontwikkeling en communicatie was inderdaad een zorg van bedrijven. In een gezamenlijke brief aan Rouseff³² uitten zij hun zorg over onder andere de consequenties van een wijziging die is toegevoegd aan de *Marco Civil*. Daarbij gaat het om het verzoek om datacenters te nationaliseren door ze in Brazilië te plaatsen. De wereldwijde datastromen zijn volgens hen essentieel voor bedrijven in alle sectoren om innovatieve en creatieve producten en diensten te creëren, om de productiviteit te verhogen, om te concurreren op buitenlandse markten, om fraude te bestrijden en om werkgelegenheid te creëren.³³

Behalve nationaal neemt Rouseff ook internationaal een duidelijke positie in. In haar speech op de Algemene Vergadering van de Verenigde Naties in september 2013 beschuldigde ze de NSA van het schenden van het internationaal recht omdat de NSA willekeurig persoonsgegevens van Braziliaanse burgers had verzameld en omdat de Braziliaanse industrie slachtoffer was van economische spionage. De kritische speech leek direct aan Obama gericht. Rouseff reageerde bijvoorbeeld als volgt op de eerdere verklaring van de Verenigde Staten dat de informatie verzameld werd om landen te beschermen tegen terrorisme: “Brazil, Mr President, knows how to protect itself. We reject, fight and do not harbour terrorist groups”.³⁴ In haar speech vraagt Rouseff de VN om toe te zien op een nieuw wereldwijd systeem voor internet-governance, een multilateraal systeem. Rouseffs speech was de eerste serieuze diplomatieke kritiek op de spionageonthullingen van de Verenigde Staten.³⁵ Haar speech werd goed ontvangen en gesteund door verdedigers van internetvrijheid en de internationale *civil society*.³⁶

In oktober 2013 werd bekend dat Angela Merkel samen met Rouseff werkte aan een VN-resolutie tegen de wereldwijde spionage van de NSA. In deze resolutie draait het voornamelijk om het recht op *privacy* in het digitale domein. In de tekst wordt niet specifiek de Verenigde Staten genoemd, maar de tekst roept op om te stoppen met het op grote schaal afluisteren en verzamelen van data. Volgens velen was dit tegen de Verenigde Staten gericht.³⁷ Op 26 november 2013 werd de resolutie in de Algemene Vergadering van de Verenigde Naties aangenomen, met vooral symbolische waarde: het is geen bindend besluit.³⁸

In haar speech bij de Verenigde Naties benadrukte Rouseff de noodzaak voor een nieuw internationaal internet-governancesysteem:

“Such multilateral mechanisms should guarantee the ‘freedom of expression, privacy of the individual and respect for human rights’ and the ‘neutrality of the network’, guided only by technical and ethical criteria, rendering it inadmissible to restrict it for political, commercial, religious or any other purposes.”³⁹

Fadi Chehadi, de voorzitter van de ICANN, en Rouseff hebben dit onderwerp besproken tijdens een ontmoeting. Dit heeft ertoe geleid dat Brazilië gastland zal zijn voor de *Global Multistakeholder Meeting on the Future of Internet Governance* (GMMFIG) op 23 en 24 april 2014.⁴⁰ Deze bijeenkomst biedt de mogelijkheid om voorstellen over de ontwikkeling van internet en internet-governance te bespreken, om consensus over universeel aanvaarde principes over internet-governance na te streven en hun institutionele kader te verbeteren.⁴¹ Volgens Milton Mueller, professor aan *Syracuse University School of Information Studies*, heeft ICANN zich niet alleen verbonden met een staatshoofd dat zeer kritisch is over de NSA-spionage en de Amerikaanse regering, maar roept de voorzitter van ICANN samen met haar een wereldwijde vergadering bijeen om een nieuw internet-governancesysteem uit te denken. Dit zou de Amerikaanse hegemonie over het internet-governancesysteem bedreigen.⁴² In een andere blog betoogde Mueller dat de rol van *stakeholders* hoog op de agenda zal staan tijdens de GMMFIG. Volgens Mueller lijkt het erop dat de conferentie in Brazilië gebruikt gaat worden om de huidige definitie van *multistakeholder governance* te betwisten. De huidige definitie geeft verschillende rechten en rollen aan statelijke en niet-statelijke actoren: “Verandering van dit systeem is nodig en het GMMFIG biedt de mogelijkheid om deze verandering te bespreken”, aldus Mueller.⁴³

Brazilië heeft na de NSA-onthullingen een duidelijke positie uitgedragen en neemt nationaal en internationaal maatregelen om een verandering te bewerkstelligen in het internationale internet-governancesysteem. Het land werkt daarbij samen met Duitsland en ook met ICANN.

