Aspekte van Regsbeheer in die Konteks van die Internet
(Aspects of Legal Regulation in the Context of the Internet)

ASPEKTE VAN REGSBEHEER IN DIE KONTEKS VAN DIE INTERNET

(ASPECTS OF LEGAL REGULATION IN THE CONTEXT OF THE INTERNET)

by

BARRIE JAMES GORDON

submitted in accordance with the requirements
for the degree of

DOCTOR OF LAWS

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF S S NEL

June 2016

Verklaring

Naam: Barrie James Gordon

Studentenommer: 3923-337-5

Graad: Legum Doctor

Titel: Aspekte van Regsbeheer in die Konteks van die Internet

Ek verklaar hiermee dat die doktorale proefskrif getiteld “Aspekte van Regsbeheer in die Konteks van die Internet” my eie werk is en dat ek alle bronne wat ek gebruik of aangehaal het, deur middel van volledige verwysings aangedui en erken het.

_____

Barrie James Gordon 20 Junie 2016

Opgedra aan my vrou, Marié, en dogters Marlize en Lizelle.

Dankbetuiging

Graag spreek ek my opregte dank en waardering uit teenoor die volgende persone vir hul bydraes tot hierdie proefskrif:

- My promotor, professor S S Nel vir haar nuttige kommentaar en redigering, asook my kollegas vir hulle aanmoediging.
- My uitgebreide familiekring vir hul ondersteuning en gebede.
- ‘n Besondere woord van dank aan my eggenoot Marié, en my dogters Marlize en Lizelle vir hul verdraagsaamheid, opofferings en volgehoue aanmoediging tydens die skryf van hierdie proefskrif. Sonder julle insette sou hierdie proefskrif nie moontlik gewees het nie.
- Ten slotte — en ook belangrikste — is ek ewig dankbaar vir die genade, krag en leiding wat ek van my God Jehova Jireh, my Voorsienier, en ons Here Jesus Christus ontvang het om hierdie proefskrif te voltooi. U het my gedagtes gerig, en ek prys U daarvoor.

***

Opsomming

Titel: Aspekte van Regsbeheer in die Konteks van die Internet

Deur: Barrie James Gordon

Graad: Legum Doctor

Studieleier: Prof. S S Nel

Die wêreld soos dit vandag bestaan, is gebaseer op die Internasionaalregtelike konsep van soewereiniteit. State het die bevoegdheid om hulle eie sake te reël, maar die ontwikkeling van die Internet as 'n netwerk wat globaal verspreid is, het hierdie beginsel verontagsaam. Dit wou voorkom asof die Internet die einde van soewereiniteit en staatskap sou beteken.

'n Geskiedkundige oorsig toon dat reguleerders aanvanklik onseker was oor hoe hierdie nuwe medium hanteer moes word. Dit het geblyk dat nuwe tegnologieë wat fragmentasie van die Internet bewerkstellig, gebruik kon word om staatsgebonde regsreëls af te dwing. Verskeie state van die wêreld het uiteenlopende metodologieë gevolg om die Internet op staatsvlak te probeer reguleer, en dit het tot die lukraak-wyse waarop die Internet tans gereguleer word, aanleiding gegee.

Hierdie studie bespreek verskeie aspekte van regsbeheer in die konteks van die Internet, en bepaal daardeur hoe die Internet tans gereguleer word. Toepaslike wetgewing van verskeie state word regdeur die studie bespreek. Vier prominente state, wat verskeie belangrike ingrepe ten aansien van Internetregulering gemaak het, word verder uitgelig. Dit is die Verenigde State van Amerika, die Volksrepubliek van Sjina, die Europese Unie as verteenwoordiger van Europese state, en Suid-Afrika. Aspekte wat op Internasionaalregtelike vlak aangespreek moet word, soos internasionale organisasies en internasionale regsteorieë ten aansien van die regulering van die Internet, word ook onder die loep geneem.

Die bevindings wat uit die studie volg, word gebruik om verskeie aanbevelings te maak, en die aanbevelings word uiteindelik in ’n nuwe model saamgevoeg om ’n sinvoller wyse van regulering van die Internet voor te stel.

Aangesien die huidige studie in die konteks van die Internasionale reg onderneem word, word die studie afgesluit met ’n bespreking van kubersoewereiniteit, wat ’n uiteensetting is van hoe soewereiniteit ten aansien van die Internet toegepas behoort te word. Die gevolgtrekking is insiggewend — die ontwikkeling van die Internet het nie die einde van soewereiniteit beteken nie, maar het dit juis bevestig.

Sleutelwoorde: Internet; soewereiniteit; regulering; selfregulering; regering; netwerk neutraliteit; ICANN; dieppakketinspeksie; tussengangers; Internet-diensverskaffers; kubersoewereiniteit; staatskap.

Summary

Title: Aspects of Legal Regulation in the Context of the Internet

By: Barrie James Gordon

Degree: Legum Doctor

Supervisor: Prof. S S Nel

The world is currently structured in different states, and this is premised on the International law concept of sovereignty. States have the capacity to structure their own affairs, but the development of the Internet as a globally distributed network has violated this principle. It would seem that the development of the Internet would mean the end of sovereignty and statehood.

A historical overview shows that regulators were initially unsure of how this new medium should be dealt with. It appeared that new technologies that could fragment the Internet, could be used to enforce state bound law. Several states of the world have used different methodologies trying to regulate the Internet at state level, and this led to the random way in which the Internet is currently regulated.

This study examines various aspects of legal regulation in the context of the Internet, and determines how the Internet is currently regulated. Appropriate legislation of several states are discussed throughout the study. Four prominent states, which made several important interventions regarding the regulation of the Internet, are highlighted further. It is the United States, the People's Republic of China, the European Union as the representative of European countries, and South Africa. Aspects that need to be addressed on International law level, such as international organizations and international legal theories regarding the regulation of the Internet, are also discussed.

The findings that follow from this study are used to make several recommendations, which in turn are used to construct a new model for a more meaningful way in which the Internet could be regulated.

Since the present study is undertaken in the context of the International law, the study is concluded with a discussion of cyber sovereignty, which is a discussion of how sovereignty should be applied with regards to the Internet. The conclusion is enlightening — the development of the Internet does not indicate the end of sovereignty, but rather confirms it.

Key terms: Internet; sovereignty; regulating; governance, self-regulation; government; network neutrality; ICANN; deep packet inspection; intermediaries; Internet service providers; cyber sovereignty; statehood.

Inhoudsopgawe

Lys van Figure

Hoofstuk 1

Inleiding en Probleemstelling

> *For something so central to the modern world, the Internet is shambolically governed. It is run by a hotch-potch of organisations with three–to–five–letter acronyms. Many of their meetings, both online and offline, are open to the public. Some — like the Internet Governance Forum are just talking shops. Decision-making is slow and often unpredictable. It is in short a bit chaotic.*[1]
>
> The Economist

1.1 Inleiding

DIE GESKIEDENIS VAN die moderne mens oor die laaste paar eeue het ontvou op 'n manier wat die wêreld in geografiese gebiede verdeel het.[2] In elkeen van hierdie gebiede is regerings saamgestel op grond van

---

1 The Economist "In Praise Of Chaos: Governments' Attempts To Control The Internet Should Be Resisted" http://www.economist.com/node/21531011 (besoek op 11 November 2014).

2 Daar word algemeen aanvaar dat die moderne konsep van individuele state, wat elkeen soewerein is, by die vrede van *Wesfalia* in 1648 begin het. Cox M, Dunne T en Booth K (red) *Empires, Systems and States: Great Transformations in International Politics* (2001) 35. Tog blyk dit egter dat hierdie konsepte nie tydens die vrede van *Wesfalia* ingevoer is nie, maar eerder dui op die vrede wat die wêreld ondervind het in die tydperk daarna. Orakhelashvili A *Research Handbook on the Theory and History of International Law* (2011) 414. Vir 'n volledige verduideliking van die oorsprong van moderne state, sien Mills A "The Private History of International Law" 2006 *International and Comparative Law Quarterly* 1 veral 17–23.

uiteenlopende filosofiese- en ideologiese beginsels.[3] Een gemeenskaplike faktor onderlê al hierdie state, naamlik soewereiniteit.[4]

Soewereiniteit behels dat elke staat van die wêreld die vermoë het om self te besluit oor die regsbeginsels wat in sy eie grondgebied sal geld.[5] Wanneer enige hof dus oor 'n regsaangeleentheid moet beslis, sal die onderliggende vraag altyd wees of dit in staat is om die saak aan te hoor — kortom, of die betrokke hof die nodige jurisdiksie het.[6]

Die ontwikkeling van die Internet[7] het hierdie fundamentele wyse waarop die wêreld gereguleer word, verontagsaam deurdat daar geen geografiese omheining tussen lande in die kuberruim[8] is nie. Hierdie realiteit het mense in staat begin stel om vryelik op die Internet oor territoriale grense heen te beweeg.[9]

---

3 Claessen H J M en Oosten J G *Ideology and the Formation of Early States* (1996) 359 stel dit so: "We view ideology as the organization of ideas and values in a society. Here we are particularly dealing with ideas and values concerning the nature of society, or more specifically, ... states".

4 Krasner S D *Sovereignty: Organized Hypocrisy* (1999) 11–12.

5 Rawlings R, Leyland P en Young A *Sovereignty and the Law: Domestic, European and International Perspectives* (2013) 35 verduidelik die ineengevlegte aard van soewereiniteit en die reg: "Sovereignty is a fundamental concept of both political and legal thought, expressing the autonomous nature of the State's political power and its specific mode of operation in a distinctively juristic form. In this way, sovereignty symbolizes the specific character of political and legal authority within modernity". Ook Fowler M R en Bunck J M *Law, Power, and the Sovereign State: The Evolution and Application of the Concept of Sovereignty* (1995) 12.

6 "In many jurisdictions, the litmus test for determining whether assertion of jurisdiction is appropriate involves analyzing whether jurisdiction is reasonable under the circumstances. While admittedly a subjective concept, courts in the U.S and Canada have regularly relied on a reasonableness standard as their guide." Geist M A "Is There a 'There' There — Toward Greater Certainty for Internet Jurisdiction" 2001 *Berkeley Technology Law Journal* 1345 1355.

7 In hierdie studie het die woorde "Internet" en "intranet" verskillende betekenisse. "Internet" word gebruik om die globale Internet te beskryf. Soos daar verder in die studie verduidelik sal word, het die globale Internet sedert die begin van die 21ste eeu 'n geweldige fragmentasie ondergaan — in so 'n mate dat die globale Internet nou reeds as 'n reeks kleiner "intranette" beskou kan word wat min of meer geografiese gebiede omsluit. Die term "intranet" word byvoorbeeld in afd 2.3.6.3 gebruik om Sjina se geografiese staat-netwerk te beskryf. Dit is nie 'n vreemde manier om hierdie strukture te konstrueer nie: Radu R, Chenou J en Weber R (red) *The Evolution of Global Internet Governance: Principles and Policies in the Making* (2014) 144 maak byvoorbeeld melding van "... pointed to the potential isolation of China's *intranet* from the global *Internet*". My kursivering.

8 Die woord kuberruim word gebruik as 'n vertaling vir die term "cyberspace". Laasgenoemde term word algemeen gebruik om die elektroniese wêreld van die Internet te beskryf. Lloyd I J *Information Technology Law* (2000) 7. Ploug T *Ethics in Cyberspace: How Cyberspace May Influence Interpersonal Interaction* (2009) 70 beskryf die kuberruim as: "[C]yberspace is some sort of place for interaction made available by networks of interconnected computers".

9 Johnson D R en Post D G "Law and Borders — The Rise of Law in Cyberspace" 1995 *Stanford Law Review*

So ’n sisteem skep enersyds geweldige geleenthede waar individue oor landsgrense met mekaar kan kommunikeer, met sosiale groepe kan skakel[10] en selfs kan handel dryf.[11] Andersyds skep dit groot probleme waar mense nou in staat is om selfs misdrywe in ’n bepaalde jurisdiksie te pleeg sonder om fisies daar aanwesig te wees.[12]

Die ontwikkeling van die Internet het ’n probleem vir individuele state geskep. Enersyds het die behoefte ontstaan om plaaslike inwoners te beskerm,[13] en andersyds het die globale aard van die Internet regulatoriese en wetgewende probleme geskep.[14] Regerings het besef dat hulle sal moet ingryp om hulle inwoners te beskerm, maar die wyse waarop dit deurgevoer kon word, was nog nie duidelik nie.[15]

Om regsbeginsels vir die Internet neer te lê, is egter nie so eenvoudig soos die promulgering van nasionale wetgewing nie.[16] Soos reeds genoem was die Internet tydens sy ontstaansjare ’n globale netwerk, en die promulgering van nasionale wetgewing is nie by magte om internasionale kwessies aan te spreek nie.[17] Daarom wil dit voorkom asof dit meer sinvol sou wees om dit vanuit ’n internasionale perspektief te reguleer.

Om die probleem te vererger het lande van die wêreld begin besef dat die

---

1367 1370. Coble H *Internet Domain Name Trademark Protection* (2000) 80 skryf in die jaar 2000: “By its very nature, the Internet is international; it knows no borders. Once connected, the entire globe is accessible”.

10 Afd 4.2.2.3.

11 Afd 4.2.2.3.

12 Wall D S “The Internet as a Conduit for Criminal Activity” 2005 *Information Technology and the Criminal Justice System* 78 82 meld byvoorbeeld: “Examples of such activities include trading in sexually explicit materials ... but also many types of fraudulent activity. The increasing prevalence of deception through Internet auctions, for example, is a vivid example of this level of opportunity”.

13 Afd 6.3.3 noem ’n voorbeeld waar onwettige sigaretverkope vanuit ’n ander staat verhinder moes word, en die metodes wat gevolg is om dit suksesvol in werking te stel.

14 Afd 3.3.2.

15 Afd 3.3.2 bespreek byvoorbeeld die saak van *Reno v American Civil Liberties Union* 521 US 844 117 S Ct 2329 138 L Ed 2d 874 (1997) waar dele van die Amerikaanse “Communications Decency Act” van 1996 ongrondwetlik verklaar is. Dit word wyd bestempel as die eerste poging wat die Amerikaanse regering aangewend het om aangeleenthede van die Internet te beheer. Grewlich K W *Governance in "Cyberspace": Access and Public Interest in Global Communications* (1999) 274;

16 Vn 15.

17 Vn 15.

Internet 'n geweldige rol speel om ekonomiese ontwikkeling te bevorder.[18] Veral eerstewêreld-lande het begin om só op die Internet staat te maak dat die ontwrigting daarvan 'n nasionale krisis tot gevolg kan hê waar miljoene mense se lewens ingrypend kan verander.[19] Die Internet word dan as 'n nasionale bate beskou, en die beskerming daarvan word krities belangrik. Dit is nie vreemd dat lande begin het om groter maatreëls in plek te stel om sy plaaslike deel van die Internet te beskerm nie.[20] Daar kan onomwonde gesê word dat die Internet 'n politieke speelbal geword het om nasionale belange te beskerm. Hierdie prentjie word volledig in hoofstuk 5 van die studie geskets.[21]

Ten spyte daarvan dat die Internet reeds meer as drie dekades oud is, word dit steeds op 'n lukraak-manier gereguleer.[22] Individuele state, nie-regeringsorganisasies en internasionale maatskappye probeer steeds eensydig hulle eie belange bevorder, en die algemene Internetgebruiker is die een wat daaronder ly. 'n Nuwe, soepeler benadering sal gevind moet word om effektiewe regulering van die Internet te bewerkstellig. Hierdie studie sal poog om 'n bydrae te lewer in hierdie verband.

1.2 Doelstelling en Afbakening van die Studie

Die regulering van die Internet word huidig op 'n lukraak metode hanteer.[23] Aanvanklik is soewereine state se wetgewers ietwat onkant gevang met die

---

18 Sternberg P *Broadband Internet's Value for Rural America* (2010) 38 noem byvoorbeeld: "The Internet, and more specifically broadband Internet, has become an integral part of the broader economy".

19 Sternberg *Broadband Internet's Value for Rural America* 38.

20 Afd 7.3.1.

21 Hfst 5.

22 Thierer A D en Crews C W *Who Rules the Net?: Internet Governance and Jurisdiction* (2003) 119 verduidelik: "... the prospect of states applying haphazard and uncoordinated multijurisdictional regulation to the Internet's seamless electronic Web raises profound questions ...". Voorbeelde van lukraak hantering van Internetregulering word bespreek in hfst 6 en 7: die VSA maak gebruik van uitgebreide spioenasie op die Internet (afd 6.4.1.5) , terwyl Sjina volledig hulle intranet reguleer (afd 6.4.2), en state soos Duitsland, Indië en Brasilië neem stappe om sensitiewe inligting binne hul grense te hou met data-lokalisering (afd 7.3.1.1).

23 Thierer *Who Rules the Net?* 119.

ontwikkeling van 'n rekenaarnetwerk wat globaal verspreid is.[24] Wette is geskep om hierdie groeiende medium te probeer reguleer, maar aanvanklike wetgewing was dikwels lomp en onuitvoerbaar.[25] Latere, verbeterde wetgewing, het uit hierdie mislukkings voortgespruit, en is vandag al relatief gesofistikeerd.[26] Verdere besonderhede sal in die voorgenome studie bespreek word.[27]

Soos wat die Internet gekommersialiseer geword het, het groot multinasionale maatskappye besef dat hulle 'n belangrike finansiële belang by die Internet het. Gevolglik wou hierdie maatskappye die Internet sover as moontlik onder hul beheer kry. Voorbeelde van pogings van die privaat sektor om hulle domein te beheer en te reguleer, is wydverspreid.[28]

Die regulering van die Internet is eintlik 'n internasionale verantwoordelikheid. Die internasionale gemeenskap het daarom vinnig tot die stryd toegetree.[29] Organisasies soos die Verenigde Nasies en die Raad van Europa[30] het hul stem dik gemaak deur die skep van verdrae om hulle deel van die Internet af te baken.

Wanneer 'n studie van Internetregulering onderneem word, sal dit noodwendig wyd uiteenlopende aangeleenthede, soos hierbo genoem, saamtrek, sodat daar 'n behoorlike geheelbeeld gevorm kan word.

Regulering van die Internet sal in hierdie studie vanuit twee hoeke benader word. Eerstens sal konsepsuele modelle wat poog om sinvolle strukture vir Internetregulering te skep, verduidelik en beoordeel word.[31] Voorgestelde modelle van Internetregulering van verskeie akademici en

---

24 Thierer *Who Rules the Net?* 119.

25 Vn 15.

26 Afd 6.4 verduidelik huidige wetgewing van vier state, te wete die Verenigde State van Amerika, Sjina, die Europese Unie en Suid-Afrika.

27 Hfst 3 hanteer 'n geskiedkundige oorsig oor die regulering van die Internet, terwyl hfst 6 en 7 huidige Internetreguleringskwessies aanspreek.

28 Afd 5.4 en afd 5.5.

29 Hfst 5 bespreek in besonderhede 'n lys internasionale organisasies wat betrokke is by die regulering van die Internet, terwyl hfst 6 verskeie state se reguleringspogings van die Internet bespreek.

30 "*Council of Europe*" in Engels. Dit word in afd 5.3.4 bespreek.

31 Hfst 4.

skrywers sal ondersoek word.[32] Tweedens sal die studie ook gevallestudies van Internetregulering beoordeel,[33] en bepaal of dit moontlik is om die huidige lukraak-metodes van Internetregulering te versoen met gepaste konsepsuele modelle.

Wanneer beide hierdie aangeleenthede bespreek word, sal dit weens die internasionale aard van Internetregulering deurgaans noodsaaklik wees om van 'n regsvergelykende metodiek gebruik te maak. Relevante Suid-Afrikaanse wetgewing, soos die Wet op Elektroniese Kommunikasies en Transaksies[34] en die Wet op die Reëling van Onderskepping van Kommunikasies en Verstrekking van Kommunikasie-verwante Inligting[35] sal ook beoordeel word.

1.3 Navorsingsvraag

In die konteks van 'n regstudie is dit waarskynlik meer sinvol om eerder 'n navorsingsvraag as 'n hipotese te formuleer.[36]

Die voorgenome studie postuleer die oorhoofse vraag:

Oorhoofse vraag Is daar enige oplossings wat voorgestel kan word om die Internet op 'n meer effektiewe wyse te reguleer as wat tans die geval is?[37]

Twee aangeleenthede sal bespreek word: eerstens sal daar aangedui moet word hoe die Internet tans gereguleer word, en dan sal metodes ondersoek

32 Afd 4.2.1.

33 Afd 3.3, afd 3.4 en afd 3.5.

34 Wet 25 van 2002.

35 Wet 70 van 2002.

36 "In a qualitative study, inquirers state research questions, not objectives (i.e., specific goals for the research) or hypotheses (i.e., predictions that involve variables and statistical tests). These research questions assume two forms: a central question and associated subquestions." Creswell JW *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (2008) 129.

37 Uit die bespreking hierbo is daar aangetoon dat die huidige wyse waarop die Internet gereguleer word, bloot lukraak is. Afd 1.2.

moet word sodat voorstelle aan die hand gedoen kan word vir 'n meer sinvolle oplossing tot Internetregulering.

Onderliggend hieraan sal 'n verskeidenheid ander vrae ondersoek word, te wete:

1. Behoort die Internet enigsins gereguleer te word?[38]

2. Indien wel, watter rol sal die bestaande beginsels aangaande soewereiniteit en jurisdiksie as basiese internasionaalregtelike regsbeginsels by Internetregulering speel?

In die voorgenome studie sal daar van die volgende veronderstellings uitgegaan word:

1. pogings om die Internet te reguleer word tans deur soewereine state, internasionale organisasies sowel as deur groot konglomerate in die privaat sektor aangewend

2. sodanige pogings tot regulering van die Internet word op 'n lukraak wyse hanteer

3. gevolglik is die Internet huidig gedompel in 'n warboel van teenstrydige reëls wat gelyktydig kan geld. Dit verwar gebruikers van die Internet en kan hul erg benadeel.

Die voorgenome studie sal die relevante literatuur oor die regulering van die Internet bespreek, beoordeel en krities ondersoek. Dit sal gedoen word met die doel om 'n voorstel wat effektief kan wees in die regulering van die Internet, te formuleer.

---

38 "Given the extraordinary potential for the Internet to promote the exchange of ideas and expand democratic principles on a global scale, one may wonder: Why permit any individual, group, agency, or government to regulate it at all? As with any powerful innovation, however, the Internet itself has great potential for abuse. Consequently, several situations exist in which its regulation is not only necessary, but also desirable." Dickerson N P "What Makes the Internet so Special? And Why, Where, How, and by Whom Should Its Content be Regulated" 2009 *Houston Law Review* 46 67. Sien ook Segura-Serrano A "Internet Regulation and the Role of International Law" 2006 *Max Planck Yearbook of United Nations Law* 191 193.

1.4 Navorsingsmetodologie

1.4.1 Benadering

Navorsingsmetodologie is 'n stel strategieë en spesifieke metodes wat gebruik word om spesifieke kwessies in navorsing uit te lig.[39] In die studie sal daar van 'n verskeidenheid van hierdie strategieë en metodes gebruik gemaak word.

In die eerste plek moet daar begryp word dat hierdie studie *multi-dissiplinêr* is. Minstens drie studievelde word interverweef, te wete Inligtingstegnologie, Internet-reg en Internasionale reg. 'n Basiese kennis van inligtingstegnologie is 'n voorvereiste om hierdie studie tot sy reg te laat kom, en daarom word die inleidende hoofstuk gebruik om rekenaar- en netwerktegnologieë te verduidelik.[40] Internet-reg hanteer die regsbeginsels wat spesifiek op die Internet van toepassing is, en hierdie studie steun swaar op sulke beginsels. Die Internasionale Reg is interverweef met Internet-reg, maar is tog identifiseerbaar aangesien dit grotendeels met aangeleenthede soos state, soewereiniteit, jurisdiksie en multilaterale ooreenkomste te doen het. Trouens, dit sou korrek wees om hierdie studie te beskou as 'n Internasionaalregtelike blik op Internet- en netwerkregulering.

Dit beteken dat die leser sal begryp wat die aard van die Internasionale Reg is. Dit word dikwels as "soft law" beskou, en daarmee word bedoel dat regsbeginsels nie altyd so konkreet soos in nasionale wetgewing vervat is

39 Mouton J en Marais H C *Basic Concepts: The Methodology of the Social Sciences (HSRC Studies in Research Methodology)* (1990) 55–56.

40 Hfst 2.

nie.[41] Die statuut van die Internasionale Geregshof[42] bepaal byvoorbeeld in artikel 38(1) dat die bronne van Internasionale Reg die volgende is:

(a) international conventions, whether general or particular, establishing rules expressly recognized by the contesting states;

(b) international custom, as evidence of a general practice accepted as law;

(c) the general principles of law recognized by civilized nations;

(d) judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.[43]

Die tweede bron van Internasionale reg, te wete internasionale gebruike, illustreer die punt dat Internasionale reg dikwels nie "hard law" bevat nie. Wanneer 'n hof, soos die Internasionale Geregshof, moet beslis oor aangeleenthede tussen state, kan dit internasionale gebruike beoordeel om tot 'n beslissing te kom. Dit verskil geheel en al van regulering op 'n nasionale vlak waar "harde" wetgewing en regspraak gebruik word om beslissings te vel.

Regulering van die Internet in die Internasionale Reg is bykans soos 'n skaakspel tussen state onderling.[44] Algemeen aanvaarbare internasionale

41 Sien vn 45 asook Chinkin C M "The Challenge of Soft Law: Development and Change in International Law" 1989 *International and Comparative Law Quarterly* 850 851 wat "soft law" so verduidelik: "Soft law instruments range from treaties, but which include only soft obligations, to non-binding or voluntary resolutions and codes of conduct formulated and accepted by international and regional organisations ('non-legal soft law'), to statements prepared by individuals in a non-governmental capacity, but which purport to lay down international principles". Thirlway H *The Sources of International Law* (2014) 165 gaan selfs sover deur te meld dat: "it could be contended that soft law is created in a radically different way, i.e. that it has its own source or system of sources; or even that soft law might 'constitute a source in its own right in addition to the traditional sources of international law'". Sien ook Abbot K W en Snidal D "Hard and Soft Law in International Governance" 2000 *International Organization* 421 421.

42 "International Court of Justice".

43 Statute of the International Court of Justice art 38(1).

44 Hierdie analogie is reeds eeue in gebruik, soos Weeramantry C G *Universalising International Law* (2004) 50 illustreer: "Kant observed that two sovereigns ... are like two people playing a game of chess in the comfort of their homes".

regsbeginsels, verdrae en konferensies word gebruik om hierdie skaakspel te speel en te regverdig. Hoofstuk 5 sal byvoorbeeld aantoon hoe state van die wêreld internasionale konferensies as platform gebruik om dit wat hulle by multilaterale ooreenkomste ingesluit wil hê, te onderhandel. Dit is belangrik vir die leser om te verstaan dat dít die aard van Internasionale reg is, en dat 'n bespreking daarvan binne die konteks van die internasionale reg val ten spyte daarvan dat dit nie "hard law" is nie.[45]

Hierdie studie sal in die tweede plek ook *regsvergelykend* van aard wees. Soos uit die groter studie sal blyk, staan dit inderwaarheid op twee bene: aan die een kant is daar die Internasionale sfeer van die groter en oorkoepelende Internet,[46] en aan die ander kant is daar die nasionale sfeer wat nasionale wetgewing hanteer.[47] Om hierdie studie tot sy reg te laat kom en 'n sinvolle model van Internetregulering voor te stel, moet beide kante van hierdie muntstuk bespreek word. Met die sfeer van nasionale wetgewing word regsvergelyking gebruik, soos wat in hoofstuk 6 gedoen sal word waar aanspreeklikheid van Internet-diensverskaffers bespreek sal word. Die Verenigde State van Amerika (hierna VSA), die Europese Unie en Groot-Brittanje, Sjina en Suid-Afrika sal oorweeg word.

Die VSA word gekies omdat dit die staat is wat die eerste met regulering van die Internet te doen gehad het.[48] In die VSA is daar ook die meeste oor hierdie onderwerp gepubliseer (omdat dit die VSA so direk raak). Verder het die regering van die VSA die meeste invloed om die hele Internet tot stilstand te kan bring weens die feit dat die belangrikste basisnaambedieners[49] (*root*

---

45 Abbot 2000 *International Organization* 421 verduidelik dat "The term hard law ... refers to legally binding obligations that are precise (or can be made precise through adjudicationor the issuance of detailed regulations) and that delegate authority for interpreting and implementing the law." Hulle meld ook verder op 421 dat "hard law is not the typical international legal arrangement...".

46 Bv hfst 2–5 en hfst 7.

47 Bv hfst 6.

48 Afd 6.4.1.1.

49 'n Bediener (in Engels 'n "server") is 'n rekenaarsisteem wat 'n spesifieke inligtingsfunksie op die Internet vervul. Gewoonlik word bedieners gebruik om inligting te stoor sodat dit later opgeroep kan word, soos byvoorbeeld 'n webbediener wat webblaaie stoor en vir gebruikers op aanvraag bedien. Dan is daar ook posbedieners ("mail servers") wat e-posse stoor, en databasisbedieners ("database servers") wat databasisse deursoek om inligting *via* die Internet aan gebruikers te bedien. In hierdie paragraaf

name servers) van die Internet daar geleë is. Omdat hierdie so 'n geweldige groot rolspeler in die Internetreguleringsdebat is, moet hierdie staat se hantering van Internetregulering noodwendigerwys bespreek word.

Die Europese Unie en Groot Brittanje verteenwoordig 'n Europese siening oor hoe die Internet gereguleer behoort te word.[50] Hierdie siening is baie meer internasionaal van aard aangesien die Europese Unie en Groot Brittanje die Internet as 'n internasionale bate beskou wat deur die hele wêreld besit en gereguleer behoort te word.

Sjina word gekies as 'n voorbeeld van 'n staat wat die Internet grotendeels op 'n nasionale vlak wil reguleer.[51] Die basisbeginsel wat hier ter sprake is, is dié van soewereiniteit.[52] Internetregulering word beskou as deel van 'n staat se verantwoordelikheid, wat *fragmentasie* van die groter Internet tot gevolg het.

Suid-Afrika se Internetreguleringspogings word eweneens bespreek en vergelyk met ander state se wetgewing, waarna verbande getrek en gevolgtrekkings gemaak word. Hierdie studie word vanuit 'n Suid-Afrikaanse regskonteks gemaak, en daarom is dit te verstane dat hierdie staat se wetgewing bespreek sal word.

Deur slegs van 'n regsvergelykende studie gebruik te maak, sal egter nie die volledige prentjie van Internetregulering skets nie. Daarom is die derde navorsingsmetode wat in die voorgenome studie gebruik sal word, om *voorgestelde modelle* noukeurig te ondersoek om vas te stel of dit antwoorde op Internetregulering bevat.[53]

Die navorsingsmetodes wat hierbo uiteengesit is, sal gebruik word om beginsels uit te lig en te verhelder. Aanbevelings vir 'n sisteem wat die Internet tot voordeel van die wêreld se inwoners kan reguleer, sal aan die

word daar melding gemaak van basisnaambedieners, wat die omskakeling van Domeinname en IP-adresse moontlik maak. Vir 'n illustrasie oor hoe basisnaambedieners werk, sien fig (2.8).

50 Afd 6.4.3.

51 Afd 6.4.2.

52 Hfst 7 bespreek die konsep van kubersoewereiniteit in besonderhede. Sjina is die voorloper hiermee, en gevolglik sal Sjina se kubersoeweiniteitspogings heelwat aandag geniet.

53 Hfst 4.

hand gedoen word.

1.4.2 Verwysingsbronne

Uit die aard van die saak is hierdie ’n akademiese werk, en word wetgewing, regspraak, akademiese boeke en -joernale gebruik om as hoofbron te dien. Ten spyte daarvan dat hierdie studie oor ’n Internetbron handel, word daar gepoog om die gebruik van webwerwe as verwysings in hierdie studie tot die minimum te beperk. Dit is egter nodig om soms van webwerwe gebruik te maak. Dikwels is webwerwe die primêre bron van die ondersoekende joernalistiek. Dan word die primêre (web)bron gebruik. Daar word ook gepoog om slegs gesaghebbende webbronne te gebruik, soos verwysings na die *New York Times* in die VSA, of die *Financial Times* in Brittanje, wat reeds vir dekades al koerante uitgee. In die teks word dit ook soms nodig om na Internasionale konferensies te verwys, en dan is die amptelike webwerf van die konferensiegebeure gebruik. Andermaal sal internasionale organisasies, soos die Internasionale Telekommunikasie Unie bespreek word, en dan word die amptelike webwerf van die organisasie as bron gebruik. *Blogs* is uit die aard van die saak geensins ’n betroubare bron nie, maar daar is wel een uitsondering: in die VSA word *blogs* toenemend deur internasionale maatskappye en die VSA-regering gebruik om hulle mediavrystellings[54] uit te reik, en dan is dit sinvol om na die *blog* te verwys as die amptelike mediavrystelling van die betrokke maatskappy of regeringsdepartement.[55] *Wikipedia* as Internet-ensiklopedie word slegs gebruik om inleidende stellings te staaf, asook in enkele uitsonderingsgevalle waar dit die beste verwysingsbron is.

---

54 “Press release” in Engels.

55 ’n Voorbeeld hiervan is te vinde in afd 3.4.3 vn 182 waar ’n belangrike aankondiging van die Amerikaanse “National Telecommunications and Information Administration” in ’n *blog* aangekondig is. Hierdie metode word toenemend in die VSA gebruik.

1.5 Internetregulering in die Konteks van die Internasionale Reg

Die gesaghebbende skrywer John Dugard verduidelik dat die Internasionale Reg beskou kan word as: "a body of rules and principles which are binding upon states in their relations with one another."[56] Hierdie siening dat Internasionale Reg slegs op nasies van toepassing is, kan as die tradisionele siening beskou word, want sedert die ontwikkeling van die Verenigde Nasies ná die tweede wêreldoorlog is internasionale organisasies al hoe meer as regmatige rolspelers in die Internasionale reg-arena beskou.[57] Dugard verduidelik hoe hierdie saak op die spits gedryf is toe die Verenigde Nasies vir Israel aanspreeklik wou hou vir die dood van graaf Bernadotte van Swede, wat 'n mediator in Palestina was, en daar gedood is.[58] Die Internasionale Geregshof het 'n adviserende opinie hieroor gelewer, en het beslis dat die Verenigde Nasies en sy filiale wél as rolspelers in die Internasionale reg beskou kan word, ten spyte daarvan dat hulle nie state[59] is nie. Die hof het verklaar:

---

56 Dugard J *International Law — A South African Perspective* (2011) 1; Waldock H (red) *Brierly's The Law of Nations* (1963) 1; Simpson G (red) *The Nature of International Law* (2001) 4.

57 Wolfrum R en Röben V *Legitimacy in International Law* (2008) 248 meld byvoorbeeld: "Today, the international system is no longer determined only by states but also influenced by a number of non-state actors".

58 Dugard *International Law* 1; Waldock *Brierly's The Law of Nations* 1; Simpson *The Nature of International Law* 4.

59 Huidig is daar 206 state in die wêreld. Hierdie hoeveelheid state kan op twee maniere bereken word, te wete:

- lidmaatskap van die Verenigde nasies, wat bestaan uit 193 lidlande (United Nations "Member States of the United Nations" http://www.un.org/en/members/index.shtml (besoek op 15 September 2014)); twee waarnemerstate (Die Vatikaanstad en Palestinië en 11 "ander" state, (Die sogenaamde 11 "ander" state se soewereiniteit word geensins algemeen aanvaar nie, alhoewel dit deur sommige lande erken word. Dit sluit gebiede soos die Cook-eilande en die Sahrawi Arabiese Demokratiese Republiek in.)

- soewereiniteitsdispute — 190 lande se soewereiniteit is buite verdenking, en 16 lande is in soewereiniteitsdispute gewikkel. Wikipedia "List of Sovereign States" http://en.wikipedia.org/wiki/List_of_sovereign_states (besoek op 15 September 2014).

> [t]hat is not the same thing as saying that it is a state, which it certainly is not, or that its legal personality and rights and duties are the same as those of a state. Still less is it the same thing as saying that it is "a super state". What it does mean is that it is a subject of international law and capable of possessing international rights and duties, and that it has capacity to maintain its rights by bringing international claims.[60]

Dus, volgens hierdie siening is state die hoofrolspelers in die arena van die internasionale reg, en kan die Verenigde Nasies en sy filiale as regspersone beskou word in enige handelinge en aksies wat geloods kan word.

Dugard verduidelik dat die internasionale reg sedert die tweede wêreldoorlog nog verder uitgebrei is.[61] Dit is gedoen deur state te verplig om menseregtebeskerming op individue toe te pas. State, die Verenigde Nasies en sy filiale is steeds die hoofrolspelers, maar individue kan volgens die Internasionale reg die begunstigdes van voordele wees.[62]

Laastens verduidelik Dugard dat ander entiteite, soos nie-regeringorganisasies en multinasionale maatskappye ook 'n rol in die internasionale reg speel. Hierdie organisasies word egter nie as volwaardige regspersone in die internasionale reg beskou nie.[63]

In die konteks van Internetregulering speel hierdie hiërargie tot 'n groot mate op dieselfde manier uit. State bly die grootste rolspelers, en internasionale organisasies is eweneens baie prominent. Wat egter interessant is, is dat "ander" rolspelers dikwels 'n kernrol speel by Internetregulering. Die beste voorbeelde hiervan is sekerlik organisasies soos die *Internet Corporation of Assigned Names and Numbers* (hierna ICANN),[64] wat 'n sleutelrol in die Internet se domeinnaamstelsel (hierna

---

60 International Court of Justice Report (1949) *Reparation for Injuries Suffered in the Service of the United Nations* 174 179 verkrygbaar by http://www.icj-cij.org/docket/files/4/1835.pdf (besoek op 20 Augustus 2014). Sien ook Amerasinghe C F *Principles of the Institutional Law of International Organizations* (2005) 92 en Slomanson W *Fundamental Perspectives on International Law* (2011) 128.

61 Dugard *International Law* 3–4.

62 Dugard *International Law* 4.

63 Dugard *International Law* 2.

64 ICANN is 'n organisasie wat deur die VSA se regering geskep is met die doel om 'n kernaangeleentheid van die Internet (Die DNS) te reguleer. Choucri N, Mistree D en Haghseta F *et al Mapping Sustainability: Knowledge e-Networking and the Value Chain* (2007) 347 verduidelik:

DNS)[65] speel, en die *Internet Engineering Task Force* (hierna IETF), wat die Internet se standaarde bepaal.[66] Volgens die meer tradisionele siening van regspersone binne die internasionale reg sal hierdie rolspelers nie as ware regspersone beskou word nie, omdat hulle nie state of een van die Verenigde Nasies se filiale is nie. Dit is problematies, en in die een-en-twintigste eeu is dit waarskynlik 'n siening wat nie langer water sal kan hou nie.

1.6 Uiteensetting van die Studie

Hoofstuk 2 bied 'n geskiedkundige oorsig oor die ontstaan van die Internet. Alhoewel so 'n hoofstuk aanvanklik vreemd mag voorkom in 'n regstudie, het dit ten doel om drie aangeleenthede aan te spreek. Ten eerste vorm die geskiedenis van die ontstaan van die Internet 'n goeie agtergrond om die gebeure wat huidig afspeel, beter te verstaan. Tweedens vertoon die Internet vandag heelwat ander eienskappe as selfs 'n dekade gelede.[67] Meestal bestaan daar steeds die siening dat die Internet 'n universele en eenvormige netwerk is, terwyl dit glad nie meer die geval is nie. Die Internet het ontwikkel van 'n globale, universele en verspreide netwerk tot 'n hoogs gefragmenteerde netwerk.[68] Hierdie feit hou geweldige gevolge

> ICANN is a private not-for-profit company which administers the Internet formerly managed by the US. government. It has an international board of directors which the European Commission has claimed is subject to too much US. political interference since changes cannot be made in the domain name system without approval of the US. Department of Commerce.

ICANN se skepping en struktuur word volledig in afd 5.4.1 bespreek.

65 Dulaney E *Linux All-in-One For Dummies* (2010) 495 verduidelik die DNS soos volg:

> "Domain Name System (DNS) is an Internet service that converts a fully qualified domain name, such as www.debian.org, into its corresponding IP address, such as 194.109.137.218. You can think of DNS as the directory of Internet hosts — DNS is the reason why you can use easy-to- remember hostnames even though TCP/IP requires numeric IP addresses."

Die DNS word volledig verduidelik in afd 2.3.4.

66 Post D G *In Search of Jefferson's Moose: Notes on the State of Cyberspace* (2009) 134 verduidelik die rol van die IETF so: "The IETF publishes and maintains the set of documents that, collectively, make up the 'Internet Standards' — the 'official' protocol set for the global TCP/IP network". Die IETF se skepping en struktuur word volledig in afd 5.4.3 bespreek.

67 Afd 2.3.6.

68 Afd 2.3.6.

vir die behoorlike regulering van die Internet in. Derdens is dit nodig om die fisiese argitektuur van die Internet te verstaan, aangesien dit eweneens die regulering daarvan fundamenteel beïnvloed. In hoofstuk 2 word die ontwikkeling van die Internet eers op 'n globale vlak bespreek, en dan word die ontwikkeling van die Suid-Afrikaanse intranet bespreek. Vanuit alle literatuur wat geraadpleeg is, wil dit voorkom asof dit die eerste keer is dat die historiese ontwikkeling van die Suid-Afrikaanse intranet en die regulering daarvan in enige akademiese studie in soveel besonderhede bespreek word.[69] Ou tydskrifartikels van dié era is gefynkam om die inligting te bekom en in 'n logiese formaat uiteen te sit.

Hoofstuk 3 hanteer die geskiedkundige oorsig oor die *regulering* van die Internet. Hier is die fokus nie op die ontwikkeling van die Internet sélf nie, maar eerder op die wyse waarop rolspelers in die wêreld te werk gegaan het om hulle eie stempel op die Internet af te druk. Rolspelers kan wissel van state en nie-regeringsorganisasies, tot multinasionale maatskappye en selfs individue. Hierdie hoofstuk toon aan hoe die reguleringsprentjie wat tans bestaan, sy ontstaan gehad het.

In hoofstuk 4 van die studie word twee oorhoofse sake hanteer. Enersyds word fundamentele konsepte wat die regulering van die Internet onderlê, bespreek. Andersyds word teoretiese modelle van hoe die Internet gereguleer kan word, bespreek.

Hoofstukke 5 en 6 bespreek die betrokke rolspelers by Internetregulering. Hoofstuk 5 bespreek nie-regeringreguleringrolspelers, wat wissel van internasionale organisasies (volgens die Internasionale Reg) tot Internetdiensverskaffers (wat gewoonlik nasionale maatskappye is). Hoofstuk 6 hanteer die rol wat state speel in die regulering van die Internet. Om dit te skets, word daar eers aangedui hoe dit vir regerings moontlik is om regulerings-ingrepe buite hulle state mee te bring, en dan word vier state se spesifieke reguleringspogings bespreek. Die state is (a) die Verenigde State van Amerika, (b) die Volksrepubliek van Sjina, (c) die Europese Unie met

[69] Afd 2.4 en afd 3.5.

inbegrepe die Verenigde Koninkryk en (d) Suid-Afrika.

Die splinternuwe konsep van kubersoewereiniteit word in hoofstuk 7 bespreek. Hiermee saam word sekere Internasionaalregtelike beginsels van jurisdiksie wat kubersoewereiniteit ondersteun, onder die loep geneem.

Hoofstuk 8 bevat die studie se samevatting, gevolgtrekkings en aanbevelings. 'n Nuwe model vir Internetregulering word voorgestel.

Hoofstuk 2

Geskiedkundige Oorsig oor die Ontstaan van die Internet

> *In only a few years, the Internet has revolutionized trade, health, education, and, indeed, the very fabric of human communication and exchange. Moreover, its potential is far greater than what we have seen in the relatively short time since its creation. In managing, promoting, and protecting its presence in our lives, we need to be no less creative than those who invented it. Clearly, there is a need for governance, but that does not necessarily mean that it has to be done in the traditional way, for something that is so very different.*[1]
>
> Kofi Annan

2.1 Inleiding

VOORDAT DIE REGULERING van die Internet in enige diepte bespreek kan word, is dit nodig om eers te verstaan wat dit is en hoe dit ontstaan het. Hierdie hoofstuk sal poog om hierdie vrae te beantwoord en ook aantoon in watter mate die Internet ontwikkel het tot dit wat dit vandag is.