5.2 DE REACTIE VANUIT INDIA OP DE NSA-ONTHULLINGEN

Uit de documenten van Snowden kwam naar voren dat de Verenigde Staten inlichtingen heeft verzameld in India via *Boundless Informant* en *Prism*. India komt op de vijfde plaats van meest door de Verenigde Staten bespioneerde staten.⁴⁴ Vergeerd werd informatie over de binnenlandse politiek en over meer strategische en commerciële belangen van India, zoals informatie over nucleaire en ruimteprogramma's.⁴⁵ Volgens Manmohan Singh, de premier van India, is er geen reden om bezorgd te zijn dat hij net als sommige andere politieke leiders wordt afgeluisterd door de NSA, “omdat hij geen mobiele telefoon of Gmail heeft”.⁴⁶

De openbare verklaring van zowel de Amerikaanse als de Indiase overheid luidde, dat er geen *surveillance* van de inhoud van internet- en telefoonnetwerken in India door de NSA had plaatsgevonden. De Amerikaanse inlichtingenprogramma's keken volgens beiden alleen naar de patronen van communicatie om terrorisme tegen te gaan.⁴⁷ Op 2 juli 2013 stelde de minister van Buitenlandse Zaken, Salman Khurshid:

“This is not scrutiny and access to actual messages. It is only computer analysis of patterns of calls and emails that are being sent. It is not actually snooping specifically on content of anybody’s message or conversation”.⁴⁸

Hij gaf aan dat de Verenigde Staten met een deel van de informatie uit haar surveillance-programma’s terroristische aanvallen in verschillende landen had weten te voorkomen. De verklaringen waren enigszins strijdig met een eerdere verklaring van het ministerie, waarin na aanleiding van de eerste onthullingen van de NSA gesteld werd dat elke schending van de privacy onacceptabel was.⁴⁹

Naar aanleiding van de onthullingen over de surveillance-programma’s van de Verenigde Staten in India is er bij het Indiase hoogerechtshof een *Public Interest Litigation (PIL)*, een speciale rechtszaak in de Indiase wet voor de bescherming van het openbaar belang, ingediend over de cyberspionage van de Verenigde Staten. De PIL gaf aan, buitenlandse bedrijven die informatie deelden met de veiligheidsdiensten van de Verenigde Staten verantwoordelijk te houden voor contractbreuk en schending van privacy. In een reactie liet de Hoge Raad weten geen jurisdictie te hebben over de Amerikaanse regering.⁵⁰

Enige tijd na de onthullingen nam de overheid wel enkele maatregelen om spionage vanuit het buitenland tegen te gaan. Ambtenaren werd in India geadviseerd om gebruik te maken van hun overheidsaccount in plaats van van e-maildiensten zoals Gmail en Hotmail.⁵¹ Veel werknemers gaven echter aan dat de kwaliteit van de overheidsmail te slecht is om er efficiënt mee te werken, waardoor velen – waaronder topambtenaren en ministers – nog altijd gebruikmaken van een Gmail- of Hotmail-account.⁵² Ook werd de diplomatische staf in Londen verteld dat zij bij het schrijven van informatiegevoelige documenten beter gebruik kon maken van typemachines dan van computers.⁵³