Met die eerste oogopslag sal dit vreemd voorkom dat 'n hoofstuk soos hierdie in 'n regstudie ingesluit word. Tog is dit nodig om die fisiese

[1] Die sekretaris-generaal van die Verenigde Nasies, K. Annan, tydens die "Global Internet Governance Forum" New York, Maart 2004. Gelbstein E en Kurbalija J *Internet Governance Issues, Actor and Divides* (2005) 7.

argitektuur van die Internet te bespreek, aangesien dit onderliggend is aan die regulering daarvan.[2] In die fisiese wêreld bestaan daar sekere natuurwette, soos swaartekrag. Dit is in so 'n mate deel van die daaglikse lewe dat dit nie bewustelik oorweeg word nie, en tog is almal daaraan onderworpe sonder enige keuse in die saak. Daarom sou dit onsinnig wees om byvoorbeeld wetgewing uit te vaardig oor mense se onderworpenheid aan swaartekrag.

Die Internet is egter anders. Dit is 'n "wêreld" wat geskep word binne die sfeer van mikroskywe, drade, rekenaars en netwerke.[3] Ál hierdie sake is binne die beheer van die mens, en deur die fisiese argitektuur van die Internet te manipuleer, is dit moontlik om die grondbeginsels wat hierdie ruimte onderlê, fundamenteel te wysig.[4] Trouens, dit het reeds in die bestaan van die Internet gebeur — want die Internet was aanvanklik 'n sentrale netwerk wat die hele aarde oorspan het, maar dit het sedert die begin van die huidige millennium al hoe meer gefragmenteerd geword.[5] Dit is eers wanneer hierdie beginsel van "Code is Law"[6] verstaan word dat dit duidelik word dat 'n begrip van die argitektuur van die Internet onderliggend aan 'n begrip van Internetregulering is. Hierdie hoofstuk dien as agtergrond vir die studie. 'n Deeglike begrip van die argitektuur van die Internet sal lei tot 'n groter insig van die regsbeginsels ten aansien van die regulering van die Internet.

2.2 Wat is die Internet?

Miljoene mense maak elke dag van die Internet gebruik om hul lewe te vergemaklik. Dit is belangrik om te weet wat die Internet is, alvorens die

2 Lessig L *Code Version 2.0* (2006) 1.

3 Traynor P, McDaniel P en La Porta T *Security for Telecommunications Networks* (2008) 2.

4 Lessig *Code Version 2.0* 1.

5 Afd 2.2.4; Werbach K "The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing it Apart" 2008 *University of California Davis Law Review* 343 397.

6 Lessig *Code Version 2.0* 1; Svantesson D J B "Borders on, or Border Around — the Future of the Internet" 2006 *Albany Law Journal of Science and Technology* 343 355.

vraag oor hoe die Internet gereguleer kan word, sinvol beantwoord kan word.[7] Verskeie definisies is geformuleer om die internet te beskryf. Hierdie definisies word vervolgens bespreek.

2.2.1 Verskillende Definisies

2.2.1.1 Definisie volgens die *Internet Engineering Task Force*

Die Internet Engineering task Force[8] definieer die Internet as 'n sisteem van ineengeskakelde pakketnetwerke wat kommunikasie onderling tussen hulle moontlik maak.[9] In die eerste plek is die Internet bloot 'n saamskakeling van individuele netwerke deur middel van 'n globale infrastruktuur.[10] In die tweede plek gebruik die rekenaars wat almal gebruik word om die Internet te vorm, almal 'n gemeenskaplike protokol wat hul in staat stel om te kommunikeer.[11] Derdens word inligting tussen die netwerke gestuur deur die gebruikmaking van datapakkette, of datagramme.[12]

Volgens die IETF is daar vier beginsels wat die Internet onderlê:

(a) Die Internet is 'n netwerk van netwerke.[13]

---

7 Die eerste paar jaar van die bestaan van die kommersiële Internet het baie opgewondenheid vir die gewone gebruiker ingehou. Sien Simon L D *Netpolicy.com: Public Agenda for a Digital World* (2000) 3–8 waar daar byvoorbeeld gemeld word:

> Almost overnight, ordinary people began to alter the habits of a lifetime in going about their normal business. Planning a vacation, a family might no longer go to a travel agent or even call an airline. Instead, the parents would consult their computer screen, looking at hilton.com, usair.com, and arizona.gov or one of thousands of other sites to make hotel or plane reservations or learn about tourist destinations.

8 Afd 5.4.3 verskaf 'n volledige bespreking van die IETF.

9 Dit word soos volg in die oorspronklike Engels uitgedruk: "An Internet communication system consists of interconnected packet networks supporting communication among host computers using the Internet protocols." Internet Engineering Task Force "Requirements for Internet Hosts: Communication Layers" http://tools.ietf.org/html/rfc1122 (besoek op 20 Augustus 2014).

10 Knake R K *Internet Governance in an Age of Cyber Insecurity* (2010) 6.

11 Internet Engineering Task Force "Requirements for Internet Hosts: Communication Layers" http://tools.ietf.org/html/rfc1122 (besoek op 20 Junie 2014) 1.1.3.

12 Internet Engineering Task Force "Requirements for Internet Hosts: Communication Layers" http://tools.ietf.org/html/rfc1122 (besoek op 20 Junie 2014) 1.1.3. Definisie van "IP Datagram" 1.3.3 17.

13 Internet Engineering Task Force "Requirements for Internet Hosts: Communication Layers" http://tools.ietf.org/html/rfc1122 (besoek op 20 Augustus 2014) 1.1.2(a).

Individuele rekenaars word nie direk aan die groter Internet geskakel nie. Aldus die IETF is skakeling tussen rekenaars en die Internet bloot "konsepsueel".[14] Hiermee word bedoel dat individuele rekenaars aan netwerke geskakel word, hierdie netwerke word op hul beurt weer aan onderlinge internetwerke geskakel, en hierdie internetwerke van die wêreld word met mekaar gekoppel om die groter Internet te vorm. Skakeling van 'n individuele netwerk aan die groter Internet word 'n "gateway" genoem.[15] In hierdie studie sal die woorde "poort" of "deurgangspoort" gebruik word om 'n "gateway" te beskryf.

(b) Deurgangspoorte is "staatloos".[16]

Hiermee word bedoel dat deurgangspoorte datagramme aanstuur sonder om die datagram sélf of sy bestemming in ag te neem. Sodoende kan datagramme wat 'n enkele boodskap uitmaak en na dieselfde individuele rekenaar op pad is, verskeie roetes volg. Elke datagram word na die roeteerder[17] gestuur wat beskikbaar is om die datagram te roeteer, en volg uiteenlopende roetes na sy uiteindelike bestemming.

Hierdie beginsel van die Internet is besig om radikaal te verander. Die gebruik van dieppakketinspeksie, wat in afdeling 5.5.1 bespreek word, sal die beginsel van staatloosheid van deurgangspoorte geheel en al

14 Internet Engineering Task Force "Requirements for Internet Hosts: Communication Layers" http://tools.ietf.org/html/rfc1122 (besoek op 20 Augustus 2014) 1.1.2(a).

15 Jin H, Yang L T en Tsai J P *Ubiquitous Intelligence and Computing* (2006) 282 verduidelik dit soos volg: "[The] Internet Gateway allocates the addresses to other *ad-hoc* nodes with its network prefix and manages the allocated addresses".

16 Internet Engineering Task Force "Requirements for Internet Hosts: Communication Layers" http://tools.ietf.org/html/rfc1122 (besoek op 20 Augustus 2014) 1.1.2(b).

17 Die woord "roeteerder" word gebruik om die Engelse konsep van "router" te beskryf. 'n Roeteerder is 'n kragtige rekenaar wat datagramme na 'n ander roeteerder stuur, dus volg die datagram 'n *sekere roete* wat deur die roeteerders bepaal word. (Daarom nie "roteerder" nie, want laasgenoemde dui 'n sirkelbeweging aan.) Vir 'n konsepsuele voorstelling van 'n roeteerder, sien fig 2.1 asook fig 2.3 waar elke node op die voorstelling 'n roeteerder illustreer. Medhi D *Network Routing: Algorithms, Protocols, and Architectures* (2010) 5 beskryf die funksies van 'n roeteerder so: "Cross-points in the Internet are known as routers. A router's functions are to read the destination address marked in an incoming IP packet, to consult its internal information to identify an outgoing link to which the packet is to be forwarded, and then to forward the packet".

ongedaan maak.

(c) Roetering behoort by deurgangspoorte en roeteerders hanteer te word.[18]
Omdat roetering 'n ingewikkelde proses is, word dit deur rekenaars gedoen wat spesifiek vir hierdie doel ontwerp is, te wete roeteerders. Roetering is 'n funksie wat nie aan bedieners[19] oorgelaat kan word nie.[20]

(d) Die Internet moet wye netwerk-variasies kan hanteer.[21]
Dit word so verduidelik: "A basic objective of the Internet design is to tolerate a wide range of network characteristics — e.g., bandwidth, delay, packet loss, packet reordering, and maximum packet size."[22] Die Internet is júís as 'n verspreide netwerk ontwerp om onwankelbaar te wees.[23]

2.2.1.2 Definisies vanuit Regspraak en Wetgewing

In die VSA is die Internet in *American Civil Liberties Union v Reno*[24] soos volg beskryf:

> The Internet is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer networks. It is thus a network of networks.[25]

---

18 Internet Engineering Task Force "Requirements for Internet Hosts: Communication Layers" http://tools.ietf.org/html/rfc1122 (besoek op 20 Augustus 2014) 1.1.2(c).

19 Hfst 1 vn 49.

20 Internet Engineering Task Force "Requirements for Internet Hosts: Communication Layers" http://tools.ietf.org/html/rfc1122 (besoek op 20 Augustus 2014) 1.1.2(c).

21 Internet Engineering Task Force "Requirements for Internet Hosts: Communication Layers" http://tools.ietf.org/html/rfc1122 (besoek op 20 Augustus 2014) 1.1.2(d).

22 Internet Engineering Task Force "Requirements for Internet Hosts: Communication Layers" http://tools.ietf.org/html/rfc1122 (besoek op 20 Augustus 2014) 1.1.2(d).

23 Afd 2.2.4 bevat meer inligting oor die Internet as verspreide netwerk.

24 929 F Supp 824 (ED Pa 1996).

25 830.

Dit is soortgelyk aan die Australiese saak van *Dow Jones and Co Inc v Gutnick,*[26] waar die Internet beskryf is as "a telecommunications network that links other telecommunication networks", en wat die vermoë het om mense in staat te stel tot "inter-communication using multiple data-formats among an unprecedented number of people using an unprecedented number of devices [and] among people and devices without geographic limitation".[27]

Meer spesifiek bestaan die Internet uit rekenaars wat spesiale sagteware naamlik die *Internet Suite* [28] gebruik om hul in staat te stel om met mekaar te kommunikeer. Dit is die *Internet Suite* wat die gom is wat verskillende netwerke aanmekaar skakel om die Internet te vorm. Die definisie van "Internet" in die Suid-Afrikaanse Wet op Elektroniese Kommunikasies en Transaksies[29] stel dit duidelik:

> "Internet" means the interconnected system of networks that connects computers around the world using the TCP/IP and includes future versions thereof.[30]

2.2.1.3 Definisie van die Russiese Federasie

Ál die definisies in afdelings 2.2.1.1 en 2.2.1.2 het 'n kernelement in gemeen. Dit is naamlik dat die Internet 'n netwerk van netwerke is. Kahn en Cerf meen egter dat hierdie siening té eenvoudig vir die moderne Internet is, en dat dit kan lei tot ongewenste resultate:

---

26 2002 HCA 56 210 CLR 575 (2002).

27 2002 HCA 56 210 CLR 575 (2002).

28 Afd 2.3.3.

29 25 van 2002.

30 Art 1 van die wet. Hierdie definisie verwys na die *Internet Suite* as TCP/IP, wat bloot 'n meer tegniese term is. Kozierok C M *The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference* (2005) 122 verduidelik die TCP/IP so: "TCP/IP consists of dozens of different protocols, of which two are usually considered the most important. The Internet Protocol (IP) is the primary 081 model network layer (layer 3) protocol that provides addressing, datagram routing, and other functions in an internetwork. The Transmission Control Protocol (TCP) is the primary transport layer (layer 4) protocol and is responsible for connection establishment and management, and reliable data transport between software processes on devices. Because these two protocols are so important, their abbreviations have come to represent the entire suite: TCP/IP".

> It is tempting to view it merely as a collection of networks and computers. However, the authors designed the Internet as an architecture that provided for both communications capabilities and information services. Governments are passing legislation pertaining to the Internet without ever specifying to what the law applies and to what it does not apply.[31]

Hierdie siening wys dat alhoewel die Internet bloot uit netwerke bestaan, die *inhoud en funksies* van die individuele netwerke radikaal kan verskil. Daar word aan die hand gedoen dat hierdie 'n korrekte beskouing is. Soms word die Internet as 'n kommunikasiemiddel gebruik. Dan het dit die eienskappe van 'n telefoon.[32] Andersyds is dit ook 'n reuse biblioteek wat enorme volumes inligting bevat.[33] Data word dus op een of ander wyse gestoor. Wanneer daar wetgewing gepromulgeer word, behoort wetgewers uiters bewus te wees van hierdie onderskeid en nie bloot die Internet as 'n enkele entiteit te beskou wat 'n eenvormige karakter het nie. Dit word dan ook veral in jurisdiksies — soos die VSA — wat onderskei tussen verskillende kommunikasiemediums soos kabel- satelliet- en algemene kommunikasiedraende dienste, 'n probleem om wetgewing uit te vaardig wat die Internet as 'n eenheid beskou.[34]

Met inagneming van hierdie kritiek wil dit voorkom asof die Russiese Federasie se definisie wat tydens die World Conference on International Telecommunications (WCIT-12) geformuleer is, meer akkuraat is:

> An international conglomeration of interconnected telecommunication networks which provides for the interaction of connected information systems and their users, by carrying their traffic using a single system of numbering, naming, addressing, identification, protocols and procedures that is defined by Internet Standards.[35]

---

31 Cooper M N (red) *Open Architecture as Communications Policy — Preserving Internet Freedom in the Broadband Era* (2004) 26.

32 *Lunney v Prodigy Services Co* 723 NE 2d 539 — NY Court of Appeals 1999 op 248–249.

33 *Cubby Inc v CompuServe Inc* 776 F Supp 135 — Dist Court SD New York 1991 op 140; *Stratton Oakmont Inc v Prodigy Services Co* 1995 WL 323710 — 1995.

34 Cooper *Open Architecture as Communications Policy* 26.

35 Russian Federation "World Conference on International Telecommunications (WCIT–12) Dubai, 3–14 December 2012: Proposals for the Work of the Conference" http://www.soumu.go.jp/main_content/000188224.pdf (besoek op 4 September 2014).

Hiermee word die *aard* van die Internet beskryf, en word die belangrike onderskeid tussen die Internet as kommunikasienetwerk en inligtingsisteem onderstreep. Tog kritiseer Hill hierdie definisie omdat dit slegs die netwerk *sélf* beskryf, en nie die spesifieke dienste en rekenaar-programme wat dit huisves nie.[36] Daar word aan die hand gedoen dat hierdie definisie bruikbaar is ten spyte daarvan dat Hill se kritiek gegrond mag wees. Dit beskryf immers die wese van die uiteenlopende moderne Internet. Hill erken dat ander definisies so wyd is dat dit nie meer net op die Internet van toepassing kan wees nie, maar selfs ander netwerke kan omvat.[37] Hill kom dan tot die gevolgtrekking dat daar geen sinvolle definisie van die Internet is nie. Dit mag moontlik so wees, maar 'n definisie wat ten minste die wese van die moderne Internet omskryf is beter as geen definisie nie.

Dit blyk dus dat dit glad nie eenvoudig is om die Internet te definieer nie. Waar sommige definisies op die strukturele aard van die Internet fokus, val die klem by ander definisies weer op die dienste wat daarop te vinde is. Hoe dit ook al sy, die Internet is nou reeds so deel van die alledaagse lewe dat meeste mense intuïtief weet waarmee hul te doen het as daar van die Internet gepraat word. Tog weet min mense hoe die argitektuur van die Internet lyk, en dit is na hierdie aangeleentheid waarna vervolgens verwys sal word.

2.2.2 Internet en Argitektuur

Verskillende rekenaars op die Internet kan in twee groepe verdeel word, te wete bedieners en roeteerders.[38] Bedieners is bloot rekenaars wat aan die Internet gekoppel is en die funksie kan verrig om inligting te stoor wat later gebruik kan word (soos teks en video), of as terminaal gebruik te kan

36 Hill R "The Internet, Its Governance, and the Multi-stakeholder Model" 2014 *Info* 16 19.

37 Hill gebruik die breër definisie van die VSA se Federal Network Council wat reeds in 1999 geformuleer is, en kom tot die gevolgtrekking dat dit egter so wyd is dat dit selfs iets soos die GSM-netwerk (selfoonnetwerk) kan beskryf. Hill 2014 *Info* 20.

38 Die IETF se *Requirements for Internet Hosts — Communication Layers* RFC:1122 1.1 verduidelik volledig die verskil tussen bedieners en roeteerders.

Bron: Oorspronklike diagram: B Gordon

Figuur 2.1: Basiese Internet-argitektuur

word om inligting te ontvang en vir ’n gebruiker aan te bied. Roeteerders daarenteen het weer die uitsluitlike doel om data-pakkette van die een roeteerder na die ander te stuur.

Skematies lyk dit soos in figuur 2.1.

In die verlede was hoofraamrekenaars met roeteerders en modems[39] gebruik om die Internet te vorm. Vandag is die posisie heel anders, en kan die fisiese argitektuur uit rekenaars bestaan wat enersyds verskillende bedryfstelsels[40] gebruik, maar ook verskillende tegnologieë, soos optiese kabels, satelliettegnologie of draadlose (*wireless*) tegnologie gebruik om rekenaars aan mekaar te koppel. Verder is die skakeling met die Internet nie meer beperk tot rekenaarterminale nie, maar vorm selfone en slimtablette

39 ’n Modem is ’n afkorting vir “modulator-demodulator”. Dit is ’n toestel wat met die plaaslike telefoonnetwerk skakel om die rekenaar se digitale sein na ’n analoë (telefoon)sein te verander. Nadat die analoogsein deur die telefoonnetwerk gestuur is, het ’n modem by die ontvanger weer die sein na ’n digitale sein omgeskakel wat deur ’n rekenaar verstaan kon word. Modems wat seine van analoog-na-digitaal omskakel, word nie meer gebruik nie, maar die naam “modem” het gebly. Toestelle wat digitale-na-digitale versending bewerkstellig, word eweneens “modems” genoem ten spyte daarvan dat dit nie seine moduleer en demoduleer nie. Gewoonlik word hierdie latere modems as ADSL-modems geïdentifiseer. Bingham J “Multicarrier Modulation for Data Transmission: An Idea Whose Time Has Come” 1990 *IEEE Communications Magazine* 5 5.

40 “Operating systems”, soos *Microsoft Windows, Linux,* of *Apple Macintosh.* Ritchie C *Operating Systems Incorporating UNIX and Windows* (2003) 1 verduidelik dit so: “Software can be classified into two distinct groups — system software and application software. Application software, as the name suggests, consists of the programs which carry out the specific processing required for user’s applications, such as an accounting system or an engineering computer-aided design package. System software is not application specific; it is oriented to the needs of the hardware and facilitates the development and running of applications. The most significant item of system software is the *operating system*, which is present in all computers except for a few very specialised applications”.

'n groterwordende deel van die wêreld se Internetgekoppelde toestelle.

2.2.3 Skakeling met Ander Tegnologieë

Die Internet se ontwikkeling hang nou saam met ander telekommunikasie-tegnologieë, soos die telefoon, radio en televisie. Trouens, dit is juis hierdie tegnologieë wat dikwels die ontwikkeling van die Internet gestimuleer en moontlik gemaak het.[41] Byvoorbeeld, voordat daar fisiese kabels was wat netwerke aan mekaar kon skakel, is telefoonargitektuur gebruik om die skakeling te bewerkstellig. Menigte gebruikers onthou nog die dae toe modems uitsluitlik deur telefoonsentrales aan die Internet gekoppel is.

Die geweldige ontwikkeling van die Internet het ook tegnologieë soos die telefoon en televisie diepliggend verander. Die telefoon is nou 'n digitale medium,[42] en elektroniese sentrales het lank reeds die meganiese sentrale vervang.[43] Die Internet het ook die domein van die tradisionele telefoon en televisie binnegedring. Internetgebaseerde telefonie soos Voice over IP (VOIP) word al hoe meer gewild, en is 'n geweldige kompetisie vir die tradisionele telefoonmaatskappye.[44] Verder bestaan daar duisende

---

41 In sy boek *Three Myths of Internet Governance* noem Collins dat die Internet nie 'n "ding" is nie, maar dat dit enersyds nou gekoppel is met die tradisionele media, en andersyds 'n intergekonnekteerde groep "lae" is wat saam die Internet vorm. Collins R *Three Myths of Internet Governance — Making sense of Networks, Governance and Regulation* (2009) 53.

Met ander woorde, die Internet is deel van die tradisionele media aangesien dit ontwikkel het *uit* die tradisionele media (bv, netwerke het ontstaan deur gebruik te maak van die telefoonnetwerk voordat daar kabels uitsluitlik vir die Internet bestaan het). Die lae waarna Collins verwys, is die *Internet Suite,* soos verduidelik in afd 2.3.3.

42 Oorspronklik het telefoonsentrales meganiese skakelaars aan- en afgeskakel, en so 'n konneksie tussen twee gebruikers bewerkstellig. Nou word alle telefoonskakelings elektronies in die sentrale hanteer, wat die diens baie vinniger en bykans foutloos maak. Newman M *Networks: An Introduction* (2010) 31 stel dit so:

> The telephone network has had roughly this same topology for most of the last hundred years and still has it today, but many of the details about how the network works have changed. In particular, at the trunk level some telephone networks are no longer circuit switched. Instead they are now digital packet switched networks that work in a manner not dissimilar from the Internet, with voice calls digitized, broken into packets, and transmitted over optical fiber links.

43 Newman *Networks* 31.

44 Vir 'n volledige verduideliking van "Voice over IP", sien Varshney U *et al* "Voice Over IP" 2002

radiostasies wat slegs op die Internet funksioneer, aangesien dit nie onderworpe is aan die toekenning van frekwensiespektrums soos die tradisionele radio nie.[45] Selfs die visuele media, wat geweldige volumes bandwydte nodig het om behoorlik te kan werk, is reeds 'n realiteit op die Internet.[46]

Selfs mediakanale wat nie direk met die Internet gekoppel is nie, het diepliggend verander. Die prominentste voorbeeld hiervan is seker die gedrukte media, waarvan koerante die sprekendste voorbeeld is. Gebruikers is in die Internet-era veel gemakliker daarmee om nuus *via* hul selfone en slimtablette te gebruik as om 'n koerant aan te skaf. Trouens, die Internet het die gedrukte media diepliggend verander, sodat video's nou ook as deel van nuusartikels weergegee word.[47] Net so raak meer spekulatiewe nuus soos vervat in *blogs*[48] al hoe meer gewild.

2.2.4 Verspreide Netwerk

Die telefoonstelsel was die eerste grootskaalse elektroniese netwerk wat mense van regoor die wêreld in staat gestel het om met mekaar te kan kommunikeer.[49] Dit was ontwikkel as 'n gesentraliseerde netwerk, wat beteken dat individuele telefone direk aan die telefoonsentrale gekoppel is. Ongelukkig het dit tot gevolg gehad dat wanneer 'n telefoonsentrale buite werking raak, *alle* telefone wat daaraan gekoppel is, onbruikbaar word.[50]

Communications of the ACM 89–96. Voice over IP word beskryf as: "VoIP involves sending voice transmissions as data packets using the Internet Protocol (IP), whereby the user's voice is converted into a digital signal, compressed, and broken down into a series of packets". Varshney 2002 *Communications of the ACM* 89.

45 Gosling W *Radio Spectrum Conservation* (2000) 215.

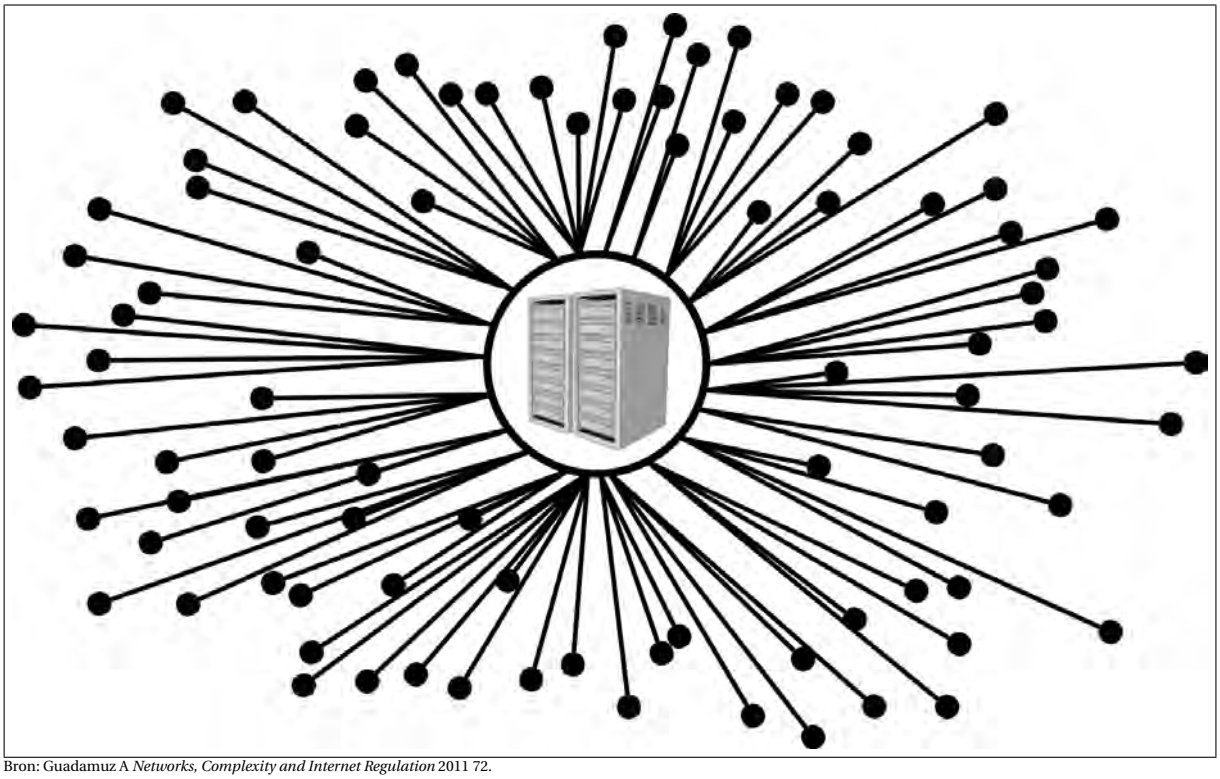
46 Voorbeelde hiervan is *Netflix* (https://www.*Netflix*.com/) en TV.com (http://http://www.tv.com/).

47 Williams J "Sites Go Straight to Video" 2000 *Editor and Publisher* 133 133 noem: "Newspapers" online versions, no longer bound by static sheets of processed pulp and ink, are now enriching stories not only with more photos and graphics, but also with movement and sound. TV has come to newspapers." Sien ook Li X *Internet Newspapers: The Making of a Mainstream Medium* (2006) 159.

48 Jean-Kenix L "Blogs as Alternative" 2009 *Journal of Computer-Mediated Communication* 790 812 wys bv dat "blogs are providing a much wider audience for mainstream views".

49 Newman *Networks* 29.

50 Newman *Networks* 30.



Bron: Guadamuz A *Networks, Complexity and Internet Regulation* 2011 72.

Figuur 2.2: Gesentraliseerde Netwerk

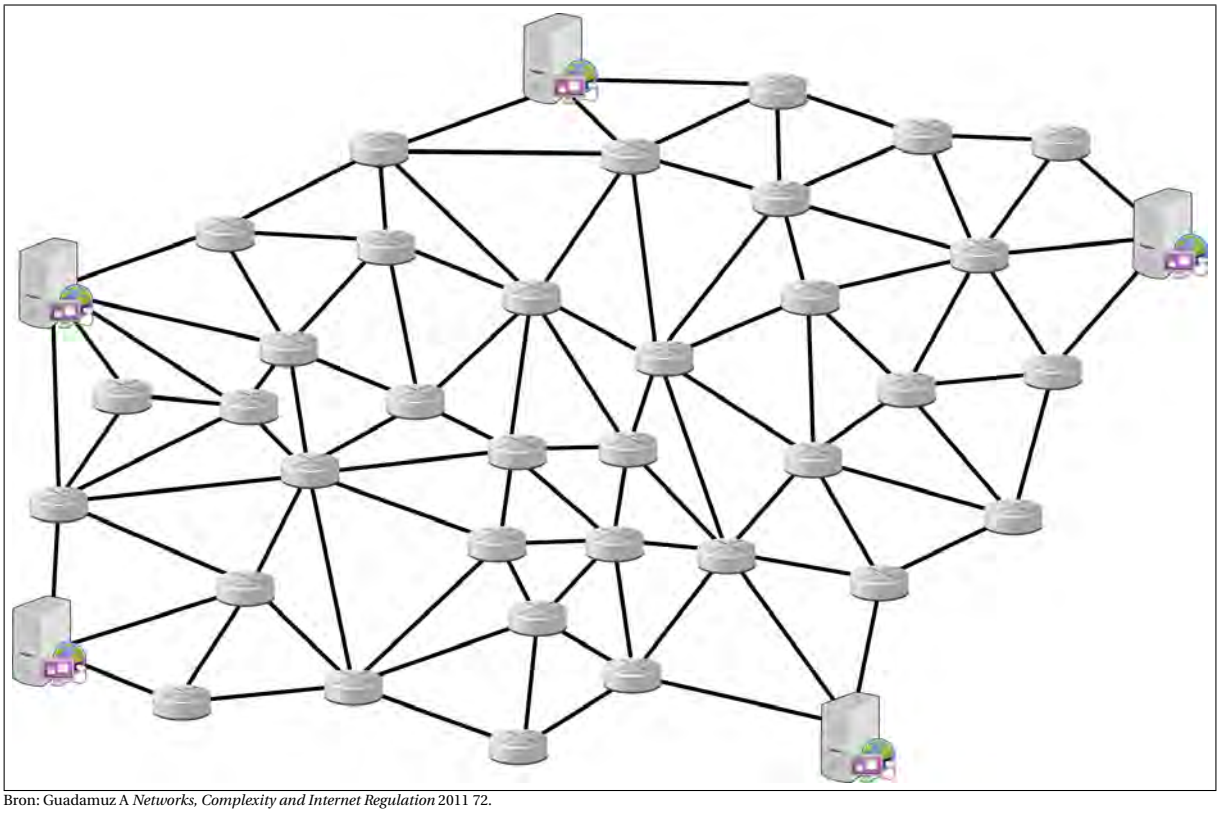
Figuur 2.2 illustreer hierdie beginsel.

Om 'n soortgelyke probleem te oorbrug, is die Internet aanvanklik ontwerp om *nie* 'n gesentraliseerde netwerk te wees nie, maar eerder 'n gedesentraliseerde, of verspreide netwerk.[51] In 'n verspreide netwerk word elke node op die netwerk aan 'n reeks ander nodes geskakel, en as een node op die netwerk ophou om te funksioneer, sal daardie node uitgeskakel word, maar sal die netwerk as geheel nog steeds kan funksioneer.[52] Figuur 2.3 toon aan hoe die Internet as verspreide netwerk lyk.

Sedert die kommersialisering van die Internet het die netwerk argitektuur geleidelik begin verander van 'n verspreide netwerk na 'n meer

51 Sears A en Jacko J *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies and Emerging Applications* (2002) 715.

52 Farivar C *The Internet of Elsewhere: The Emergent Effects of a Wired World* (2011) 30 stel dit so: "Kleinrock suggested that if they could break up the data into smaller pieces, it would be easier to send and there would be no single point of failure — the data would still be transmitted even if some node along the way were suddenly taken offline. If there were a failure along the way, the final node could re-request packets".



Bron: Guadamuz A *Networks, Complexity and Internet Regulation* 2011 72.

Figuur 2.3: Verspreide Netwerk

gesentraliseerde netwerk. Die ontwikkeling daarvan word in afdeling 2.3 bespreek.

2.2.5 Samevatting

Die Internet is fundamenteel anders as die fisiese wêreld, aangesien eersgenoemde se argitektuur volledig binne die beheer van die mens is.[53] Die belang daarvan word duidelik wanneer die gevolge daarvan besef word — deur die argitektuur van die Internet te verander, beïnvloed dit eweneens die beginsels waarvolgens dit funksioneer.[54]

In wese is die Internet 'n netwerk wat die aardbol oorspan.[55] Dit bestaan uit verskeie kleiner netwerke wat almal 'n gemeenskaplike protokol

53 Afd 2.1.

54 Afd 2.1.

55 Afd 2.2.1.

gebruik om versending van data moontlik te maak.[56] Die inhoud van data kan uiteenlopend wees, en om hierdie probleem die hoof te bied, word gestandaardiseerde datagramme gebruik om data te roeteer.[57] Dit word gedoen deur roeteerders, wat rekenaars is wat spesifiek 'n versendingsfunksie verrig.[58] Hierteenoor is daar ander bediener-rekenaars wat inligting berg vir latere gebruik, soos die aanbied van 'n webblad, video, of selfs interaktiewe dienste soos die bespreking van vlugkaartjies of hotelverblyf.[59] Die Internet is aanvanklik ontwerp om 'n verspreide netwerk te wees om stabiliteit en ononderbroke diens te verseker.[60]

2.3 Die Ontwikkeling van die Internet

Vervolgens sal die ontwikkeling van die Internet bespreek word. Hierdie oorsig is nie bloot van historiese belang nie, maar skep die basis van hoe dit moontlik sou wees om die Internet te kan reguleer. Daar sal aangetoon word hoe die ontwerpers van die Internet dit aanvanklik voorgestel het, en dat dit ontwikkel het op 'n heel ander wyse as wat die ontwerpers daarvan aanvanklik bedoel het. Deur die geskiedenis van die ontwikkeling van die Internet te bestudeer, word 'n duideliker prentjie gevorm oor die verskillende metodes wat gebruik kan word om die Internet uiteindelik te kan reguleer.

2.3.1 Rekenaartegnologie

Sonder die ontwikkeling van rekenaartegnologie sou die Internet nie moontlik gewees het nie. Voordat 'n instrument as 'n rekenaar geklassifiseer kan word, moet dit aan twee basiese vereistes voldoen, te wete die hantering

56 Afd 2.2.1.

57 Afd 2.2.1.3.

58 Afd 2.2.2.

59 Afd 2.2.2.

60 Afd 2.2.4.

van geoutomatiseerde berekenings, asook programmeerbaarheid.[61] Eersgenoemde slaan op die vermoë om wiskundige bewerkings te kan doen, terwyl laasgenoemde aandui dat die instrument op so 'n manier gerig moet kan word dat instruksies daarvoor gegee kan word om die berekeninge op 'n bepaalde manier te kan uitvoer.

Die eerste instrumente wat geoutomatiseerde transaksies kon hanteer, was waarskynlik die abakus, wat reeds duisende jare voor Christus in verskeie wêrelddele soos Persië,[62] Egipte[63] en in die Romeinse Ryk algemeen gebruik is.[64] In 1642 is die eerste meganiese optelmasjien gebou.[65] Hierdie tegnologie is verder verfyn totdat die elektroniese optelmasjien in die vroeë 1960's verskyn het. In die 1970's en 1980's het sakrekenaars 'n algemene verskynsel in huise geword.[66] Geoutomatiseerde funksies was dus nou algemeen beskikbaar, maar hierdie masjiene was nie programmeerbaar nie.

Daar is reeds hierbo aangedui dat 'n rekenaar aan twee basiese vereistes moet kan voldoen, te wete geoutomatiseerde funksies en programmeerbaarheid. Die eerste programmeerbare masjien was, eienaardig genoeg, 'n weeftoestel. In 1801 het Joseph Marie Jacquard 'n weefmasjien ontwerp wat met ponskaarte geprogrammeer kon word om sekere patrone in matte in te weef.[67] Hierdie ponskaartmetode is later deur vroeë rekenaars oorgeneem.

In 1837 het Charles Babbage die eerste programmeerbare meganiese rekenaar gekonsepsualiseer.[68] Hy het prototipes van dele daarvan gebou,

---

61 Die *Collins English Dictionary* stel dit soos volg: "a device, usually electronic, that processes data according to a set of instructions". Collins English Dictionary (2003).

62 Dit wil voorkom asof die eerste abakus reeds in 2700–2300 vC in gebruik was deur die Sumeriërs. Ifrah G *The Universal History of Computing: From the Abacus to the Quantum Computer* (2001) 11.

63 Smith D E *History of Mathematics* (1958) 160.

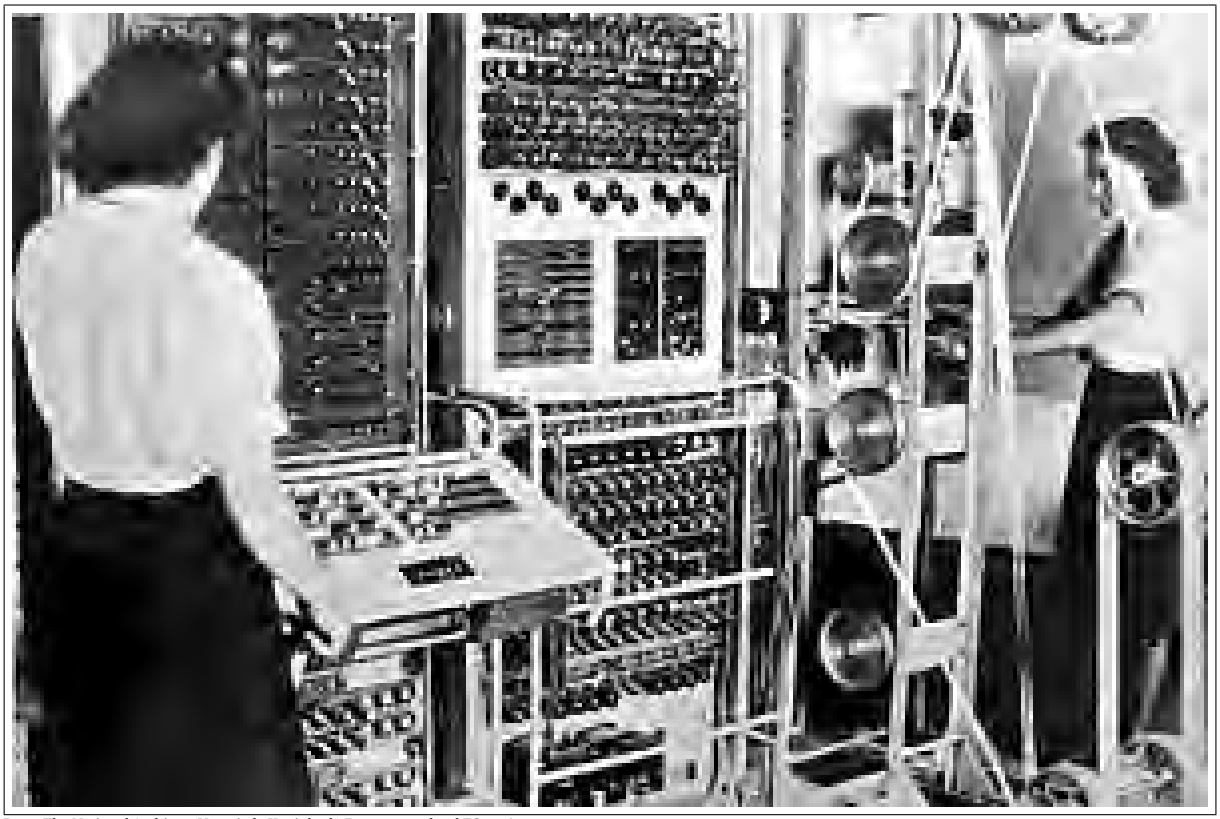
64 Ifrah *The Universal History of Computing* 15.

65 Felt D E *Mechanical Arithmetic, or The History of the Counting Machine* (1916) 10.

66 Hamrick K B "The History of the Hand-Held Electronic Calculator" 1996 *The American Mathematical Monthly* 633 636.

67 Essinger J *Jacquard's Web: How a Hand-Loom Led to the Birth of the Information Age* (2007) 36. Selfs die mees ingewikkelde patroon het nie meer as ongeveer 4000 ponskaarte nodig gehad om die ontwerp te kon uitvoer nie.

68 Hyman A *Charles Babbage: Pioneer of the Computer* (1985) 123–126, waar die ontwikkeling van die "difference engine" (soos dit toe genoem is), geskets word.



Bron: The National Archives (Verenigde Koninkryk) Documentrekord FO850/234.

Figuur 2.4: Die Wêreld se Eerste Programmeerbare Rekenaar, die *Colossus.*

maar die volledige rekenaar is nooit in Babbage se leeftyd gebou nie, aangesien dit ongeveer 8000 onderdele gehad het en ongeveer 5 ton sou weeg.[69] Die planne daarvan is egter bewaar, en in 2002 is dit uiteindelik gebou.[70] Dit het behoorlik gefunksioneer.

Die eerste programmeerbare rekenaar, genaamd die *Colossus,* is in 1943 deur ingenieur Tommy Flowers en kollegas vir die Britse geheime diens gebou. Dit moes ge-enkodeerde boodskappe wat hooggeplaaste Duitse militêre personeel vir mekaar tydens die tweede Wêreldoorlog gestuur het, dekodeer.[71] Daar is tien van hierdie superrekenaars gebou, en die elfde een is voltooi toe die tweede wêreldoorlog net tot 'n einde gekom het.

---

69 British Broadcasting Corporation "Victorian 'Supercomputer' is Reborn" http://news.bbc.co.uk/2/hi/technology/7391593.stm (besoek op 20 Augustus 2014).

70 Computer History Museum "The Babbage Engine" http://www.computerhistory.org/babbage/ (besoek op 20 Augustus 2014).

71 Copeland B J *Colossus: The Secrets of Bletchley Park's Codebreaking Computers* (2006) 1–3.

Flowers en sy span het elf maande geneem om die *Colossus* te bou. Die eerste prototipe het 1500 vakuumbuise bevat, en die tweede prototipe 2400 vakuumbuise. Dit kon 5000 karakters per sekonde prosesseer.[72]

Hierna het daar heelwat ontwikkelinge tot stand gekom wat rekenaartegnologie in 'n nuwe era geplaas het. Die belangrikste hiervan is sekerlik die ontwikkeling van die transistor, wat die oudmodiese en onbetroubare vakuumbuise vervang het. Dit is gevolg deur die ontwikkeling van die mikroskyfie, wat alle elektroniese toestelle van sakrekenaars tot wasmasjiene gemoderniseer het.[73] Hiermee het die era van die rekenaar aangebreek.

2.3.2 Rekenaarnetwerke

Soos wat rekenaars algemeen in die sestiger- en sewentigerjare by groot regeringsinstansies, multinasionale maatskappye en veral universiteite in gebruik geneem is, het die behoefte ontstaan om die rekenaars met mekaar te verbind.[74] 'n Verskeidenheid projekte is regoor die wêreld aangepak in 'n poging om hierdie droom 'n realiteit te maak.[75]

Een van die belangrikste ontwikkelings tydens hierdie era was die ontwikkeling van sogenaamde "packet switching" (hierna pakketskakeling).[76] Telefoonsentrales het van "circuit switching" gebruik gemaak, en dit het beteken dat wanneer 'n telefoonoproep gemaak is, daar 'n direkte skakeling tussen die twee partye gemaak word deurdat sentrales 'n fisiese konneksie tussen die partye teweeg bring. Dit het die gevolg gehad dat daar net soveel lyne beskikbaar was as waarvoor die sentrale voorsiening gemaak het.[77]

---

72 Copeland *Colossus* 126.

73 Saxena A N *Invention of Integrated Circuits: Untold Important Facts* (2009) 127 waar die patent van Jack Kilby, die ontwerper van die mikroskyfie, bespreek word. Sien ook Hamrick 1996 *The American Mathematical Monthly* 633.

74 Green P *Computer Network Architectures and Protocols* (2012) 14.

75 Green *Computer Network Architectures and Protocols* 15.

76 Dean T *Network+ Guide to Networks* (2012) 206.

77 Sien fig 2.2 vir 'n illustrasie van hierdie beginsel.

Pakketskakeling werk egter heel anders. Hiervolgens is die lyn altyd beskikbaar vir alle gebruikers op dieselfde tyd. Inligting word in pakkette saamgevoeg, en elke pakket kry 'n kopstuk wat inligting bevat oor die herkoms en bestemming van die pakket. Die pakkette word aangestuur van die een roeteerder na die ander, totdat dit uiteindelik sy eindbestemming bereik.[78] Elke e-posboodskap of webblad kan in duisende afsonderlike datagramme verdeel word, en elke datagram volg sy eie roete. Dit is dus nie vreemd dat 'n enkele e-pos of webblad tussen verskillende lande en kontinente geroeteer kan word nie. Figuur 2.5 toon 'n skematiese voorstelling van pakketskakeling.

Om die gedagte van pakketskakeling beter te visualiseer, kan pakketgeskakelde data met 'n posbus vergelyk word. Briewe word almal in dieselfde posbus geplaas om gepos te word. Wanneer die posman egter die briewe uit die posbus haal, begin 'n proses waar verskillende briewe eers in streke, en dan in kleiner groepies ingedeel word, totdat dit uiteindelik by die ontvanger uitkom. Net so gebruik pakketgeskakelde data almal dieselfde data-lyn om pakkette te versend, en is dit nie nodig dat 'n toegewyde ("dedicated") lyn vir elke rekenaarnetwerk vereis word nie.[79]

Volledigheidshalwe kan daar genoem word dat die konsep van pakketskakeling onafhanklik van mekaar deur twee pioniers ontwikkel is. Die eerste was Paul Baran, wat in die vroeë sestigerjare by die RAND Corporation gewerk het en "message block switching" vir hulle ontwerp het.[80] Die tweede was Donald Davies, wat werksaam was by die Britse National Physical Laboratory. Nadat Davies sy werk bekend gemaak het, is hy ingelig van die werk van Baran.[81] Die term "packet switching" van Davies is egter behou om die tegnologie te beskryf.

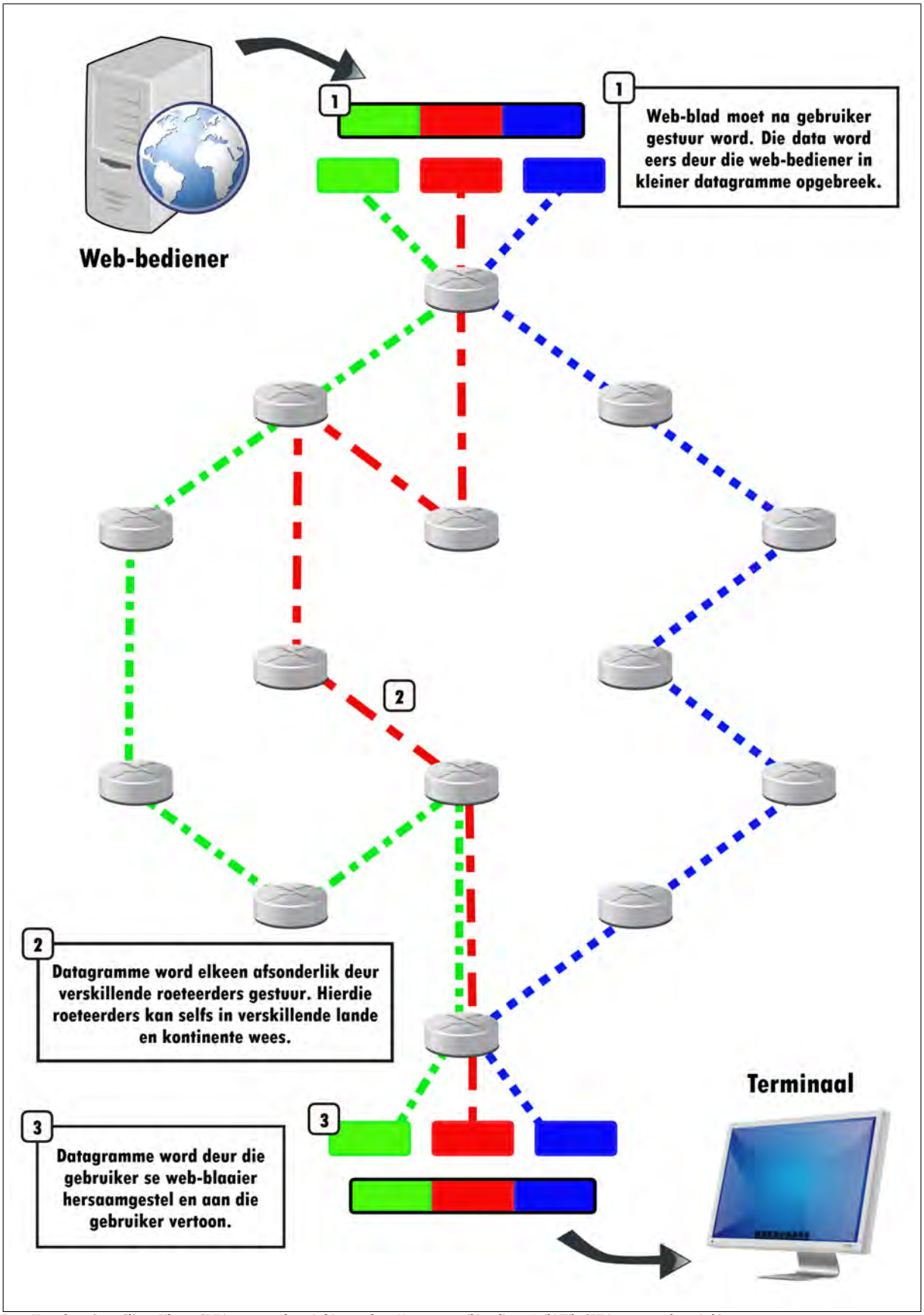
---

78 Gadsby A (red) *Longman Dictionary of Contemporary English* (1995) 1017 definieer "packet switching" so: "A method of sending data on telephone lines that breaks long messages into pieces and puts them together again when they are received".

79 Vir meer oor pakketskakeling, sien Dean *Network+ Guide to Networks* 206.

80 Stewart W "*Paul Baran Invents Packet Switching*" http://www.livinginternet.com/i/ii_rand.htm (besoek op 20 Augustus 2014).

81 Wikipedia "Donald Davies" http://en.wikipedia.org/wiki/Donald_Davies (besoek op 20 Augustus 2014).



Bron: Vertaal van Open Clipart Library *CPT-internet-packetswitching.svg* (http://commons.wikimedia.org/wiki/File:CPT-internet-packetswitching.svg).

Figuur 2.5: Pakketskakeling

Pakketskakelingstegnologie was die gebeurtenis wat die ontwikkeling van netwerke vir navorsingsdoeleindes regoor die wêreld laat posvat het. Netwerke soos die Merit Network, Telenet, die Cyclades, NSFNet en die ARPANET het almal ontwikkel as gevolg van pakketskakelingstegnologie. Dit word vervolgens bespreek.

2.3.2.1 Merit Netwerk

Die Merit[82] netwerk was 'n samewerkingsooreenkoms tussen die universiteit van Michigan, die Staatsuniversiteit van Michigan en Wayne Staatsuniversiteit om hulle hoofraamrekenaars aan mekaar te koppel. Hierdie netwerk is reeds in 1966 gevorm met die doel om inligting en rekenaargebruik tussen die universiteite te deel. Hierdie netwerk is so uitgebrei dat dit in die vroeë negentigerjare skakeling van die hele staat van Michigan met die Internet bewerkstellig het.[83]

2.3.2.2 Telenet

Telenet was die eerste kommersiële pakketgeskakelde netwerk wat vir die algemene publiek in die VSA beskikbaar was.[84] Die maatskappy het in 1974 begin besigheid doen, en het 'n kliëntebasis gehad wat gewissel het van regeringsorganisasies en groot multinasionale maatskappye, tot enkelgebruikers wat met 'n inbeldiens "dial-up" toegang tot die netwerk verkry het.[85] Hierdie netwerk was veral gewild omdat dit nasionale toegang tot verskillende "bulletin board services"[86] verskaf het.

---

82 The Michigan Educational Research Information Triad (MERIT). Buzacott A *Advanced Network Technology* (1993) 73.

83 Aupperle E M "Merit—Who, What, and Why" 1998 *Library Hi Tech* 15 15.

84 Kleinrock L "An Early History of the Internet" 2010 *IEEE Communications Magazine* 26 34.

85 Aupperle 1998 *Library Hi Tech* 21.

86 Tella A *Library and Information Science in Developing Countries: Contemporary Issues* (2011) 47 verduidelik wat 'n "bulletin board service" is: "A bulletin board is a public discussion area where people can post messages without sending them to a particular e-mail address and the messages can still be viewed by anyone who accesses the board".

2.3.2.3 Cyclades

In die vroeë 1970's is die Cyclades-netwerk in Frankryk gestig in 'n poging om 'n soortgelyke algemene navorsingsnetwerk vir Frankryk te wees as wat die ARPANET vir die VSA was.[87] (Die ARPANET word hieronder bespreek). Die Cyclades-netwerk was die eerste netwerk wat suksesvolle aflewering van die databoodskap aan die gasheerrekenaars oorgelaat het, en nie aan die netwerk self nie.[88] Hierdie netwerk het 'n groot invloed op die uiteindelike ontwikkelaars van die Internet, naamlik Vinton Cerf en Bob Kahn gehad. Dit was juis hierdie twee persone wat die "Transmission Control Protocol/Internet Protocol" (hierna TCP/IP)[89] ontwikkel het — wat die "gom" is wat vandag nog die Internet aanmekaar hou.[90] Gasheerrekenaars het met die versendingspakket 'n ontvangsversoek aangeheg, en indien die ontvangende rekenaar nie die ontvangserkenning gegee het nie, sou die gasheerrekenaar aanhou om die betrokke pakket te stuur totdat die ontvangserkenning gegee word.[91]

2.3.2.4 ARPANET

Die ARPANET[92] kan beskou word as die direkte voorloper tot die Internet, en daarom sal dit in meer besonderhede bespreek word.

Die Amerikaanse departement van verdediging het in 1958 die "Ad-

87 Murray A D *The Regulation of Cyberspace: Control in the Online Environment* (2007) 65.

88 Murray *The Regulation of Cyberspace* 65.

89 Afd 2.2.1.2 vn 30.

90 Murray *The Regulation of Cyberspace* 68.

91 Murray *The Regulation of Cyberspace* 68; Pelkey J "Entrepreneurial Capitalism and Innovation: A History of Computer Communications 1968–1988" http://www.historyofcomputercommunications.info/Book/6/6.3-CYCLADESNetworkLouisPouzin1–72.html (besoek op 20 Augustus 2014).

92 Die ARPANET is die netwerk wat deur die "United States Advanced Research Project Agency" (ARPA) geskep is. Lindsay D *International Domain Name Law:* ICANN *and the UDRP* (2007) 1 verduidelik: "The Internet (with an upper-case 'I') refers to the network of interconnected networks resulting from research on computer networking, which commenced in the 1960's and was funded by the *United States Advanced Research Project Agency (ARPA)*. The research was first implemented in an experimental network, which became known as ARPANET".

vanced Research Project Agency" (hierna ARPA)[93] gestig met die doel om verskillende netwerke aan mekaar te skakel.[94] Dit was 'n direkte reaksie op Rusland se suksesvolle Sputnik ruimtesending.[95] Die Amerikaanse regering was deeglik daarvan bewus dat die Sowjet-Unie hulle voorgespring het met ruimtetegnologie, en ARPA se aanvanklike mandaat was spesifiek om tegnologie te ontwikkel dat Amerika nie weer deur 'n soortgelyke voorval verras word nie.[96]

Alhoewel ARPA dus deur die departement van Verdediging befonds is, het dit 'n wye sfeer van tegnologiese ontwikkelings hanteer. Daarom was daar navorsingsinstitute en selfs universiteite betrek om nuwe tegnologieë wat vir die verdedigingsdepartement nuttig kan wees, te ontwikkel.[97]

Die gedagte van 'n netwerk binne ARPA is in 1963 deur Licklider ontwikkel. Hy is aangestel by ARPA as hoof van die departement van Gedragswetenskappe, en het 'n sogenaamde "Intergalactic Computer Network" in gedagte gehad.[98] Hierdie netwerk in Licklider se verbeelding het verbasende ooreenkomste gehad met hoe die Internet nou funksioneer.

Voordat Licklider egter sy planne vir die "Intergalactic Computer Network" kon uitvoer, het hy ARPA verlaat. Tog het sy gedagtes bly voortbestaan in twee wetenskaplikes wat by ARPA agtergebly het, te wete Ivan Sutherland en Bob Taylor.[99]

ARPA het hoofraamrekenaars aan verskeie universiteite en navorsingsinstitute met regeringsfondse verskaf. In Taylor se kantoor het hy drie

---

93 Defense Advanced Research Projects Agency "Bridging the Gap: Powered by Ideas" 2005 *Defence Advanced Research Projects Agency* 1 1.

94 Gigante A "Blackhole in Cyberspace: The Legal Void in the Internet" 1997 *John Marshall Journal of Information Technology and Privacy Law* 413 413.

95 Murray *The Regulation of Cyberspace* 61.

96 Murray *The Regulation of Cyberspace* 61.

97 Defense Advanced Research Projects Agency *Defence Advanced Research Projects Agency* 9.

98 Die Memorandum wat Licklider gebruik het om die ARPANET aan te kondig, word by hierdie skakel weergegee: "Memorandum for Members and Affiliates of the Intergalactic Computer Network". Licklider J C R "Memorandum for Members and Affiliates of the Intergalactic Computer Network" http://www.kurzweilai.net/memorandum-for-members-and-affiliates-of-the-intergalactic-computer-network (besoek op 20 Augustus 2014).

99 Kleinrock 2010 *IEEE Communications Magazine* 29.

afsonderlike rekenaarterminale gehad wat aan drie verskillende navorsingsinstitute gekoppel was. Hy het hierdie drie rekenaarterminale gebruik as illustrasie waarom 'n ineengeskakelde netwerk ontwikkel moes word:

> For each of these three terminals, I had three different sets of user commands. So, if I was talking online with someone at S.D.C., and I wanted to talk to someone I knew at Berkeley, or M.I.T., about this, I had to get up from the S.D.C. terminal, go over and log into the other terminal and get in touch with them. I said, "Oh Man!", it's obvious what to do: If you have these three terminals, there ought to be one terminal that goes anywhere you want to go. That idea is the ARPANET.[100]

Nadat die bou van die netwerk op tender uitgegaan het, is dit aan BBN Technologies toegeken wat die netwerk in 1969 gebou het.[101] BBN Technologies het 'n breedvoerige en gespesifiseerde tenderdokument saamgestel om spesifiek uit te spel wat hulle kon lewer. Hierdie tenderdokument is net so aanvaar, en het dus as 'n bloudruk gedien om die netwerk te ontwikkel.[102]

Die aanvanklike netwerk was relatief klein. 'n Bestaande rekenaar is aangepas om 'n sogenaamde Interface Message Processor, of IMP, te vorm. Hierdie IMP was direk aan die netwerk gekoppel op dieselfde wyse waarop 'n roeteerder vandag sal funksioneer, en kon tot vier gasheerrekenaars hanteer en aan 'n maksimum van ses ander IMP's koppel. Figuur 2.6 toon dit aan. Die ARPANET is op 29 Oktober 1969 in gebruik geneem toe twee rekenaars aan mekaar gekoppel is.[103] Aan die einde van 1972 was daar reeds 24 rekenaars aan die ARPANET gekoppel. Teen Junie 1974, 62 rekenaars, en

---

100 Markoff J "An Internet Pioneer Ponders the Next Revolution" http://web.archive.org/web/20080922095019/http://partners.nytimes.com/library/tech/99/12/biztech/articles/122099outlook-bobb.html (besoek op 22 Augustus 2014).

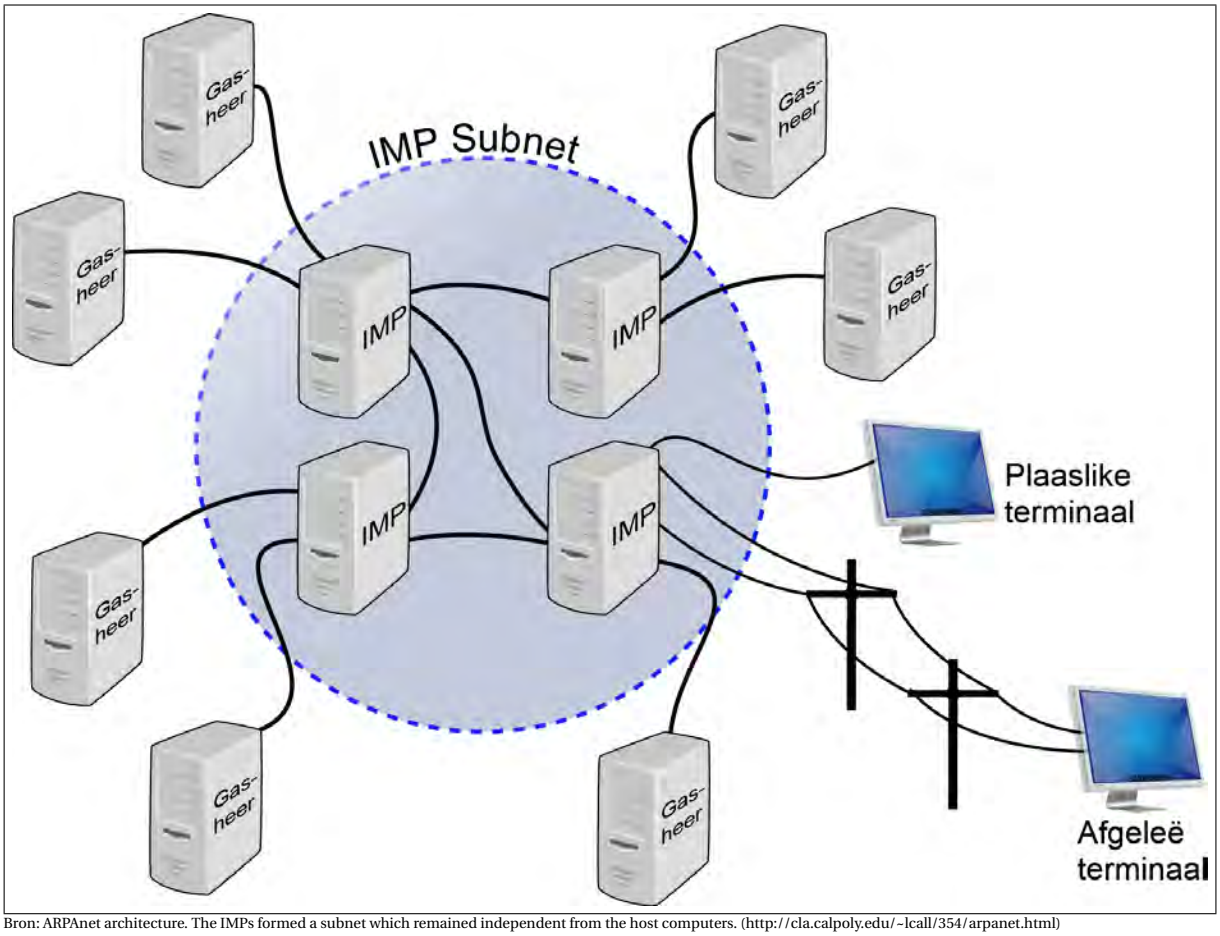
101 Kleinrock 2010 *IEEE Communications Magazine* 30.

102 Steward W "IMP — Interface Message Processor" http://www.livinginternet.com/i/ii_imp.htm (besoek op 22 Augustus 2014).

103 Leonard Kleinrock verduidelik hoe die eerste toets gedoen is nadat die eerste twee rekenaars van die ARPANET aan mekaar gekoppel is:

> At the UCLA end, they typed in the "l" and asked SRI if they received it; "got the l" came the voice reply. UCLA typed in the "o", asked if they got it, and received "got the o". UCLA then typed in the "g" and the darned system CRASHED! Quite a beginning. On the second attempt, it worked fine!

Kleinrock 2010 *IEEE Communications Magazine* 32.



Bron: ARPAnet architecture. The IMPs formed a subnet which remained independent from the host computers. (http://cla.calpoly.edu/~lcall/354/arpanet.html)

Figuur 2.6: Voorstelling van die Vroeë ARPANET

teen 1977 reeds 111 rekenaars. [104]

2.3.2.5 Samevatting

Rekenaartegnologie het uiteraard die ontwikkeling van die Internet voorafgegaan.[105] 'n Toestel kan slegs as 'n rekenaar beskou word indien dit aan twee vereistes voldoen, te wete die hantering van geoutomatiseerde berekenings, en programmeerbaarheid.[106] Die eerste toestel wat aan hierdie vereistes voldoen het, was die *Colossus,* wat in die Verenigde Koninkryk gebruik is om geheime Duitse boodskappe tydens die tweede wêreldoorlog

104 Steward W "ARPANET — The First Internet" http://www.livingInternet.com/i/ii_arpanet.htm (besoek op 22 Augustus 2014).

105 Afd 2.3.1.

106 Afd 2.3.1.

te ontsyfer.[107]

In die sestiger- en sewentigerjare het rekenaartegnologie wydverspreid genoeg geword dat daar die behoefte ontstaan het om die rekenaars met mekaar te koppel.[108] Die ontwikkeling van pakketskakeling het dit moontlik gemaak om hierdie doel te verwesenlik.[109] Pakketskakeling vorm vandag nog die meganisme waarop data versend en ontvang word.[110]

Verskeie universiteite en instansies in die VSA het probeer om netwerke te skep wat tussen kampusse en besigheidstakke kon funksioneer. Suksesvolle voorbeelde hiervan is die Merit netwerk,[111] Telenet,[112] Cyclades,[113] en ARPANET.[114] Laasgenoemde is deur 'n Amerikaanse regeringsinstansie ontwikkel, en dit sou die voorloper van die Internet wees.[115]

2.3.3 Die *Internet Suite*

Teen die vroeë tagtigerjare was daar reeds honderde rekenaars aan die ARPANET gekoppel.[116] Een groot probleem was egter dat die verskillende rekenaarnetwerke nog nie 'n gemeenskaplike protokol gehad het om inligting moeiteloos van een netwerk na die ander te stuur nie. Hierdie kritieke ontwikkeling is deur CERN,[117] die Europese Organisasie vir Kernnavorsing,

107 Afd 2.3.1.

108 Afd 2.3.2.

109 Afd 2.3.2.

110 Afd 2.3.2.

111 Afd 2.3.2.1.

112 Afd 2.3.2.2.

113 Afd 2.3.2.3.

114 Afd 2.3.2.4.

115 Afd 2.3.2.4.

116 Zelkowitz M V *Distributed Information Resources* (1999) 182. Frye C *Privacy-enhanced Business: Adapting to the Online Environment* (2001) 11 meld: "The number of computers connected to the ARPANET grew at a slow but steady pace through the mid-1970's, adding about one node a month. That steady level of growth continued until about 1984, when the number of nodes on the ARPANET began doubling about every year".

117 Die akroniem CERN word verkry van *Conseil Européen pour la Recherche Nucléaire,* wat die Franse benaming van die Europese Kern-agentskap is. Wikipedia "CERN" https://en.wikipedia.org/wiki/CERN (besoek op 22 Augustus 2014).

aangepak.[118] Die gevolg was die ontwikkeling van die sogenaamde *Internet Suite* in 1982, wat 'n versameling rekenaarprogramme was wat maklike kommunikasie tussen netwerke moontlik gemaak het.[119] Die belangrikste hiervan was die twee protokolle genaamd TCP/IP of "Transmission Control Protocol" en "Internet Protocol".[120] Hierdie twee protokolle vorm vandag steeds die ruggraat van die Internet deurdat dit 'n gemeenskaplike taal is waardeur rekenaars met mekaar kan kommunikeer.[121] Dit vorm ook die basis van die Internet se vermoë om data deur 'n menigte verskillende roeteerders te stuur en weer op een plek byeen te bring.[122]

Die belangrikheid van die ontwikkeling van die *Internet Suite* kan nie onderskat word nie. Benewens die ontwikkeling van die fisiese argitektuur van die Internet, speel die *Internet Suite* 'n kritieke rol om die Internet korrek te laat funksioneer.[123]

Soos hierbo genoem bestaan die *Internet Suite* uit 'n groep protokolle wat saam die argitektuur van die fisiese rekenaars van die Internet bestuur. Die *Internet Suite* vorm as geheel egter ook 'n aantal "lae" ("layers" in Engels) waar die een laag se werking afhanklik is van die vorige laag. Saam maak die lae van die *Internet Suite* kommunikasie moontlik.[124]

Die lae van die *Internet Suite* kan soos volg verduidelik word:

Die basislaag is die Skakellaag (Link Layer).[125] Dit is die eerste sagtewarelaag bokant die fisiese rekenaar, en skakel rekenaars in 'n plaaslike

---

118 Gigante 1997 *John Marshall Journal of Information Technology and Privacy Law* 414.

119 Reed C *Internet Law: Text and Materials* (2004) 12.

120 Reed *Internet Law: Text and Materials* 12.

121 Gigante 1997 *John Marshall Journal of Information Technology and Privacy Law* 414.

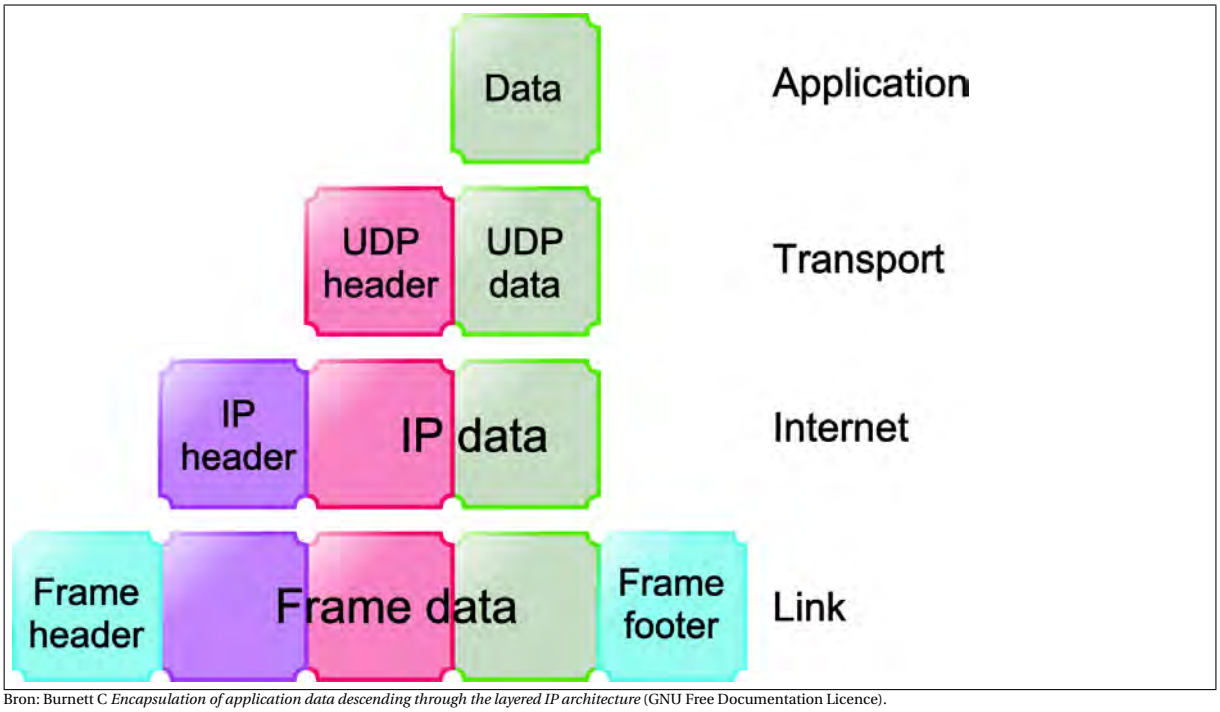
122 TCP/IP has three key features that make "internetting" possible:
(1) computers using different operating systems can communicate with each other;
(2) each transmission is broken up into digital packets of a few thousand bytes; and
(3) each digital packet is routed dynamically, i.e., each packet is separately directed to its destination along the route the network determines is most convenient for that packet at the time it arrives for forwarding.

Gigante 1997 *John Marshall Journal of Information Technology and Privacy Law* 414.

123 Reed *Internet Law: Text and Materials* 12.

124 Reed *Internet Law: Text and Materials* 12.

125 Guadamuz A *Networks, Complexity and Internet Regulation* (2011) 74.



Bron: Burnett C *Encapsulation of application data descending through the layered IP architecture* (GNU Free Documentation Licence).

Figuur 2.7: Inhoud van Datagram in Verhouding tot Internet-argitektuur.

netwerk (local area network) met mekaar.[126] Die gevolg is dat die Skakellaag slegs koppeling bewerkstellig met ander rekenaars wat *fisies* (met kabels) aan mekaar gekoppel is.

Die tweede laag is die Internetlaag.[127] Dit het die funksie om elke rekenaarnetwerk op die Internet te identifiseer met sy unieke IP-adres.[128] Hierdie laag word onderskei van die daaropvolgende lae deurdat dit geensins poog om kommunikasie tussen rekenaars te bewerkstellig nie, maar bloot om die betrokke plaaslike netwerk te kan identifiseer. Dus, ander rekenaarnetwerke wat buite die plaaslike netwerk gekoppel is, kan nou geïdentifiseer word.[129]

Die derde laag is die Vervoerlaag (Transport layer).[130] Dit reguleer kommunikasie tussen gasheerrekenaars, en reguleer die stuur en ontvang

126 Guadamuz *Networks, Complexity and Internet Regulation* 74.

127 Guadamuz *Networks, Complexity and Internet Regulation* 74.

128 Afd 2.3.4 bevat meer inligting oor IP-adresse).

129 Guadamuz *Networks, Complexity and Internet Regulation* 74.

130 Guadamuz *Networks, Complexity and Internet Regulation* 74.

van datagramme.[131]

Die laaste en hoogste laag van die *Internet Suite* is die sogenaamde "Application layer".[132] Dit het die funksie om spesifieke programme te ondersteun. Die "Send Mail Transfer Protocol" (SMTP) word byvoorbeeld spesifiek gebruik om e-posboodskappe te stuur, terwyl die "Hyper Text Transfer Protocol" (HTTP) weer gebruik word om weblêers te stuur.[133]

Sonder dat meeste regsgeleerdes dit besef, hou die *Internet Suite* 'n geweldige uitdaging vir die regspleging in. Benkler toon aan hoe die *Internet Suite* vir doeleindes van die reg tot drie lae vereenvoudig kan word, te wete 'n fisiese laag, 'n logiese laag, en 'n inhoud-laag.[134] Lessig het hierdie drie lae in eenvoudiger taal herbenoem, naamlik die fisiese-, kode- en inhoud-lae.[135] Die probleem wat dit vir regsgeleerdes skep, is dat wetgewing huidig op al drie lae toegepas word. Dit skep 'n probleem, want elke daaropvolgende laag is afhanklik van 'n voorafgaande laag om behoorlik te funksioneer, en wanneer ál die lae deur wetgewing gereguleer word, ondermyn die verskillende wetgewende ingrepe mekaar. 'n Praktiese voorbeeld hiervan is kopieregwetgewing. Meeste lande se kopieregwetgewing maak voorsiening vir 'n "fair use"-geval waar klein uittreksels uit 'n kopiereghoudende werk gebruik mag word vir spesifieke doeleindes, soos die gebruik van 'n kwotasie uit 'n boek, of 'n kort snit uit 'n film.[136] Dit sou 'n wetgewende ingreep op die inhoud-laag wees. Indien kopiereghouers egter gemagtig word om tegnologiese maatreëls in werking te stel om te verhoed dat 'n DVD byvoorbeeld nie gekopieer kan word nie, is dit 'n ingreep op die fisiese laag. Die onderliggende argitektuur is verander, en is dit nie moontlik om 'n snit van die DVD te bekom vir — byvoorbeeld — 'n voorlegging nie. Die een wetgewende ingreep ondermyn die ander een, aangesien "fair use" nou

131 Guadamuz *Networks, Complexity and Internet Regulation* 74.

132 Guadamuz *Networks, Complexity and Internet Regulation* 74.

133 Guadamuz *Networks, Complexity and Internet Regulation* 74.

134 Benkler Y "From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access" 1999 *Federal Communication Law Journal* 561 568.

135 Lessig L *The Future of Ideas: The Fate of the Commons in a Connected World* (2002) 23.

136 Benkler 1999 *Federal Communication Law Journal* 569.

onmoontlik word. Dieselfde geld vir die *Internet Suite.*[137]

Dus, die lae van die *Internet Suite* kan deur reguleerders gebruik word om effektiewe regulering te laat geskied — maar wetgewende ingrepe behoort versigtig gedoen te word om nie teenstrydige bepalings te skep nie.

Noudat die *Internet Suite* verduidelik is, is dit belangrik om die groter prentjie te verstaan van hoe inligting oor die Internet beweeg. Twee kernkonsepte in hierdie verband is die Domeinnaamstelsel en die Internet Protokol. Dit word vervolgens bespreek.

2.3.4 Die Domeinnaamstelsel en die Internet Protokol

Soos direk hierbo verduidelik is die Internetlaag (tweede laag van die *Internet Suite)* daarvoor verantwoordelik om elke rekenaar op die Internet te identifiseer. Dit word gedoen deur ’n Internet Protokol-adres (hierna IP-adres) toe te ken.[138] Omdat dit bloot ’n reeks nommers is, vind mense dit moeilik om die adresse te onthou. Om hierdie rede het dit reeds vroeg in die ontwikkeling van die Internet duidelik geword dat ’n bykomende stelsel nodig is om sin uit die miljoene IP-adresse te maak.[139]

In die vroeë ontwikkeling van die Internet was Jon Postel, wat werksaam was by die Stanford Research Institute (SRI), verantwoordelik vir die moeisame taak om die ARPANET se IP-adresse te onderhou.[140] Postel was die eerste persoon wat hierdie taak opgelê is, en hy het dit vir etlike dekades alleen verrig.[141]

---

137 Lessig *The Future of Ideas* 24.

138 Elke rekenaar op die Internet het ’n eie IP-adres, en ’n voorbeeld daarvan lyk so: 172.16.254.1. Hierdie is ’n voorbeeld van ’n IPv4 Internetadres. Sedert die Internet so ’n ongelooflike groei getoon het, het dit gou geblyk dat daar spoedig nie genoeg IP-adresse vir al die rekenaars in die wêreld sal wees nie, en het die *IETF* die nuwe IPv6 adresstelsel ontwikkel. Dit behels ’n 128 bit adresstelsel (in teenstelling met die 32 bit adresstelsel van IPv4), en lyk bv so: 2001:db8:0:1234:0:567:8:1. Let egter daarop dat alle IP-adresse eintlik binêre nommers is, en die voorstelling soos hier aangetoon bloot in tekslêers as menslik leesbare metode voorgestel word. Dean *Network+ Guide to Networks* 158 verduidelik in besonderhede hierdie konsepte. Sien ook Wikipedia “IP Address” http://en.wikipedia.org/wiki/IP_address (besoek op 22 Augustus 2014).

139 Shinder D L *Scene of the Cybercrime: Computer Forensics Handbook* (2002) 257.

140 Murray *The Regulation of Cyberspace* 97.

141 Goldsmith J en Wu T *Who Controls the Internet? lllusions of a Borderless World* (2006) 29.

Aanvanklik was die hantering van IP-adresse relatief moeiteloos, aangesien dit maar 'n handjievol was. Met verloop van tyd was daar egter duisende IP-adresse wat skielik onbeheerbaar geword het.[142] Postel het reeds vroeg in sy hantering van die IP-adresstelsel besef dat hy nie hierdie taak kan verrig as daar nie 'n makliker sisteem geskep kon word nie. Hy het 'n versoek gerig tot die *IETF* dat 'n stelsel ontwikkel word wat IP-adresse beter kan hanteer.[143] Die oplossing is voorgestel deur Paul Mockapetris wat aangevoer het dat elke IP-adres 'n ooreenstemmende "naam" moet hê. Mockapetris het daad by die woord gevoeg, en die domeinnaamstelsel (DNS) in 1983 uitgerol.[144]

Dus, die DNS behels dat die IP-adres met 'n naam vervang word. Die IP-adres word dus nou nie meer as primêre bron deur mense gebruik nie, maar eerder die domeinnaam, soos www.*Google*.com. 'n Tekslêer is geskep wat die IP-adres teenoor die ooreenstemmende domeinnaam aandui, en dit op 'n basisnaambediener ("root name server") stoor.

Hierdie proses word grafies in figuur 2.8 voorgestel.

Wanneer 'n persoon, byvoorbeeld 'n webgebruiker,[145] met sy rekenaar 'n versoek aan 'n webbediener[146] rig om 'n spesifieke webblad te ontvang, moet die webgebruiker se rekenaar eers uitvind waar die webbediener is. Om dit te doen word 'n versoek na 'n basisnaambediener gestuur. Indien die basisnaambediener weet waar die webbediener is, sal die resultaat aan die webgebruiker se rekenaar verskaf word. Indien nie, sal die basisnaambediener (in hierdie voorbeeld die DNS1-bediener) 'n ander basisnaambediener moet raadpleeg vir die inligting. Wanneer die DNS1-bediener die inligting ontvang het, sal dit in sy eie databasis gestoor word

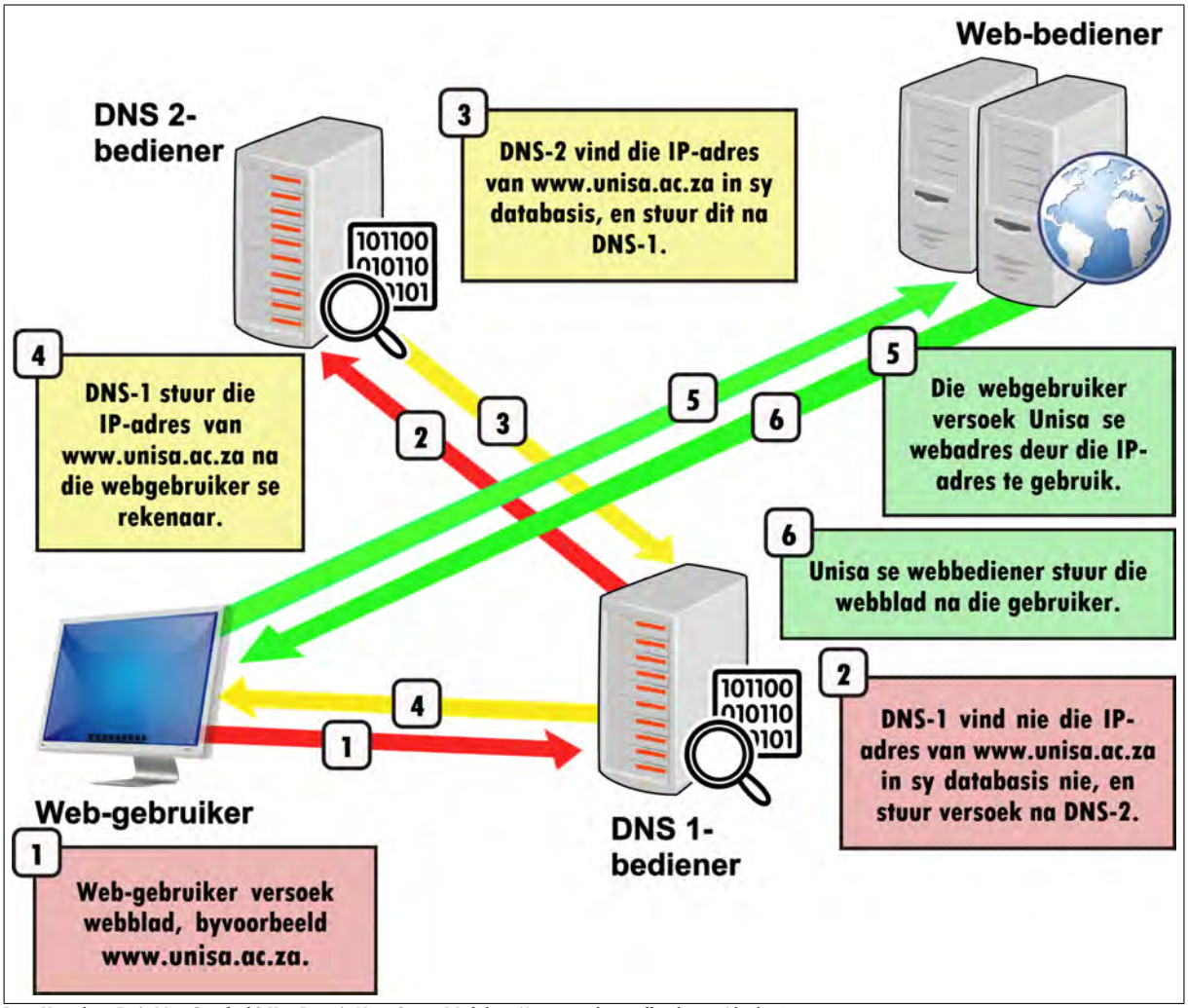
142 Murray *The Regulation of Cyberspace* 97.

143 Murray *The Regulation of Cyberspace* 97.

144 Mockapetris P "Domain Names — Concepts and Facilities" http://tools.ietf.org/html/rfc882 (besoek op 22 Augustus 2014).

145 Die voorbeeld van 'n webgebruiker word hier gebruik, maar die proses bly dieselfde in die geval van 'n e-possgebruiker, videogebruiker of enigeen wat 'n data-lêer op die Internet aanvra.

146 Sien vn 145 direk hierbo wat aantoon dat verskeie moontlikhede moontlik is. Die versender kan dus ook 'n e-posbediener, data-bediener of enige ander bediener verteenwoordig.



Bron: Vertaal van Brain M en Crawford S *How Domain Name Servers Work* (http://computer.howstuffworks.com/dns.htm).

Figuur 2.8: Werking van die Domeinnaamstelsel (DNS).

(vir enige verdere versoeke) en sal die IP-adres vir die webgebruiker se rekenaar aangestuur word. Eers dán sal die webgebruiker se rekenaar direk met die webbediener kan skakel om die spesifieke webblad te verkry. Hierdie hele proses geskied binne etlike millisekondes.

Met hierdie verduideliking blyk dit duidelik dat basisnaambedieners op die Internet 'n kritieke funksie verrig. Trouens, as die basisnaambedieners ophou funksioneer, sal die Internet binne 'n paar uur onbruikbaar word.

Dit is eweneens duidelik dat die persoon of instansie wat die basisnaambedieners beheer, effektiewelik beheer oor die hele Internet kan uitoefen. Hierdie is 'n baie belangrike punt rakende Internetregulering, en

word breedvoerig in hoofstuk 3 bespreek.[147]

Toe die domeinnaamstelsel ontwikkel is, was daar aanvanklik net een basisnaambediener. Dit het later gegroei tot een wortelbasisnaambediener, en dertien basisnaambedieners wat uit die een wortel gevoed is.[148] Die basisnaambedieners van die moderne Internet word egter nie meer deur net dertien basisnaambedieners bedien nie. Wat nou gebeur is dat dertien bediener-adresse, deur 'n proses genaamd *Anycast,*[149] op hulle beurt die versoek na 'n verskeidenheid basisnaambedieners,[150] wat naby die gebruiker is, kan stuur.[151] Figuur 2.9 illustreer die verspreiding van hierdie basisnaambedieners. (Elke nommer dui op die hoeveelheid basisnaambedieners in daardie omgewing).