Vergeleken met Brazilië is er vanuit India een vrij mild antwoord gekomen op de onthullingen over de NSA-spionage in India. Er worden verschillende redenen voor de terughoudendheid van India genoemd. Grote delen van de middenklasse en de elite in India zijn bijvoorbeeld ‘in de ban’ van de Verenigde Staten en storen zich niet aan de praktijken van de NSA. Daarnaast is de bevolking in India gewend geraakt aan toenemende *surveillance* en weegt de bevolking het af tegen de bestrijding van terrorisme en onrust. India wil wellicht ook de steeds sterkere band met de Verenigde Staten niet in gevaar brengen. Het land heeft om veel redenen belang bij een strategische relatie met de Verenigde Staten. Bij regionale veiligheid is de Verenigde Staten een grootmacht tegenover China. Daarnaast zorgt de VS ervoor dat India toegang heeft tot schaliegas, wapens en hoogwaardige technologie. India waardeert ook de kennis en kunde van de VS en Groot-Brittannië in de bestrijding van terrorisme en deze vorm van bestrijding bestaat voor een deel uit het inlichtingenapparaat. Wellicht uit India daarom geen openlijke kritiek op de Verenigde Staten.⁵⁴

Krantenartikelen hekelden de houding die de Indiase overheid aanneemt ten opzichte van de onthullingen van de NSA wel. Een artikel in *The Hindu* meldde bijvoorbeeld dat de officiële verklaring van de overheid dat de Verenigde Staten om terrorisme te voorkomen alleen keek naar patronen van communicatie en niet naar de inhoud, ver van de waarheid af ligt, zo niet ronduit misleidend is.⁵⁵ Volgens Anja Kovacs, directeur van het *Internet Democracy Project*, had het verzamelen van data geen breder doel, zoals de samenleving als geheel te beschermen tegen terrorisme, maar ging het om controle.⁵⁶ Een ander artikel in *The Hindu* betoogt dat premier Singh Brazilië moet volgen in de kritiek op de NSA-spionage: Brazilië heeft de weg voor India al voor een deel vrijgemaakt.⁵⁷

In de kranten en door de *civil society* wordt mild betoogd dat de overheid een andere houding moet aannemen ten opzichte van de NSA-spionage, maar er is geen massale publieke verontwaardiging waardoor de overheid tot een andere reactie wordt gedwongen.⁵⁸ Er lijkt geen grote binnenlandse discussie plaats te vinden over buitenlandse spionage en terrorismebestrijding wordt gezien als een legitieme reden ervoor.

6. CONCLUSIE

De BRIC-landen zijn opkomende landen met een grote, nog sterk groeiende internetpopulatie. Deze landen laten steeds meer hun stem horen in het internationale internet-governancedebat. Brazilië en India blijken een andere positie in te nemen dan China en Rusland, de twee andere BRIC-landen.

Er zijn kritische kanttekeningen te plaatsen bij de internetvrijheid in zowel India als Brazilië, maar in beide landen wordt het internet niet systematisch gefilterd. De overheden van beide landen geven binnenlandse actoren, zoals het bedrijfsleven, de industrie en de *civil society*, de ruimte om hun stem in het debat te laten horen en soms de overheid voor misstanden verantwoordelijk te houden. Hierin verschillen ze van meer autoritaire regimes. Dit werd duidelijk bij het WCIT in Dubai 2012, toen India's positie veranderde door binnenlandse druk van de *civil society* en delen van de industrie; de minister hield duidelijk rekening met hun standpunten. In Brazilië wordt de *civil society* betrokken in het debat over de *Marco Civil*. Daarnaast zijn zowel de *civil society* als de private sector vertegenwoordigd in CGI.br.

Brazilië nam na de onthullingen van Snowden een duidelijke positie in tegen de Verenigde Staten. Rouseff annuleerde haar officiële staatsbezoek aan de Verenigde Staten, ze hield op de Algemene Vergadering van de Verenigde Naties een kritische speech over de af luisterpraktijken en stelde samen met Merkel een VN-resolutie op over recht op *privacy* in het digitale domein. Samen met ICANN organiseert Rouseff de GMMFIG voor april 2014, een conferentie om de toekomst van internet en internet-governance te bespreken. Met het nemen van nationale maatregelen probeert Rouseff het internet in Brazilië minder afhankelijk te maken van de Verenigde Staten. Deze reactie laat zien dat Brazilië de leidende rol van de Verenigde Staten in internet-governance betwist. Tijdens het WCIT in 2012 was de positie die Brazilië uitdroeg minder eenduidig, waarschijnlijk door de samenstelling van de delegatie en door de nationale debatten die op dat moment speelden. Bij het WCIT en pre-Snowden was al wel te zien dat Brazilië soms tegen de leidende rol van de Verenigde Staten inging. De leider van de Braziliaanse vertegenwoordiging gaf bij het WCIT bijvoorbeeld al aan geen voorstander van ICANN te zijn, omdat ICANN te veel beïnvloed wordt door de Verenigde Staten. De nationale plannen van Rouseff om het internet onafhankelijker van de Verenigde Staten te maken, zoals het aanleggen van intercontinentale kabels, waren gedeeltelijk al voor de onthullingen over de NSA in gang gezet.