In hierdie studie sal daar by verskeie geleenthede na die regulering van die basisnaambedieners verwys word. Soms word die sinoniem basis-DNS-sisteem gebruik,[152] en by tye sal daar ook na die IANA-funksie[153] verwys word om die regulering van die basisnaambedieners te beskryf.[154] Wanneer die Amerikaanse regering na die basis-DNS-dienste verwys, word die term "IANA-funksie" gebruik.[155] *"*IANA*"* is 'n akroniem vir *"Internet Assigned Numbers Authority",* en dit was die naam van die departement waarvan Postel die hoof was.[156]

---

147 Afd 3.4.1.

148 Werbach 2008 *University of California Davis Law Review* 356.

149 Loshin P *IPv6 Clearly Explained* (1999) 110 verduidelik: "When a host issues a request to an anycast address for some information, the closest server associated with that anycast address will respond".

150 Ten tyde van hierdie skrywe was daar 386 basisnaambedieners oor die wêreld versprei. Wikipedia "Wikipedia "Root Name Server" http://en.wikipedia.org/wiki/Root_name_server (besoek op 3 Oktober 2014).

151 Albitz P en Liu C *DNS and BIND* (2001) 27 verduidelik: "... resolution has to start at the root name servers. This makes the root name servers crucial to the operation of DNS; if all the Internet root name servers were unreachable for an extended period, all resolution on the Internet would fail." Sien ook Wikipedia "Root Name Server" http://en.wikipedia.org/wiki/Root_name_server (besoek op 3 Oktober 2014).

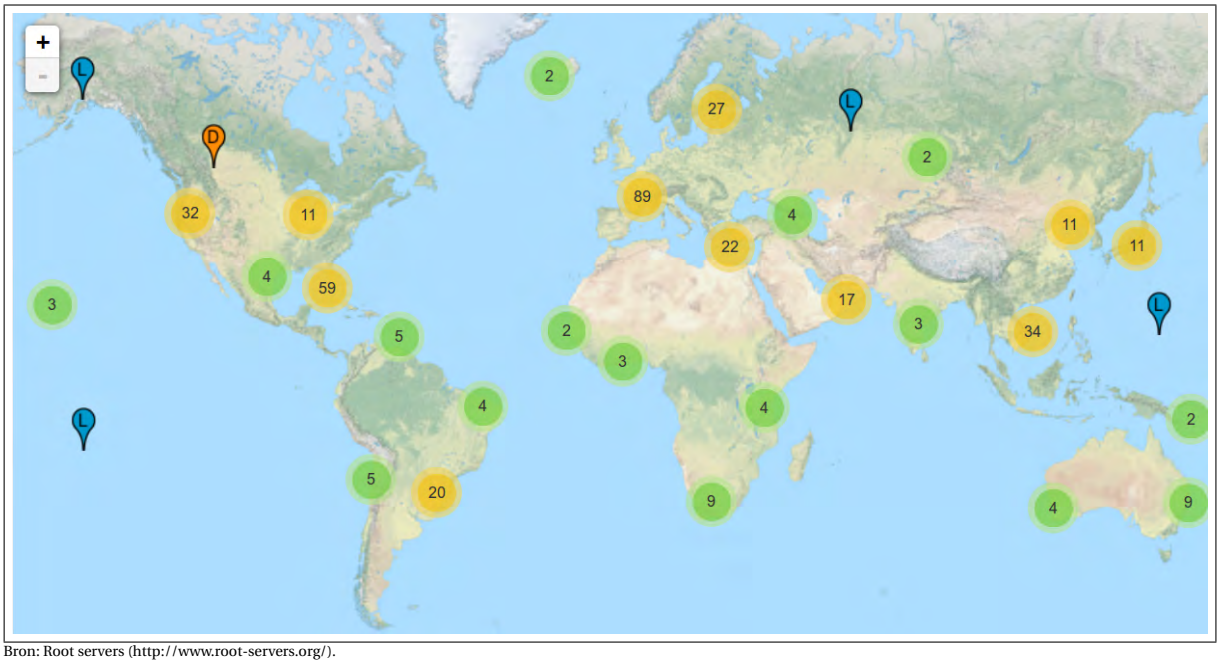
152 Bv afd 7.3.1.3.

153 IANA is 'n akroniem vir *"Internet Assigned Numbers Authority"*. Afd 3.4.3.

154 Bv afd 4.2.4.1.

155 National Telecommunications and Information Administration "NTIA Announces Intent to Transition Key Internet Domain Name Functions" https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions (besoek op 3 Oktober 2014).

156 DeNardis L *Protocol Politics: The Globalization of Internet Governance* (2009) 144.



Bron: Root servers (http://www.root-servers.org/).

Figuur 2.9: Ligging van Basisnaambedieners in 2014.

***

Reeds teen die einde van die tagtigerjare was die hele argitektuur van die Internet ontwikkel. Daarna het ander wetenskaplikes hierdie argitektuur gebruik om verdere ontwikkelinge daar te stel. Die bekendste hiervan is die ontwikkeling van die wêreldwye web, of WWW, wat deur Tim Berners Lee en Robert Cailliau ontwikkel is. Dit word vervolgens bespreek.

2.3.5 Die Wêreldwye Web

2.3.5.1 Web Gekonsepsualiseer

Die Wêreldwye web is reeds so vroeg as 1945 gekonsepsualiseer toe die elektriese ingenieur Vannevar Bush in 'n artikel getiteld "As we may think", in "The Atlantic"[157] geskryf het dat "wholly new forms of encyclopedias

[157] "The Atlantic" is 'n prominente tydskrif in Amerika wat by sy stigting in 1857 in Boston, Massachusetts voorgehou is as 'n literêre en kulturele tydskrif. Dit het vir 150 jaar 'n uitstekende reputasie gehad, maar is relatief onlangs ná 'n reeks finansiële neerlae tot 'n algemene redaksionele tydskrif omskep. In 1945, toe Bush daarin geskryf het, was dit 'n publikasie van hoogstaande gehalte. Bush se beweegrede vir sy bydrae was dat hy bekommerd was oor die rigting wat die natuurwetenskap ingeslaan het in die oorlogsjare. Die wetenskap word oorwegend vir dood en verwoesting gebruik — was sy argument —

will appear, ready made with a mesh of associative trails running through them, ready to be dropped into the memex and there (be) amplified".[158] Die "memex" waarna Bush hier verwys, is 'n elektromeganiese sisteem waarvolgens duisende bladsye mikrofiche op so 'n manier geskakel word dat dit na mekaar verwys op 'n hipertekswyse.[159] Hiperteks verwys na 'n dokument waar 'n deel van die teks gekies kan word om 'n verdere verduideliking weer te gee. Die teks word gewoonlik gekies deur daarop te kliek met 'n rekenaarmuis, of met moderne slimtablette daarop te druk met die vinger. Bush se memex is egter nooit ontwikkel nie, maar die gedagte van 'n ineengeskakelde sisteem van kruisverwysings het bly voortleef.

Ted Nelson was 'n sosioloog en filmmaker, en het ook die nodigheid van 'n ineengeskakelde web van inligting probeer realiseer.[160] In 1965 het hy 'n aanbieding by die *Association for Computing Machinery* gemaak waar hy 'n hiperteks-sisteem beskryf het. Daar was hy die eerste persoon om die term "hypertext" te gebruik.[161] In 1960 het hy probeer om hierdie droom te realiseer met die skepping van *Project Xanadu.*[162] Oor die volgende paar dekades het hy daaraan gewerk, maar kon dit nooit suksesvol uitvoer nie.[163]

---

en hy wou toesien dat inligting en die wetenskap weer vir die uitbouing van die mensdom gebruik word. Daarom het hy juis oor die memex-sisteem geskryf — sodat 'n inligtingstelsel ontwikkel kan word wat vir die groter mensdom van waarde kan wees. Wardrip-Fruin N en Montfort N (red) *The New Media Reader* (2003) 35.

158 The Atlantic Monthly "As We May Think" http://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/ (besoek op 20 April 2012).

159 Bush visualiseer die memex soos volg:

> Consider a future device for individual use, which is a sort of mechanized private file and library. It needs a name, and, to coin one at random, "memex" will do. A memex is a device in which an individual stores all his books, records, and communications, and which is mechanized so that it may be consulted with exceeding speed and flexibility. It is an enlarged intimate supplement to his memory.
>
> It consists of a desk, and while it can presumably be operated from a distance, it is primarily the piece of furniture at which he works. On the top are slanting translucent screens, on which material can be projected for convenient reading. There is a keyboard, and sets of buttons and levers. Otherwise it looks like an ordinary desk.

Bush 1945 *The Atlantic Monthly.*

160 Murray *The Regulation of Cyberspace* 71.

161 Wardrip-Fruin *The New Media Reader* 133.

162 Murray *The Regulation of Cyberspace* 71; Morrow G "Hypertext May Let PC Users Create Unique Structures for Data Organization" 1988 *Infoworld* 42.

163 Wolf G "The Curse of Xanadu" http://www.wired.com/wired/archive/3.06/xanadu.html (besoek op 22

2.3.5.2 *Enquire*

Dit was nie voor 1980 dat 'n jong rekenaarwetenskaplike genaamd Tim Berners-Lee weer met hierdie probleem begin worstel het nie.[164] Berners-Lee se eerste poging tot 'n hiperteksstelsel het ontstaan toe hy kontrakwerk by CERN,[165] die Europese kern-agentskap, in 1980 gedoen het.[166] Daar was ongeveer 10 000 werknemers by CERN, en gevolglik was daar 'n magdom projekte gelyktydig aan die gang. Daar het 'n behoefte ontstaan om hierdie massa inligting op 'n samehangende wyse te groepeer. Berners-Lee se oplossing was die skepping van 'n stelsel wat hy *Enquire* genoem het.[167]

Enquire het ten doel gehad om spesifiek CERN se inligting te struktureer, en die doel was nooit om die stelsel buite hierdie organisasie te gebruik nie.[168]

Die *Enquire*-stelsel het gefunksioneer op die beginsel dat elke dokument as't ware 'n kataloguskaart is.[169] 'n Kaart was redelik goed gestruktureerd, met inligting oor die outeur van die kaart, groepe, en dokumente waarna dit op 'n hiperteks-wyse verwys het.[170] Mense kon saamwerk om die kaarte te sorteer, te indekseer, nuwe kaarte te skep, en oues te verwyder. In vandag se terme het die *Enquire*-stelsel meer gelyk soos 'n *Wiki*[171] as 'n webblad.

Augustus 2014).

164 Hey A J G en Pápay G *The Computing Universe: A Journey through a Revolution* (2014) 224.

165 "Conseil Européen pour la Recherche Nucléaire" in Frans.

166 Hogan A *Reasoning Techniques for the Web of Data* (2014) 20 Hey *The Computing Universe: A Journey through a Revolution* 224.

167 Volgens Berners-Lee was die *Enquire* sisteem geïnspireer deur 'n boek getiteld *Enquire Within Upon Everything*. Die gedagte was dus om 'n stelsel te skep wat enige vorm van inligting met enige ander vorm van inligting te kan katalogiseer.

168 Hogan *Reasoning Techniques for the Web of Data* 20.

169 Hogan *Reasoning Techniques for the Web of Data* 20.

170 Berners-Lee T *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web* (2000) 4–9; Hogan *Reasoning Techniques for the Web of Data* 20.

171 'n *Wiki* is 'n webdiens (*web service*) wat spesiale wiki sagteware gebruik om 'n stelsel te skep waar 'n menigte mense saam aan 'n artikel, of reeks artikels kan werk. Black P, Delaney H en Fitzgerald B "Legal Issues for Wikis: The Challenge of User-generated and Peer-produced Knowledge, Content and Culture" 2007 *Murdoch University Electronic Journal of Law* 246. Teehan K *Wikis: The Educator's Power Tool* (2010) 1 verduidelik die oorsprong van die woord "wiki": "The word wiki derives from a Hawaiian word that means quick. This definition is applicable to this tool, as a wiki is a Web site that can be created in a hurry. Wikis have many uses, among which are managing information, knowledge, and ideas." Die

Die *Enquire*-stelsel het beperkte sukses binne CERN geniet. Berners-Lee het egter heelwat uit hierdie projek geleer, en het raakgesien dat daar verskeie tekortkominge met die stelsel was. Eerstens was *Enquire* nie vir almal toeganklik nie (net vir die personeel by CERN). Tweedens het die *Enquire*-stelsel vereis dat beide die kaart wat die hiperteksverwysing bevat, *en* die kaart waarna verwys word, gewysig moes word om die skakeling tussen die twee te bewerkstellig. Dit het die stelsel onnodig moeilik gemaak. Derdens het die stelsel net ten opsigte van dokumente binne die CERN stelsel gewerk, en kon eksterne databasisse en inligting nie verwys word nie.[172]

2.3.5.3 Projek WorldWideWeb

In 1990 het Berners-Lee die geleentheid gekry om 'n hiperteks-stelsel op die regte manier te ontwerp. Hy het sy bestuurshoofde oortuig dat dit in die belang van CERN sou wees om 'n hipertekssstelsel — soos *Enquire* — daar te stel vir algemene gebruik.[173] Hy het goedkeuring gekry om met die projek voort te gaan, en het in samewerking met Robert Cailliau begin werk aan die nuwe stelsel. Nadat 'n verskeidenheid name oorweeg is, het Berners-Lee op "World Wide Web" besluit.[174]

Uit die projek het die web-protokol (HTTP)[175] voortgespruit, en Berners-Lee en Cailliau het ook die webbedienersagteware geskryf wat nodig was

bekendste wiki is sekerlik Wikipedia, alhoewel die twee nie sinoniem is nie. Wikipedia is maar net 'n voorbeeld van 'n wiki. Anderson J J *Wikipedia: The Company and Its Founders* (2011) 10–12. Daar bestaan menigte wiki's op die Internet waar medewerkers saamwerk om inligting oor 'n betrokke onderwerp of sagtewareprogram te orden.

Die eerste wiki-sagteware is deur Ward Cunningham geskep, en hy beskryf 'n wiki as "the simplest online database that could possibly work". Cunningham W "What is Wiki" http://wiki.org/wiki.cgi?WhatIsWiki (besoek op 22 Augustus 2014). Cunningham se eerste wiki was die WikiWikiWeb, geskep op 25 Maart 1995. Choate MS *Professional Wikis* (2008) 1.

172 Berners-Lee T "Information Management: A Proposal" http://www.w3.org/History/1989/proposal.html (besoek op 22 Augustus 2014).

173 Berners-Lee *Weaving the Web* 23; Sofroniou A *Surfing the Internet, Then, Now, Later* (2014) 47.

174 Berners-Lee *Weaving the Web* 23. Tegnies was die projek getiteld "WorldWideWeb" (sonder spasies). Swedin E G *Science in the Contemporary World: An Encyclopedia* (2006) 26.

175 Mohapatra S *E-Commerce Strategy: Text and Cases* (2012) 36 verduidelik HTTP so: "HTTP is used for communicating between web client and web server".

om dokumente te huisves. Verder was dit nodig om 'n "browser", of snuffelprogram te skryf sodat webblaaie gelees kan word. Berners-Lee het hierdie sagteware geskryf, en die eerste snuffelprogram was genoem *WorldWideWeb*.[176] Om egter verwarring te voorkom is die snuffelprogram se naam later verander na *Nexus*.[177]

Interessant genoeg was die *Nexus*-program nie net 'n snuffelprogram nie, maar ook 'n web-redigeerder ("web editor") wat dus nie net webblaaie kon lees nie, maar dit ook kon skryf en aanpas.[178]

Berners-Lee se aanvanklike voorlegging vir die skep van die web is aan sy bestuurshoofde op 12 November 1990 voorgelê.[179] Hy het geskat dat dit drie maande sou neem om die aanvanklike werk te doen om die stelsel in werking te stel, en nog ses maande om 'n web te skep wat deur gebruikers verander en aangepas sou kon word. Ongelooflik genoeg het Berners-Lee en Cailliau al die voorbereidingswerk teen einde Desember 1990 afgehandel om 'n werkende web te kon demonstreer.[180] Op 6 Augustus 1991 het Berners-Lee hul skepping aan die alt.hypertext-nuusgroep bekendgestel, en dit word dan ook as die amptelike datum gereken waarop die web vir enige gebruiker regoor die wêreld toeganklik geword het.[181]

2.3.5.4 Die Web Ontwikkel

Aanvanklik was die wêreldwye web slegs in akademiese kringe gebruik, en het dit nie veel aftrek buite hierdie gemeenskap gekry nie.[182] Daar was 'n

176 Net soos die oorhoofse projek — sien vn 174.

177 Hofmann M *Content Networking: Architecture, Protocols, and Practice* (2005) 5 en 283.

178 Hofmann *Content Networking: Architecture, Protocols, and Practice* 283.

179 Tetlow P *Understanding Information and Computation: From Einstein to Web Science* (2016) 7.

180 Berners-Lee T "WorldWideWeb: Summary" https://groups.*Google*.com/forum/?fromgroups=#!msg/alt.hypertext/eCTkkOoWTAY/bJGhZyooXzkJ (besoek op 2 September 2014).

181 Tetlow *Understanding Information and Computation: From Einstein to Web Science* 7; Berners-Lee T "WorldWideWeb: Summary" https://groups.*Google*.com/forum/?fromgroups=#!msg/alt.hypertext/eCTkkOoWTAY/bJGhZyooXzkJ (besoek op 2 September 2014).

182 Eagle L, Dahl S en Czarnecka B *et al Marketing Communications* (2014) 202.

ander protokol — Gopher — wat baie meer in gebruik was, en uitstekend gewerk het. Die skeppers van die Gopher protokol het egter besluit om lisensiegelde vir die gebruik daarvan te vra.[183] Ongeveer dieselfde tyd het CERN aangedui dat hulle die web-protokol kosteloos vir alle gebruikers wêreldwyd beskikbaar sou stel.[184] Hierdie gebeure het die web-protokol baie bevoordeel, en dit het begin veld wen.

Die webprotokol het 'n geweldige hupstoot gekry toe die *National Centre for Supercomputing Applications* by die Universiteit van Illinois die *Mosaic* snuffelprogram ontwikkel het.[185] Hierdie program kon 'n verskeidenheid protokolle hanteer, onder andere die webprotokol (HTTP) en Gopher. Die uitstaande kenmerk was egter dat dit geweldig gebruikersvriendelik was, en leke kon met min moeite die snuffelprogram aanpas vir eie gebruik. Aangesien die web-protokol gratis was (en Gopher nie — soos hierbo aangetoon is), het die webprotokol in hierdie tyd baie aanhang geniet.

In Desember 1990 het Berners-Lee die eerste webblad geskryf (en die eerste webbediener daargestel). Teen November 1992 was daar reeds ten minste 26 webbedieners gekoppel.[186] Teen Oktober 1993 het die Web reeds 1% van die totale Internetverkeer beslaan.[187] Twee maande later — Desember 1993 — het dit reeds 2.5% van die totale Internetverkeer

183 Die Gopher-protokol is deur die Universiteit van Minnesota ontwikkel. Dit het anders as die web gewerk deurdat die protokol 'n hiërargie gebruik het waar menu's baie prominent gebruik is. In Februarie 1991 het die universiteit aangekondig dat lisensiegelde op die gebruik van die protokol gehef sal word. Dit het onmiddellik veroorsaak dat dié protokol sy glans verloor het. Kozierok *The TCP/IP Guide* 1434. In September 2000 het die universiteit van Minnesota aangekondig dat Gopher nou onder die GNU GPL ("general public licence") geplaas word en dus vir enigeen kosteloos beskikbaar is, maar teen daardie tyd was dit te laat, aangesien die web reeds die dominante posisie in die wêreld ingeneem het. Kostecke S "UMN Gopher Released under the GPL" https://groups.*Google*.com/forum/#!msg/comp.infosystems.gopher/4A-LS_A6qtA/nT89yWKzzsIJ (besoek op 22 Augustus 2014).

184 CERN het op 30 April 1993 aangekondig dat HTTP — die web protokol — kosteloos vir alle Internetgebruikers beskikbaar gestel word. Berners-Lee T "Ten Years Public Domain for the Original Web Software" http://tenyears-www.web.cern.ch/tenyears-www/ (besoek op 27 Julie 2012).

185 Ellis K en Kent M *Disability and New Media* (2011) 71.

186 Cailliau R "A Little History of the World Wide Web" http://www.w3.org/History.html (besoek op 25 Augustus 2014).

187 W3C "History of the Web" http://www.w3c.it/education/2012/upra/documents/origins.pdf (besoek op 25 Augustus 2014).

opgeneem.

Op hierdie stadium was die web nog steeds grootliks deur die akademiese sektor gebruik.[188] Die jaar 1995 was die keerpunt waar die web algemeen deur die publiek begin gebruik is, en die Netscape-snuffelprogram was die wyse waarop die web besoek is.[189] *Microsoft* het die waarde van die web ingesien en die eerste weergawe van hulle *Internet Explorer* snuffelprogram bekendgestel.[190]

Nou het die Web as't ware ontplof.[191] Teen Januarie 1994 was daar reeds twee miljoen websnuffelaars, waarvan 95% daarvan die Mosaic-snuffelprogram[192] gebruik het. Die web het teen 11% *per week* gegroei![193] Kommersialisering van die Internet het begin posvat, en teen die draai van die eeu was die voorste 280 Internetmaatskappye 'n verbysterende $2.948 triljoen dollars werd.[194]

2.3.5.5 W3 Consortium

Reeds teen 1993 het dit duidelik geblyk dat die web besig was om met rasse skrede uit te brei.[195] Dit het so geweldig ontwikkel dat veral die skeppers van snuffelprogramme eensydig begin het om nuwe uitbreidings op die web-protokol in werking te stel.[196] Dit het 'n groot probleem geskep, aangesien sulke protokol-uitbreidings nie gestandaardiseer was nie, en dit kon meebring dat inligting op die web ontoeganklik is.

---

188 Eagle *Marketing Communications* 202.

189 Campbell J *1995: The Year the Future Began* (2015) 32.

190 Campbell *1995* 38.

191 Campbell *1995* 32.

192 Hierdie snuffelprogram was baie gewild by web-gebruikers, aangesien dit die eerste was wat 'n grafiese beheerfunksie gehad het. Shelly G B en Frydenberg M *Web 2.0: Concepts and Applications* (2010) 7; Hiraoka L S *Underwriting the Internet: How Technical Advances, Financial Engineering, and Entrepreneurial Genius are Building the Information Highway* (2005) 64.

193 W3C "History of the Web" http://www.w3c.it/education/2012/upra/documents/origins.pdf (besoek op 25 Augustus 2014).

194 Murray *The Regulation of Cyberspace* 72–73. Die eerste e-handel-webwerf was Pizza Hut, wat in 1994 begin het om Pizzas oor die Internet te verkoop. Murray *The Regulation of Cyberspace* 73 vn 47.

195 Afd sub:2.3.5.4.

196 Association for Information Management *Managing Information* (1995) 267.

Berners-Lee het in hierdie tyd na Massachusetts verhuis waar hy die W3-Consortium gestig het met die "Massachusetts Institute of Technology" (hierna MIT) as hoofkwartier.[197] In 1995 het die "Institut National de Recherche en Informatique et en Automatique" (INRIA) — wat in Frankryk gesetel is — die Europese gasheer van die W3-Consortium geword.

Sedertdien het die W3-Consortium na 18 wêreldkantore uitgebrei — met 'n tak ook in Suid-Afrika.[198]

Die werk van die W3-Consortium is baie belangrik, en tot dusver het hulle dit baie suksesvol uitgeoefen. Uitbreidings op die web-protokol is geweldig — van gewone teks tot volledige multimedia en virtuele realiteit-uitbreidings.[199]

2.3.5.6 Web-dienste

Die web het so geweldig veld gewen dat dit wyer begin ontwikkel het as wat Berners-Lee aanvanklik voorgestel het. Die bekendste uitbreiding van die web-protokol is sekerlik die beskikbaarstelling van webdienste.[200] Dit behels dat die web-protokol gebruik word om nie net statiese bladsye op te dien nie, maar volledige programme aan te bied.[201] Dit is dus moontlik om 'n sagtewareprogram in 'n websnuffelprogram aan te bied — soos om woordverwerkingsfunksies in 'n webblad te plaas.[202]

Webdienste het die funksionaliteit om vir 'n spesifieke webwerf aangepas te kan word.[203] 'n Reisagentskap-webwerf kan byvoorbeeld

197 Mathiason J *Internet Governance: The New Frontier of Global Institutions* (2009) 38; Bank D *Breaking Windows: How Bill Gates Fumbled the Future of Microsoft* (2001) 199.

198 W3C-SA "Contact W3C-SA" http://www.w3c.org.za/officecontact.html (besoek op 25 Augustus 2014).

199 World Wide Web Consortium "About W3C" https://www.w3.org/Consortium/ (besoek op 25 Augustus 2014).

200 Alonso G *Web Services: Concepts, Architectures and Applications* (2004) 124.

201 Alonso meen dat so 'n definisie te simplisties is. In sy boek definieer hy webdienste in tegniese terme, maar dit is vir hierdie regstudie nie nodig om verder daaraan aandag te gee nie. Alonso *Web Services: Concepts, Architectures and Applications* 124–125.

202 Stair R *Principles of Information Systems* (2013) 316: "Today's Web development applications allow developers to create Web sites using software that resembles a word processor".

203 Zimmermann O, Tomlinson M en Peuser S *Perspectives on Web Services: Applying SOAP, WSDL and UDDI to Real-World Projects* (2012) 161 Topley K *Java Web Services in a Nutshell* (2003) 10.

aanlynbesprekings vir vliegtuigbesprekings aanvaar — en dit volledig prosesseer met 'n webdiensprogram.[204] Webdienste is vandag 'n algemene verskynsel op die web.

2.3.5.7 Die Sosiale Web

Een van die nuwer ontwikkelinge van die web is die sosiale funksie daarvan.[205] Dit word soms sosiale media of bloot Web 2.0 genoem.[206] Dit dui nie op 'n nuwe tegniese spesifikasie van die web nie, maar eerder op die vindingryke nuwe metodes waarop die web gebruik kan word om sosialisering te bewerkstellig. Die sosiale web het so 'n groot rol in die gebruik van die web begin speel dat dit tereg as 'n sosiale web-fenomeen beskryf kan word.[207] Waar die web aanvanklik gebruik is om statiese bladsye te vertoon, het dit nou in 'n sisteem ontwikkel waar die gebruiker nie net meer die *ver*bruiker van die inligting is nie, maar ook die skepper daarvan. Trouens, in sosiale web-analises word persone nou as nodes in 'n netwerk beskou.[208] Blogs en sosiale netwerke het soos paddastoele opgeskiet, en sommige sosiale netwerke soos *Facebook* en *Twitter* se ledetalle oorskry reeds meeste lande se bevolkingsgetalle.[209] Joshua Porter beskryf in sy boek *Designing for the Social Web* dat gebruikers "visit MySpace, *Facebook*, and other social network sites at least once per day, (and) this lengthy stay is

---

204 Barry D K *Web Services, Service-Oriented Architectures, and Cloud Computing: The Savvy Manager's Guide* (2012) 12.

205 Golbeck J *Analyzing the Social Web* (2013) 1 noem byvoorbeeld: "Social media has become the dominant method of using the Internet, and it has infiltrated and changed the way millions of people interact and communicate".

206 Kurbalija J *An Introduction to Internet Governance* (2012) 156–157.

207 Webdienste is maar slegs een aspek van die groter Web 2.0. Kurbalija stel dit duidelik: "With the development of Web 2.0 platforms — blogs, forums, document-sharing websites, and virtual worlds — the difference between the user and the creator has blurred. Internet users can create large portions of Web content, such as blog posts, *YouTube* video's, and photo galleries." Kurbalija *An Introduction to Internet Governance* 156–157..

208 Golbeck *Analyzing the Social Web* 2 verduidelik: "Classic social network analysis studies a network's structure. In a social network, a person is considered a node or vertex, and a relationship between people is a link or edge. When all the people and relationships are identified, there are many statistics that can provide insight into the network".

209 Wikipedia "Facebook" https://en.wikipedia.org/wiki/Facebook (besoek op 25 Augustus 2014).

habitual. In other words, the social web is becoming a way of life".[210]

Hierdie woorde is reeds in 2008 geskryf, en sedert daardie tyd het hierdie fenomeen eksponensiëel gegroei, aangesien *Facebook* en *Twitter* programme deesdae op slimfone en tablette beskikbaar is.

Een van die mees kommerwekkende aspekte van die sosiale media is die verdwyning van die reg op privaatheid. Andrews stel dit selfs nog sterker wanneer sy noem dat die sosiale kontrak — wat die basis van demokrasie vorm — besig is om te verbrokkel:

> Unlike in a democracy, *Facebook* is unilaterally redefining the social contract — making the private now public and the public now private. Private information about people is readily available to third parties. At the same time, public institutions, such as the police, use social networks to privately undertake activities that previously would have been subject to public oversight. Even though cops can't enter a home without a warrant, they scrutinize *Facebook* photos of parties held at high school students' homes.[211]

2.3.5.8 Semantiese Web

Berners-Lee het reeds so vroeg as 1998 'n semantiese web voorsien.[212] Veltman verduidelik Berners-Lee se visie soos volg:

> He articulated the vision of a semantic web, whereby one can separate rhyme from reason: i.e. the subjective dimensions of art and poetry from the objective dimensions of logic, which is one definition of science.[213]

Hierdie verduideliking is egter maar nog net die begin van Berners-Lee se visie. 'n Semantiese web in die ware sin van die woord sal so gestruktureerd wees dat *rekenaars* die inligting wat beskikbaar is, sal kan verstaan en daarop reageer. In die *Scientific American* van Mei 2001 skryf Berners-Lee dat:

---

210 Porter J *Designing for the Social Web* (2008) 18.

211 Andrews L *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy* (2012) 5.

212 W3C "Semantic Web Road Map" https://www.w3.org/DesignIssues/Semantic.html (besoek op 25 Augustus 2014).

213 Veltman K "Challenges for a Semantic Web" http://semanticweb2002.aifb.uni-karlsruhe.de/proceedings/Position/veltmann.pdf (besoek op 25 Augustus 2014).

> The Semantic Web is not a separate Web but an extension of the current one, in which information is given well-defined meaning, better enabling computers and people to work in cooperation. The first steps in weaving the Semantic Web into the structure of the existing Web are already under way. In the near future, these developments will usher in significant new functionality as machines become much better able to process and "understand" the data that they merely display at present.[214]

In hierdie artikel skryf Berners-Lee dat die semantiese web byvoorbeeld rekenaar-"agente" in staat sal stel om vir mense afsprake te maak by die dokter en dan ook sommer voorskrifmedisyne by die apteek te bestel. Volgens hom is die basis van die semantiese web reeds 'n werklikheid — maar dit moet nog in werking gestel word.[215]

2.3.5.9 Die Web se Toekoms

Dit is moeilik om te voorspel wat die toekoms van die web sal inhou, maar dit wil tog voorkom asof daar 'n paar algemene riglyne is wat waarskynlik sal realiseer. In die eerste plek wil dit voorkom asof die volgende web-rewolusie sal wees om die magdom inligting wat op die web beskikbaar is, vir mense meer hanteerbaar te maak.[216] Waar die web aanvanklik ontwikkel is om inligting beskikbaar te stel, het dit ontwikkel na 'n sosiale web. Ontwikkeling sal nou rondom die individu geskied. Kozlowski stel die drie ontwikkelinge mooi in *Forbes Magazine:* "Their web — our web — your web".[217]

'n Verdere ontwikkeling van die web is die verskuiwing na mobiele media. Waar rekenaarterminale in die verlede die toegangskanale na die web was, is dit nou toenemend deur slimfone en rekenaartablette.[218]

Die mees indrukwekkende ontwikkeling wat die Internet reeds besig is

---

214 Berners-Lee T, Hendler J en Lassila O "The Semantic Web" 2001 *Scientific American* 28–37.

215 Berners-Lee 2001 *Scientific American* 28–37.

216 Hacid M, Ras Z W en Zighed A *et al Foundations of Intelligent Systems* (2003) 4.

217 Kozlowski L "The Future of the Web Looks a Lot Like You" http://www.forbes.com/sites/lorikozlowski/2012/06/15/the-future-of-the-web-looks-a-lot-like-you/ (besoek op 25 Augustus 2014).

218 O'Farrell M J *et al Mobile Internet for Dummies* (2008) 47–49.

om te ondergaan, is sekerlik die nuwe "Internet of things".[219] Daarvolgens sal huishoudelike toestelle op so 'n wyse aan die Internet gekoppel kan word dat dit nuwe funksionaliteit kan meebring,[220] soos byvoorbeeld 'n yskas wat produkte kan bestel wanneer dit opgebruik word.[221]

2.3.5.10 Samevatting

Hierdie afdeling het die proses van die ontwikkeling van die Wêreldwye web geskets.[222] Die konsep daarvan is reeds in 1945 aangebied,[223] maar dit het eers in 1990 tot stand gekom.[224] Aanvanklik was dit slegs in akademiese kringe gebruik, maar toe dit eers aan die groter mensdom bekend gestel is, het dit geweldig begin groei.[225]

Die W3 Consortium is geskep om die ontwikkeling van nuwe tegnologieë vir die web, soos web-dienste,[226] te standaardiseer.[227] Die ontwikkeling van die sosiale web het die 21ste eeu ingelui, en dit is tot vandag toe baie gewild.[228] Nuwe tegnologieë wat tans op die web in werking gestel word, is inligtings-ordening en die "Internet of things".[229]

---

219 Bahga A en Madisetti V *Internet of Things: A Hands-On Approach* (2014) 20 verduidelik: "Internet of Things is a new revolution in the capabilities of the endpoints that are connected to the Internet, and is being driven by the advancements in capabilities (in combination with lower costs) in sensor networks, mobile devices, wireless communications, networking and cloud technologies".

220 Uckelmann D, Harrison M en Michahelles F *Architecting the Internet of Things* (2011) 100.

221 De Saint-Exupéry A *Vision and Challenges for Realising the Internet of Things* (2010) 16 noem spesifiek hierdie voorbeeld, aangesien dit reeds ontwikkel is.

222 Afd 2.3.5.

223 Afd 2.3.5.

224 Afd 2.3.5.4.

225 Afd 2.3.5.4.

226 Afd 2.3.5.6.

227 Afd 2.3.5.5.

228 Afd 2.3.5.7.

229 Afd 2.3.5.9.

2.3.6 Gefragmenteerde Internet

2.3.6.1 Inleiding

In hierdie hoofstuk is daar tot op hede beskryf hoe die Internet ontwikkel het vanuit meganiese masjiene wat basiese berekeningsfunksies kon verrig, tot die ontwikkeling van rekenaarnetwerke wat internasionale grense kon oorspan.[230] Daar is ook verduidelik hoe die fisiese argitektuur van die Internet die ontwikkeling van nuwe protokolle, soos die Web, moontlik gemaak het.[231] Nou verskuif die fokus weer na die groter Internet (in plaas van bloot die Web), en sal die nuwe, en krities belangrike, uiteensetting gegee word van hoe die Internet 'n drastiese ontwikkeling ondergaan het wat die oorspronklike ontwerpers en ingenieurs nie voorsien het nie — die fragmentering daarvan.

Daar is reeds vroeg in hierdie hoofstuk aangetoon dat die Internet gekonsepsualiseer is as 'n verspreide netwerk.[232] Die voordeel van so 'n stelsel is dat dit nie maklik buite werking gestel kan word nie. Daarom is dit juis in hierdie formaat ontwikkel en gebou. Trouens, in die laat 1990's het dit gelyk asof die vroeë Internetvaders geheel en al in hul doelwit geslaag het om 'n universele en uniforme Internet te skep, want selfs die Amerikaanse "Supreme Court"[233] het in die saak van *Reno v American Civil Liberties Union*[234] beslis dat die Internet "fundamenteel anders" is.[235]

Dit was 'n kragdadige stelling wat wyd deur die Internetwêreld

230 Afd 2.2.

231 Afd 2.3.5.

232 Afd 2.2.4.

233 Die woorde "Supreme Court" word doelbewus nie vertaal met "hoë hof" nie, aangesien die Amerikaanse "Supreme Court" die hoogste hof van appél is, terwyl die Afrikaanse term "hoë hof" kan dui op enige hoër hof. In die konteks van hierdie uitspraak — wat spesifiek gehandel het op die tersydestelling van 'n wet — sou dit meer korrek gewees het om die term "Supreme Court" met "Konstitusionele hof" te vertaal. Om egter enige verwarring te voorkom is daar besluit om tog eerder die direkte Engelse term te gebruik.

234 521 US 844 (1997).

235 Regter Sandra Day O'Connor meld in die uitspraak op 889–890 dat: "The electronic world is fundamentally different".

geresoneer het. David Sobel, een van die regsgeleerdes wat namens die respondent opgetree het, het prontuit gesê dat: "[The Court] clearly came down on the side of this being a new medium, that it is inappropriate to graft old broadcast laws onto the Internet. ... There is very little room for further regulation of the Internet".[236]

Die Internet was dus op hierdie stadium 'n eenheidsnetwerk wat die hele wêreld oorspan het.[237] Dit skep dadelik 'n probleem vir state wat hul gebied en burgers wil reguleer.[238] Onafhanklike state het dikwels totaal uiteenlopende ideologieë, en om sulke uiteenlopende denkwyses onder een sambreel bymekaar te bring is 'n onbegonne taak.[239] Daarom was dit net 'n kwessie van tyd totdat verskillende state sou begin ingryp om hulle stukkie van die groter Internet te probeer beheer. Die gevolg daarvan is dat die Internet huidig nie meer net een groot verspreide netwerk is soos aan die einde van die vorige eeu nie, maar eerder 'n groep geografiese intranette[240] wat saamgegroepeer is om die groter Internet te vorm.[241]

Die vraag wat hieruit ontstaan is hoe kan state van die wêreld die Internet reguleer indien dit 'n eenheidsnetwerk is wat grense ignoreer? Interessant genoeg het die antwoord hierop gekom deur 'n reeks hofsake tussen twee groepe met uiteenlopende opinies oor Nazi-memorabilia. *Licra*

---

236 Wired "CDA Struck Down" http://archive.wired.com/politics/law/news/1997/06/4732 (besoek op 25 Augustus 2014).

237 Mehdi K P *Dictionary of Information Science and Technology, Volume 1* (2006) 361 beskryf die Internet so: "A worldwide system of computer servers from which users at any computer can extract information or knowledge".

238 Die ideologie van 'n globale Internet wat onreguleerbaar is weens die feit dat dit een verspreide netwerk is, word verduidelik in Boele-Woelki K *Internet — Which Court Decides? Which Law Applies?* (1998) 23. Omdat hierdie werk voor die draai van die eeu geskryf is, verduidelik dit die *status quo* van 'n ongefragmenteerde Internet van daardie tyd. Sien ook Simon *Netpolicy.com* 44 waar daar spesifiek tydens hierdie tydsvak gesê word dat: "by design, the Net is truly and uniquely worldwide. Content created in one country can be viewed in any other country or number of countries at any time or as many times as users wish".

239 Afd 6.4.

240 Die term intranet word spesifiek hier gebruik om dit te onderskei van die groter Internet. In hierdie studie sal "intranet" deurgaans gebruik word om staatsgebonde netwerke te beskryf, m.a.w. die intranet van die staat teenoor die groter globale Internet.

241 Sommige van die regsbeginsels wat hier ter sprake is, word bespreek in hfst 6 en 7.

v Yahoo[242] het op twee kontinente afgespeel, en aangesien hierdie saak daartoe aanleiding gegee het dat die wese van die Internet fundamenteel verander het, word dit vervolgens in meer besonderhede bespreek.

2.3.6.2 Die *Licra v Yahoo* hofsake

Tydens die tweede helfte van die negentigerjare het die sogenaamde dotcom-borrel ontstaan. Dit het meegebring dat Internetbesighede oral soos paddastoele opgespring en eksponensiëel gegroei het.[243] 'n Verdere uitvloeisel van hierdie fenomeen is dat daar in 'n betreklik kort tydjie multinasionale besighede wat uitsluitlik besigheid op die Internet doen, ontstaan het. Een hiervan was *Yahoo*, wat tydens die draai van die eeu die grootste Internetsoekenjin was.[244]

Die Internet van hierdie tyd was werklik 'n globale, onverdeelbare netwerk. Multinasionale maatskappye soos *Yahoo* het besigheid gedoen met die siening dat hulle binne 'n nuwe medium funksioneer wat nie aan individuele state se wette gehoor hoef te gee nie, aangesien dit nie tegnologies moontlik was om dit te doen nie.[245] Hierdie siening het in hooftrekke ooreengestem met die *Reno*-uitspraak waar die hof bevind het dat die Internet "fundamenteel anders" is.[246] So 'n siening sou binnekort in die *Yahoo v Licra*-beslissings getoets word.

---

242 Afd 2.3.6.2.

243 Ofek E en Richardson M "Dotcom Mania: The Rise and Fall of Internet Stock Prices" 2003 *The Journal of Finance* 1113.

244 Marckini F *Search Engine Positioning* (2001) 184. Sedertdien het Google hierdie posisie oorgeneem. Jones K B *Search Engine Optimization: Your Visual Blueprint for Effective Internet Marketing* (2013) 15.

245 Afd 2.3.6.2.1.

246 Afd 3.3.2.

2.3.6.2.1 *Licra v Yahoo (1)*[247]

In Februarie 2000 het Marc Knobel, 'n Franse Jood wat hom beywer vir die uitwissing en bevegting van Neo-Nazibedrywighede, in Parys op die Internet raakgesien dat daar 'n menigte Neo-Nazi aandenkings op *Yahoo*.com se VSA veilingswebwerwe te koop aangebied word.[248] Hierdie VSA veilingswebwerwe was spesifiek bedoel vir gebruikers in die VSA, en nie vir internasionale klante nie. Tog kon websnuffelaars van enige nasionaliteit dit beskou, en ook meedoen aan die veilings, maar die reg van die VSA sou enige verkope beheer.[249]

Die verkoop van enige Nazi-verwante artikels word volgens Franse wetgewing verbied,[250] maar is nie verbode volgens Amerikaanse wetgewing nie. Knobel het reeds in 1998 op soortgelyke artikels op "America Online" (hierna AOL) se webwerwe afgekom, en *AOL* versoek om die verkoop van sulke artikels te verbied. *AOL* het hieraan gehoor gegee aangesien hulle 'n anti-AOL media-skokgolf wou vermy.[251]

Knobel het gedink dat sy versoek aan *Yahoo* 'n soortgelyke gevolg sou hê, maar dit was nie die geval nie.[252] Die eienaar van *Yahoo*, Jerry

---

247 *Uejf et Licra v Yahoo Inc et Yahoo France*, Tribunal De Grande Instance De Paris, N° RG: 00/05308, May 22, 2000. Die oorspronklike hofsaak is in Frans, maar 'n Engelse vertaling daarvan is beskikbaar by: Lapres D "*Licra and the Uejf v Yahoo Inc and Yahoo France*" http://www.lapres.net/yahen11.html (besoek op 11 November 2013). Ook Chatillon G *Internet International Law* (2005) 148–149.

248 Schultz T "Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface" 2008 *The European Journal of International Law* 799 809.

249 Lapres D "*Licra and the Uejf v Yahoo Inc and Yahoo France*" http://www.lapres.net/yahen11.html (besoek op 11 November 2013). Ook Chatillon *Internet International Law* 148–149.

250 Art R645-1 van die Franse Strafkode (Code Pénal).

251 Volledigheidshalwe kan genoem word dat *AOL* 'n Internetdiensverskaffer is wat in Washington DC funksioneer. Hierdie maatskappy het besigheid gedoen binne die hoofstad van die VSA waar positiewe diplomatieke betrekkinge en potensiële negatiewe mediaskokgolwe in 'n ernstige lig beskou word. Daarom was dit nie vreemd dat *AOL* aan Knobel se versoek sou voldoen om die verkoop van Nazi-memorabilia te staak nie. Daarteenoor was *Yahoo* 'n skepping van die Silikonvallei aan die ooskus van Amerika, waar die werkskultuur heel anders is. Hier was die fokus op kompetisie en die ontwikkeling van nuwe tegnologieë, en dikwels was die uitvoerende direkteure (en eienaars) van Silkikonvallei-gebaseerde besighede gewoonlik baie winsgedrewe, met min simpatie vir enigiets wat nie daardie doel ondersteun nie. Goldsmith *Who Controls the Internet?* 1–2.

252 Knobel het op 5 April 2000 die "cease and desist"-brief aan *Yahoo* gestuur. Greenberg M H "A Return to Lilliput: The *Licra v Yahoo* Case and the Regulation of Online Content in the World Market" 2003 *Berkeley Technology Law Journal* 1191 1206.

Yang, het aangevoer dat 'n Franse burger wat vanuit Frankryk die VSA-webwerf van *Yahoo*.com besoek, nie die bevoegdheid het om enige eise aan 'n Amerikaanse Internetbesigheid te stel nie, en het bloot die versoek geïgnoreer.[253]

Knobel was nie met hierdie toedrag van sake tevrede nie, en met die hulp van die Internasionale Liga teen Rassisme en Anti-Semitisme[254] het hy vir *Yahoo* in April 2000 in 'n Franse hof gedagvaar om die verkoop van Nazi-goedere te verbied. Die saak van *Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France c. Yahoo Inc et Société Yahoo France* (*Licra et UEJF v Yahoo and Yahoo France*) was die eerste van 'n reeks hofsake op twee kontinente wat die hele aangeleentheid van Internetfragmentasie op die spits gedryf het, en wat die geskiedenis van die Internet onherroeplik verander het.[255]

Knobel se argument was eenvoudig: "In the United States (these auctions) might not be illegal, but as soon as you cross the French border, it's absolutely illegal".[256] *Yahoo* se saak het egter net so oortuigend geklink —

253 Greenberg 2003 *Berkeley Technology Law Journal* 1206.

254 Die "International League Against Racism and Anti-Semitism", of *Ligue Internationale Contre le Racisme et l'Antisémitisme (Licra)* in Frans, is reeds in 1926 in Frankryk gestig, en het dus sedert sy ontstaan sterk Franse bande. Wikipedia "International League against Racism and Anti-Semitism" https://en.wikipedia.org/wiki/International_League_against_Racism_and_Anti-Semitism (besoek op 11 November 2013). Daarom was dit bloot logies vir Knobel om hierdie organisasie se hulp in te roep om 'n groot multinasionale Internetbesigheid soos *Yahoo* aan te vat.

255 Hierdie reeks hofsake is 'n klassieke voorbeeld van die reg se ontoereikendheid om sonder 'n soliede jurisdiksionele basis 'n saak ten volle te kan bereg. Greenberg 2003 *Berkeley Technology Law Journal* 1205–1206 stel dit baie goed:

> [The] dispute between the French plaintiffs and *Yahoo* serves as a sad illustration of the inability of the litigation process, either in France or in the United States, to deal with the complex cultural and legal issues that arise when material posted lawfully on servers in one country violates the law when viewed by web surfers in another country. The courts in each country attempt to walk the fine line between preserving their sovereignty and preserving the principle of international comity. The results are less than satisfying on all sides. Perhaps the most disappointing element of this dispute is that after more than three years of litigation, the parties are no better off than when they started, and the issues they attempted to address in the litigation are still unresolved.

256 Schultz 2008 *The European Journal of International Law* 810; Straziuso J "Associated Press, French Anti-Racist Group Sues *Yahoo*" http://www.apnewsarchive.com/2000/French-Anti-Racist-Group-Sues-*Yahoo*/id-1a0475ef8b88a12f717b6975f67a5043 (besoek op 2 Januarie 2013).

Jerry Yang het opgemerk: "The French tribunal wants to impose a judgment in an area over which it has no control. The court is not taking into account the technology and the very nature of the Internet."[257] *Yahoo* se visie-president, Heather Killen, het Yang se argument bevestig: "The people who create (*Yahoo* France) are subject to French jurisdiction. However, we do not believe that www.*Yahoo*.com — which is created and maintained and developed by teams in the US and is in the English language and actively promoted to a US audience — we don't believe that the site is subject to French jurisdiction."[258] Killen het ook die beleid van 'n nuwe, onreguleerbare Internet ondersteun deur spesifiek te sê: "We have many countries and many laws and just one Internet."[259] Verder het *Yahoo* aangevoer dat dit tegnologies onmoontlik is om Franse burgers toegang tot die Amerikaanse *Yahoo*-webwerwe te weier, en dat hul dus nie in staat is om enigsins 'n hofbevel wat so iets beveel, te kan uitvoer nie.[260]

Die hof het op 22 Mei 2000 'n interimhofbevel toegestaan wat bevestig het dat die verkoop van die memorabilia onder Franse wetgewing onwettig is, en 'n paneel deskundiges aangestel om 'n finale verslag op te stel van hoe dit moontlik kan wees (indien enigsins), om te voorkom dat *Yahoo* deur sy internasionale Internetportaal Franse wetgewing oortree.[261]

Die span deskundiges het op 6 November 2000 hulle verslag aan die hof voorgelê, en op 20 November van daardie jaar is 'n finale hofbevel uitgereik wat *Yahoo* aansê om aan Franse wetgewing te voldoen.[262]

Die span deskundiges se verslag aan die hof het 'n baie groot invloed op die uitspraak gehad.

---

257 Hunter M "Interview with Jerry Yang from Liberation (16-6-00) Article by Launet Edouard" in "Business e-Ethics: *Yahoo* on Trial (B)" 2001 *INSEAD* 4956.

258 Hu J en Hansen E "*Yahoo* Auction Case May Reveal Borders of Cyberspace" http://news.cnet.com/*Yahoo*-auction-case-may-reveal-borders-of-cyberspace/2100-1023_3-244365.html (besoek op 11 November 2013).

259 Goldsmith *Who Controls the Internet?* 2.

260 Greenberg 2003 *Berkeley Technology Law Journal* 1207. Goldsmith *Who Controls the Internet?* 3.

261 Greenberg 2003 *Berkeley Technology Law Journal* 1207.

262 Greenberg 2003 *Berkeley Technology Law Journal* 1213.

Voordat daar verduidelik word hoe hierdie hofsaak verder verloop het, is dit egter nodig om kortliks iets oor die paneel van deskundiges te meld — asook wat hul bevindings was.

Die hof het besluit om drie deskundiges in die paneel aan te stel — een uit Frankryk, 'n ander vanuit Europa, en 'n derde deskundige van Amerika.[263] Die bekendste van die drie deskundiges was Vincent Cerf,[264] wat allerweë as die "Vader van die Internet" beskou word.[265] Die Europese deskundige was Ben Laurie, 'n Internet-protokolontwerper en skrywer van die alombekende Apache-websagteware. Die derde kundige was die Fransman Francois Wallon.[266]

Aldus Laurie was die deskundiges se opdrag bloot om die vraag te antwoord of dit tegnies moontlik is dat *Yahoo* aan die hofbevel wat teen hulle gegee is, te kan voldoen, en indien nie, wat gedoen kan word om aan die hofbevel gehoor te gee.[267]

Dit het geblyk dat hierdie vraag nie geredelik beantwoord kon word nie, en die drie deskundiges het die verslag begin met 'n vrywaringsverklaring:

> The undersigned consultants are at pains to point out that their brief is limited to answering the technical questions put by the Court. In no circumstances may their answers be construed as constituting a technical or moral backing of the decisions of the court or, on the contrary, a criticism of these decisions.[268]

Die deskundiges het hul verslag begin met 'n verduideliking van die feite van die saak, en het dan verder verduidelik wat die Internet is. Die Internet Protokol-adressisteem is in meer besonderhede bespreek, aangesien geo-

263 Greenberg 2003 *Berkeley Technology Law Journal* 1210 vn 93.

264 Greenberg 2003 *Berkeley Technology Law Journal* 1210 vn 93.

265 Schell B H *The Internet and Society: A Reference Handbook* (2007) 175.

266 Goldsmith *Who Controls the Internet?* 7; Schultz 2008 *The European Journal of International Law* 819.

267 Laurie B "An Expert's Apology" http://www.apache-ssl.org/apology.html (besoek op 25 Augustus 2014).

268 Die verslag van die deskundiges is by die Franse hofbevel aangeheg. Die oorspronklike hofbevel is uit die aard van die saak in Frans, maar die Engelse vertaling daarvan is beskikbaar by Gomez J J "*Licra and UEJF v Yahoo Inc and Yahoo France*" http://www.lapres.net/yahen11.html. (besoek op 27 Februarie 2013).

plasingsmetodes[269] grootliks van hierdie protokol gebruik maak om mense in 'n geografiese posisie op die aarde te plaas. Die domeinnaamstelsel wat aan die Internet Protokol gekoppel is, is ook verduidelik.[270]

Hierna het die drie deskundiges die metodes verduidelik hoe dit moontlik kan wees om persone geografies te plaas. Dit is:

- Geo-plasing
- Identifisering van nasionaliteit deur gebruikers

Geo-plasing maak gebruik van die gebruiker se Internetprotokol om hom te identifiseer. Hierdie metode is slegs ongeveer 70% akkuraat.

Die tweede metode is om elke gebruiker te versoek om sy nasionaliteit aan te dui voordat die webwerf gebruik word. Die deskundige Vincent Cerf het verskeie redes aangevoer waarom so 'n benadering eenvoudig onwerkbaar is.[271]

Ten spyte van die kritiek teen die verskillende metodes om 'n Internetgebruiker se ligging te bepaal, het die drie deskundiges saamgestem dat dit wel moontlik is om met 'n akkuraatheid van ongeveer 70–80% die ligging van 'n persoon op aarde te plaas.[272]

---

269 Die Engelse term is "geo-location". Geen gepaste Afrikaanse vertaling kon gevind word nie, en gevolglik is hierdie term geskep om die gebruik van Engelse terminologie in die Afrikaanse teks te beperk. Sien Gentile C, Alsindi N en Raulefs R *et al Geolocation Techniques: Principles and Applications* (2012) 4 vir meer inligting oor hoe geo-plasingsmetodes funksioneer.

270 Afd 2.3.4 bevat 'n volledige bespreking van die DNS en IP-protokol.

271 Vinton Cerf skryf in die verslag:

> "It has been proposed that users identify where they are at the request of the web server, such as the one(s) serving *Yahoo*.fr — or *Yahoo*.com. There are several potential problems with this approach. For one thing, users can choose to lie about their locations. For another, every user of the web site would have to be asked to identify his or her location since the web server would have no way to determine *a priori* whether the user is French or is using the Internet from a French location. Some users consider such questions to be an invasion of privacy. While I am not completely acquainted with privacy provisions in the Europe Union, it might be considered a violation of the rights of privacy of European users, including French users to request this information. Of course if this information is required solely because of the French Court Order, one might wonder on what grounds all other users all over the world are required to comply.

Gomez J J "*Licra v Yahoo*" http://www.lapres.net/yahen11.html (besoek op 25 Augustus 2014).

272 Greenberg 2003 *Berkeley Technology Law Journal* 1215.

Die hof het hierdie verslag aanvaar, en verder aangevoer dat *Yahoo* reeds van geo-plasingsmetodes gebruik maak om Franse advertensies aan Franssprekende webgebruikers aan te bied, en gevolglik was dit moontlik vir *Yahoo* om aan die hofbevel gehoor te gee.[273] Die interimhofbevel is bevestig, en *Yahoo* is drie maande gegee om daaraan te voldoen alvorens daar hewige monetêre boetes van ongeveer 100 000 Frank per dag gehef sou word.[274]

2.3.6.2.2 *Yahoo v Licra (2)*[275]

Yahoo was nie met hierdie toedrag van sake tevrede nie, maar in plaas daarvan om teen die beslissing in Frankryk te appelleer, het hulle 'n Amerikaanse hof genader om 'n verklarende bevel uit te reik oor of die Franse uitspraak op *Yahoo* in Amerika van toepassing was.[276] *Licra* het egter terselfdertyd die hof genader om die aksie af te wys, maar dit het nie geslaag nie.[277]

Yahoo het met hul saak rakende 'n verklarende bevel voortgegaan, en hier het die hof beslis dat die Franse hof se uitspraak *Yahoo* se Eerste Amendement-regte[278] geskend het.[279]

---

273 Greenberg 2003 *Berkeley Technology Law Journal* 1215.

274 Gomez J J "*Licra and UEJF v Yahoo Inc and Yahoo France*" http://www.lapres.net/yahen11.html. (besoek op 27 Februarie 2013).

275 *Yahoo Inc v La Ligue Contre Le Racisme Et* 145 F Supp 2d 1168.

276 *Yahoo Inc v La Ligue Contre Le Racisme Et* 145 F Supp 2d 1168 1171: "*Yahoo* now seeks a declaration by this Court that the order of the French court is unenforceable in the United States because it contravenes the Constitution and laws of the United States."

277 *Yahoo Inc v La Ligue Contre Le Racisme Et* 145 F Supp 2d 1168 1172.

278 Die Eerste Amendement-regte van die Amerikaanse grondwet het op die 15e Desember 1791 in werking getree. Alhoewel dit aanvanklik net op godsdiensvryheid van toepassing was, is dit later uitgebrei om voorsiening te maak vir 'n verskeidenheid gevalle van vryheid van spraak. Hieronder val aspekte soos persvryheid, godsdiensvryheid, en laster. Schultz D A *Encyclopedia of the United States Constitution* (2010) 273; Anoniem "Charters of Freedom — A New World is at Hand" http://www.archives.gov/exhibits/charters/bill_of_rights.html (besoek op 3 Mei 2013). Die teks van die Eerste Amendement kan gelees word by Ciment J *Social Issues in America: An Encyclopedia* (2015) 1497.

279 *Yahoo Inc v La Ligue Contre Le Racisme* 169 F Supp 2d 1181.

2.3.6.2.3 *Yahoo v Licra (3)*[280]

Licra het hierdie uitspraak egter na die VSA Hof van Appèl vir die 9de rondgang geneem (dus in die staat wat direkte jurisdiksie oor *Yahoo* het).[281] Hierdie hof het egter in 2004 die hof *a quo* se beslissing omvergewerp deur te beslis dat die laer hof verkeerdelik "algemene jurisdiksie"[282] gevestig het aangesien *Licra* nie "continuous and systematic contacts with the forum state" gehad het nie.[283] Eweneens is die vestiging van "spesifieke jurisdiksie" ook afgewys.[284]

Hierna het die hof verduidelik dat *Yahoo* 'n kommersiële voordeel daaruit verkry om die Amerikaanse webwerwe aan Franse burgers voor te hou. Trouens, die hof het opgemerk dat: "the company displays advertising banners in French to those users whom it identifies as French".[285] Verder het die hof opgemerk dat *Yahoo* nie aan die een kant die voordeel van 'n wêreldwye mark kan hê en dan agter die eerste Amendement van die Amerikaanse grondwet kan skuil wanneer dit ander landswette oortree nie.[286]

Die gevolg van hierdie uitspraak was dat *Yahoo* wél aan die beslissing van die Franse hof moes voldoen.

---

280 *Yahoo Inc v La Ligue Contre Le Racisme* 379 F 3d 1120 — Court of Appeals 9th Circuit 2004.

281 *Yahoo Inc v La Ligue Contre Le Racisme* 379 F 3d 1120 — Court of Appeals 9th Circuit 2004.

282 "Algemene jurisdiksie" en "spesifieke jurisdiksie" is gespesialiseerde regsterme in die VSA-regstelsel. Sien Wang F F *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China* (2010) 66 en Dunham B W *Introduction to Law* (2008) 197 vir 'n uiteensetting van hierdie tipes jurisdiksie in die VSA-reg.

283 *Yahoo Inc v La Ligue Contre Le Racisme* 379 F 3d 1123.

284 *Yahoo Inc v La Ligue Contre Le Racisme* 379 F 3d 1123.

285 *Yahoo Inc v La Ligue Contre Le Racisme* 379 F 3d 1126.

286 *Yahoo Inc v La Ligue Contre Le Racisme* 379 F 3d 1126. "*Yahoo* cannot expect both to benefit from the fact that its content may be viewed around the world and to be shielded from the resulting costs — one of which is that, if *Yahoo* violates the speech laws of another nation, it must wait for the foreign litigants to come to the United States to enforce the judgment before its First Amendment claim may be heard by a US court."

2.3.6.2.4 *Yahoo v Licra (4)*[287]

Op hierdie stadium was *Yahoo* egter in 'n penarie, want ongeveer vyf jaar het reeds verloop sedert die Franse hof sy uitspraak gegee het waarin daar beslis is dat *Yahoo* aan die Franse hofbevel gehoor moet gee, of stywe daaglikse boetes moet betaal. Om alles te kroon het *Yahoo* sedert die Franse hofbevel reeds heelwat veranderinge aangebring om Franse burgers te waarsku wanneer hulle nazi-memorabilia-webwerwe sou teëkom.[288] *Licra* het ook reeds aangedui dat hulle nie die Franse hof sou nader om die interimhofbevel te bekragtig solank *Yahoo* voortgaan met hulle huidige (positiewe) optrede nie.[289] *Yahoo* was egter van mening dat hulle tegnies nog nie aan die Franse hofbevel gehoor gegee het nie, en dat hierdie uitspraak soos 'n swaard oor hulle koppe hang.[290] Om hierdie rede het *Yahoo* besluit om 'n verklarende bevel na die volbank van die Hof van Appèl vir die 9de rondgang te neem.[291]

Die 2006-volbankbeslissing was 'n tegniese een. Die jurisdiksievraag is in besonderhede aangespreek, en die beslissing was nie eenparig nie, maar die meerderheidsbeslissing het bepaal dat die Amerikaanse howe wél jurisdiksie oor die saak het.[292] Die hof van eerste instansie se beslissing is dus bevestig. Wat egter van meer belang is, is dat die volbank beslis het dat *Yahoo* se eerste Amendement-regte *nie* geskend was nie (en dus die hof van eerste instansie se beslissing op hierdie punt omvergewerp het).[293] Die uiteinde van die saak was egter dat die hof in die meerderheidsbeslissing van mening was dat *Yahoo* niks te vrees gehad het solank hulle voortgaan met hulle waarskuwings aan Franse burgers ten opsigte van nazi-memorabilia

287 *Yahoo Inc v La Ligue Contre Le Racisme* 433 F 3d 1199 Court of Appeals 9th Circuit 2006 1218.

288 *Yahoo Inc v La Ligue Contre Le Racisme* 433 F 3d 1199 Court of Appeals 9th Circuit 2006 1218.

289 *Yahoo Inc v La Ligue Contre Le Racisme* 433 F 3d 1199 Court of Appeals 9th Circuit 2006 1218.

290 *Yahoo Inc v La Ligue Contre Le Racisme* 433 F 3d 1199 Court of Appeals 9th Circuit 2006 1218.

291 *Yahoo Inc v La Ligue Contre Le Racisme* 433 F 3d 1199 Court of Appeals 9th Circuit 2006 1201.

292 *Yahoo Inc v La Ligue Contre Le Racisme* 433 F 3d 1199 Court of Appeals 9th Circuit 2006 1201.

293 *Yahoo Inc v La Ligue Contre Le Racisme* 433 F 3d 1199 Court of Appeals 9th Circuit 2006 1211.

nie.[294] Die minderheidsbeslissing was geensins so oortuig hiervan nie.[295] Daar word aan die hand gedoen dat die minderheidsbeslissing die tegnies-korrekte een is, want Yahoo het steeds belange in Frankryk waarop 'n hof beslag kan lê, asook werknemers van die maatskappy wat voor 'n hof gedaag kan word.[296]

Soos wat oor die algemeen die geval is wanneer regsake van die Internet bereg word, was die hof se beslissing maar eintlik mosterd na die maal, aangesien die tegnologie in die vyf jaar wat dit geneem het om die finale uitspraak te kry, reeds so ingrypend verander het dat die beslissing vir alle praktiese doeleindes onnodig was. Die Internet was een globale netwerk in die jaar 2000, maar was reeds diep gefragmenteerd in 2005. Die *Licra v Yahoo* hofsake was bloot die vonk wat die fragmentasieproses aan die gang gesit het. In daardie sin het dié hofsake die Internet onherroeplik verander, ten spyte daarvan dat die finale uitspraak nie werklik enige sinvolle bydrae tot konstruktiewe Internetregulering kon lewer nie.

2.3.6.3 Fragmentering Gaan Voort

Die fragmentasie van die Internet is tot op hede nog geensins afgehandel nie. Trouens, dit wil lyk asof hierdie verskynsel net verder en verder uitkring.[297] Lande soos Sjina en Egipte het in die laaste paar jaar baie gedoen om hul eie geografiese intranet van die groter Internet af te sper.[298] Sjina is aan die voorgrond met hierdie proses, en hulle "Great Firewall of China"

---

294 *Yahoo Inc v La Ligue Contre Le Racisme* 433 F 3d 1199 Court of Appeals 9th Circuit 2006 1221. Die hof meld: "In sum, it is extremely unlikely that any penalty, if assessed, could ever be enforced against Yahoo! in the United States".

295 Die hof meld op 1242–1243: "Uncertainty about whether the sword of Damocles might fall is precisely the reason Yahoo! seeks a determination of its First Amendment rights in federal court. ... Instead, the majority turns Yahoo!'s uncertainties against it — relegating it to the French courts for clarification and absolution".

296 Sien in hierdie verband ook die Duitse *Compuserve*-beslissing wat in afd 6.3.1 bespreek word.

297 Hfst 7 bespreek hierdie verskynsel in meer besonderhede.

298 Die skepping van geografiese staats-intranette word verder hieronder in 6.4.2 bespreek.

is geweldig uitgebreid en verbasend effektief.[299] Die fragmentering van die Internet deur lande soos Sjina sal later in die studie hanteer word.[300]

2.3.6.4 Samevatting

In die laat 1990's is die Internet as 'n nuwe sfeer beskou wat as't ware nie aan landswette gehoorsaam hoef te wees nie, aangesien die tegnologie nie bestaan het om onderskeid te tref tussen web-besoekers van spesifieke state nie.[301] Dit het egter alles verander toe die saak van *Yahoo v Licra* in 'n Franse hof begin is — en dit uiteindelik die fragmentering van die Internet op die voorgrond geplaas het.[302]

Yahoo v Licra (1) het in 'n Franse hof afgespeel waar die hof beslis het dat Yahoo van 'n verskeidenheid tegnieke gebruik moet maak om te verhoed dat Nazi-memorabilia in Frankryk besigtig word.[303] Yahoo was van mening dat dit nie aan so 'n bevel gehoor kan gee nie, aangesien die tegnologie nie voldoende ontwikkel het om dit moontlik te maak nie. Gevolglik het Yahoo hom tot 'n hof in die VSA gewend. In *Yahoo v Licra (2)* het die hof in 'n verklarende bevel aangetoon dat Yahoo se Eerste Amendement-regte geskend is.[304]

Licra het op sy beurt weer hierdie beslissing na die VSA Hof van Appèl vir die 9de rondgang geneem, en daar is in *Yahoo v Licra (3)* tot die gevolgtrekking gekom dat die hof *a quo* fouteer het — dat *Yahoo* nie aan die een kant die voordeel van 'n wêreldwye mark kan hê en dan agter die

299 Stevenson C "Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World" 2007 *Boston College International and Comparative Law Review* 531 537.

300 Afd 6.4.2. Voorbeelde van ander state wat ook ingrepe in hul staat-intranette gemaak het, is Egipte tydens die 2011-rewolusie toe die hele land se Internet op een dag opgeskort is. Dainotti A *et al* "Analysis of Country-wide Internet Outages Caused by Censorship" Verrigtinge van die 2011 "ACM Sigcomm Conference on Internet Measurement Conference" 2011; Zhuo X, Wellman B en Yu J "Egypt: The First Internet Revolt?" 2011 *Peace Magazine* 6–10. Ander state soos Brasilië, Indië en Duitsland het ook al op ander wyses ingrepe gemaak om hulle staat-intranette te isoleer. Afd 7.3.1.1.

301 Afd 2.3.6.

302 Afd 2.3.6.2.

303 Afd 2.3.6.2.1.

304 Afd 2.3.6.2.2.

eerste Amendement van die Amerikaanse grondwet skuil wanneer dit ander landswette oortree nie.[305]

Ten tyde van hierdie hofbevel het daar reeds ongeveer vyf jaar verloop, en het die tegnologie reeds so ontwikkel dat dit wél moontlik was om spesifieke webgebruikers te verhinder om sekere inligting te bekom — en Yahoo het reeds daarvan gebruik gemaak. Tog het Yahoo gemeen dat as hulle die saak net daar laat, hulle steeds onder die swaard van die Franse hof se bevel van daaglikse boetes staan. Daarom het die vierde saak van *Yahoo v Licra (4)* gevolg om 'n verklarende bevel van die aangeleentheid te bekom.[306] In die eerste plek het die meerderheidsbeslissing bepaal dat die Amerikaanse hof wél jurisdiksie het. Tweedens was die meerderheidsbeslissing van die hof van mening dat Yahoo niks te vrees het van 'n Franse hof nie, terwyl die minderheidsbeslissing hierdie standpunt gekritiseer het.[307]

Die gevolg van hierdie reeks beslissings was dat dit aanleiding gegee het tot 'n beweging wat die Internet toenemend gefragmenteer het.[308] Hierdie tendens is steeds aan die gang.[309]

***

Noudat die ontwikkeling van die globale Internet in besonderhede bespreek is en daar ook uitgewys is hoe dit uiteindelik gefragmenteer het, is dit nodig om ook die ontwikkeling van die Internet in die Suid-Afrikaanse konteks onder die loep te neem.

305 Afd 2.3.6.2.3.

306 Afd 2.3.6.2.4.

307 Afd 2.3.6.2.4.

308 Afd 2.3.6.2.4.

309 Hfst 7.

2.4 Ontwikkeling van die Internet in Suid-Afrika

2.4.1 Inleiding

In die sestiger- en sewentigerjare van die vorige eeu het hoofraamrekenaargebruik aan universiteite reg oor die wêreld begin toeneem.[310] Hierdie tendens het ook in Suid-Afrika plaasgevind, en universiteite reg oor Suid-Afrika het hoofraamrekenaars vir hulle universiteitsgebruik aangeskaf.[311] Hierdie rekenaars het nog almal onafhanklik gefunksioneer.

Rekenaardepartemente het begin eksperimenteer met die gedagte om rekenaars in netwerke aaneen te skakel. Ongelukkig was hierdie nie 'n maklike taak nie, aangesien rekenaars nie gestandaardiseer was nie, en ook omdat Suid-Afrika op daardie stadium in 'n wurggreep van sanksies was, wat beteken het dat die verkryging van rekenaars en netwerktoerusting baie moeilik was.[312] Tog het die verskillende rekenaardepartemente volgehou en stukkie-vir-stukkie het deurbrake gevolg. Mike Lawrie verduidelik dat by Rhodes universiteit hulle dit in Januarie 1988 reggekry het om protokolle te skryf wat rekenaars in die Fisika-, Chemie- en Besigheidsinligtingsdepartemente met dié van die rekenaarsentrum kon skakel.[313] Hulle het dus hul eie klein plaaslike netwerk, of LAN,[314] geskep.

Intussen het die universiteite in die noorde van Suid-Afrika, te wete

---

310 2.3.2.

311 Arditti R en Brennan P *Science and Liberation* (1980) 192 skets 'n beeld van rekenaargebruik in die sestiger- en sewentigerjare in Suid-Afrika: "South Africa was late among the industrialized nations to enter the computer era. The first computer, a British one, was installed in 1959. During the 1960s the computers industry in South Africa expanded at a rate of more than 30% annually, and by 1970 there were an estimated 400 computers in the country with a value of some $100 million".

312 Delener N *Strategic Planning and Multinational Trading Blocs* (1999) 107 verduidelik: "South Africans have a high regard for American telecommunications equipment and services, but because of the combined effect of past sanctions and local closed procurement practices, US companies were not able to participate in this market."

313 Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014) 10.

314 "Local Area Network" in Engels. Sadiku M N O en Ilyas M *Simulation of Local Area Networks* (1994) 2 definieer 'n plaaslike netwerk so: "A LAN is a data communication system, usually owned by a single organization, that allows similar or dissimilar digital devices to talk to each other over a common transmission medium".

Potchefstroom universiteit, die Universiteit van Pretoria en die Universiteit van die Witwatersrand dit reggekry om almal met die Wetenskaplike en Nywerheidsnavorsingsraad (WNNR) te skakel. Hierdie organisasies het almal IBM-rekenaars[315] gebruik, en gevolglik was die skakeling heelwat makliker.[316]

Na intensiewe samewerking tussen Rhodes-universiteit en die universiteit van Potchefstroom is die twee netwerke aan mekaar geskakel, en kon e-poskommunikasie vryelik tussen die verskillende organisasies beweeg.[317]

2.4.2 Pogings tot Internasionale Skakeling

Noudat die groot universiteite in Suid-Afrika met e-pos kon skakel, het dit nodig geword om Suid-Afrika aan die groter Internet e-posstelsel te skakel. Hierdie ingewikkelde taak is nog verder bemoeilik deur sanksies wat teen Suid-Afrika van krag was.[318]

Die universiteit van Kaapstad het onder leiding van Dr Fred Goldstein dit reggekry om in 1988 'n e-posskakeling met UUNet in die VSA te bewerkstellig.[319] Hierdie skakeling is egter na drie weke opgeskort weens die sanksies teen Suid-Afrika.[320] Suid-Afrika se universiteitsnetwerk was dus nog nie met die groter Internet geskakel nie.

Intussen het Professor Pat Terry — wat die hoof van die Departement

315 "International Business Machines".

316 Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014) 10.

317 Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014) 10.

318 Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014) (besoek op 25 Augustus 2014) 2.

319 Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014) (besoek op 25 Augustus 2014) 2.

320 Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014) 10; Wilson C "Chris Pinkham: Veteran of the Virtual" http://www.techcentral.co.za/chris-pinkham-veteran-of-the-virtual/25403/ (besoek op 25 Augustus 2014).

Rekenaarwetenskap aan Rhodes universiteit was — betrokke geraak by die skryf van ISO-standaarde vir die Modula-2 programmeringstaal.[321] Dit het meegebring dat hy deel geword het van 'n internasionale kommissie wat die nodige standaard moes skryf. Een van die lede van dieselfde tegniese komitee was Randy Bush, 'n rekenaarwetenskaplike van Oregon in die VSA. Op besoek aan huis van Bush in Augustus 1988 het Terry opgemerk dat hy verbaas was hoe "agter" hy geraak het met die werk van sy kollegas in die tegniese komitee, en het vir Bush uitgevra hoe hy so op hoogte gebly het met nuwe verwikkelinge in die veld. Bush het Terry meegedeel dat die Amerikaanse lede van die tegniese komitee met elektroniese pos gekommunikeer het. Terry het nou ingesien hoe krities belangrik e-pos vir navorsing is, en die elektroniese posstelsel wat Bush gebruik het, het Terry so beïndruk dat hy dit na Suid-Afrika wou bring. Om Terry hiermee te help, het Bush twee belangrike insette gelewer: Eerstens het hy vir Terry die nodige sagteware gegee om 'n internasionale netwerkskakeling daar te stel, en nog meer belangrik het Bush vir Terry die versekering gegee dat hy vir Terry direk aan die Fidonet netwerk waaraan Bush gekoppel was, sou skakel.[322]

Terug in Suid-Afrika het Pat Terry en sy kollegas begin om die elektroniese posstelsel in werking te stel. Een kollega wat nou by hierdie projek betrokke was, was Mike Lawrie.

Lawrie noem dat die privaat e-posstelsel tussen Rhodes universiteit en Bush se woning in Portland, Oregon in die VSA reeds teen 10 September 1988 gefunksioneer het.[323] Dit het dus ongeveer twee weke geneem om die stelsel in gebruik te neem. Die stelsel was egter beperk tot e-pos, en dit was in die vorm van 'n a-sinkroniese inskakeldiens ("dial up") wat beteken het dat daar gereeld 'n internasionale oproep na Randy Bush se netwerk gemaak

321 Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014) 16.

322 Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014) 16.

323 Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014) 15.

sou word om e-posse te stuur en te ontvang.[324]

In Februarie 1989 is die stelsel vir algemene gebruik aan die Rhodes-universiteitsgemeenskap beskikbaar gestel. Lawrie noem dat dit 'n groot dag vir die span was toe die netwerk na drie weke nog gefunksioneer het, gesien in die lig van die onaangename stel wat die universiteit van Kaapstad afgetrap het weens sanksies teen Suid-Afrika.[325]

2.4.3 Die Universiteitsnetwerk Bars uit sy Nate

Die netwerk het baie goed gefunksioneer, en dit het so gewild geword dat die koste daarvan buitensporig gestyg het. Lawrie verduidelik dat die netwerk — wat op hierdie stadium nog net e-posse kon stuur en ontvang — op 'n stadium bykans R90 000 per maand gekos het. "It worked out at 1c or 2c per e-mail message. There was just that much traffic."[326]

Benewens die sanksies teen Suid-Afrika, was een van die grootste struikelblokke om die Suid-Afrikaanse intranet[327] met die groter Internet te skakel, die telekommunikasiemonopolie van Telkom. Dit het 'n beleid gehad om enige "derdepartyverkeer" op sy telefoonnetwerk te verbied. Lawrie verduidelik dit soos volg:

---

324 Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014) 15.

325 Lawrie skryf:

> It was a significant day in our lives when the Fidonet gateway was still operating in production three weeks after it was opened for general campus use at Rhodes, in February 1989. This was because we had heard that quite a few months earlier, UCT had operated a UUCP connection to UUNET in the USA, and that this link had been closed down for political reasons after three weeks. We really could not believe that we had done better than this — we had broken through the sanctions barrier on a zero budget operation without having to resort to any cloak and dagger exercises. We had also beaten the South African government of the day, which was desperately trying to control every last form of communication in and out of the country.

Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014) 10.15.

326 Wilson C "Mike Lawrie: SA's Internet Pioneer" http://www.techcentral.co.za/mike-lawrie-sas-Internet-pioneer/24774/ (besoek op 25 Augustus 2014).

327 Die term "intranet" word hier gebruik, aangesien Suid-Afrika nog maar 'n eie landswye intranet gehad het, en nog nie regtig deel was van die groter Internet nie. Sien ook hfst 1 vn 7.

> If you and I had a dedicated circuit between us, and I had another to someone else, I could use both to communicate with each end, but I couldn't let you connect through me to point C.[328]

Die derdeparty-reël het slegs gegeld vir sogenaamde "leased lines", wat telefoonlyne is wat 'n permanente skakeling met 'n telefoonsentrale het.[329] Hierdie reël het juis die skakeling verbied wat Rhodes universiteit met Randy Bush se huis nodig gehad het. Gevolglik kon die telefoonlyn nie bekom word nie.

Om egter die volgende verloop van gebeure te verstaan, is dit nodig om effens terug te beweeg na 1985 en 'n proses te verduidelik wat gelyklopend met hierdie gebeure plaasgevind het.

2.4.4 Uninet

Terwyl die Suid-Afrikaanse internet in die middel tagtigerjare ontwikkel is, is die Komitee van Universiteitshoofde van Suid-Afrika in 1985 die taak opgelê om rekenaarnetwerkskakeling tussen universiteite te formaliseer, asook om die Suid-Afrikaanse intranet met die res van die wêreld te skakel.[330] Die subkomitee wat hierdie mandaat moes uitvoer kon egter nie daarin slaag om dit te doen nie. Om hierdie probleem die hoof te bied, het die Stigting vir Navorsingsontwikkeling (FRD),[331] in samewerking met die tegniese komitee van die Komitee van Universiteitshoofde in 1987 die proses begin om skakeling tussen Suid-Afrikaanse universiteitsnetwerke daar te stel.[332] Dit was die begin van die universiteitsnetwerk, of Uninet.

---

328 Wilson C "Mike Lawrie: SA's Internet Pioneer" http://www.techcentral.co.za/mike-lawrie-sas-Internet-pioneer/24774/ (besoek op 25 Augustus 2014).

329 Wilson C "Mike Lawrie: SA's Internet Pioneer" http://www.techcentral.co.za/mike-lawrie-sas-Internet-pioneer/24774/ (besoek op 25 Augustus 2014).

330 Knoch C "Uninet — The South African Academic and Research Network" http://web.archive.org/web/20030419023522/http://www.idrc.ca/acacia/outputs/op-unin.htm (besoek op 2 Augustus 2014).

331 In Engels die "Foundation for Research Development", of FRD, wat vandag die "National Research Foundation" (NRF) is.

332 Knoch C "Uninet — The South African Academic and Research Network" http://web.archive.org/web/20030419023522/http://www.idrc.ca/acacia/outputs/op-unin.htm (besoek op 2 Augustus 2014).

Uninet is beskou as 'n "collaborative project among tertiary educational institutions (and) research councils".[333] Dit het vinnig gegroei aangesien dit geheel deur die FRD befonds is. Die universiteitsnetwerk, wat in die vroeë tagtigerjare deur elke universiteit op 'n lukraak wyse ontwikkel is, het as 'n eenheid begin funksioneer onder die naam Uninet.

Op hierdie stadium het die Suid-Afrikaanse intranet dus uit twee oorde ontwikkelingshulp ontvang — aan die een kant was daar die universiteite wat die kennis en vaardighede gegee het om die netwerk te laat werk, en aan die ander kant die FRD wat dit befonds het.[334]

2.4.5 Onderhandelinge met Telkom

Soos in afdeling 2.4.3 verduidelik, het Telkom die "derdeparty-reël" in plek gehad wat organisasies verbied het om mekaar se netwerkskakeling te gebruik as 'n groter netwerk wat vir almal toeganklik is.[335] Telkom het soms 'n uitsondering op die reël aanvaar. Dit het behels dat as die lyngebruiker kon aantoon dat die belange van 'n "common interest group" gedien word, die derdeparty-reel verslap kon word.[336]

Ongelukkig het Telkom aangevoer dat die verhouding tussen Rhodes universiteit en die huis van Randy Bush nie 'n gemeenskaplike belangegroep is nie, en het gevolglik geweier om 'n direkte "leased line" toe te staan.[337]

Vic Shaw, wat eers by die WNNR gewerk het en later die bestuurder van die FRD geword het, het hierdie saak verder met Telkom gevoer. Die

[333] Knoch C "Uninet — The South African Academic and Research Network" http://web.archive.org/web/20030419023522/http://www.idrc.ca/acacia/outputs/op-unin.htm (besoek op 2 Augustus 2014).

[334] Knoch C "Uninet — The South African Academic and Research Network" http://web.archive.org/web/20030419023522/http://www.idrc.ca/acacia/outputs/op-unin.htm (besoek op 2 Augustus 2014).

[335] Wilson C "Mike Lawrie: SA's Internet Pioneer" http://www.techcentral.co.za/mike-lawrie-sas-Internet-pioneer/24774/ (besoek op 25 Augustus 2014).

[336] Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014) 15.17.

[337] Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014) 15.17.

universiteite van Suid-Afrika was nou deel van die meer formele Uninet-netwerk, en Shaw het aangevoer dat die universiteite van Suid-Afrika 'n gemeenskaplike belangegroep vorm — en dat die direkte lyn dus verskaf moet word onder 'n verslapte derdeparty-reël. Telkom het uiteindelik geswig onder die druk van die FRD, en die lyn kon onder die "gemeenskaplike belangegroep"-uitsondering gebruik word.[338]

2.4.6 Protokolstandaardisering

Terwyl daar gesukkel is om die direkte "leased line" van Telkom te verkry, het Lawrie en sy span voortgegaan om hulle netwerk gereed te kry vir Suid-Afrika se koppeling aan die groter Internet.[339] Tot op daardie stadium was alle kommunikasie beperk tot e-pos. Die Internet het egter heelwat meer gebied, soos om lêers via die FTP-protokol ("file transfer protocol") te kan aflaai, en om die gewilde Usenet[340] te kan gebruik.[341]

Om hierdie funksies te kan gebruik het beteken dat die protokolle wat op Uninet gebruik is, met die res van die internasionale Internet gestandaardiseer sou moes word. Rhodes universiteit het in die loop van 1990 en vroeg in 1991 TCP/IP werkswinkels aangebied om al die persone wat aan die Uninet netwerk werk, daarmee vertroud te maak.[342] Hierdie standaarde is regoor die netwerk geïmplementeer.

---

338 Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014) 15.17.

339 Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014) 27.

340 Usenet is 'n wêreldwye platform waar sake van enige onderwerp bespreek word. Jim Ellis van Duke universiteit in die VSA het dit die eerste keer in 1979 gekonsepsualiseer, en is dit so vroeg as 1980 reeds geïmplementeer. Dit het behels dat gebruikers boodskappe kon lees en pos na verskillende onderwerpe, en dat dit dan vir almal beskikbaar is om te lees. Usenet was die voorloper van die Internet Forums wat huidig bestaan. Lueg C en Fisher D *From Usenet to CoWebs: Interacting With Social Information Spaces* (2003) 23.

341 Teen hierdie tyd is die gewilde wêreldwye web, of WWW, nog nie ontwikkel nie.

342 Die eerste TCP/IP werkswinkel is op 6–8 Augustus 1990 gehou. Die laaste werkswinkel het op 29–31 Januarie 1991 plaasgevind. Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014) 26.

2.4.7 Suid-Afrika Word Gekoppel aan die Internet

Die vroeë 1990's het verreikende politieke veranderinge in Suid-Afrika teweeg gebring, en dit het die geleentheid geskep dat die .ZA landskodedomein[343] verkry kon word. In Oktober 1990 het personeel by die Rhodes universiteit op 'n besoek aan die VSA met Sue Kirkpatrick en Doug MacGowan, wat aan die Stanford Research Institute betrokke was, kennis gemaak.[344] Dit het geblyk dat die groter Internet nou vir organisasies buite die Amerikaanse militêre sfeer en akademiese instansies in die VSA oop was.[345]

Dit het Lawrie die geleentheid gegee om namens Rhodes universiteit en Uninet (waarby hy beide in 'n bestuursposisie betrokke was) 'n aansoek te bring om die .ZA landskodedomein te bekom.[346] Omdat dit geblyk het dat die politieke situasie in Suid-Afrika besig was om te verander, is die aansoek oorweeg.[347] Vinton Cerf het in 'n e-posboodskap in November 1990 aan Lawrie geskryf:

> I am pleased to report that the IAB, in consultation with the Federal Networking Council working group chairmen, concluded that the recent policy expressed in RFC1174 and endorsed by the FNC provides grounds for positive consideration of the request by Rhodes University to take responsibility for the .ZA domain.[348]

---

343 In Engels "Country Code Top Level Domain", of bloot ccTLD.

344 Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014) 29.

345 Cerf V "IAB Recommended Policy on Distributing Internet Identifier Assignment and IAB Recommended Policy Change to Internet "Connected" Status" http://tools.ietf.org/html/rfc1174 (besoek op 2 September 2014). Hierdie dokument van die IETF, wat bloot as RFC1174 bekend staan, het verduidelik waarom die Internet nou nie meer eksklusief vir militêre en akademiese gebruik is nie, maar wel beskikbaar is vir 'n groter gehoor.

346 E-poskommunikasie tussen Vinton Cerf en Mike Lawrie oor die verkryging van die .ZA domein. Cerf V "Re: Registration of .ZA Domain" http://web.archive.org/web/20041012150242/http://www2.frd.ac.za/uninet/history/zacleard.htm (besoek op 2 September 2014).

347 Cerf V "Re: Registration of .ZA Domain" http://web.archive.org/web/20041012150242/http://www2.frd.ac.za/uninet/history/zacleard.htm (besoek op 2 September 2014).

348 Cerf V "Re: Registration of .ZA Domain" http://web.archive.org/web/20041012150242/http://www2.frd.ac.za/uninet/history/zacleard.htm (besoek op 2 September 2014).

Lawrie was in ekstase oor hierdie nuus:

> This is really and truly a great day for us here in South Africa! Many thanks indeed for all of your help in clarifying the situation for us.[349]

Die .ZA domein is op 7 November 1990 toegestaan.[350]

Randy Bush was die eerste persoon om 'n e-pos vanuit die buiteland na 'n .ZA-domein te stuur. Suid-Afrika was uiteindelik met gebruikmaking van die .ZA domein aan die Internet gekoppel. Dit het plaasgevind op die 12de November 1991 om 10:44.[351] Randy Bush se eerste e-pos word weergegee in figuur 2.10.