India distantieert zich nauwelijks van de Verenigde Staten in het internet-governancedebat. India betwist de positie van de Verenigde Staten niet en gaat mee in de verklaring van de Verenigde Staten over de activiteiten van de NSA in India. Op het WCIT nam India uiteindelijk ook een soortgelijke positie in, mede bepaald door de inbreng van de *civil society* en een deel van de industrie. Het is onduidelijk of India

deze positie ook innam om mee te gaan met het standpunt van de Verenigde Staten en Europa. Bij het WCIT was India tijdens het voorbereidingsproces en tijdens de conferentie zelf nog bezig om een standpunt te formuleren. De uiteindelijke verklaring, waarin India aangaf eerst verdere consultaties met binnenlandse actoren te houden, liet zien dat India wellicht nog geen vastliggend standpunt heeft.

India en Brazilië zijn staten met potentieel een grote en nieuwe inbreng in het governancedebat over het internet. Het is daarom interessant om inzicht te krijgen in de positie van deze twee landen. Hun positie wijkt af van die van Rusland en China, de twee andere BRIC-landen, maar dat hoeft niet te betekenen dat ze het huidige westerse internet-governancesysteem steunen. Momenteel zijn beide landen 'swing states', die hun positie nog aan het bepalen zijn. Dit paper laat zien welke positie deze landen hebben ingenomen bij het WCIT in Dubai in 2012 en na de onthullingen over de NSA in 2013. Deze inzichten geven wellicht een beter beeld van de manier waarop het standpunt over internationale internet-governance van deze twee landen zich zal ontwikkelen.

NOTEN

- 1 International Telecommunication Union (ITU), Metadata for the percentage of individuals using the Internet, 2000-2012, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls
- 2 World Bank, “Countries and Economies”, 2012, <http://data.worldbank.org/country>
- 3 International Telecommunication Union (ITU), Metadata for the percentage of individuals using the Internet, 2000-2012, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls
- 4 “On Internet, Brazil is beating US at its own game”, *Al Jazeera America*, 20 september 2013, <http://america.aljazeera.com/articles/2013/9/20/brazil-internet-dilmarousseffnsa.html>
- 5 World Bank, “Countries and Economies”, 2012, <http://data.worldbank.org/country>
- 6 “NSA spied on Indian embassy and UN mission, Edward Snowden files reveal”, *The Guardian*, 25 september 2013, http://www.theguardian.com/world/2013/sep/25/nsa-surveillance-indian-embassy-un-mission?CMP=twt_gu
- 7 “Celso Amorim diz que Brasil é vulnerável contra ataques cibernético”, *Correio Braziliense*, 22 september 2013.
- 8 “Industry Promoting Activities”, Department of Electronics and Information Technology, <http://deity.gov.in/content/industry-promotion-activities>
- 9 Diamond, J. “India’s National Cyber Security Policy in Review” (blog), The Centre for Internet and Society, 31 juli 2013, <http://cis-india.org/internet-governance/blog/indias-national-cyber-security-policy-in-review>
- 10 Xynou, M. “India’s ‘Big Brother’: The Central Monitoring System (CMS)” (blog), The Centre for Internet and Society, 8 april 2013, <http://cis-india.org/internet-governance/blog/indias-big-brother-the-central-monitoring-system>
- 11 “Tem de reduzir o roaming internacional”, *O Estado de S. Paulo*, 4 december 2012, <http://www.estadao.com.br/noticias/impresso,tem-de-reduzir-o-roaming-internacional-,968929,o.htm>
- 12 “O dono da rede”, *O Estado de S. Paulo*, 3 december 2012.
- 13 “India (Republic of) Proposal for the work of the conference” (ITU, WCIT-12, Document 21-E) [http://www.itu.int/md/meetingdoc.asp?lang=en&parent=S12-WCIT12-121203-C&source=India\(Republicof\)](http://www.itu.int/md/meetingdoc.asp?lang=en&parent=S12-WCIT12-121203-C&source=India(Republicof))
- 14 “Civil society & industry oppose India’s plans to modify ITRs”, *The Hindu*, 23 november 2012 <http://www.thehindu.com/news/national/civil-society-industry-oppose-indias-plans-to-modify-itrs/article4124046.ece>
- 15 “A week ahead of global internet meet, Sibal to hold open house today”, *The Hindu*, 27 november 2012, <http://www.thehindu.com/news/national/a-week-ahead-of-global-internet-meet-sibal-to-hold-open-house-today/article4137715.ece>
- 16 “Submission by Indian civil society organisations on proposals for the future ITRs and related processes”, ITU, 7 november 2012, <http://www.itu.int/en/wcit-12/Pages/public.aspx>