2.4.8 Samevatting

Hoofraamrekenaars is sedert die sestiger- en sewentigerjare al hoe meer by universiteite in gebruik geneem. Dit was ook die geval in Suid-Afrika.[352] Ongelukkig het elke rekenaar afsonderlik gefunksioneer, en die behoefte om rekenaars aan mekaar te koppel, het ontstaan.[353]

Verskeie universiteite in Suid-Afrika het dit reggekry om skakeling tussen hulle plaaslike rekenaars te bewerkstellig.[354] Dit is later uitgebrei na skakeling tussen universiteite.[355]

As gevolg van sanksies teen Suid-Afrika, was dit bykans onmoontlik om skakeling met die buitewêreld te verkry nie.[356] Dit is geïllustreer toe die

---

349 Cerf V "Re: Registration of .ZA Domain" http://web.archive.org/web/20041012150242/http://www2.frd.ac.za/uninet/history/zacleard.htm (besoek op 2 September 2014).

350 Anoniem "IANA Report on the Redelegation of the .za Toplevel Domain" https://www.IANA.org/reports/2005/za-report-05aug05.pdf (besoek op 25 Augustus 2014); Lawrie M "The History of the Internet in South Africa" http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf (besoek op 25 Augustus 2014).

351 Wilson C "The SA Internet Turns 20" http://www.techcentral.co.za/the-sa-Internet-turns-20/27371/ (besoek op 2 September 2014).

352 Afd 2.4.

353 Afd 2.4.

354 Afd 2.4.1.

355 Afd 2.4.1.

356 Afd 2.4.2.

```
From: Randy Bush <randy@psg.com>
Subject: The first ping
To: ccfj@quagga.ru.ac.za (F.F. Jacot Guillarmod),
      ccdw@quagga.ru.ac.za (Dave Wilson),
      barret@daisy.ee.und.ac.za (Alan Barrett),
      fsg@ucthpx.uct.ac.za (Fred Goldstein)
      nerd@percival.rain.com (Michael Galassi)
Date: Tue, 12 Nov 91 0:57:21 PST
Message-Id: <m0kgtvt-000b0LC@rain.psg.com>

Well, the line keeps going up and down, and the telcos have not completed
testing yet. But, for the record book, the first ping from North America to
[Sub-Saharan] Africa

rain:/home/randy> ping 146.231.64.2
146.231.64.2 is alive
rain:/home/randy> date
Tue Nov 12 00:44:47 PST 1991

And to push the envelope, all mail for Africa which comes to rain.psg.com
will now go SMTP, i.e. This message!

Fantastic!

randy
```

Bron: Wilson C *The SA Internet Turns 20* (http://www.techcentral.co.za/the-sa-internet-turns-20/27371/).

Figuur 2.10: Randy Bush se Eerste E-pos Nadat Suid-Afrika aan die Internet Gekoppel is.

universiteit van Kaapstad in 1988 dit reggekry het om Suid-Afrika aan die groter Internet te koppel, maar hierdie skakeling het slegs drie weke geduur voordat dit beëindig is.[357]

'n Vriendskap tussen Pat Terry, 'n akademikus van Rhodes, en Randy Bush, 'n rekenaarwetenskaplike in die VSA, het daartoe gelei dat Rhodes universiteit in Suid-Afrika en die huis van Randy Bush in die VSA met 'n gewone telefoonlyn aan mekaar gekoppel kon word om basiese e-posse te kan stuur en ontvang.[358] Hierdie koppeling het die eerste stabiele skakeling tussen Suid-Afrika en die groter Internet verleen.[359] Dit was egter slegs 'n tydelike maatreël, en 'n meer permanente oplossing sou wees om 'n "leased-line" van Telkom te verkry.[360] Ongelukkig was so 'n koppeling teen Telkom se beleid, maar met behulp van die FRD wat druk op Telkom kon

357 Afd 2.4.2.

358 Afd 2.4.2.

359 Afd 2.4.2.

360 Afd 2.4.5.

uitoefen, is die lyn bekom.[361]

Intussen het Mike Lawrie, wat die tegniese aspekte van die koppeling by Rhodes universiteit hanteer het, met die owerhede onder leiding van Vinton Cerf onderhandel om die .ZA domein te bekom, en dit namens Suid-Afrika te administreer.[362] Omdat die politieke situasie in Suid-Afrika gunstig vir die buiteland voorgekom het, is hierdie aansoek toegestaan, en is Suid-Afrika uiteindelik met die .ZA domein aan die Internet gekoppel.[363]

2.5 Gevolgtrekking

Hierdie hoofstuk het 'n geskiedkundige oorsig oor die ontstaan van die Internet gebied. Ten spyte daarvan dat hierdie 'n regstudie is, was dit nodig om die basis van Internet-ontwikkeling te skets.[364] Dit vorm die fondament van meer ingewikkelde konsepte wat in verdere hoofstukke sal volg.

Daar is aangetoon dat dit moeilik is om die Internet te definieer.[365] Sommige definisies hanteer die aard van die Internet, terwyl ander definisies weer die funksie daarvan aandui.[366] Definisies vanuit die regspraak en wetgewing is ook oorweeg,[367] maar na vele oorwegings is die volgende definisie as die mees bruikbare een aanvaar:

> An international conglomeration of interconnected telecommunication networks which provides for the interaction of connected information systems and their users, by carrying their traffic using a single system of numbering, naming, addressing, identification, protocols and procedures that is defined by Internet Standards.[368]

361 Afd 2.4.5.

362 Afd 2.4.7.

363 Afd 2.4.7.

364 Afd 2.1.

365 Afd 2.2.

366 Afd 2.2.

367 Afd 2.2.

368 Russian Federation "World Conference on International Telecommunications (WCIT—12) Dubai, 3–14 December 2012: Proposals for the Work of the Conference" http://www.soumu.go.jp/main_content/000188224.pdf (besoek op 4 September 2014).

Rekenaar-argitektuur is volgende bespreek.[369] Verskille tussen bedieners en roeteerders is aangetoon, en die wyse waarop daar gebruik gemaak word van pakketskakeling om data oor die Internet te stuur, is bespreek.[370]

Dit is belangrik om te begryp dat die Internet as 'n verspreide netwerk ontwikkel is.[371] Die voordeel daarvan is dat dit die gladde funksionering van die Internet bewerkstellig.[372] Indien een node van die netwerk ophou funksioneer, sal dit nie die werking van die hele netwerk beïnvloed nie.[373]

Die ontwikkeling van die Internet is ook in oënskou geneem.[374] Die ontwikkeling van verskeie netwerke is bespreek,[375] en daar is aangetoon hoe die ARPANET die voorloper van die Internet was.[376]

Die wyse waarop netwerke met mekaar skakel, is aangedui, en in hierdie konteks is veral die *Internet Suite* bespreek.[377] Daar is aangetoon dat dit 'n geweldige uitdaging vir reguleerders skep, aangesien verskeie vlakke van 'n netwerk gereguleer word, en wanneer 'n laer vlak gereguleer word, beïnvloed dit enige pogings tot regulering op 'n hoër vlak.[378] Die voorbeeld van kopieregwetgewing is gebruik om hierdie dilemma te illustreer.[379]

Daar word dikwels in hierdie studie na die domeinnaamstelsel en die Internet protokol verwys, en daarom is die werking daarvan bespreek.[380] Basisnaambedieners vorm deel van hierdie sisteem, en is van kritiese belang by die behoorlike funksionering van die Internet.[381] Die bestuur van die verskeie basisnaambedieners op die Internet word die IANA-funksie

369 Afd 2.2.2.
370 Afd 2.2.2.
371 Afd 2.2.4.
372 Afd 2.2.4.
373 Afd 2.2.4.
374 Afd 2.3.
375 Afd 2.3.2.
376 Afd 2.3.2.4.
377 Afd 2.3.3.
378 Afd 2.3.3.
379 Afd 2.3.3.
380 Afd 2.3.4.
381 Afd 2.3.4.

genoem.[382] Dit is eweneens verduidelik.

Die Internet bestaan uit verskeie funksies, en die Wêreldwye web is sekerlik die gewildste hiervan. Die proses van ontwikkeling is aangetoon,[383] en verskeie funksies, soos webdienste[384] en die sosiale web[385] is bespreek.

Sedert die vroeë 2000's het die Internet 'n stille transformasie ondergaan van 'n eenheidsnetwerk na 'n hoogs gefragmenteerde netwerk.[386] Dit het begin met vier hofsake wat tussen die web-reus *Yahoo* en die Franse "International League Against Racism and Anti-Semitism" gewoed het.[387] Die gevolg hiervan was die ontwikkeling van 'n gefragmenteerde Internet wat heelwat makliker is om te reguleer as die vroeëre eenheidsnetwerk.[388] Hierdie fragmentasie is steeds aan die gang.[389]

Die ontwikkeling van die Internet in Suid-Afrika is bespreek.[390] Daar is aangetoon hoe verskeie persone in die land en ook in die buiteland saamgewerk het om die Internet in Suid-Afrika 'n werklikheid te maak ten spyte van moeilike omstandighede wat die land ondervind het.[391] Op 12 November 1991 word Suid-Afrika formeel aan die groter Internet gekoppel.[392]

***

Die ontwikkeling van die Internet — globaal, en in Suid-Afrika — is in hierdie hoofstuk hanteer. Aanvanklik was die groot werk om die fisiese argitektuur van die Internet te ontwerp en dit in werking te stel. Daar was baie min behoefte aan enige vorm van regulering. Hierdie posisie het egter

382 Afd 2.3.4.
383 Afd 2.3.5.
384 Afd 2.3.5.6.
385 Afd 2.3.5.7.
386 Afd 2.3.6.
387 Afd 2.3.6.2.
388 Afd 2.3.6.2.
389 Afd 2.3.6.3.
390 Afd 2.4.
391 Afd 2.4.
392 Afd 2.4.7.

drasties in die daaropvolgende dekade verander, en dit is juis die geskiedenis van Internet*regulering* waaraan vervolgens aandag geskenk sal word.

Hoofstuk 3

Geskiedkundige Oorsig oor die Regulering van die Internet

> *The Internet is the post office, the newspaper, the broadcast media, the telecommunication media, the retail shopping mall, the neighbourhood pub all in one. It raises issues of privacy, free expression, content regulation, commerce and consumer protection, crime, national security and more. Bringing together a critical mass of actors into any kind of collective action is hard enough, but pulling them into binding or influential institutional arrangements is even harder.*[1]
>
> Milton Mueller

3.1 Inleiding

IN DIE VORIGE hoofstuk is daar aangetoon hoe die Internet ontwikkel het. Tegniese standaarde (protokolle soos die *Internet Suite*) is ontwikkel om rekenaars in staat te stel om met mekaar te kan kommunikeer. Die DNS vorm die basis hiervan en is steeds vandag die ruggraat van die Internet.[2]

---

1 Mueller M L en Wagner B "Finding a Formula in Brazil: Representation and Legitimacy in Internet Governance" 2014 *Internet Policy Observatory* 8 12.

2 Afd 2.3.4.

Die tegniese ontwikkeling van standaarde was as't ware die eerste vorm van regulering van die Internet. Vir die netwerk om enigsins te kan funksioneer, was dit nodig dat ooreengekome standaarde sou geld.[3] Hierdie ontwikkeling was relatief pynloos, aangesien dit bloot die ontwikkeling van die argitektuur van die Internet geverg het. Rekenaarwetenskaplikes wat betrokke was met die ontwikkeling van die Internet, het in verskillende *fora*, soos die Internet Engineering Task Force (IETF)[4] besluite geneem oor hoe die Internet sou funksioneer.[5] 'n Voorbeeld hiervan is die inwerkingstelling van IPv6.[6]

Tegniese regulering was in 'n sekere sin die makliker vorm van regulering. Rekenaarprogrammeerders het gedoen wat nodig was om die netwerk korrek te laat funksioneer.[7] Omdat IT-personeel[8] die primêre gebruikers van die Internet was, was sosiale regulering onnodig. Soos wat die Internet meer gewild geword het en meer mense van uiteenlopende agtergronde die Internet begin gebruik het, het dit duidelik geword dat tegniese regulering alléén nié meer voldoende sou wees nie, maar dat een of ander vorm van sosiale regulering nodig geword het.[9]

3.2 Begripverheldering

In hierdie studie word 'n verskeidenheid benamings gebruik om die regulering van die Internet te bespreek. Eerstens word daar die term

3 Afd 2.3.3.

4 Afd 5.4.3.

5 MacLean D F (red) *Internet Governance: A Grand Collaboration* (2004) 196.

6 Hagen S *IPv6 Essentials* (2014) 1 verduidelik dit inleidend so: "IPv6 is a protocol designed to handle the growth rate of the Internet and to cope with the demanding requirements on services, mobility, and end-to-end security".

7 MacLean *Internet Governance: A Grand Collaboration* 196.

8 Die term IT-personeel ondervang enigeen wat Inligtingstegnologie as 'n loopbaan beoefen.

9 Van Hoose D *ECommerce Economics* (2011) 284 meld: "During the first few years of its existence, the Internet was relatively unregulated territory. This is no longer the case. ... [T]he Federal Communications Commission (FCC), which has long regulated the telecommunications firms through which packets of data traverse the Internet, is seeking to regulate the structure of the Internet itself".

"regsbeheer" gebruik. Dit word byvoorbeeld in die titel van hierdie studie gebruik met die doel om 'n wye term vir regulering te verteenwoordig. In Engels word verskeie terme soos "regulation", "governance" en selfs "control" gebruik, en elkeen hiervan het 'n meer gespesialiseerde betekenis as "regsbeheer". Die term "regsbeheer" in die konteks van die huidige studie vervat al die ander terme. Dit verwys na die gewone konteks van reëls wat gebruik word om 'n gemeenskap te orden. Soms is hierdie reëls egter nie nét regsreëls soos dit gewoonlik as wetgewing of regspraak aangetref word nie, maar selfs ook "sagte" reëls van sosiale vernedering of verleentheid,[10] en is die reguleringsrolspelers dikwels private individue.[11]

Die tweede term wat ook mildelik in die huidige studie gebruik word, is "regulering" van die Internet. Die Verklarende Handwoordeboek van die Afrikaanse taal verduidelik regulering as die "Handeling van te reguleer; reëling, reëlmatigmaking; *Verantwoordelik wees vir die regulering van iets*", en reguleer word weergegee as "Reël, vasstel, in orde bring, reëlmatig

---

10 Segura-Serrano A "Internet Regulation and the Role of International Law" 2006 *Max Planck Yearbook of United Nations Law* 192 218–219 verduidelik 'n voorbeeld van sogenaamde "soft law". Die VSA en die Europese Unie het beide streng maatreëls wat databeskerming reguleer. Kortliks behels dit dat daar streng maatreëls geld om data buite die VSA én die Europese Unie te laat vloei. Om databeskerming tussen die twee partye moontlik te maak, het die VSA en die Europese Unie 'n bilaterale verstandhouding tussen hulle dat dataverspreiding tussen die twee partye nie in stryd sal wees met hulle datahanteringswette nie. Dit is nie 'n amptelike ooreenkoms nie, maar bloot 'n "verstandhouding". Dit kan as "soft law" beskou word, soos Segura-Serrano uiteensit:

> From an International Law perspective, the Safe Harbor agreement is clearly not an International Treaty. It has neither been signed nor ratified by the parties, and so it is not subject to the Vienna Convention on the Law of Treaties. At most, it could be maintained that it is a "Gentlemen's Agreement," or political agreement, but not even an "Executive Agreement." Some scholars consider it as an example of a new kind of international regulation. This Safe Harbor agreement would then be an example of a "soft-law", as opposed to a "hard-law" instrument, although regarding its effects it may very well achieve a *de facto* harmonization of data privacy protection. Compared to the intellectual property protection afforded by hard-law, i.e. international treaties, it is again striking that Internet regulation in this area of data privacy rights has only been achieved by a soft-law instrument.

Vir meer inligting oor die klassifikasie van "harde" teenoor "sagte" reg, sien Weber R H "Future Design of Cyberspace Law" 2012 *Journal of Politics and Law* 3. Vir 'n verduideliking van nuwe vorme van "sagte" reg, sien 4–6.

11 Marsden C T *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (2011) 44. Sien ook afd 4.2.2.4.

maak, bepaal, regulariseer".[12] Die Oxford-woordeboek verduidelik dit meer verstaanbaar: "A rule or directive made and maintained by an authority" en "The action or process of regulating or being regulated".[13] In die konteks van die reg word dit soos volg gedefinieer: "The term regulation refers to a set of binding rules issued by a private or public body".[14] Met regulering word daar dus bedoel dat 'n outoriteitsfiguur ingryp om 'n veranderde struktuur daar te stel. Die veronderstelling is dat die sisteem ná die regulering meer effektief sal wees as voordat die regulering daarvan begin het. Met regulering van die Internet word daar beoordeel hoe die Internet geherstruktureer kan word om dit meer funksioneel vir alle rolspelers te maak.

In die derde plek word die Engelse term "governance" algemeen in literatuur gebruik wanneer regulering van die Internet bespreek word. Hierdie term is ietwat moeilik om in Afrikaans te vertaal, en dit wil voorkom asof die woord "bestuur" die mees korrekte is.[15] Ongelukkig is dit steeds nie 'n goeie vertaling nie, aangesien die woord "bestuur" groter ooreenkomste met die Engelse term "management" vertoon. Dit is om hierdie rede dat "bestuur" nie algemeen in hierdie studie gebruik word nie, maar eerder die term "regulering" verkies word. Interessant genoeg vorm die basisvorm van "governance" 'n goeie beeld van wat eintlik met hierdie term bedoel word: die Latynse woord "gubernator" dui op die kaptein van 'n skip — die persoon wat algehele beheer oor die skip en sy inhoud kan uitoefen.[16]

Grewlich wys dat die term "governance" van die Internet nie noodwendig dieselfde betekenis het as hoe dit algemeen in die Engelse taal gebruik word nie:

> Governance normally presupposes that there exist entities and communities

12 Odendal F F en Gouws R H *Verklarende handwoordeboek van die Afrikaanse Taal* (2005) 923.

13 Stevenson A *Oxford Dictionary of English* (2010) 1497.

14 Mwenda K K *Legal Aspects of Financial Services Regulation and the Concept of a Unified Regulator* (2006) 5.

15 Nguyen N *Essential 120000 English-Afrikaans Words Dictionary* (2014) 1628 vertaal "governance" met "bestuur".

16 Casson L *Ships and Seamanship in the Ancient World* (2014) 318 verduidelik dit so: "once the ship was under way, the *gubernator* seems to have had fairly wide authority in all matters relating to its handling". Sien ook Weber R H *Shaping Internet Governance: Regulatory Challenges* (2010) 2.

> that have a physical or legal existence as subjects of law. The question then is to what extent the Internet community already does have an existence, as it is still coalescing. And once the coalition has finally reached a certain maturity, how could a largely decentralized entity with global presence, administered in an innovative distributed fashion, be effectively self governed?[17]

Uit die staanspoor is dit duidelik dat Grewlich se definisie gekleur word deur die bril van die Internet as 'n afsonderlike ruimte,[18] en dat selfregulering[19] die *de facto* wyse van regulering sal wees.

Daar word aan die hand gedoen dat hierdie definisie geheel en al korrek was vir die Internet van 1999, toe Grewlich hierdie stelling gemaak het. Sedert daardie tyd het die Internet grondliggend verander, en het daar ten minste twee belangrike veranderinge plaasgevind: in die eerste plek is die gemeenskappe van die Internet reeds baie goed gevestig,[20] en in die tweede plek is die Internet nie meer vandag een onverdeelbare netwerk nie.[21] Die gevolg hiervan is dat die Internet van vandag 'n groter ooreenkoms vertoon met staatsgrense as wat in 1999 die geval was.[22] Dit is nou reeds moontlik dat state meer verantwoordelikheid neem vir die bestuur van hul staat-intranette.[23] Regerings van die wêreld is vandag meer geneë om makro-regulatoriese ingrepe te lewer as wat in 1999 die geval was.[24] Dus wil dit voorkom asof die term "governance" in vandag se Internet baie meer ooreenkomste vertoon met die algemene gebruik daarvan in die algemene Engelse spreektaal.

Weber gee die volgende (meer moderne) definisie van wat "Internet

17 Grewlich K W *Governance in "Cyberspace": Access and Public Interest in Global Communications* (1999) 53.

18 Sien afd 4.2.2.1 vir 'n volledige verduideliking van hierdie konsep.

19 Sien afd 4.2.2.2 vir 'n volledige verduideliking van hierdie vorm van regulering.

20 Afd 4.2.2.3 bespreek hierdie verskynsel in meer besonderhede.

21 Afd 2.3.6.

22 Hfst 6 en 7 hanteer hierdie aangeleentheid in meer besonderhede.

23 Afd 7.3. Let daarop dat die benaming "staat-intranet" in hierdie studie dui op die netwerk van die land, of staat, wat vir gebruik deur al sy inwoners beskikbaar is, en *nie* die konsep van 'n netwerk wat slegs vir die regering of staats-instansie beskikbaar is nie. "Staat-intranet" word dus volgens die Internasionale reg se konsep van 'n staat beoordeel as die oorkoepelende netwerk wat in 'n betrokke staat of land ontwikkel word om almal te dien.

24 Afd 7.3.

Governance" behels:

> (T)he discussion on the appropriate allocation of duties and responsibilities as well as the proper structuring of the concerned "organs", thereby balancing performance-based strategic management and financial/economic control.[25]

Die belangrike aspek van hierdie definisie is dat elke rolspeler sy funksie het om te verrig, en dat die korrekte balans tussen (oorwegend) die staat as hoofreguleerder en private entiteite (as finansiële reguleerders) gevind behoort te word.[26]

Die definisie van "Internet governance" wat deur die *Working Group on Internet Governance* (WGIG) voorgehou word, is soos volg:

> Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.[27]

Hiervolgens blyk dit duidelik dat die reguleringsrolspelers by Internetregulering multidimensioneel is, waar regerings, die privaat sektor en selfs die burgerlike samelewing 'n rol het om te speel (hierdie rolspelers sal later in hoofstukke 5 en 6 bespreek word). Reguleringsrolspelers is oor die algemeen almal dit eens dat hierdie multidimensionele metode van regulering die korrekte een is, maar ongelukkig is daar geen eenstemmigheid oor watter rol elke groep behoort te vertolk nie.[28] Die verskil in opinie hieroor is so sterk dat reguleringsrolspelers huidig in twee opponerende groepe verdeel is.[29] Die ongelukkige gevolg hiervan is dat Internetregulering 'n politieke speelbal en magstryd geword het.[30]

---

25 Weber *Shaping Internet Governance* 2.

26 Weber *Shaping Internet Governance* 5.

27 Desai N "Report of the Working Group on Internet Governance" http://www.wgig.org/docs/WGIG-REPORT.pdf (besoek op 2 Januarie 2014) par. 10.

28 Dieselfde dokument van die WGIG wat hierdie definisie voorhou, het ook elke rolspeler se funksie uiteengesit. Sien afd 4.2.4.3, veral vn 258, vn 259 en vn 260 vir 'n beskrywing hiervan. Dit wil voorkom asof hierdie onderskeid geheel en al van die tafel gevee is in verskeie multilaterale konferensies in die laaste dekade. Sien hfst 5 en 7.

29 Afd 4.2.4.

30 Afd 4.2.4.

Die *crux* van die saak bly egter dat Internetregulering op makro vlak nie deur individuele state op 'n lukraak-wyse geïmplementeer kan word nie. Dit is iets wat op globale vlak hanteer moet word, en deur dit te doen is verskeie rolspelers nodig.

Die verskillende begrippe is verduidelik. Daar sal nou in die oorblywende deel van hierdie hoofstuk aangetoon word hoe regsbeheer van die Internet sedert die middel negentigerjare ontvou het. Die aanvanklike gedagte van Internetregulering was dat geen regulering nodig is nie, want die netwerk was aanvanklik klein, en slegs die mense wat die Internet ontwikkel het, het dit gebruik.[31] Dit het alles verander toe algemene (nie-tegniese) gebruikers die meerderheid op die Internet begin vorm het.

In hierdie tyd het die sogenaamde LambdaMOO-insident plaasgevind, en gebruikers het besef dat een of ander vorm van regulering van die Internet nodig sou wees.[32] Ten spyte daarvan dat — in die breë beskou — dit uiteindelik nie 'n belangrike reguleringskwessie was nie, is dit wél die eerste opgetekende geval waar regulering nodig geword het, en om hierdie rede word dit in meer besonderhede hieronder bespreek.[33]

3.3 Die Oorsprong van Selfregulering

3.3.1 Die LambdaMOO-insident

Teks-avontuurspeletjies[34] was die eerste speletjies wat op vroeë rekenaars beskikbaar was.[35] Dit was bloot 'n teksbeskrywing op 'n rekenaarskerm wat aangedui het waar die speler homself bevind.[36] Deur sekere eenvoudige

31 Afd 2.3.2.4.

32 Afd 3.3.1.

33 Afd 3.3.1.

34 "Text adventure games" in Engels.

35 Wolf M J P (red) *Encyclopedia of Video Games: The Culture, Technology, and Art of Gaming* (2012) 12.

36 Wolf *Encyclopedia of Video Games* 12 verduidelik dat 'n rekenaarprogrammeerder genaamd Willie Crowther sy liefde vir grot-verkenning en kartering gekombineer het om die eerste teks-avontuurspeletjie getiteld "Colossal Cave Adventure" in 1975 te skep.

bevele op die rekenaar in te tik, kon die speler van een plek na die ander, of van kamer tot kamer beweeg.[37] Dit is belangrik om daarop te let dat hierdie voorstelling alles teksbeskrywings was, en dat daar geen grafiese voorstellings vertoon was nie. Elke gebruiker het dus sy eie voorstelling van die beskrywing in sy eie verbeelding ontwikkel.

In die vroeë tagtigerjare het dit moontlik geword om hierdie teks-speletjies op rekenaarnetwerke te speel en sodoende ook met ander spelers in verbinding te tree om 'n meer interaktiewe ervaring daar te stel.[38] Hierdie ontwikkeling het bekend gestaan as die "Multi-user dungeon", of MUD.[39]

In die laat tagtigerjare is MUD-sagteware so aangepas dat voorwerpe op die speletjie-platform geskep kon word[40] en dat gebruikers van die stelsel interaktief daardie voorwerpe kon manipuleer.[41] Hierdie nuwe eienskap het tot 'n naamverandering van die platform aanleiding gegee, en is dit bloot 'n MOO — "Multi-user dungeon: Object Oriented" — genoem.[42] Een van hierdie aanlyn-virtuele gebiede was die LambdaMOO.[43]

Dus, die gevolg van hierdie aanpassing was dat wanneer 'n persoon 'n betrokke kamer besoek, hy nie net die teksbeskrywing van die kamer op sy rekenaarskerm sou sien nie, maar ook bykomende inligting van voorwerpe in die omgewing. Wanneer voorwerpe van een kamer na 'n ander geskuif word, sou dit in die nuwe kamer beskryf word.[44]

'n Verdere ontwikkeling van LambdaMOO was dat gebruikers op sosiale vlak met mekaar kon skakel — amper soos om saam in 'n sitkamer te sit en

---

37 Wolf *Encyclopedia of Video Games* 13 verduidelik dit soos volg: "The all-text game consisted of descriptions of a series of connected rooms through which a player moved by typing responses such as "n" for "north" or "d" for "down." The player also needed several objects, like keys or a lamp, during the game. Such games came to be known as text adventures."

38 Mason R *Globalising Education: Trends and Applications* (2005) 21.

39 Sloane S *Digital Fictions: Storytelling in a Material World* (2000) 168.

40 Soos 'n virtuele tafel of stoel.

41 Mason *Globalising Education* 21.

42 Ivory J D *Virtual Lives: A Reference Handbook* (2012) 129.

43 Ivory *Virtual Lives* 129.

44 Ivory *Virtual Lives* 129.

te gesels.[45]

In Maart 1993[46] is die gebruikers van LambdaMOO getraumatiseer toe een van LambdaMOO se gebruikers, 'n ene Mr Bungle, 'n voodoo-poppie-voorwerp geprogrammeer het wat ander gebruikers se *avatars* (gebruikersidentiteite) kon manipuleer sonder hulle insette of toestemming.[47] Met behulp van hierdie virtuele voodoo-poppie-voorwerp het hy seksuele gruweldade teen twee vroulike LambdaMOO gebruikers gepleeg.[48] Dit het alles gebeur in die gewildste kamer in LambdaMOO tot aanskoue van ander gebruikers wat op daardie stadium in die kamer was.[49]

Dit is belangrik om weer eens daarop te wys dat hierdie insident afgespeel het in die vorm van teks op 'n rekenaarskerm, aangesien grafiese voorstellings op daardie stadium nog nie moontlik was nie.[50]

Die insident het dadelik hewige kritiek ontlok.[51] Mr Bungle se twee slagoffers het dadelik gereageer met afgryse en woede dat hul "verkrag" is, en geëis dat Mr Bungle van die stelsel verwyder moet word.[52]

Om dit te doen sou die reëls van LamdaMOO gevolg moet word, en dit het behels dat die hele gemeenskap oor die lot van Mr Bungle sou moes besluit.[53] Die beleidsdokument wat LambdaMOO gereguleer het, het bloot algemene verklarings van gepaste gedrag bevat, en nie spesifiek aangetoon watter proses gevolg sou moes word in die geval van wangedrag nie.[54]

Die sosiale kamer in LambdaMOO het die vergaderplek geword om oor die lot van Mr Bungle te besluit.[55] Die doel was om die nodige

45 Ivory *Virtual Lives* 129.

46 Dibbell J "A Rape in Cyberspace or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database Into a Society" 1994 *Annual Survey of American Law* 471 471.

47 Dibbell 1994 *Annual Survey of American Law* 471.

48 Dibbell 1994 *Annual Survey of American Law* 471.

49 Dibbell 1994 *Annual Survey of American Law* 471.

50 Dibbell 1994 *Annual Survey of American Law* 471.

51 Dibbell 1994 *Annual Survey of American Law* 471.

52 Dibbell 1994 *Annual Survey of American Law* 479.

53 Dibbell 1994 *Annual Survey of American Law* 479.

54 Dibbell 1994 *Annual Survey of American Law* 485.

55 Dibbell 1994 *Annual Survey of American Law* 475.

ooreenstemming te kry om die oortreder van die stelsel te verwyder — in effek 'n virtuele doodsvonnis.[56]

Dibbel — 'n prominente gebruiker van LambdaMOO — beskryf die gebeure van die vergadering in ryke besonderhede.[57] Enersyds was daar gebruikers wat aangevoer het dat die verwydering van Mr Bungle se rekening ongegrond is, aangesien hy geen amptelike reël van LamdaMOO verontagsaam het nie.[58] Daar is bygevoeg dat sulke reëls en meganismes spoedig ontwikkel behoort te word, asook dat beamptes aangestel moet word om sulke administratiewe take te verrig.[59]

Andersyds was daar gebruikers wat van mening was dat gedrag soos dié van Mr Bungle onmiddellike verwydering van die stelsel noodsaak.[60]

'n Derde groep — wat Dibble die "technolibertarians" noem — het aangevoer dat die aanwesigheid van "ongewenste elemente" op die MOO onvermydelik is, en dat dit hanteer moet word deur die ontwikkeling van nuwe tegnologiese meganismes — soos om in hierdie geval 'n rekenaarinstruksie wat reeds in die MOO bestaan het te gebruik om te voorkom dat enige kommentaar van 'n spesifieke gebruiker op die rekenaarskerm verskyn (in wese 'n tegnologiese manier om 'n spesifieke gebruiker te ignoreer).[61]

Laastens het Dibble aangetoon dat daar 'n groep was wat van mening was dat regulering van die elektroniese domein geensins nodig is nie.[62]

Die vergadering is baie goed bygewoon en argumente is oor en weer gevoer. Ongelukkig het geen besluit gevolg nie. Een van die hoof-administrateurs van die MOO het aangedui dat hy Mr Bungle se optrede in 'n baie ernstige lig beskou het.[63] Oomblikke nadat die vergadering tot

56 Dibbell 1994 *Annual Survey of American Law* 475.

57 Dibbell 1994 *Annual Survey of American Law* 481.

58 Dibbell 1994 *Annual Survey of American Law* 479.

59 Dibbell 1994 *Annual Survey of American Law* 479.

60 Dibbell 1994 *Annual Survey of American Law* 479.

61 Dibbell 1994 *Annual Survey of American Law* 479.

62 Dibbell 1994 *Annual Survey of American Law* 480.

63 Dibbell 1994 *Annual Survey of American Law* 484.

'n einde gekom het, is Mr Bungle se "avatar" eensydig van LambdaMOO verwyder.[64]

Die skepper van LamdaMOO het na hierdie gebeure aangekondig dat hy binne dae 'n stelsel in werking sou stel waar elke lid van LambdaMOO sake van gemeenskaplike belang kon oopstel in 'n referendum, en waar elke lid stemgeregtig was. Dit is inderdaad gedoen, en LambdaMOO het hierna op 'n demokratiese wyse gefunksioneer.[65]

Dit is insiggewend hoe die uiteenlopende standpunte in die vergadering oor Mr Bungle se lot geweldige ooreenkomste vertoon met reguleringsaangeleenthede van die Internet wat vandag nog problematies is.[66] Die eerste groep gebruikers se standpunt was dat regulering nodig is om regsekerheid in die aanlyn-wêreld te bring. Dit kom in wese ooreen met die hoogste laag van netwerkbeheer wat reeds in hoofstuk 2 bespreek is, te wete die inhoudlaag.[67] Regulering daarvan sal dieselfde uitwerking hê as regulering in die fisiese wêreld, waar argitektuur grootliks nie onder die mens se beheer is nie.[68]

Die tweede groep se standpunt was dat Mr Bungle se rekening summier verwyder moet word. Dit het te doen met die derde laag van die netwerk, waar inhoud gestoor word.[69]

Die standpunt van die derde groep blyk die interessantste te wees. Hiervolgens word tegnologiese meganismes voorgestel is om regulering te bewerkstellig. Deur die argitektuur — die tweede laag — te manipuleer, kan regulatoriese maatreëls in plek gestel word.[70] Die netwerk kan so gemanipuleer word dat dit outomaties die bestaan van 'n sekere gebruiker uitfiltreer — asof hy nie bestaan nie. Dit sluit aan by Benkler wat meld dat 'n

64 Dibbell 1994 *Annual Survey of American Law* 485.

65 Dibbell 1994 *Annual Survey of American Law* 485.

66 Hfst 4.

67 Afd 2.3.3.

68 Afd 2.3.3.

69 Afd 2.3.3.

70 Afd 2.3.3 en afd 4.2.3.

laer vlak inset regulering op ’n hoër vlak beïnvloed.[71]

Die standpunt van die laaste groep was dat geen regulering van die aanlyn-wêreld nodig is nie. Dit was ’n baie gewilde siening van die tyd, soos wat vervolgens bespreek gaan word.

3.3.2 Visie van ’n Grenslose Wêreld

John Perry Barlow was ’n prominente Internet-figuur van die vroeë negentigerjare.[72] Hy was ’n groot voorstander van die Internet as ’n nuwe grensgebied *(frontier)*, en dat hierdie nuwe kuberruimte sy eie reëls moet bevat.[73] In een artikel skryf hy:

> Imagine discovering a continent so vast that it may have no end to its dimensions. Imagine a new world with more resources than all our future greed might exhaust, more opportunities than there will ever be entrepreneurs to exploit, and a peculiar kind of real estate that expands with development.[74]

Die vroeë negentigerjare was die goue era van die gedagte van Internetself-regulering.[75] Die siening van daardie tyd was dat aangesien die Internet alle territoriale grense verontagsaam, dit onreguleerbaar is deur enige enkele soewereine staat.[76] Met so ’n argument volg dit dan dat selfregulering die enigste werkbare opsie tot regulering moet wees.

Barlow stig in Julie 1990 die *Electronic Frontier Foundation* (hierna) met die doel om die Internet as ’n internasionale gebied bekend te stel.[77] Een van die stigtingsdoelwitte van die EFF was spesifiek om die kuberruimte van soewereine state se inmenging te beskerm.[78]

---

71 Afd 2.3.3.

72 Poole W *The Internet: Biographies* (2005) 8.

73 Poole *The Internet* 8; afd 4.2.2.1.

74 Barlow J P “Electronic Frontier: Coming Into the Country” 1991 *Communications of the ACM* 19 19.

75 Sien ook afd 4.2.2.2 vir ’n volledige bespreking van dié onderwerp.

76 Sien ook afd 4.2.2.2 vir ’n volledige bespreking van dié onderwerp.

77 Jones S (red) *Encyclopedia of New Media: An Essential Reference to Communication and Technology* (2002) 269–270.

78 Jones *Encyclopedia of New Media* 270.

Die EFF was dadelik baie gewild. Verskeie groot maatskappye, soos *Microsoft* en *Hewlett Packard* het die stigting ondersteun.[79]

Die eerste poging deur soewereine state om aangeleenthede op die Internet te reguleer, het vanaf die Amerikaanse regering in die vorm van die Communications Decency Act van 1996[80] gekom. Hierdie wetgewing is deur die EFF beskou as 'n oorlogsverklaring op die soewereiniteit van die Internet, aangesien dit 'n klousule bevat het wat alle "onsedelike" seksuele kommunikasie of beelde wat deur minderjariges beskou kan word, op die Internet verbied het.[81] Aangesien daar op hierdie stadium nog geen metode of tegnologie beskikbaar was om tussen minderjariges en volwassenes op die Internet te onderskei nie, het dit prakties behels dat alle kommunikasie of beelde wat vir minderjariges verbode was, eweneens vir elke Internetgebruiker verbode sou wees.[82]

Barlow het dadelik 'n teenaanval geloods. Hy skryf op hierdie stadium die bekende *Declaration of Cyberspace Independence* waarin hy 'n ernstige waarskuwing aan regerings van die dag rig:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.[83]

Die EFF het ook 'n baie kragtige wapen in hul arsenaal gehad, naamlik die eerste wysiging van die Amerikaanse grondwet.[84] Hierdie byvoeging verbied

---

79 Jones *Encyclopedia of New Media* 270.

80 Communications Decency Act of 1996 (C D A) Pub L No 104–104 (Tit V) 110 Stat 133 (Feb 8 1996) gekodifiseer by 47 USC §§223 230.

81 Katz L S *Publishing and the Law: Current Legal Issues* (2013) 131.

82 Moorefield T "Communications Decency Act of 1996" 1997 *Boston University Journal of Science and Technology Law* 281 284 verduidelik: "The district court was not so optimistic about age or credit card verification procedures designed to limit access by children. The court found no 'effective way' to determine a user's age. Furthermore, current technology does not allow the use of a credit card for age verification".

83 Barlow J P "A Declaration of the Independence of Cyberspace" https://projects.eff.org/~barlow/Declaration-Final.html (besoek op 4 Maart 2014).

84 Vir meer inligting oor die geskiedenis van die eerste wysiging op die Amerikaanse grondwet, sien Rabban D M in Simmons R C (red) *The United States Constitution: The First 200 Years* (1989) 36.

die Amerikaanse regering om vryheid van spraak te reguleer. Goldsmith verduidelik dit so:

> The First Amendment to the US Constitution limits the government's ability to regulate speech, and on a communications network like the Internet, everything is potentially "speech." A website, e-mail, and even a MUD are all arguably expressive and thus potentially protected by the First Amendment.[85]

Dus, volgens die EFF het die Amerikaanse regering nie die reg gehad om kommunikasie op die Internet te reguleer met die inwerkingtreding van die Communications Decency Act nie.

Die gevolg hiervan was dat die EFF, in samewerking met die "American Civil Liberties Union", die geldigheid van die hierdie wet betwis het. Die saak wat hieruit voortgespruit het, *American Civil Liberties Union v Reno*,[86] is na die Amerikaanse hooggeregshof verwys.[87] In sy werk getiteld "Defending Free Speech in the Digital Age" som Godwin die belangrikheid van die saak korrek op: "Suddenly, the very legal status of Cyberspace itself was put to the test in a genuine constitutional battle". [88]

Die hooggeregshofregters het met 'n sewe tot twee meerderheid ten gunste van die eisers beslis.[89] Die Communications Decency Act is ongrondwetlik verklaar.[90] Dit was 'n groot oorwinning vir die EFF, maar die uitspraak het verder opgemerk dat die Internet "constitute[s] a unique medium — known to its users as 'cyberspace' — located in no particular geographical location but available to anyone, anywhere in the world".[91] Selfs die regters het dus aanvaar dat die Internet "anders" is, en anders hanteer behoort te word.

---

85 Goldsmith J en Wu T *Who Controls the Internet? lllusions of a Borderless World* (2006) 19.

86 *American Civil Liberties Union v Reno* 929 F Supp 824 (ED Pa 1996).

87 *Reno v American Civil Liberties Union* 521 US 844 117 S Ct 2329 138 L Ed 2d 874 (1997).

88 Godwin M *Cyber Rights: Defending Free Speech in the Digital Age* (2003) 333.

89 *Reno v American Civil Liberties Union* 521 US 844 117 S Ct 2329 138 L Ed 2d 874 (1997) 848.

90 Die hof verklaar op 854: "This would effect a complete ban even for adults of some expression, albeit 'indecent,' to which they are constitutionally entitled, and thus would be unconstitutional...". *Reno v American Civil Liberties Union* 521 US 844 117 S Ct 2329 138 L Ed 2d 874 (1997) 848.

91 *Reno v American Civil Liberties Union* 521 US 844 117 S Ct 2329 138 L Ed 2d 874 (1997) 851 asook Barlow J P "Next Economy of Ideas" 2000 *Wired* 8.

Die uitspraak is nie net beskou as 'n oorwinning vir vryheid van spraak nie, maar ook dat die eerste wysiging van die Amerikaanse grondwet enigiets wat met die Internet te doen het, sal beskerm.[92] In 'n afsonderlike uitspraak wat by die meerderheid gevoeg is, het regter Sandra Day O'Connor spesifiek gesê dat "the electronic world is fundamentally different".[93]

In sy kommentaar op die uitspraak het EFF prokureur David Sobel pront-uit verklaar dat "[The Court] clearly came down on the side of this being a new medium, that it is inappropriate to graft old broadcast laws onto the Internet".[94]

Hierdie uitspraak het aangetoon dat 'n staat nie bloot 'n wet kan maak en dit sonder meer op die Internet probeer toepas nie.

***

In hierdie afdeling is die historiese oorsprong van selfregulering op die Internet bespreek. Gedurende die laaste gedeelte van die negentigerjare het die geweldige kommersiële potensiaal van die Internet merkbaar geword, en het state begin kennis neem van hierdie nuwe medium.[95] Omdat die Internet in die VSA ontstaan het, was dit nie vreemd dat hierdie staat die eerste sou wees om met Internetregulering te worstel nie.[96] Dit het gou duidelik geword dat die DNS-funksie[97] die kritieke faktor van Internetbeheer sou vorm, en daarom het die VSA ingegryp om dit volledig onder sy beheer te neem.[98] Dit word hieronder bespreek.

---

92 Godwin *Cyber Rights* 330; Walker S *In Defense of American Liberties: A History of the ACLU* (1999) vii.

93 *Reno v American Civil Liberties Union* 521 US 844 117 S Ct 2329 138 L Ed 2d 874 (1997) 889; Wu T "Copyright's Communications Policy" 2004 *Michigan Law Review* 278 303–304.

94 Wired "CDA Struck Down" http://archive.wired.com/politics/law/news/1997/06/4732 (besoek op 4 Maart 2014).

95 Hess F M en Horn M B *Private Enterprise and Public Education* (2013) 160; Henderson H *Encyclopedia of Computer Science and Technology* (2009) 44 meld: "With its ability to display extensive information and interact with users, the World Wide Web of the mid-1990's clearly had commercial possibilities".