- 17 “Civil society & industry oppose India’s plans to modify ITRs”, *The Hindu*, 23 november 2012 <http://www.thehindu.com/news/national/civil-society-industry-oppose-indias-plans-to-modify-itrs/article4124046.ece>
- 18 “A week ahead of global internet meet, Sibal to hold open house today”, *The Hindu*, 27 november 2012, <http://www.thehindu.com/news/national/a-week-ahead-of-global-internet-meet-sibal-to-hold-open-house-today/article4137715.ece>
- 19 “Sibal snowed in with issues of free speech”, *The Hindu*, 28 november 2012, <http://www.thehindu.com/todays-paper/tp-national/sibal-snowed-in-with-issues-of-free-speech/article4141875.ece>
- 20 Kovacs, A. (2013) “WCIT 2012: India sets an example” (blog), Internet Democracy Project, <http://internetdemocracy.in/2013/01/india-sets-an-example/>
- 21 Samarajiva, R. (2013). “Nuanced and progressive: An assessment of India’s stance at WCIT” (blog), LIRNEasia, <http://lirneasia.net/2013/01/nuanced-and-progressive-an-assessment-of-indias-stance-at-wcit/>
- 22 “Tijdljijn NSA-schandaal”, *NOS*, 23 november 2013, <http://nos.nl/artikel/578315-tijdljijn-nsa-schandaal.html>
- 23 “Tijdljijn NSA-schandaal”, *NOS*, 23 november 2013, <http://nos.nl/artikel/578315-tijdljijn-nsa-schandaal.html>
- 24 “Tijdljijn NSA-schandaal”, *NOS*, 23 november 2013, <http://nos.nl/artikel/578315-tijdljijn-nsa-schandaal.html>
- 25 Greenwald, G., Kaze, R. & Casado, J. “EUA espionaram milhões de e-mails e ligações de brasileiros”, *O Globo*, 6 juli 2013, <http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934>
- 26 “Brazil: Answers Are Sought on N.S.A. Spying”, *New York Times*, 9 september 2013, <http://www.nytimes.com/2013/09/10/world/americas/brazil-answers-are-sought-on-nsa-spying.html>
- 27 “President Rousseff wil niet naar vs”, *NOS*, 17 september 2013, <http://nos.nl/artikel/552385-president-rousseff-wil-niet-naar-vs.html>
- 28 “On Internet, Brazil is beating US at its own game”, *Al Jazeera America*, 20 september 2013, <http://america.aljazeera.com/articles/2013/9/20/brazil-internet-dilmarousseffnsa.html>
- 29 “Brazil Angered Over Report N.S.A. Spied on President”, *New York Times*, 2 september 2013, http://www.nytimes.com/2013/09/03/world/americas/brazil-angered-over-report-nsa-spied-on-president.html?_r=0
- 30 Brown, I. (1 november 2013) “Will NSA revelations lead to the Balkanisation of the Internet?”, *The Guardian*, <http://www.theguardian.com/world/2013/nov/01/nsa-revelations-balkanisation-internet>
- 31 Brown, I. (1 november 2013) “Will NSA revelations lead to the Balkanisation of the Internet?”, *The Guardian*, <http://www.theguardian.com/world/2013/nov/01/nsa-revelations-balkanisation-internet>
- 32 “Brazil’s Vision on Internet Governance: Managing Sovereignty, Privacy and Technology”, Wilson Center, 23 oktober 2013, <http://www.wilsoncenter.org/event/brazil%E2%80%99s-vision-internet-governance-managing-sovereignty-privacy-and-technology>

- 33 “Brazil’s Vision on Internet Governance: Managing Sovereignty, Privacy and Technology”, Wilson Center, 23 oktober 2013, <http://www.wilsoncenter.org/event/brazil%E2%80%99s-vision-internet-governance-managing-sovereignty-privacy-and-technology>
- 34 “Brazilian president: US surveillance a 'breach of international law'”, *The Guardian*, 24 september 2013, <http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance#rpctoken=1830251653&forcesecure=1>
- 35 “Brazilian president: US surveillance a 'breach of international law'”, *The Guardian*, 24 september 2013, <http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance#rpctoken=1830251653&forcesecure=1>
- 36 “Brazil: the New Internet Freedom Champion?” (blog), Global Voices Advocacy Online, 15 oktober 2013, <http://advocacy.globalvoicesonline.org/2013/10/15/brazil-the-new-internet-freedom-champion/>
- 37 “Resolutie voor privacy in digitale era”, *NOS*, 2 november 2013, <http://nos.nl/artikel/569942-resolutie-voor-privacy-in-digitale-era.html>
- 38 “Steun voor VN-resolutie spionage”, *NOS*, 26 november 2013, <http://nos.nl/artikel/579616-steun-voor-vnresolutie-spionage.html>
- 39 “Brazilian president: US surveillance a 'breach of international law'”, *The Guardian*, 24 september 2013, <http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance#rpctoken=1830251653&forcesecure=1>
- 40 Mueller, M. (19 november 2013) “Booting up Brazil” (Blog), Internet Governance Project, <http://www.internetgovernance.org/2013/11/19/booting-up-brazil>
- 41 “Announcement of the Brazilian Internet Steering Committee about the Global Multistakeholder Meeting on Internet Governance”, Brazilian Network Information Center, 26 november 2013, <http://www.nic.br/imprensa/releases/2013/rl-2013-62.htm>
- 42 Mueller, M. (11 oktober 2013) “The core Internet institutions abandon the US Government” (blog), Internet Governance Project, http://www.internetgovernance.org/2013/10/11/the-core-internet-institutions-abandon-the-us-government/?utm_source=rss&utm_medium=rss&utm_campaign=the-core-internet-institutions-abandon-the-us-government
- 43 Mueller, M. (18 december 2013) “Revisiting ‘roles’: On the agenda for Brazil” (blog), Internet Governance Project, <http://www.internetgovernance.org/2013/12/18/revisiting-roles-on-the-agenda-for-brazil/>
- 44 “NSA spied on Indian embassy and UN mission, Edward Snowden files reveal”, *The Guardian*, 25 september 2013, http://www.theguardian.com/world/2013/sep/25/nsa-surveillance-indian-embassy-un-mission?CMP=tw_t_gu
- 45 “NSA spied on Indian embassy and UN mission, Edward Snowden files reveal”, *The Guardian*, 25 september 2013, http://www.theguardian.com/world/2013/sep/25/nsa-surveillance-indian-embassy-un-mission?CMP=tw_t_gu
- 46 “Geen NSA-paniek in India: premier is digibeet”, *NOS*, 27 oktober 2013, <http://nos.nl/op3/artikel/567529-geen-nsapaniek-in-india-premier-is-digibeet.html>
- 47 “NSA targets Indian politics, space & n-programmes”, 24 september 2013, *The Hindu*, <http://www.thehindu.com/news/national/nsa-targets-indian-politics-space-nprogrammes/article5161299.ece?ref=relatedNews>