96 Mathiason J *Internet Governance: The New Frontier of Global Institutions* (2009) 70.

97 Afd 2.3.4

98 Goldsmith *Who Controls the Internet?* 36.

3.4 Die Oorsprong van Regeringsbeheer

3.4.1 Beheer oor die DNS

Die basis-DNS-bedieners vorm die kern van die Internet.[99] Daarsonder sal die Internet binne ure ophou funksioneer.[100]

Tydens die ontstaan van die DNS het John Postel, 'n rekenaarwetenskaplike wat by die Stanford Research Institute (SRI) gewerk het, die taak gehad om die DNS te administreer.[101] In hierdie tyd was die registrasie van domeinname gratis.[102]

In die laat tagtigerjare het die Amerikaanse departement van verdediging hul beleid verander om alle kontrakte wat vir die privaat sektor bedoel was, met 'n tenderprosedure uit te gee.[103] Toe die ooreenkoms met Stanford Research Institute in 1990 verstryk het, het die registrasie van domeinname op tender uitgegaan. 'n Groot regeringskontrakteur, Government Systems Inc het die tender gekry, en het kort voor lank die domeinregistrasiefunksie aan 'n klein en onbekende kontrakteur, Network Solutions Inc (hierna NSI) gesubkontrakteer.[104] Die gevolg hiervan was ietwat vreemd: Postel en Stanford Research Institute sou die beleidsfunksie van domeinregistrasie behou, en sou dus beheer hê oor watter nuwe topvlakdomeins geregistreer mag word, maar Network Solutions Inc het die dag-tot-dag registrasie van domeinname oorgeneem.[105]

Op die oog af het dit gelyk asof hierdie reëling tot almal se voordeel sou

99 Afd 2.3.4.

100 National Research Council *Signposts in Cyberspace: The Domain Name System and Internet Navigation* (2005) 97 stel dit so: "The root zone and the root name servers are critical to the Operation of the DNS. The effective and reliable operation of the DNS, and of the Internet, is entirely dependent on the accuracy and integrity of the root zone file (and its copies) and the security, reliability, and efficiency of the root name servers".

101 Goldsmith *Who Controls the Internet?* 34.

102 Goldsmith *Who Controls the Internet?* 34.

103 Goldsmith *Who Controls the Internet?* 35.

104 Goldsmith *Who Controls the Internet?* 35.

105 Goldsmith *Who Controls the Internet?* 38.

wees — Postel sou nie meer met die administratiewe las gelaat word om domeine te registreer nie, maar sou nog steeds hoëvlakbeheer oor die DNS behou.[106] Tog het dit beteken dat nie Postel nie, maar Network Solutions Inc die fisiese beheer oor die registrasie van domeinname sou oorneem. Wat nog meer van belang is, is dat laasgenoemde maatskappy nou ook die basisnaambediener ("root name server") sou beheer.[107] Die organisasie wat hierdie bediener beheer, het effektiewelik beheer oor die Internet.[108]

Aanvanklik was die verhouding tussen Postel en NSI gemoedelik. Toe NSI egter besluit om 'n fooi van $100 vir elke domeinnaamregistrasie te vra, het verhoudings vertroebel.[109] Dit het beteken dat NSI 'n geweldige profyt op 'n geoutomatiseerde diens gemaak het: in 1999 het hul met minimale insetkoste 'n inkomste van $200 miljoen verkry.[110]

Die gevolg hiervan was dat Postel en bykans almal wat meegewerk het om die Internet te ontwikkel, die NSI beskou het as 'n gierige monopolie, en het besluit om sake in eie hande te neem om hulle skepping (die Internet) te probeer red.[111]

Die prominentste persoon tydens hierdie fase was Vinton Cerf. Hy was — net soos Postel — van mening dat die ontwikkeling van die Internet op die verkeerde pad is, en dat dit nodig was om 'n organisasie te stig wat oorhoofse regulering van die Internet kan behartig. Hierdie gedagterigting het uitgeloop op die stigting van die *Internet Society* (hierna ISOC).[112] Dit is in 1992 gestig nadat Cerf en andere 'n dokument, getiteld *Announcing the Internet Society* bekend gestel het.[113] Die primêre doel van ISOC sou wees:

---

106 Goldsmith *Who Controls the Internet?* 38.

107 Goldsmith *Who Controls the Internet?* 38.

108 Goldsmith *Who Controls the Internet?* 38.

109 Goldsmith *Who Controls the Internet?* 35.

110 Goldsmith *Who Controls the Internet?* 35.

111 Goldsmith *Who Controls the Internet?* 35; Cranor L F *Communications Policy and Information Technology: Promises, Problems, Prospects* (2002) 8; Franda M F *Governing the Internet: The Emergence of an International Regime* (2001) 49.

112 Goldsmith *Who Controls the Internet?* 37. Sien ook afd 5.4.2.

113 Cerf V, Kahn B en Chapin L "Announcing the Internet Society 1992" http://www.Internetsociety.org/Internet/Internet-51/history-Internet/announcing-Internet-society

> [t]o facilitate and support the technical evolution of the Internet as a research and education infrastructure and to stimulate involvement of the academic, scientific, and engineering communities (among others) in the evolution of the Internet.[114]

Mueller verwys na hierdie gebeure as 'n poging om Internetregulering te self-privatiseer.[115]

Hierdie toedrag van sake het nie goed byval by die Amerikaanse regering gevind nie.[116] Die VSA departement van Energie wou weet watter gesag ISOC het om enigsins 'n reguleringsfunksie van die Internet uit te voer.[117] Cerf se antwoord hierop was dat, alhoewel die Internet ontwikkel is met hulpbronne van die Amerikaanse regering, dit in die negentigerjare ontwikkel het tot 'n internasionale verskynsel en dat regulering nie meer outoritêr deur die Amerikaanse regering uitgeoefen behoort te word nie, maar eerder op die internasionale speelveld hanteer moet word.[118]

ISOC het in 1997 'n projek geloods om Internetregulering binne hulle beheer te kry.[119] In samewerking met die *International Ad Hoc Committee* — wat primêr internasionale handelsmerkeienaars verteenwoordig — is die sogenaamde "Generic Top-Level Domain Memorandum of Understanding," of gTLD-MoU, ontwikkel.[120] Dit was 'n dokument wat ten doel gehad het om Internetregulering binne 'n internasionale organisasie genaamd die *International Council of Registrars* (hierna CORE), te plaas.[121] Laasgenoemde was 'n organisasie wat eintlik maar onder die beheer van ISOC was. Hierdie plan het ten doel gehad om die monopolie van Network Solutions te verbreek en ook om 'n groter onafhanklikheid van die Amerikaanse regering ten

(besoek op 11 September 2014).

114 Cerf V, Kahn B en Chapin L "Announcing the Internet Society 1992" http://www.Internetsociety.org/Internet/Internet-51/history-Internet/announcing-Internet-society (besoek op 11 September 2014).

115 Mueller M L *Ruling the Root: Internet Governance and the Taming of Cyberspace* (2002) 95–96.

116 Goldsmith *Who Controls the Internet?* 36.

117 Goldsmith *Who Controls the Internet?* 37.

118 Goldsmith *Who Controls the Internet?* 37.

119 Goldsmith *Who Controls the Internet?* 37.

120 Goldsmith *Who Controls the Internet?* 37.

121 Goldsmith *Who Controls the Internet?* 38.

opsigte van Internetregulering te verkry.[122] Daar is ook baie moeite gedoen om die plan 'n internasionale kleur te gee. Dit is gedoen deur 'n amptelike ondertekening van die dokument in Genéve te hou.[123]

Die Amerikaanse regering het nie hierdie toedrag van sake aanvaar nie, en het by monde van Ira Magaziner — wat die Internet se beleidmaker in die Wit Huis was — laat blyk dat hulle nie enige pogings om die beheer van die Internet te skaak, sal duld nie.[124] Dit was duidelik dat daar 'n konfrontasie sou plaasvind.

In Desember 1997 het die onvermydelike gebeur — die konfrontasie tussen Ira Magaziner, wat die Amerikaanse Regering verteenwoordig, en Jon Postel, wat ISOC se agenda nastreef, het by een van die IETF se algemene vergaderings plaasgevind.[125] In 'n privaatvergadering tussen die twee groepe het Magaziner baie duidelik laat blyk dat die Internet deur regeringsbefondsing geskep is, en dat beide die *Internet Assigned Numbers Authority* (hierna IANA),[126] waarvan Postel die hoof was, en NSI onder kontrak van die Amerikaanse regering optree. Die Amerikaanse regering bly in beheer van die Internet en sou nie hierdie bevoegdheid prysgee nie.[127]

Postel het hierdie hardhandige optrede van Magaziner nie waardeer nie, en het met die samewerking van sy kollegas by ISOC besluit om aan te toon dat die Amerikaanse regering nie praktiese beheer oor die Internet het nie. Op 28 Januarie 1998 skryf Postel 'n e-pos aan agt van die twaalf administrateurs wat die Internet se basisnaambedieners beheer, en vra dat hulle hul basisnaambedieners na sy rekenaar verwys.[128] Dit sou beteken dat Postel se rekenaar die sentrale kernbasisnaambediener word, en dat die

122 Goldsmith *Who Controls the Internet?* 38.

123 International Telecommunications Union "Press Release: 80 Organizations Sign MoU to Restructure the Internet" http://www.itu.int/newsarchive/press_releases/1997/itu-08.html (besoek op 11 September 2014).

124 Goldsmith *Who Controls the Internet?* 40.

125 Goldsmith *Who Controls the Internet?* 40.

126 Die *Internet Assigned Numbers Authority* (IANA) was 'n afdeling van die Stanford Research Institute. Bayuk J, Healey J en Rohmeyer P *Cyber Security Policy Guidebook* (2012) 94.

127 Goldsmith *Who Controls the Internet?* 40.

128 Goldsmith *Who Controls the Internet?* 43.

ander kernbasisnaambediener van NSI uitgeskakel sou word. Omdat Postel soveel gesag by hierdie administrateurs gehad het, het al agt administrateurs aan Postel se versoek gehoor gegee — en het Postel se eie rekenaar die kernbasisnaambediener van die Internet geword.[129]

Hierdie toedrag van sake het slegs 'n week geduur, maar in hierdie tyd het Postel die totale beheer oor die Internet gehad.[130] Hy het geen skade aangerig nie, maar wou bloot aan die Amerikaanse regering toon dat hy en ISOC wel die beheer gehad het om die Internet tot stilstand te bring as hul daartoe gedwing word.[131]

In 'n telefoonoproep versoek Magaziner vir Postel om te verduidelik waarmee hy besig is, en Postel antwoord dat hul bloot 'n toets doen.[132] Nadat Magaziner vir Postel dreig met regsoptrede, gee Postel gehoor en verwys die Internet weer na die rekenaars van NSI.[133]

Na hierdie verwikkelinge maak Magaziner dit baie duidelik dat enige pogings om met die DNS van die Internet te peuter as 'n misdaad beskou sal word.[134]

Etlike dae na hierdie gebeure stel die Amerikaanse regering 'n groenskrif vry waar daar uiteengesit word hoe die beheer van die DNS hanteer sal word. Daarin maak hulle dit baie duidelik dat hulle die beheer oor die DNS sal behou.[135] Enige pogings van CORE en ISOC om beheer van die DNS te neem, word deur dié optrede van die tafel gevee.[136]

Nege maande na hierdie gebeure sterf Postel skielik aan hartversa-

129 Goldsmith *Who Controls the Internet?* 43.

130 Goldsmith *Who Controls the Internet?* 43.

131 Goldsmith *Who Controls the Internet?* 45. Paul Vixie, een van die administrateurs van die agt basisnaambedieners wat aan Postel se versoek gehoor gegee het, het opgemerk dat: "watching the events of that week was like watching a sailboat stare down a battleship".

132 Goldsmith *Who Controls the Internet?* 46.

133 Goldsmith *Who Controls the Internet?* 46.

134 Mueller *Ruling the Root* 162.

135 National Telecommunications and Information Administration "Statement of Policy on the Management of Internet Names and Addresses" http://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses (besoek op 11 September 2014).

136 Goldsmith *Who Controls the Internet?* 46.

king.[137] Internetselfregulering was — net soos Postel — iets van die verlede.

3.4.2 VSA Regering Onder Druk

Noudat die VSA geheel en al beheer oor die DNS bevestig het, het 'n ander probleem dadelik ontstaan. Die Internet het 'n internasionale fenomeen geword, en state van die wêreld het begin besef dat hierdie nuwe skepping 'n strategiese rol in hulle eie ekonomiese ontwikkeling sou speel.[138] Aangesien die ideologieë van verskillende state radikaal verskil, het dit 'n probleem geskep dat die VSA in beheer van die wêreld se Internet is.[139] Die Amerikaanse regering was terdeë hiervan bewus, en daarom is daar dadelik begin om 'n sisteem te skep wat vir die VSA gunstig sou wees, maar ook 'n kleur van 'n internasionale karakter sou verleen. Mathiason verduidelik:

> Clearly unsure of its position, the United States government reverted to procedures that were used nationally when regulations were contemplated, a period of public comment. The national entity concerned with telecommunications regulation, the National Telecommunications and Information Administration (NTIA) issued a request for comments on a series of specific questions about Internet governance in general and about detailed aspects of the domain name registration question.[140]

Met inagneming van die publieke insette en kommentar wat ontvang is, is

---

137 Goldsmith *Who Controls the Internet?* 46.

138 Boucadair M *Handbook of Research on Redesigning the Future of Internet Architectures* (2015) 6 verduidelik: "The original policy document for ICANN promised to end US supervision after two years. US supervision, however, continued until 2006 under the subsequent contract. While this was not a major source of controversy within ICANN itself, it was a critical source of contention among other governments".

139 Boucadair *Handbook of Research on Redesigning the Future of Internet Architectures* 6. Die staat of organisasie wat beheer oor die Internet se DNS het, het effektiewelik beheer oor die hele Internet.Poole *The Internet* 176 meld:

> China ... has campaigned vigorously to move ICANN and the Internet to international or United Nations' control: China has, according to some press reports, attracted broad support From India, Russia, Egypt, Vietnam, Brazil, South Africa, Syria, and Saudi Arabia. Although ICANN does not govern the Internet, putting it under international control or supervision would, in the view of these nations, be a first step toward reducing U.S. dominance.

140 Mathiason *Internet Governance* 53.

daar eers 'n groenskrif en later 'n witskrif ontwikkel, en die voorstel wat die beste byval by die Amerikaanse regering gevind het was die gedagte van 'n nie-winsgewende organisasie wat die DNS sou bestuur, maar wél onder die toesig van die Verenigde State.[141] Die gevolg was die ontwikkeling van die *Internet Assigned Names and Numbers* (hierna ICANN).[142]

Alhoewel dit nie op die oog af so mag voorkom nie, was die skepping van ICANN 'n totale vreemdheid binne die sfeer van die internasionale publiekreg. Soos reeds in hoofstuk 1 uiteengesit, was die internasionale publiekreg aanvanklik 'n sisteem waar slegs state van die wêreld seggenskap gehad het.[143] Later het dit uitgebrei sodat internasionale organisasies wat deur multilaterale verdrae geskep is, ook *locus standi* in die internasionale publiekreg-arena kon hê.[144] Die skepping van ICANN het nie aan enige van hierdie vereistes voldoen nie.[145] Dit was 'n eensydige skepping van die Amerikaanse regering waar Amerika die volle seggenskap oor ICANN gehad het, alhoewel die skyn geskep is dat dit internasionaal van aard was.[146] Hierdie feit het nie ongesiens by die res van die wêreld se state verbygegaan nie,[147] en die Internasionale Telekommunikasie Unie (ITU) is ingespan om

141 Vir 'n volledige uiteensetting van die groen- en witskrif, sien Mathiason *Internet Governance* 54–58. Volledigheidshalwe kan daar genoem word dat die witskrif bepaal dat die Internet deur vier beginsels, te wete stabiliteit, kompetisie, private koördinasie en verteenwoordiging beheer moet word. Mathiason *Internet Governance* 56.

142 Mathiason *Internet Governance* 58. Sien afd 5.4.1 vir 'n volledige bespreking van ICANN.

143 Afd 1.5.

144 Afd 1.5.

145 Afd 5.2 verduidelik in besonderhede die vereistes waaraan 'n organisasie moet voldoen om amptelik deur die Verenigde Nasies as 'n internasionale organisasie beskou te word. ICANN voldoen nie aan hierdie vereistes nie.

146 Choucri N, Mistree D en Haghseta F *et al Mapping Sustainability: Knowledge e-Networking and the Value Chain* (2007) 347 verduidelik:

> ICANN is a private not-for-profit company which administers the Internet formerly managed by the US. government. It has an international board of directors which the European Commission has claimed is subject to too much US. political interference since changes cannot be made in the domain name system without approval of the US. Department of Commerce.

147 Die ITU se Plenipotentiary 98-konferensie stel dit so: "However, the US has since come up with its own proposal, which has raised concerns in both political circles and in the Internet community at large." International Telecommunications Union "Plenipotentiary 98 – A New Beginning for the ITU?" http://www.itu.int/newsarchive/press/PP98/Documents/Backgrounder1_General.html (besoek op 29 Oktober 2014).

teenvoeter vir die Amerikaanse skepping ICANN te wees.

Die ITU het geweet dat hierdie saak 'n maak-of-breek kwessie vir sy eie voortbestaan sou wees. Die 1998 gevolmagtigde vergadering[148] stel dit duidelik:

> As the world stands on the brink, not only of the next millennium but of a powerful new age of information and communications capabilities, the world's pre-eminent telecommunications organization also finds itself at a crossroads. As it prepares to convene for its fifteenth Plenipotentiary Conference in just a few weeks, the challenge facing the ITU is stark and simple: re-adapt quickly to a rapidly changing telecommunications environment, or find itself marginalized or at worst irrelevant in the future development of the world's communications networks.[149]

Die ITU het dus die erns van sy mandaat verstaan. As 'n amptelike internasionale organisasie van die Verenigde Nasies is daar by die ITU se 1998 gevolmagdigde vergadering versoek dat 'n amptelike versoek aan die uitvoerende raad van die Verenigde Nasies gerig moet word om 'n "World Summit on the Information Society" (WSIS) byeen te roep om spesifiek die groter beheer van die Internet aan te spreek.[150] Die uitvoerende raad van die Verenigde Nasies het hierdie versoek goedgekeur, en die beplanning van die wêreldberaad het begin.[151]

Mathiason verduidelik die werking van Verenigde Nasies-wêreldberade soos volg:

> The key events for intergovernmental summits are the preparatory meetings. These are intended to solve most procedural and substantive issues and, under the best of circumstances, bring an almost agreed text to the final event so that either the final document can be approved without debate or the debates can be focused on a limited number of issues on which agreement had not been reached.[152]

148 "Plenipotentiary meeting" in Engels. Sien ook International Telecommunications Union "Brief Guide to ITU Conferences, Assemblies and Events" https://www.itu.int/en/history/Documents/GuideToConferencesAssembliesEvents.pdf (besoek op 3 September 2014) vir meer inligting oor die besluitnemingsvermoëns by gevolmagtigde vergaderings.

149 International Telecommunications Union "Plenipotentiary 98 – A New Beginning for the ITU?" http://www.itu.int/newsarchive/press/PP98/Documents/Backgrounder1_General.html (besoek op 29 Oktober 2014).

150 Mathiason *Internet Governance* 98.

151 Mathiason *Internet Governance* 98.

152 Mathiason *Internet Governance* 102.

Alhoewel daar aanvanklik drie voorbereidingsvergaderings beplan was, is daar verskeie informele vergaderings gehou wat elkeen dan weer sy insette by die voorbereidingsvergaderings ingedien het. Dit het duidelik geblyk dat Internetregulering soos deur die VSA-regering en ICANN voorgehou is, nie by die res van die wêreld byval gevind het nie.[153]

Aangesien daar soveel uiteenlopende sienings van state was, het die *World Summit on the Information Society* eintlik maar net twee belangrike uitkomste gehad, naamlik 'n tweede wêreldkonferensie wat in 2005 in Tunisië gehou sou word, asook die skepping van 'n nuwe voertuig om Internetregulering te bewerkstellig.[154] Hierdie voertuig het gekom in die vorm van die "Working Group on Internet Governance" (WGIG).[155]

Aangesien dit die ITU was wat die Verenigde Nasies genader het om die WSIS byeen te roep, was dit ook die eerste organisasie wat begin het om voorbereidings maak vir die *World Summit on the Information Society II* (WSIS-II) wat in Tunisië gehou sou word. 'n Vergadering is in Februarie 2004 gehou waar 'n verskeidenheid van Internetregulerings-aspekte bespreek is.[156] Een aangeleentheid wat prominensie geniet het, was dat die Internet — ideaal gesproke — nie deur net één organisasie beheer moes word nie. Dit was 'n duidelike steek na die VSA sonder om dit by name te noem.

Sonder om in onnodige besonderhede te verval, kan genoem word dat die voorbereidingsvergaderings van die WSIS-II ietwat moeisaam was.[157] 'n Finale voorbereidingsvergadering moes inderhaas voor die aanvang van die WSIS-II gehou word om sinvolle voorstelle na die wêreldberaad te kon neem.[158] Die belangrikste uitkoms van die WSIS-II was die transformering van die WGIG (wat deur die WSIS in die lewe geroep is) na die nuwe Internet

153 Brasilië het bv by die tweede voorbereidingsvergadering genoem dat die: "Internet has evolved into a global public good and its governance should constitute a core issue of the Information Society agenda". Mathiason *Internet Governance* 104.

154 Mathiason *Internet Governance* 112.

155 Die "Working Group on Internet Governance" word uitvoerig in afdeling 5.3.2.1 bespreek.

156 Mathiason *Internet Governance* 112.

157 Mathiason *Internet Governance* 116–124.

158 Mathiason *Internet Governance* 116–124.

Governance Forum (IGF). Die IGF is vir 'n aanvanklike tydperk van vyf jaar in die lewe geroep, maar dit is uiteindelik verleng.[159]

Op die oomblik is die IGF steeds die primêre gespreksforum vir Internet-regulerings-aangeleenthede.[160]

3.4.3 Die IANA-funksie

ICANN is in 1998 geskep met die doel om die internasionale gemeenskap tevrede te stel dat die Internet deur 'n "internasionale organisasie"[161] beheer word.[162] Die aanvanklike beplanning was dat die VSA se *National Telecommunications and Information Administration* (hierna NTIA) saam met ICANN die IANA-funksie vir twee jaar sou hanteer, en dat ICANN dit daarna volledig sou oorneem.[163] Die oorskakeling het nooit plaasgevind nie.[164]

Intussen het die internasionale gemeenskap ongeduldig geraak dat die oorskakeling nie plaasvind nie, en konferensies soos die WSIS en WSIS-II is byeengeroep om dit te bespreek.[165] Hierdie aangeleentheid is ook telkemale in die IGF-vergaderings aangeroer.[166]

Op 5 Junie 2013 word die eerste van Edward Snowden se spioenasie-dokumente onthul.[167] Dit sou die begin wees van 'n kettingreaksie wat die

---

159 Afd 5.3.2 verskaf 'n volledige bespreking van die IGF.

160 Afd 5.3.2.

161 ICANN is geensins 'n internasionale organisasie volgens die vereistes van die Internasionale Reg nie. Sien afd 5.2.

162 Banerjee I *The Internet and Governance in Asia: A Critical Reader* (2007) 264.

163 Banerjee *The Internet and Governance in Asia* 264 verduidelik: "On 25 November 1998, the US Department of Commerce formally recognized ICANN as the appointed private sector governance entity. The initial expectations for ICANN was that it would operate within the parameters of a Memorandum of Understanding (MoU) between ICANN and the US Department of Commerce for a transition period of two years, after which it would assume an autonomous role in administration of these resources".

164 Banerjee *The Internet and Governance in Asia* 264.

165 Afd 3.4.2.

166 Afd 5.3.2.1.

167 The Guardian "Edward Snowden and the NSA Files — Timeline" http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline (besoek op 8 Mei 2016).

regering van die VSA sou verplig om die oordrag van die IANA-funksie te versnel. Die eerste dokument wat deur Snowden gelek word, onthul hoe die *Foreign Intelligence Surveillance Court* (hierna FISC) 'n hofbevel toegestaan het om Verizon, een van die VSA se grootste Internetdiensverskaffers, te beveel om met die Amerikaanse regering saam te werk en sodoende op miljoene VSA-inwoners te spioeneer.[168] Dit was die begin van 'n aantal onthullings wat die hele wêreld geskok het, aangesien die spioenasie nie slegs tot die VSA beperk was nie, maar oor die hele wêreld plaasgevind het — veral deur die "Five Eyes"-groep.[169] Hierdie grootskaalse spioenasie het bykans uitsluitlik op die Internet plaasgevind. Daarom was dit nie vreemd nie dat 'n groot groep rolspelers[170] op 7 Oktober 2013 die *Montevideo Statement on the Future of Internet Cooperation* uitgereik het.[171] Die kort verklaring van een bladsy maak vier belangrike stellings:

(a) Die belangrikheid van 'n "globally coherent" eenheids-Internet word bevestig, en 'n waarskuwing word gerig dat alle rolspelers daarteen moet waak om nie verdere fragmentasie van die Internet toe te laat nie. Daar word veral genoem dat die respek van die wêreld se Internetgebruikers nie ondermyn moet word deur "recent revelations

168 The Guardian "Edward Snowden and the NSA Files — Timeline" http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline (besoek op 8 Mei 2016).

169 Die "Five Eyes" het sy oorsprong in die tweede wêreldoorlog waar die VSA en Brittanje 'n geheime verdrag gesluit het om intelligensie onder mekaar uit te ruil. Hierdie verdrag het later bekend gestaan as die *UKUSA-agreement*. Dit is in 1955 uitgebrei om Australië, Kanada en Nieu-Zeeland in te sluit, en is dus vandag die grootste intelligensiesamewerkingsooreenkoms in die Engelsprekende wêreld. Dixon P *Surveillance in America: An Encyclopedia of History, Politics, and the Law* (2016) 171 meld: "Many of the documents released by Snowden showed the extent to which the Five Eyes members routinely shared sensitive, top secret surveillance intelligence with one another. Since then, officials familiar with the Five Eyes operations have come forward to defend the program's value and practices. 'The benefits of membership are immense, say intelligence experts'".

170 Die verklaring is gesamentlik uitgereik deur ICANN, die verskillende streeks-domeinregistrateurs AFRINIC, ARIN, LACNIC en APNIC, asook die *Internet Architecture Board, Internet Engineering Task Force, Internet Society* en *World Wide Web Consortium*. Internet Corporation for Assigned Names and Numbers "Montevideo Statement on the Future of Internet Cooperation" https://www.ICANN.org/news/announcement-2013-10-07-en (besoek op 8 Mei 2016).

171 Internet Corporation for Assigned Names and Numbers "Montevideo Statement on the Future of Internet Cooperation" https://www.ICANN.org/news/announcement-2013-10-07-en (besoek op 8 Mei 2016).

of pervasive monitoring and surveillance" nie.

(b) Internetreguleringsmeganismes moet bevorder word deur die multi-belangegroepreguleringsmodel.

(c) Die IANA-funksie moet so gou as moontlik na ICANN oorgedra word, en

(d) Die IPv6 protokol behoort so gou as moontlik regoor die Internet geïmplementeer te word.[172]

Die doel van die verklaring is baie duidelik: die VSA-alliansie se wye Internet-monitering word ten sterkste veroordeel. Die dag nadat die *Montevideo*-verklaring uitgereik is, vergader die hoof van ICANN met die president van Brasilië, en die NETmundial-proses word aangekondig.[173] Hiervolgens sou die "further evolution of the Internet governance ecosystem" verskerp word.[174] In wese het dit behels dat die VSA uitgevang is dat hy globale spioenasie op die Internet uitvoer, en dat hierdie staat nie alleen gelaat kan word met effektiewe beheer van die basis van die Internet, naamlik die IANA-funksie nie. Die NETmundial-konferensie is vir April 2014 beplan.[175]

Die VSA het besef wat hierdie proses sou inhou, en het op die 14de Maart 2014 'n persverklaring uitgereik waar hulle aankondig dat daar besluit is om die IANA-funksie na 'n ander groep oor te skuif.[176] Hierdie was 'n briljante skuif, aangesien die VSA met hierdie stap sy *bona fides* gewys het dat dit wel bereid is om die IANA-funksie na ICANN te skuif. Dit het

172 Internet Corporation for Assigned Names and Numbers "Montevideo Statement on the Future of Internet Cooperation" https://www.ICANN.org/news/announcement-2013-10-07-en (besoek op 8 Mei 2016).

173 Kruger L G *Internet Governance and the Domain Name System: Issues for Congress* (2014) 22.

174 Kruger *Internet Governance and the Domain Name System* 22.

175 Kruger *Internet Governance and the Domain Name System* 22.

176 National Telecommunications and Information Administration "NTIA Announces Intent to Transition Key Internet Domain Name Functions" http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions (besoek op 8 Mei 2016).

ook meegebring dat hulle die reëls vir die nuwe reguleerder kon neerlê (en het dit ook uiteengesit in die persverklaring).[177] Die verklaring is 'n maand voor die NETmundial-konferensie gemaak, wat beteken dat die multi-belangegroepreguleringsmodel voorkeur sou geniet om die IANA-funksie oorgedra te kry.

Die gevolg van hierdie verwikkelinge was dat die NETmundial-konferensie oorweldigende steun vir die multi-belangegroepreguleringsmodel voorgehou het, ten spyte daarvan dat daar state was wat die regeringebeheerde reguleringsmodel voorgehou het.[178] Die nie-bindende NETmundial-verklaring maak byvoorbeeld nie eers melding van die regeringsbeheerde reguleringsmodel nie, ten spyte daarvan dat dit by die *World Conference on International Telecommunications* van 2012 (hierna WCIT-12) oorweldigende sukses geniet het.[179]

Die persverklaring wat die oordrag van die IANA-funksie aangekondig het, het aangedui dat die NTIA slegs bereid sou wees om die IANA-funksie oor te dra indien daar aan vier vereistes (of beginsels) voldoen sou word, te wete:

(a) ondersteuning en uitbreiding van die multi-belangegroepregulerings-model;

(b) versekering van die behoud van die veiligheid, stabiliteit en behoorlike werking van die Internet se DNS;

(c) voldoening aan die behoeftes en verwagtinge van die gebruikers van die "IANA-dienste", en

(d) behoud van die openheid van die Internet.[180]

177 National Telecommunications and Information Administration "NTIA Announces Intent to Transition Key Internet Domain Name Functions" http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions (besoek op 8 Mei 2016).

178 NETmundial "NETmundial Multistakeholder Statement" http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf (besoek op 8 Mei 2016).

179 Afd 4.2.4.3.

180 National Telecommunications and Information Administration "NTIA Announces Intent to Transition

Hiermee het die regering van die VSA dit baie duidelik gemaak dat dit slegs die IANA-funksie sal oordra aan 'n groep wat die multi-belangegroepreguleringsmodel voorstaan. In wese het dit beteken dat die VSA slegs die IANA-funksie aan ICANN sou oordra, en aan geen ander groep nie (daar is geen ander multi-belangegroep wat so lank bestaan en spesifiek ontwikkel is om die IANA-funksie te vervul nie). Die VSA het ook verklaar dat die openheid van die Internet 'n voorvereiste van die oordrag is, wat beteken dat enige regeringsinmenging in ICANN nie geduld sal word nie.

Na hierdie gebeure het intense onderhandelinge gevolg: ICANN bestaan uit 'n verskeidenheid groepe, en almal moes insette lewer oor die oordragproses. Op 10 Maart 2016 het ICANN 'n lywige verslag aan die NTIA gestuur wat die volledige oorgangsplan uiteensit.[181] Daar word in die verslag aangedui in watter mate ICANN aan die vier vereistes van die NTIA voldoen.

Die NTIA het op 'n persverklaring die ontvangs van die oordragsversoek erken, en aangedui dat dit ongeveer negentig dae sal neem om die verslag te oorweeg.[182] Hierna sal 'n aanbeveling aan die Amerikaanse kongres gemaak word vir finale oorweging.[183]

Die huidige kontrak betreffende die IANA-funksie verstryk op die 30ste September 2016.[184] Daar word verwag dat 'n besluit oor die IANA-funksie teen daardie tyd beskikbaar behoort te wees.[185]

Key Internet Domain Name Functions" http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions (besoek op 8 Mei 2016).

181 Internet Corporation for Assigned Names and Numbers *IANA Stewardship Transition Proposal and Enhancing* ICANN *Accountability Recommendations* (2016). Verkrygbaar op die Internet by Internet Corporation for Assigned Names and Numbers "IANA Stewardship Transition Proposal and Enhancing ICANN Accountability Recommendations" https://www.ICANN.org/en/system/files/files/IANA-stewardship-transition-package-10mar16-en.pdf (besoek op 8 Mei 2016).

182 National Telecommunications and Information Administration "Reviewing the IANA Transition Proposal" https://www.ntia.doc.gov/blog/2016/reviewing-IANA-transition-proposal (besoek op 8 Mei 2016).

183 National Telecommunications and Information Administration "Reviewing the IANA Transition Proposal" https://www.ntia.doc.gov/blog/2016/reviewing-IANA-transition-proposal (besoek op 8 Mei 2016).

184 National Telecommunications and Information Administration "An Update on the IANA Transition" https://www.ntia.doc.gov/blog/2015/update-IANA-transition (besoek op 8 Mei 2016).

185 National Telecommunications and Information Administration "Reviewing the IANA Transition

Die vraag wat onwillekeurig na vore tree, is watter tipe bedeling ICANN aan die NTIA voorgelê het wat aan hulle vereistes sal voldoen. Die antwoord hierop is te vinde in die oordragsdokument aan die NTIA, wat beskikbaar is vir die groter publiek.[186]

ICANN doen aan die hand dat die IANA-funksie aan hulle oorgedra word, maar dat 'n nuwe filiaal binne ICANN die IANA-funksie oorneem.[187] ICANN noem dit die *Post-Transition* IANA. Die enkele belangrikste stelling in die bykans 600-bladsy pakket[188] is waarskynlik die volgende:

> The Names community proposed to ... Form a new, separate legal entity, Post-Transition IANA (PTI), as an affiliate (subsidiary) of ICANN that would become the IANA Functions Operator for names, in contract with ICANN. *The legal jurisdiction in which* ICANN *resides is to remain unchanged.*[189]

Die *crux* van ICANN se voorstel is dat die IANA-funksie aan hulle oorgedra word, maar dat die jurisdiksie van ICANN self onveranderd bly.[190] Dit beteken dat ICANN steeds 'n nie-winsgewende maatskappy sal wees wat ingelyf is volgens die wette van Kalifornië.[191] ICANN self bly onder die

Proposal" https://www.ntia.doc.gov/blog/2016/reviewing-IANA-transition-proposal (besoek op 8 Mei 2016).

186 Internet Corporation for Assigned Names and Numbers *IANA Stewardship Transition Proposal and Enhancing ICANN Accountability Recommendations* (2016). Verkrygbaar op die Internet by Internet Corporation for Assigned Names and Numbers "IANA Stewardship Transition Proposal and Enhancing ICANN Accountability Recommendations" https://www.ICANN.org/en/system/files/files/IANA-stewardship-transition-package-10mar16-en.pdf (besoek op 8 Mei 2016).

187 Internet Corporation for Assigned Names and Numbers *IANA Stewardship Transition Proposal and Enhancing ICANN Accountability Recommendations* (2016) 4. Die relevante gedeelte van die bepaling in Par X009 lees soos volg: "Accordingly, under the combined proposal, PTI [Post Transition IANA] would perform all of the IANA functions currently covered by the NTIA contract, with the necessary staffing and resources to do so".

188 Die pakket bestaan uit 'n verskeidenheid dokumente, maar word in een lêer op die Internet vrygestel. Verkrygbaar by Internet Corporation for Assigned Names and Numbers "IANA Stewardship Transition Proposal and Enhancing ICANN Accountability Recommendations" https://www.ICANN.org/en/system/files/files/IANA-stewardship-transition-package-10mar16-en.pdf (besoek op 8 Mei 2016).

189 My kursivering. Internet Corporation for Assigned Names and Numbers *IANA Stewardship Transition Proposal and Enhancing* ICANN *Accountability Recommendations* (2016) 4.

190 My kursivering. Internet Corporation for Assigned Names and Numbers *IANA Stewardship Transition Proposal and Enhancing ICANN Accountability Recommendations* 4.

191 Oestreich J E *International Organizations as Self-directed Actors: A Framework for Analysis* (2012) 250; Smith G J H *Internet Law and Regulation* (2007) 152; Schwabach A *Intellectual Property: A Reference Handbook* (2007) 106.

jurisdiksie van die VSA.[192] Die enigste verskil wat hierdie voorstel teweeg sal bring, is dat die Amerikaanse regering (deur die werking van die NTIA) nie meer beheer oor die IANA-funksie sal hê nie, maar wel 'n organisasie wat onder die jurisdiksie van die VSA-regering staan.

Hierdie subtiele maar kritieke feit het nie ongesiens verby gegaan nie. Die Russiese minister van Telekommunikasie het duidelik gestel dat "ICANN would remain a US corporation and the functions of the NTIA would just be resolved within the ICANN procedures, and be totally laid on US ground."[193] Uit 'n regsoogpunt is die minister tegnies korrek. Dit bly 'n ope vraag of die VSA nie tog sy mag eensydig sal kan uitoefen in 'n geval van 'n noodtoestand nie.[194] ICANN bly immers binne die VSA se jurisdiksie, en gevolglik kan invloed eensydig deur die VSA op dié organisasie uitgeoefen word.[195]

Dit bly 'n ope vraag of regerings van die wêreld van mening sal wees dat die nuwe IANA-sisteem 'n vrye Internet tot gevolg het. As die Russiese minister se uitlatings enigsins die state van die wêreld se opinie weerspieël, wil dit voorkom asof hierdie nuwe bedeling nie die gewenste uitwerking sal hê nie.

***

'n Oorsig oor Internetregulering in die Internasionale sfeer is tot op hede verskaf. Hierdie studie word egter ook onderneem met 'n sterk Suid-Afrikaanse inslag, en daarom word 'n geskiedkundige oorsig van Internetregulering in Suid-Afrika vervolgens bespreek. Soos hieronder sal blyk vertoon die Suid-Afrikaanse Internetreguleringsgeskiedenis merkwaardige ooreenkomste met dit wat in die Internasionale sfeer bespreek is.

---

192 Internet Corporation for Assigned Names and Numbers IANA *Stewardship Transition Proposal and Enhancing* ICANN *Accountability Recommendations* 4.

193 Intellectual Property Watch "ICANN Meeting In Marrakesh: More Hiccups On Way To IANA Transition" http://www.ip-watch.org/2016/03/08/ICANN-meeting-in-marrakesh-more-hiccups-on-way-to-IANA-transition/ (besoek op 8 Mei 2016).

194 Hfst 7.

195 Hfst 7.

3.5 Internetregulering in Suid-Afrika

In die vroeë 1990's het Suid-Afrika deur vele politieke veranderinge gegaan.[196] Dit is dus vanselfsprekend dat pogings om die Internet te reguleer, nie hoog op die politieke agenda was nie. Die ontwikkeling van die Suid-Afrikaanse Internet is in afdeling 2.4.7 bespreek waar Mike Lawrie en sy span dit reggekry het om die Suid-Afrikaanse Internet met 'n direkte lyn aan huis van Randy Bush te skakel. Mike Lawrie het die .ZA domein in November 1990 geregistreer, en was die voog daarvan.[197] Tydens registrasie het Lawrie egter gemeen dat dit nie wenslik is om die domein in eie naam te hanteer nie, maar eerder onder die toesig van 'n organisasie, naamlik die FRD (wat die amptelike bestuurders en eienaars van die Uninet netwerk was).[198] Dit is so deur die Amerikaanse Administrateurs aanvaar.[199] Lawrie het egter in 1994 as die bestuurder van Uninet begin werk, en dus die direkte taak gekry om die .ZA naam te administreer.[200]

Vanaf ongeveer 1995 het die Internet wêreldwyd begin om 'n meer kommersiële gedaanteverwisseling te ondergaan. 'n Staat se plaaslike landskodedomein (soos .ZA) het 'n kritiese hulpbron geword. Daar het stemme vanuit die Suid-Afrikaanse regering opgegaan dat die .ZA domeinnaam nie onder die beheer van 'n individu (naamlik Mike Lawrie) kon wees nie.[201] Lawrie was terdeë hiervan bewus, en het reeds so vroeg as 1998 probeer

196 Gibson J L en Gouws A *Overcoming Intolerance in South Africa: Experiments in Democratic Persuasion* (2005) 176 som dit so op: "During the 1990's, the old apartheid regime dissolved, democratic reform swept the land, the ANC consolidated its power, and the economy rode a roller coaster of change."

197 Afd 2.4.7.

198 Internet Assigned Numbers Authority "IANA Report on the Redelegation of the .za Toplevel Domain" https://www.IANA.org/reports/2005/za-report-05aug05.pdf (besoek op 9 Mei 2016).

199 Internet Assigned Numbers Authority "IANA Report on the Redelegation of the .za Toplevel Domain" https://www.IANA.org/reports/2005/za-report-05aug05.pdf (besoek op 9 Mei 2016).

200 Internet Assigned Numbers Authority "IANA Report on the Redelegation of the .za Toplevel Domain" https://www.IANA.org/reports/2005/za-report-05aug05.pdf (besoek op 9 Mei 2016).

201 Internet Assigned Numbers Authority "IANA Report on the Redelegation of the .za Toplevel Domain" https://www.IANA.org/reports/2005/za-report-05aug05.pdf (besoek op 9 Mei 2016); ITWeb "Minister, Internet Community Rift 'healed'" http://www.itweb.co.za/index.php?option=com_content&view=article&id=133786 (besoek op 9 Mei 2016).

om ’n gepaste organisasie te vind wat as voog van die .ZA domein sou kon dien.[202]

Die regering het die eerste keer hul standpunt geformaliseer toe die Suid-Afrikaanse departement van Kommunikasie op 30 Julie 1999 ’n besprekingsdokument op e-handel uitgevaardig het.[203] Daarin is daar spesifiek die vraag gevra of dit wenslik sou wees om ’n afsonderlike entiteit daar te stel om domeinname te hanteer. [204]

Hierdie siening is deur die privaat sektor geïnterpreteer as ’n poging om te oorreguleer.[205] Die gedagte het bestaan dat die Internet heeltemal goed gewerk het sonder regeringsinmenging, en die *status quo* dus maar eenvoudig gehandhaaf kon word.

Om hierdie probleem van regeringsinmenging die hoof te bied, is daar gepoog om ’n meer legitieme basis vir die regulering van die .ZA domeinnaam te vind. Mike Lawrie en Mike Silber, ’n vooraanstaande Internetregskundige, het ’n nuwe nie-winsgewende organisasie, te wete Namespace ZA gestig.[206] Die stigtingsvergadering van Namespace ZA het op 31 Augustus 2001 plaasgevind.[207] In dieselfde jaar ontvang IANA ’n formele versoek van Lawrie om die .ZA na Namespace ZA te delegeer, maar omdat daar nie wye konsensus was oor die versoek nie, word dit nie toegestaan nie.[208]

---

202 Internet Assigned Numbers Authority “IANA Report on the Redelegation of the .za TopLevel Domain” http://www.IANA.org/reports/2005/za-report-05aug05.pdf (besoek op 9 Mei 2016) 1.

203 Department of Communications “Discussion Paper on Electronic Commerce Policy” http://www.polity.org.za/polity/govdocs/discuss/ecomm.html (besoek op 11 September 2014).

204 Punt 6.3 van die besprekingsdokument het spesifiek genoem: “Should South Africa create formal governance structures such as a domain name registration authority? Who should take responsibility for these functions?” Department of Communication “Discussion Paper on Electronic Commerce Policy” http://www.polity.org.za/polity/govdocs/discuss/ecomm.html (besoek op 11 September 2014).

205 De Wet P “The Tyranny of the Majority” http://www.itweb.co.za/index.php?option=com_content&view=article&id=87538:the-tyranny-of-the-majority&catid=79:columnists (besoek op 30 Oktober 2014).

206 De Wet P “Namespace Moves Towards Controlling ZA Names” http://www.itweb.co.za/index.php?option=com_content&view=article&id=93404 (besoek op 11 September 2014).

207 De Wet P “Namespace Moves Towards Controlling ZA Names” http://www.itweb.co.za/index.php?option=com_content&view=article&id=93404 (besoek op 11 September 2014).

208 Internet Assigned Numbers Authority http://www.IANA.org/reports/2005/za-report-05aug05.pdf (besoek op 11 September 2014) 2.