- 48 “It is not actually snooping: Khurshid on US surveillance”, *The Hindu*, 2 juli 2013, <http://www.thehindu.com/news/national/it-is-not-actually-snooping-khurshid-on-us-surveillance/article4873351.ece>
- 49 “It is not actually snooping: Khurshid on US surveillance”, *The Hindu*, 2 juli 2013, <http://www.thehindu.com/news/national/it-is-not-actually-snooping-khurshid-on-us-surveillance/article4873351.ece>
- 50 “What India can Learn from the Snowden Revelations” (blog), Centre for Internet and Society, 25 oktober 2013, <http://cis-india.org/internet-governance/blog/yahoo-october-23-2013-what-india-can-learn-from-snowden-revelations>
- 51 “NSA surveillance may cause breakup of internet, warn experts”, *The Guardian*, 1 november 2013, <http://www.theguardian.com/world/2013/nov/01/nsa-surveillance-cause-internet-breakup-edward-snowden>
- 52 “Indian government wakes up to risk of Hotmail, Gmail”, Centre for Internet and Society, 30 december 2013, <http://cis-india.org/news/afp-december-7-2013-annie-banerjee-indian-government-wakes-up-to-risk-of-hotmail-gmail>
- 53 “NSA surveillance may cause breakup of internet, warn experts”, *The Guardian*, 1 november 2013, <http://www.theguardian.com/world/2013/nov/01/nsa-surveillance-cause-internet-breakup-edward-snowden>
- 54 “Waiting for Greenwald: why India can’t stay mute on NSA spying”, 3 december 2013, *The Hindustan Times*, <http://www.hindustantimes.com/comment/analysis/waiting-for-greenwald-why-india-can-t-stay-mute-on-nsa-spying/article1-1158485.aspx>
- 55 “NSA targets Indian politics, space & n-programmes”, *The Hindu*, 24 september 2013, <http://www.thehindu.com/news/national/nsa-targets-indian-politics-space-nprogrammes/article5161299.ece?ref=relatedNews>
- 56 “NSA spied on Indian embassy and UN mission, Edward Snowden Files reveal”, *The Guardian*, 25 september 2012, http://www.theguardian.com/world/2013/sep/25/nsa-surveillance-indian-embassy-un-mission?CMP=tw_t_gu
- 57 “Spying on a strategic partner”, *The Hindu*, 27 september 2013, <http://www.thehindu.com/opinion/editorial/spying-on-a-strategic-partner/article5172013.ece?ref=relatedNews>
- 58 “Waiting for Greenwald: why India can’t stay mute on NSA spying”, *The Hindustan Times*, 3 december 2013, <http://www.hindustantimes.com/comment/analysis/waiting-for-greenwald-why-india-can-t-stay-mute-on-nsa-spying/article1-1158485.aspx>

LITERATUUR

- Bergen, P., D. Serman, E. Schneider en B. Cahall (2014) *Do NSA's Bulk Surveillance Programs Stop Terrorists?*, Washington D.C: New America Foundation. http://newamerica.net/publications/policy/do_nsa_bulk_surveillance_programs_stop_terrorists.
- Canabarro, D.R. en T. Borne (2013) *Brazil and the Fog of (cyber)War*, ncdg Policy Working Paper. no. 13-002. http://www.umass.edu/digitalcenter/research/working_papers/13_002_Canabarro-Borne_BrazilandFogofCyberWar.pdf.
- Carr, J. (2012) *Inside Cyber Warfare*, Sebastopol: O'Reilly Media.
- Clemente, D. (2013) *Adaptive Internet Governance: Persuading the Swing States*, Internet Governance Papers, paper no. 5. <http://www.cigionline.org/publications/2013/10/adaptive-internet-governance-persuading-swing-states>.
- Deibert, R. en R. Rohozinski (2011) 'Contesting Cyberspace and the Coming Crisis of Authority', blz. 21-41 in R. Deibert, R. Rohozinski, J. Palfrey en J. Zittrain (red.) *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*, Cambridge: MIT Press.
- Deibert, R., J. Palfrey, R. Rohozinski en J. Zittrain (2008) *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge: MIT Press.
- Department of Electronics and Information Technology (2013) *National Cyber Security Policy-2013* (ncsp-2013). <http://deity.gov.in/content/national-cyber-security-policy-2013-1>.
- Department of Information Technology (2011) *National Cyber Security Policy*, draft v1.0, 26 March 2011. http://deity.gov.in/hindi/sites/upload_files/dithindi/files/ncsp_060411.pdf.
- Ebert, H. en T. Maurer (2013a) 'Contested Cyberspace and Rising Powers', *Third World Quarterly*, 34, 6: 1054-1074.
- Ebert, H. en T. Maurer (2013b) 'Cyberspace and the Rise of the brics', *Journal of International Affairs*. <http://jia.sipa.columbia.edu/cyberspace-and-rise-brics>.
- Faris, R. en U. Gasser (2013) 'Government as Actors', blz. 19-24 in U. Gasser, R. Faris en R. Heacock (red.) *Internet Monitor 2013: Reflections on the Digital World*, The Berkman Center for Internet & Society, Publication no. 2013-27. http://cyber.law.harvard.edu/publications/2013/reflections_on_the_digital_world.
- Freedom House (2013a) *Freedom on the Net 2013: Brasil*. <http://www.freedomhouse.org/report/freedom-net/2013/brazil>.
- Freedom House (2013b) *Freedom on the Net 2013: India*. <http://www.freedomhouse.org/report/freedom-net/2013/india>.
- Global Partners Digital (2013) *Internet Governance: Towards Greater Understanding of Global South Perspectives* (May 2013 report). <http://www.gp-digital.org/publication/global-south/>.

- Hammond, B. (2013) 'Failure to Reach Consensus at WCIT prompts calls for renewed effort to Support Multistakeholder Approach', *Telecommunications Reports*, 79, 1: 48-52.
- Hill, R. (2013) 'wcit: failure or success, impasse or way forward?', *International Journal of Law and Information Technology*, 21, 3: 313-328.
- IDSA Task Force Report (2012) *India's cyber security challenge*, New Delhi: Institute for Defense Studies and Analysis. OpenNet Initiative (2012) *India*. <https://opennet.net/research/profiles/india>.
- Lewis, A. (2013) *Internet Governance: Inevitable Transitions*, CIGI, Internet Governance Papers, Paper no.4. <http://www.cigionline.org/publications/2013/10/internet-governance-inevitable-transitions>.
- Maurer, T. (2012) *What is at stake at WCIT? An Overview of WCIT and the ITU's role in Internet Governance* (policy brief), Washington D.C: New America Foundation. http://newamerica.net/publications/policy/whats_at_stake_at_wcit.
- Moraes, C. (2014) *Ontwerpverslag over het surveillanceprogramma van de nsa in de vs, toezichhoudende instanties in verschillende lidstaten en gevolgen voor de grondrechten van eu burgers en voor de trans-Atlantische samenwerking op het gebied van justitie en binnenlandse zaken*, Europees Parlement: Commissie burgerlijke vrijheden, justitie en binnenlandse zaken, (2013/2188(ini)).<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//ep//nonsgml+comparl+pe-526.085+02+doc+pdf+Vo//nl&language=nl>.
- Mueller, M. en B. Wagner (2014) *Finding a Formula for Brazil: Representation and Legitimacy in Internet Governance*. http://www.internetgovernance.org/wordpress/wp-content/uploads/MiltonBenWPdraft_Final.pdf.
- iObservatório da internet.br (2011) *Internet Policy Report: Brazil 2011*. <http://observatoriodainternet.br/internet-policy-report-brazil-2011>.
- Shih, E., A. Venkatesh, S. Chen en E. Kruse (2013) 'Dynamic Use Diffusion Model in a Cross-National Context: A Comparative Study of the United States, Sweden, and India', *Journal of Product Innovation Management*, 30, 1: 4-16.
- Varon Ferraz, J. en M. Maciel (2012) *Report: Brazilian Preparation for World Conference on International Telecommunications (wcit-12)*. https://www.dropbox.com/s/lnrhfond3db3oz/wcit_Brazilian_report_dez_final.pdf.
- Wilson, D. en R. Purushothaman (2006) 'Dreaming with bricks: The path to 2050', blz. 3-45 in C.J. Subhash (red.) *Emerging Economies and the Transformation of International Business*, Cheltenham: Edward Elgar Publishing.