Ongelukkig het die .ZA-kwessie in 'n politieke speelbal ontaard. In Junie 2002 reik die departement van Kommunikasie 'n verklaring uit wat Namespace ZA aankla van "hankering back to an era where a tiny minority controlled the wealth of the country".[209] Volgens die departement funksioneer Namespace ZA "as a forum of a few individuals who are only interested in boosting their unfettered egos at the expense of the entire country".[210] Hierdie verklaring word egter vinnig deur die departement van Kommunikasie teruggetrek.[211]

Die verhouding tussen Lawrie en die departement van Kommunikasie het in 2002 so versuur dat Lawrie openlik gedreig het om nie die .ZA domein aan die regering te delegeer nie. Hy het ook daad by die woord gevoeg deur die Internetroetelêers van .ZA na die buiteland te skuif, (sodat dit vir die Suid-Afrikaanse regering onmoontlik sou wees om die domein met geweld oor te neem).[212]

Intussen het die wetgewer die Wet op Elektroniese Kommunikasies en Transaksies 25 van 2002 uitgevaardig. Daarin bring hul met artikel 59 'n regspersoon getiteld die ".ZA Domeinnaamowerheid" tot stand. Volgens artikel 60 sou dit 'n artikel 21 nie-winsgewende organisasie wees. Op hierdie stadium het Namespace ZA en die regering egter tot 'n vergelyk gekom deurdat artikel 60(3) spesifiek bepaal dat die nuwe owerheid se lede met sy totstandkoming sal bestaan uit al die bestaande lede van Namespace ZA, asook die minister van Kommunikasie. Op 18 Mei 2007 het die .ZA Domeinnaamowerheid die werking van die .ZA domein oorgeneem.[213]

---

209 De Wet P "Govt Slammed Namespace 'By Mistake'" http://www.hellkom.co.za/newsviewer/local/1862/Govt-slammed-Namespace-by-mistake- (besoek op 11 September 2014).

210 De Wet P "Govt Slammed Namespace 'By Mistake'" http://www.hellkom.co.za/newsviewer/local/1862/Govt-slammed-Namespace-by-mistake- (besoek op 11 September 2014).

211 De Wet P "Govt Slammed Namespace 'By Mistake'" http://www.hellkom.co.za/newsviewer/local/1862/Govt-slammed-Namespace-by-mistake- (besoek op 11 September 2014) meld: "It went out by mistake; it was published by mistake."

212 October A "Internet Users Relax — .za Domain is Safe" http://www.iol.co.za/news/politics/Internet-users-relax-za-domain-is-safe-1.51648#.UIGMmFLNdNA (besoek op 11 September 2014).

213 Staatskoerant 29903 (18 Mei 2007).

3.6 Gevolgtrekking

Hierdie hoofstuk het die geskiedkundige oorsig oor die regulering van die Internet in oënskou geneem. Eerstens is die belangrike konsepte van "regsbeheer", "regulering", "governance" en "control" bespreek, en is daar uitgewys hoe hierdie konsepte in die huidige studie hanteer word. Die omvang van die verskillende konsepte is ook bespreek.[214]

Die eerste opgetekende geval waar dit geblyk het dat regulering van die vroeë Internet nodig was, is die sogenaamde LambaMOO-insident.[215] Nadat 'n gebruiker van dié netwerk-platform hom aan erge wangedrag skuldig gemaak het, moes mede-gebruikers besluit watter oplossing die gewenste uitwerking sou hê om die sosiale platform te beskerm. Verskeie moontlikhede is oorweeg.[216] Dit het gewissel van die verwydering van die gebruiker se rekening, tot tegnologiese maatreëls wat ingestel kon word om die nodige regulering te bewerkstellig.[217] Hierdie voorbeeld het aangetoon hoe ingewikkeld dit sou wees om regulering van die Internet te bewerkstellig, aangesien die regulering van een vlak daarvan, soos die fisiese argitektuur, ook ander vlakke, soos inhoud, kan beïnvloed.[218] Dit het ook aangetoon hoe netwerk-administrateurs oor die algemeen gemaklik was met die gedagte om die netwerk sélf te administreer om die werking daarvan te verseker (tegniese regulering), en dit het weer daartoe gelei dat die aanvanklike gedagte van selfregulering op sosiale vlak nie vreemd sou voorkom nie.[219]

Aangesien die vroeë Internet 'n eenheidsnetwerk gevorm het, was dit dikwels beskou as 'n afsonderlike ruimte wat nie reguleerbaar is nie.[220]

214 Afd 3.2.

215 Afd 3.3.1.

216 Afd 3.3.1.

217 Afd 3.3.1.

218 Afd 3.3.1.

219 Afd 3.3.1.

220 Afd 3.3.2.

Die *Electronic Freedom Foundation* (EFF) word gestig om juis hierdie doel te bevorder.[221] Wanneer die *Communications Decency Act* in die VSA gepromulgeer word om vryheid van spraak op die Internet te reguleer, verwys die EFF en die *American Civil Liberties Union* (ACLU) hierdie wetgewing na die Amerikaanse hooggeregshof in *Reno v American Civil Liberties Union*, waar dele daarvan ongrondwetlik verklaar word.[222] Dit word wydverspreid as 'n oorwinning vir die onreguleerbaarheid van die Internet beskou.[223] Hierna begin fragmentasie van die Internet plaasvind,[224] wat reguleringspogings makliker maak.[225]

Die Amerikaanse regering het gedurende die middel 1990's besef dat die Internet 'n belangrike bron vir ekonomiese groei sou word, en wou beheer oor die DNS neem om hierdie strategiese hulpbron te beskerm.[226] Daar is reeds op daardie stadium besef dat die werking van en beheer oor die basis-DNS-bedieners van kritieke belang is, aangesien dit die korrekte funksionering van die Internet beïnvloed.[227]

Nadat die DNS ontwikkel is, is dit vir etlike jare deur Jon Postel onderhou.[228] In 1990 het hierdie posisie verander toe die Amerikaanse regering dit op tender uitgegee het, en dit deur *Network Solutions Inc* oorgeneem is. Laasgenoemde het begin om 'n fooi vir elke domeinnaamregistrasie te hef, en het sodoende 'n geweldige profyt op 'n proses wat geoutomatiseer was, gemaak. Dit het die oorspronklike ontwerpers van die Internet gegrief.[229] Die ISOC is gevorm om hierdie probleem te probeer beredder en beheer van die Internet se DNS weer in rekenaarkundiges (en nie politici nie) se hande

221 Afd 3.3.2.
222 Afd 3.3.2.
223 Afd 3.3.2.
224 Afd 2.3.6.
225 Hfst 6 en 7.
226 Afd 3.4.1.
227 Afd 3.4.1.
228 Afd 3.4.1.
229 Afd 3.4.1.

te plaas.[230]

Hierdie toedrag van sake is nie deur die Amerikaanse regering aanvaar nie.[231] Postel en andere is ingelig dat die Internet ontwikkel is deur finansiële insette van die Amerikaanse regering, en dat hulle beheer daaroor neem.[232] In 'n uitsonderlike geval van teëkanting teen die Amerikaanse regering neem Postel eiehandig beheer oor die Internet se DNS vir 'n week.[233] Die struweling tussen Postel en regeringsamptenare word beredder, en die Amerikaanse regering neem die DNS onder hulle beheer.[234]

Amerikaanse regeringsbeheer van die basis-DNS is egter nie goed deur die internasionale gemeenskap aanvaar nie.[235] Die VSA-regering skep die *Internet Corporation for Assigned Names and Numbers* (ICANN), 'n nie-winsgewende maatskappy wat ingelyf word ingevolge die wette van die staat van Kalifornië.[236] Die doel daarmee was om die IANA-funksie aan ICANN oor te gee, en aangesien ICANN insette van 'n multi-belangegroep ontvang, sou dit kon blyk dat die IANA-funksie in die internasionale sfeer is. Hierdie konstruksie vind nie byval by meeste state van die wêreld nie.[237] In 'n poging om die IANA-funksie te internasionaliseer, word die WSIS en WSIS-II-prosesse van stapel gestuur. Ten spyte van hierdie internasionale ingrepe, bly die VSA in beheer van die IANA-funksie.[238] Die gevolg van die WSIS en WSIS-II-prosesse is dat die *Internet Governance Forum* (IGF) geskep word, wat 'n multi-belangegroepreguleringsmodel voorstaan, en tot op hede die grootste internasionale gespreksforum van Internetregulerings-aangeleenthede is.[239]

230 Afd 3.4.1.
231 Afd 3.4.1.
232 Afd 3.4.1.
233 Afd 3.4.1.
234 Afd 3.4.1.
235 Afd 3.4.2.
236 Afd 3.4.3 vn 191.
237 Afd 3.4.2.
238 Afd 3.4.2.
239 Afd 3.4.2.

In Junie 2013 onthul Edward Snowden dat die VSA 'n wye spioenasie-program op die Internet in werking het.[240] Dit word deur die wêreld ten strengste veroordeel, en planne om die IANA-funksie onder internasionale beheer te stel, word verskerp.[241] Die VSA se reaksie hierop is om aan te kondig dat die tyd ryp is om die IANA-funksie af te gee.[242] Die gevolg hiervan is dat die multi-belangegroepreguleringsmodel by die NETmundial-konferensie steun ontvang, aangesien die VSA dit as 'n voorvereiste vir 'n IANA-funksie-oordrag gestel het.[243] Verskeie groepe verbonde aan ICANN werk aan 'n aansoek om die IANA-funksie na ICANN oor te dra, en dit word op 10 Maart 2016 aan die NTIA (wat die VSA regering verteenwoordig), oorhandig.[244] Hierdie aansoek sal deur die NTIA oorweeg moet word om te bepaal of dit aan die vereistes vir oorhandiging voldoen, en 'n verslag sal aan die Amerikaanse kongres oorhandig word vir finale besluit.[245] Dit wil voorkom asof 'n finale besluit oor die IANA-funksie so gou as September 2016 kan volg.[246]

Die ontwikkeling van Internetregulering binne Suid-Afrika is ook bespreek.[247] Net soos in die VSA is die intranet van Suid-Afrika deur rekenaartegnici ontwikkel, en is die poging van regulering daarvan deur die nasionale regering as inmenging beskou.[248] Die Wet op Telekommunikasie en Transaksies 25 van 2002 is uitgevaardig, en ingevolge artikel 60 daarvan word die .ZA domein deur 'n onafhanklike organisasie, te wete die .ZA Domeinnaamowerheid, beheer.[249]

***

Uit die bespreking hierbo is dit duidelik dat state van die wêreld

240 Afd 3.4.3.
241 Afd 3.4.3.
242 Afd 3.4.3.
243 Afd 3.4.3.
244 Afd 3.4.3.
245 Afd 3.4.3.
246 Afd 3.4.3.
247 Afd 3.5.
248 Afd 3.5.
249 Afd 3.5.

aanvanklik onseker was oor hoe om regulering van die Internet — wat ’n eenheidsnetwerk was — te bewerkstellig. Beheer is op ’n lukraak-wyse geïmplementeer en suksesse en mislukkings het gevolg. Die vraag wat nou ontstaan is: watter teoretiese konsepte en modelle is al ontwikkel om regulering van die Internet op ’n meer gepaste wyse te hanteer? In die volgende hoofstuk sal dit oorweeg word.

Hoofstuk 4

Fundamentele Konsepte en Teoretiese Modelle ten opsigte van die Internet

Getting information off the Internet is like taking a drink from a fire hydrant.[1]
Mitchell Kapor

4.1 Inleiding

IN DIE BREË beskou is regulering geensins 'n nuwe konsep nie. Trouens, dit is so oud soos die mensdom self. Reeds sedert die vroegste tye het mense besef dat dit beter is om in gemeenskappe te funksioneer, aangesien daar vele voordele daarin geleë is — soos byvoorbeeld beskerming teen ander groepe wat hul eie belange voorop stel.[2] Hierdie vorm van selfregulering het later ontwikkel in meer formele vorms van regulering en dit het uiteindelik gelei tot 'n wêreld waar soewereine state die gemeenskappe binne hulle grense reguleer.[3]

1 Micheuz P *20 Years of Computers and Informatics in Austria's Secondary Academic Schools* (2005) 27.

2 Nolon J R *Well Grounded: Using Local Land Use Authority to Achieve Smart Growth* (2001) 44.

3 Johnson D M *The Historical Foundations of World Order: The Tower and the Arena* (2008) 341.

Net soos regulering in die fisiese wêreld 'n ontwikkelingsproses ondergaan het (en steeds ondergaan), het regulering van die Internet ook vanuit 'n basiese en eenvoudige konsep ontwikkel tot een wat al hoe ingewikkelder begin word het. Daar is baie raakpunte tussen regulering van die fisiese wêreld en regulering van die Internet, maar daar is ook nuwe kwessies wat nog nooit by die regulering van die fisiese wêreld ter sprake gekom het nie.

Die doel van hierdie hoofstuk is om sekere basiese beginsels wat ter sprake is by Internetregulering, uiteen te sit. Sekere teorieë en voorstelle aangaande Internetregulering sal ook onder die loep geneem word. Dit verskaf die teoretiese onderbou vir die res van die studie.

4.2 Modelle van Internetregulering

4.2.1 Inleiding

Daar kan met reg aangevoer word dat regsbeginsels menslike natuur oor die algemeen beheers, en dat dit daarom nie sinvol sou wees om "nuwe" reëls vir die kuberruim te formuleer nie.[4] Daarom bestaan daar talle voorbeelde van waar bestaande regsbeginsels gebruik word om gedrag op die Internet te reguleer.[5] Van der Merwe verduidelik byvoorbeeld hoe die misdaad van opsetlike saakbeskadiging voor die inwerkingtreding van die Wet op Elektroniese Kommunikasies en Transaksies[6] gebruik is om onwettige toegang tot rekenaarsisteme[7] te reguleer.[8] Die groot voordeel van die reg lê juis daarin dat beginsels in verskeie situasies geld en bloot op nuwe feite toegepas kan word.

---

4 Van der Merwe D P en Roos A *et al Information and Communications Technology Law* (2016) 69.

5 Van der Merwe *Information and Communications Technology Law* 74–77.

6 Wet 25 van 2002.

7 Hierdie gedrag word in die omgangstaal "hacking" genoem. Holt T J en Schell B H *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (2010) 20 definieer krakery as "an illegal act or series of illegal acts committed by non-physical means and by concealment or guile, to obtain money or property, to avoid the payment or loss of money or property, or to obtain business or personal advantage".

8 Van der Merwe *Information and Communications Technology Law* 74.

Die probleem wat die kuberruim egter skep, is dat sekere fundamentele konsepte wat in die fisiese wêreld geld, nie noodwendig in die kuberruim geld nie. Wanneer bestaande regsbeginsels dan toegepas word, gee dit dikwels aanleiding tot ongewenste resultate. Twee voorbeelde word vervolgens genoem om hierdie punt te illustreer:[9]

- In die fisiese wêreld word die verkoop van pornografie aan minderjariges verbied.[10] Die wyse waarop hierdie regsbeginsel afgedwing word, is om pornografiese materiaal in 'n gebied te plaas waar kinders nie kan kom nie, soos byvoorbeeld winkels wat spesifiek hierdie media verkoop.[11] Dit is dan moeilik vir 'n kind om fisies in kontak met pornografie te kom. Die verkoopsklerk van 'n pornografie-winkel kan dadelik 'n minderjarige identifiseer, aangesien die minderjarige nie geredelik deur sy voorkoms kan wegsteek dat hy inderdaad nog 'n kind is nie. Hy projekteer as't ware sy status as kind aan enigeen wat hom sou teëkom, en kan nie daarvan afstand doen of dit maklik verberg nie. Alhoewel dieselfde beginsel van die nie-verkoop van pornografie aan minderjariges in die kuberruim geld, kan 'n minderjarige baie makliker verberg dat hy 'n kind is. Die "status" van kind-wees word nie soos in die fisiese wêreld geprojekteer nie. Gevolglik word dit baie moeiliker om sodanige regsbeginsels af te dwing.[12]

- Gestel 'n klant se naam en identiteitsnommer word neergeskryf wanneer hy 'n selfbedieningswinkel betree. Indien 'n winkelklerk hom orals volg, en notas maak oor produkte waarin die klant belang stel, sal dit baie verdag voorkom. Meeste klante sal hierdie

9 Lessig gebruik hierdie twee voorbeelde om dieselfde punt te illustreer. Lessig L "The Law of the Horse: What Cyberlaw Might Teach" 1999 *Harvard Law Review* 501 506 asook Lessig L "The New Chicago School" 1998 *Journal of Legal Studies* 661 662.

10 In Suid-Afrika word die klassifikasie en handel van pornografiese materiaal, wat films en foto's insluit, uitvoerig deur die Wet op Films en Publikasies 65 van 1996 gereguleer. Vir 'n uitvoerige bespreking van hierdie bepalings, sien Watney M "Regulation of Internet Pornography in South Africa (1)" 2006 *Tydskrif vir die Hedendaagse Romeins Hollandse Reg* 227 232–236.

11 Art 24(1) van die Wet op Films en Publikasies 65 van 1996.

12 Watney 2006 *Tydskrif vir die Hedendaagse Romeins Hollandse Reg* 229.

> tipe gedrag as 'n skending van hulle privaatheid beskou.[13] In die kuberruim speel hierdie situasie hom bykans in elke elektroniese transaksie af — webwerwe hou rekord van watter produkte deur klante beskou word, en daar word selfs bepaal hoe lank die klant aan die betrokke produk aandag gegee het.[14] Dit word dan met die klant se volledige identiteit (wanneer 'n klant die produk koop) gestoor om pasgemaakte advertensies aan die klant in die toekoms aan te bied. In hierdie feitestel is die klant in die kuberruim salig onbewus daarvan dat hy in soveel besonderhede dopgehou word, terwyl dit in die fisiese wêreld baie maklik opgemerk sou kon word.[15]

Beide hierdie voorbeelde illustreer onderliggend dieselfde probleem. In die fisiese wêreld bestaan daar sekere basisbeginsels wat onveranderlik is, byvoorbeeld dat 'n kind nie geredelik kan voorgee dat hy 'n kind is nie. Sy liggaamsbou verraai sy status. Eweneens kan afluistering en waarneming meer geredelik in die fisiese wêreld bespeur word, terwyl dit in die kuberruim bykans onsigbaar is. Die onderliggende probleem lê in die fundamenteel verskillende *argitektuur* wat die fisiese wêreld en die kuberruim het. Eersgenoemde bestaan uit die fisiese wêreld en -natuur, terwyl laasgenoemde uit binêre kode in 'n globale rekenaarnetwerk bestaan. Eersgenoemde kan nie geredelik verander word nie ('n kind kan nie sy kindskap verberg nie), terwyl laasgenoemde geheel en al binne die sfeer van

---

13 Stevens G *Privacy Protections for Personal Information Online* (2011) 10 vn 61 verduidelik dat 'n effektiewe stelsel van "Do Not Track" kan 'n moontlike antwoord op hierdie probleem wees: "[A] robust, effective Do Not Track system would ensure that consumers can opt out once, rather than having to exercise choices on a company-by-company or transaction-by-transaction basis".

14 Qin Z *Introduction to E-commerce* (2010) 193; Wacks R *Privacy: A Very Short Introduction* (2015) 16 noem bv dat: "These companies track one's every keystroke…".

15 Qin *Introduction to E-commerce* 193–194 verduidelik bv dat inligting oor klante in die kuberruim nie slegs ingewin word vir eie gebruik nie, maar selfs verkoop word aan derde partye. Daarom is die fokus van verbruikers-privaatheid verbreed om drie aangeleenthede in te sluit, naamlik (a) persoonlike inligtingsbeskerming (waar die fokus val op die beskerming van persone se persoonlike inligting, soos identiteitsnommers, adresse, ens.), (b) kommunikasie-beskerming (waar die klem lê op die privaatheid van 'n verbruiker se kommunikasies, bv e-pos-korrespondensie asook die persoon se e-posadres, ens.), en (c) persoonlike-lewe-beskerming (waar die fokus geplaas word op beskerming teen ongevraagde e-pos "spam").

die mens se beheer staan.[16]

Sedert die ontstaan van die Internet is daar al gepoog om antwoorde op hierdie tipe vrae te verkry. Akademiese literatuur het ook gepoog om antwoorde te verskaf en modelle neer te lê om moontlike Internetregulering-sisteme daar te stel.[17] Dit word vervolgens bespreek.

4.2.2 Akademiese Literatuur van die Negentigerjare

Tussen ongeveer 1994 en 1999 is die Internet aan die groter mensdom bekend gestel.[18] Dit is dan ook tydens hierdie tyd dat regsgeleerdes begin het om te besin oor hoe die nuwe medium, wat op daardie stadium nog die hele wêreld oorspan het om 'n grenslose netwerk te vorm, beheer moet word. Die negentigerjare het tot interessante teorieë oor Internetregulering gelei,[19] en daar was in hooftrekke twee groot kampe: die eerste was persone soos Menthe, Johnson en Post wat aangevoer het dat die Internet 'n afsonderlike internasionale ruimte was, en dan was daar persone soos Jack Goldsmith wat aangetoon het dat die Internet nie so ver buite die beheer van die staat was nie.[20] Aangesien hierdie teorieë vandag slegs historiese waarde het, sal dit bloot vlugtig hieronder bespreek word.

---

16 Lessig 1999 *Harvard Law Review* 505.

17 Sien bv afd 3.3.1 vir die illustrasie van die LambdaMOO-geval waar daar gepoog is om selfregulering daar te stel nadat ongewenste gedrag plaasgevind het.

18 Afd 2.3.5.4.

19 Alhoewel dit nie wye ondersteuning geniet het nie, was daar selfs akademici wat gemeen het dat die Internet as 'n onafhanklike staat beskou moet word. Flaming H "The Rules of Cyberspace: Informal Law in a New Jurisdiction" 1997 *Illinois Bar Journal* 174 174; Gong J *et al* "Defining and Addressing Virtual Property in International Treaties" 2011 *Boston University Journal of Science and Technology Law* 101 136.

20 Menthe D C "Jurisdiction in Cyberspace: A Theory of International Spaces" 1998 *Michigan Telecommunications Technology Law Review* 69 69; Johnson D R en Post D G "Law and Borders — The Rise of Law in Cyberspace" 1996 *Stanford Law Review* 1367 1367 en Goldsmith J L "Against Cyberanargy" 1998 *University of Chicago Law Review* 1199 1199.

4.2.2.1 Die Internet as 'n Afsonderlike Internasionale Ruimte

Aangesien die Internet in die negentigerjare van die vorige eeu 'n grenslose, internasionale netwerk gevorm het,[21] was dit normaal dat raakpunte met bekende sisteme gesoek sou word om regulering daarvan moontlik te maak. Drie sisteme wat in die internasionale reg bekend was, het ooreenkomste met die kuberruim vertoon, naamlik Antarktika, die oop see en die lugruim.[22] Al drie hierdie sisteme behoort aan niemand spesifiek nie, en internasionale verdrae is geskep om dit as *res communes* te beskerm — dit is die gemeenskaplike erfenis van die hele wêreld.[23] Menthe verduidelik:

> As a fourth international space, cyberspace should be governed by default rules that resemble the rules governing the other three international spaces, even in the absence of a regime-specific organizing treaty, which the other three international spaces have.[24]

Menthe verduidelik hoe al drie hierdie sisteme dieselfde beginsels het wat hulle onderlê: wanneer 'n staat 'n skip na Antarktika stuur en dit op die oop see vaar, of 'n vliegtuig of ruimteskip in die lugruim of ruimte in stuur, sal dit altyd geïdentifiseer kan word aan die hand van die staat se nasionaliteit. Hy meld: "nationality, not territoriality, is the basis for the jurisdiction to prescribe in outer space, Antarctica, and the high seas".[25]

---

21 In die geheel beskou is hierdie stelling waar — die Internet wás in die vorige eeu 'n eenheidsnetwerk. Tog was daar uitsonderings deurdat persone hulle in groepe met gemeenskaplike belange verdeel het, en dit tot geografiese onderskeid gelei het. 'n Goeie voorbeeld hiervan is 'n webwerf wat die ideologie van 'n bepaalde politieke party bevorder. Sulke persone sal gewoonlik van dieselfde geografiese gebied wees, en daarom was territorialiteit wat gevestig was op groepsbelange, 'n werklikheid in die ou eenheids-Internet. Zook M "The Geographies of the Internet" 2006 *Annual Review of Information Science and Technology* 53 57.

22 Balleste R *Internet Governance: Origins, Current Issues and Future Possibilities* (2015) 140; Svantesson J B "Borders on, or Border Around — the Future of the Internet" 2006 *Albany Law Journal of Science and Technology* 343 366; 70; Menthe 1998 *Michigan Telecommunications Technology Law Review* 70.

23 Antarktika word gereguleer deur die Antarctic Treaty 12 UST 794 / 402 UNTS 71 / 19 ILM 860 (1980) / UKTS 97 (1961), Cmnd 1535 / ATS 12 (1961), die oop see deur die United Nations Convention on the Law of the Sea 1833 UNTS 3 / [1994] ATS 31 / 21 ILM 1261 (1982) en die lugruim deur die Convention on International Civil Aviation 15 UNTS 295, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies 610 UNTS 205 / 6 ILM 386 (1967) / [1967] ATS 24 en Convention on the Registration of Objects Launched into Outer Space 1023 UNTS 15.

24 Menthe 1998 *Michigan Telecommunications Technology Law Review* 85.

25 Menthe 1998 *Michigan Telecommunications Technology Law Review* 83.

Hiermee saam voer Menthe aan dat daar in beginsel slegs twee basishandelinge is wat op die Internet kan plaasvind, en dit is die oplaai van inligting ("uploading"), en die aflaai daarvan ("downloading"). *Alle* ander handelinge is bloot 'n kombinasie van hierdie basishandelinge.[26]

Dus, as hierdie beginsels in die kuberruim toegepas word, beteken dit eenvoudig dat alle op- en aflaai van inligting met die nasionaliteit van die gebruiker gestempel word: "In cyberspace, persons bring nationality into the international space of cyberspace through their actions".[27] Dit beteken dan ook dat strydigheid van regsbeginsels relatief maklik opgelos kan word, want daar kan slegs twee state wees wat jurisdiksie kan uitoefen — óf die staat van die persoon wat die inligting oplaai, óf die staat van die persoon wat dit aflaai.[28] Hierdie sisteem omvorm die kuberruim tot 'n ruimte wat maklik reguleerbaar is:

> The theory of international spaces turns cyberspace from a place of infinitely competing jurisdictions into a place where normal jurisdictional analysis can continue.[29]

Die gevolg van hierdie teorie is dat die Internet as 'n afsonderlike internasionale ruimte beskou kan word waar die nasionaliteit van die gebruiker in op- en aflaaihandelinge verdeel word wat met die nasionaliteit van die gebruiker gestempel word. Regspleging op die Internet word bloot 'n geval van feitebevindings ten opsigte van die gebruiker se nasionaliteit, en die relevante regsbeginsels van die staat word dan toegepas. [30]

Svantesson is nie beïndruk met hierdie model nie.[31] Hy noem dat Menthe nie rekening hou met die feit dat die Internet nie 'n fisiese bestaan

---

26 Hierdie teorie word volledig uiteengesit in Menthe 1998 *Michigan Telecommunications Technology Law Review* 73-75.

27 Menthe 1998 *Michigan Telecommunications Technology Law Review* 93. Hy meld ook op 93: "An uploader marks a file or a webpage with his nationality. We may not know 'where' a webpage is, but we know who is responsible for it".

28 Menthe 1998 *Michigan Telecommunications Technology Law Review* 94.

29 Menthe 1998 *Michigan Telecommunications Technology Law Review* 94.

30 "The question then becomes a highly factual inquiry, requiring the court to determine the extent to which the person maintaining the ... site is involved in the uploading and downloading of material". Menthe 1998 *Michigan Telecommunications Technology Law Review* 95.

31 Svantesson 2006 *Albany Law Journal of Science and Technology* 365.

voer nie (terwyl Antarktika, die oop see en die ruimte wél ’n fisiese dimensie inneem).[32] Om dit te illustreer noem hy die voorbeeld waar lasterlike opmerkings op die Internet geplaas word. Op die Internet sal dit baie meer skadelik wees as in enige ander van die drie ruimtes waarvan Menthe praat. Hy sê:

> When placed on the Internet, the message can be read, and cause damage, in virtually every country on the planet due to the accessibility of material in cyberspace. In contrast, a message placed in an international space is extremely unlikely to ever even be noted by anybody.[33]

Trouens, meld Svantesson, die feit dat die Internet ’n nie-fisiese bestaan voer, illustreer dat dit so min met die ander ruimtes in gemeen het dat enige sinvolle assosiasie daarmee onsinnig is.[34]

Menthe het die basis vir die Internet as afsonderlike ruimte uiteengesit, maar dit was ander akademici wat die reguleringsmeganismes van daardie ruimte volledig uiteengesit het. Hier was Johnson en Post die voorlopers, en hulle het gemeen dat die Internet by uitstek geskik is vir ’n nuwe vorm van regulering — selfregulering.[35] Dit sal vervolgens bespreek word.

4.2.2.2 Selfregulering as Voorkeurmetode

4.2.2.2.1 Inleiding

Twee van die toonaangewendste akademici van hierdie tyd — Johnson en Post — het in verskeie artikels aangevoer dat die internasionale aard van die Internet wat oor territoriale grense heen strek, dit onregeerbaar maak deur ’n enkele soewereine staat. In een van hul gesaghebbendste artikels — And How Shall the Net be Governed? — het hulle aangevoer dat die enigste werkbare manier waarop die Internet gereguleer kan word, selfregulering

32 Svantesson 2006 *Albany Law Journal of Science and Technology* 365.

33 Svantesson 2006 *Albany Law Journal of Science and Technology* 365.

34 Svantesson 2006 *Albany Law Journal of Science and Technology* 366.

35 Johnson en Post 1996 *Stanford Law Review* 1367.

is.[36]

In hierdie stuk het Johnson en Post vier moontlike reguleringsmodelle beoordeel, te wete regulering deur:

- bestaande soewereine state (deur uitoefening van ekstra-territoriale jurisdiksie)
- multilaterale ooreenkomste in die Internasionale reg;
- die ontwikkeling van 'n internasionale organisasie om die reguleringsfunksie te behartig, en
- selfregulering. [37]

Die outeurs bespreek die voor- en nadele van elkeen van hierdie reguleringsmodelle.

4.2.2.2.2 Regulering deur 'n Soewereine Staat

Regulering deur 'n soewereine staat skep met die intrapslag 'n verskeidenheid probleme. Johnson en Post voer tereg aan dat geen soewereine staat die bevoegdheid het om besluite ten aansien van die Internet — wat 'n globale trefwydte het — te neem nie.[38] Sou dit wel gebeur dat 'n dominante rolspeler, soos die VSA, wel sodanige ingrypings maak, sal dit 'n universele, langtermyninvloed hê.[39] So 'n reguleringsmodel van die Internet sal ook tot gevolg hê dat daar — soos in die koloniale era — 'n "land grab" sal plaasvind waar elke soewereine staat sal gryp van die Internet wat daar beskikbaar is. Kortom, volgens Johnson en Post is hierdie reguleringsmetode onwerkbaar.

---

36 Johnson D R en Post D G "And How Shall the Net be Governed?" in Kahin B (red) *Coordinating the Internet* (1997) 62.

37 Johnson "And How Shall the Net be Governed?" 67.

38 Johnson "And How Shall the Net be Governed?" 69.

39 Johnson "And How Shall the Net be Governed?" 70.

4.2.2.2.3 Regulering deur Multilaterale Ooreenkomste in die Internasionale Reg

Die tradisionele manier waarop soewereine state sake van gemeenskaplike belang tussen hulself hanteer, is deur die werking van die Internasionale reg. Meer spesifiek sal lande bilaterale-, of multilaterale ooreenkomste/verdrae aangaan om die betrokke saak te reël. Dit is dus net logies om ondersoek in te stel of hierdie meganisme nie dalk die oplossing tot Internetregulering kan bevat nie.

Johnson en Post voer hier tereg aan dat die verdragproses van die Internasionale reg 'n pynlik stadige proses is.[40] Om 'n multilaterale ooreenkoms te formuleer kan maklik etlike jare in beslag neem. Dan kan die ratifisering en inwerkingtreding daarvan nog etlike jare, of soms selfs dekades neem. Om hierdie instrument in die vinnig-veranderende wêreld van die Internet te wil gebruik, sal doodeenvoudig nie kan werk nie. Die proses is bloot te stadig en omslagtig.

Verder argumenteer Johnson en Post dat multilaterale ooreenkomste verreweg in die meeste gevalle dokumente is wat algemene beginsels uiteensit. Dit is egter die spesifieke besonderhede wat gewoonlik probleme skep.[41] Die globale aard van die Internet toets gereeld die grense van bestaande regsbeginsels, veral wanneer nuwe tegnologieë geskep word wat op die Internet werksaam is.

4.2.2.2.4 Regulering deur 'n Internasionale Organisasie

In die Internasionale reg is daar vir dekades reeds voorbeelde van internasionale organisasies wat deur 'n multilaterale ooreenkoms geskep is om sake van gemeenskaplike belang namens soewereine state te reguleer. 'n Goeie voorbeeld hiervan is die Organisasie vir Internasionale Burgerlugvaart[42]

40 Johnson "And How Shall the Net be Governed?" 70.

41 Johnson "And How Shall the Net be Governed?" 71.

42 "International Civil Aviation Organisation". Die organisasie is in die lewe geroep deur die *Chicago Convention on International Civil Aviation* wat op die 7de Desember 1944 onderteken is. Abeyratne

(hierna ICAO). Dit is reeds sedert 1947[43] werksaam, en reguleer sedertdien alle globale aangeleenthede betreffende burgerlugvaart.[44]

Die ontstaan van die ICAO kan baie leidrade verskaf op 'n vraag of so 'n organisasie in staat is om die Internet te reguleer. Reeds vroeg in die 20ste eeu — met die ontstaan van burgerlugvaart — is daar besef dat lugvaart 'n saak van internasionale belang is. In 1919 is die voorloper van die ICAO, naamlik die International Commission for Air Navigation gestig.[45] Dit het in sy huidige vorm voortbestaan totdat dit in 1947 omskep is in die ICAO.[46] Dit hanteer sedertdien alle aangeleenthede rakende burgerlugvaart, wat — net soos die Internet — 'n internasionale bate is.

Johnson en Post is skepties of 'n internasionale organisasie in staat is om die Internet te kan reguleer.[47] In die eerste plek beteken dit dat indien so 'n organisasie enige vorm van legitimiteit wil hê, soewereine state hulself gebonde sal moet hou aan die besluite van die organisasie. Dit is nie onmoontlik nie, aangesien die ICAO 'n goeie voorbeeld daarvan is waar state die internasionale organisasie se besluite aanvaar en bevestig.

Die probleem is egter dat die Internet 'n multidimensionele ruimte is waar regulering op 'n wye spektrum noodsaaklik is.[48] Waar die ICAO slegs

---

R *Aviation Security Law* (2010) 8. MacKenzie D *ICAO: A History of the International Civil Aviation Organization* (2010) voorwoord x.

43 Giemulla E M (red) *International and EU Aviation Law: Selected Issues* (2011) 80.

44 ICAO geniet 'n wyd-uiteenlopende status op nasionale en internasionale vlak. Giemulla *International and EU Aviation Law* 80. verduidelik:

> ICAO has the status of a "specialized agency of the United Nations" in the sense of *Article 7 of the United Nations Charter,* by virtue of the *Agreement between the United Nations and ICAO* of 1947, which came into force on 13 May 1947, and by virtue of the Convention on the Privileges and Immunities of the Specialized Agencies of 21 November 1947. It possesses legal personality, both at the level of international law (Article II of the 1947 Convention) as well as at the level of national law (Article 47 of the Convention on International Civil Aviation). Under the latter provision, ICAO shall enjoy full juridical personality wherever compatible with the constitution and laws of the State concerned.

45 Ingevolge artikel 34 van die Parys-konvensie van 1919. Diederiks-Verschoor I H P en Butler M A *An Introduction to Air Law* (2006) 5.

46 Vn 44 hierbo.

47 Johnson "And How Shall the Net be Governed?" 72.

48 Johnson "And How Shall the Net be Governed?" 72.

met tegniese regulering ten aansien van die burgerlugvaart te doen het, het die Internet die bykomende probleem van sosiale regulering. Trouens, selfs by die Internet was tegniese regulering nog nooit 'n probleem nie, aangesien tegniese aangeleenthede rakende die Internet deur die IETF gereguleer word.[49] Hulle speel presies dieselfde rol ten aansien van die Internet as wat ICAO ten aansien van internasionale burgerlugvaart speel.[50] Dit is juis nie die tegniese regulering wat die probleem is nie, maar juis sosiale regulering. Met soewereine state wat uiteenlopende ideologiese verskille het, is dit juis sosiale regulering waaroor daar nie eenstemmigheid bereik kan word nie.

Een van Johnson en Post se grootste probleme met Internetregulering deur 'n internasionale organisasie is die moontlikheid dat dit deur faksies geskaak kan word. Hulle maak die punt baie duidelik wanneer hulle sê:

> It is not easy to set up an appropriate balance of powers within a new organization with quasi-governmental powers when the participants and constituents come from geographic places that have widely divergent views regarding democratic institutions, centralized authority and even "fairness" itself.[51]

Dit is 'n baie geldige punt van kritiek. Elders in hierdie studie[52] word die stigting en werking van die Internet Corporation for Assigned Names and Numbers *(*ICANN*)* hanteer, en word daar verduidelik hoe die werking van faksies binne en buite ICANN 'n groot probleem teweeg bring.

4.2.2.2.5 Selfregulering

Nadat die drie voorafgaande reguleringsmodelle bespreek is, hanteer Johnson en Post die aangeleentheid van selfregulering.[53] Volgens hulle is dit die enigste werkbare model van Internetregulering. Wanneer die konteks vanwaar Johnson en Post hierdie stellings uiter, beskou word, kan hierdie

49 Afd 5.4.3.

50 Afd 5.4.3.

51 Johnson "And How Shall the Net be Governed?" 73.

52 Afd 5.4.1.

53 Johnson "And How Shall the Net be Governed?" 73.

siening begryp word. Die artikel is geskryf in 1996, toe die Internet nog grootliks in sy kinderskoene was. Selfregulering was al wat Internetburgers[54] geken het. Daar was nog nie enige regulatoriese organisasies soos ICANN nie, en die tegnologiese ontwikkelinge om die Internet te fragmenteer — soos wat vandag beskikbaar is — het nog nie bestaan nie.[55]

Johnson en Post se grootste argument ten gunste van selfregulering is dat die Internet ontstaan het sonder enige vorm van regeringsinmenging. Hulle stel dit so:

> Consider what makes the net work. The net itself solves an immensely difficult collective action problem: how to get large numbers of individual computer networks, running diverse operating systems, to communicate with one another for the common good. And, yet, the net is really nothing more than a set of voluntary standards regarding message transmission, routing, and reception. There is not now and never was a central governmental body that decreed or voted to adopt a law stating that TCP/IP is required to be used by those wishing to communicate electronically on a global scale, or that HTTP is required to be used if you wish to communicate over a particular portion of the global network (the World Wide Web).
>
> The "rule-making" process for baseline protocols of the net had none of the vices of centralized, top down, bureaucratic or political, governance. The rules instead evolved from the decentralized decisions by individuals to adopt a promising standard because it served their own interests.[56]

Die grootste punt van kritiek wat teen hierdie siening ge-uiter kan word, is dieselfde as wat hierbo ten aansien van regulering deur 'n internasionale organisasie bestaan. Tegniese regulering waarna Johnson en Post in die gekwoteerde gedeelte hierbo verwys, is nie die probleem van Internetbeheer nie. Dit is eerder sosiale regulering wat problematies is.[57] Met die Internet het mens te doen met tegniese- en sosiale- aangeleenthede, en selfregulering is problematies wanneer sosiale kwessies ter sprake is.

Tog is dit interessant dat dit op die oog af gelyk het asof Johnson en Post dalk tog die spyker op die kop geslaan het met hulle aanvaarding van die

54 "Netizens" in Engels. Jackson J *Introducing Language and Intercultural Communication* (2014) 232 beskryf netizens as "individuals who actively engage in online interactions".

55 Afd 2.3.6.

56 Johnson "And How Shall the Net be Governed?" 74.

57 Marsden C T (red) *Regulating the Global Information Society* (2005) 31.

selfreguleringsmodel. In 1997 het die Amerikaanse hof in *Reno v American Civil Liberties Union*[58] beslis dat 'n gedeelte van die Communications Decency Act, wat gepoog het om versending van pornografiese materiaal aan minderjariges deur middel van die Internet strafbaar te stel, ongeldig is.[59] Dit was vet op die vuur vir regulering-skeptici soos Johnson en Post, want dit was die bewys waarvoor hulle gesoek het dat die Internet onreguleerbaar is deur soewereine state.

In sy artikel getiteld "Against Cyberanarchy" argumenteer Goldsmith dat selfregulering soos Johnson en Post voorstel, 'n Utopia is aangesien dit moontlik is om met bestaande regsbeginsels die Internet grootliks te kan orden.[60] Hy noem byvoorbeeld dat indien 'n staat poog om wette te maak wat die hele Internet raak, dit slegs in daardie betrokke jurisdiksie afdwingbaar sal wees.[61] Hy verduidelik dan ook in fyn besonderhede hoe 'n betrokke staat sy eie inwoners kan beskerm deur byvoorbeeld die tussengangers in transaksies te reguleer.[62] 'n Voorbeeld hiervan is waar 'n staat regulasies vir sy plaaslike Internet-diensverskaffers neerlê en sodoende 'n regulerende funksie verrig.[63]

Interessant genoeg het Goldsmith reeds in hierdie artikel, wat in 1998 geskryf is, verduidelik hoe die Internet besig is om 'n transformasie te ondergaan waardeur dit meer gefragmenteerd word.[64] Soos reeds in afdeling 2.3.6.2 hierbo bespreek is, het die *Yahoo*-saak twee jaar later dié punt op die spits gedryf. Goldsmith noem byvoorbeeld hoe state soos Sjina, Singapore

58 521 US 844 (1997).

59 Afd 3.3.2.

60 Goldsmith J L "Against Cyberanarchy" 1998 *University of Chicago Law Review* 1199 1199.

61 "The skeptics' concerns are further attenuated, however, by limitations on every nation's ability to enforce its laws. A nation can purport to regulate activity that takes place anywhere. The Island of Tobago can enact a law that purports to bind the rights of the whole world. But the effective scope of this law depends on Tobago's ability to enforce it".

Goldsmith 1998 *University of Chicago Law Review* 1216.

62 Goldsmith 1998 *University of Chicago Law Review* 1223. Sien ook afd 6.3 vir 'n volledige verduideliking van die Internet se tussengangers en hoe state hierdie rolspelers gebruik om te reguleer.

63 Afd 6.3.

64 Goldsmith 1998 *University of Chicago Law Review* 1227.

en die Verenigde Arabiese Emirate reeds op daardie stadium begin het om die eenvoudige filters wat beskikbaar was, vir hul eie gebruik in te span.[65]

In sy gevolgtrekking verduidelik Goldsmith dat die kuberruim geensins van die "real-space" verskil nie, en dat huidige regsreëls goed daar toegepas kan word sonder die nodigheid om dit as 'n afsonderlike ruimte te beskou.[66]

Post was nie vir hierdie toedrag van sake te vinde nie, en het 'n opvolgartikel getiteld "Against 'Against Cyberanarchy'" gepubliseer.[67] Daarin argumenteer hy dat die kuberruim tóg anders is, en as sodanig anders behandel moet word. Eerstens noem Post dat die *skaal* van die Internet verskil.[68] Om te illustreer gebruik hy die voorbeeld van *Religious Tech Center v Netcom On-line Comm*[69] Dit was 'n relatief eenvoudige saak van kopieregskending, maar toe die basisbeginsels van kopieregskending op die Internet toegepas word, het dit geblyk dat: "every single Usenet server in the worldwide link of computers transmitting Erlich's message to every other computer would be liable".[70] Dus, die gebruikmaking van die basisbeginsels van kopieregskending het 'n onjuiste en onwerkbare gevolg gehad toe dit op die Internet toegepas word. Regter Whyte het sélf opgemerk dat: "it does not make sense to hold the operator of each computer liable as an infringer merely because his or her computer is linked to a computer with an infringing file".[71] Post se argument wys dus dat die ineengeskakelde Internet

---

65 Goldsmith 1998 *University of Chicago Law Review* 1227.

66 Goldsmith 1998 *University of Chicago Law Review* 1250.

67 Post D G "Against 'Against Cyberanarchy'" 2002 *Berkeley Technology Law Journal* 1365 1365.

68 Post verduidelik:

> The tree is one thing; the forest, though it is nothing more than a large number of trees, is another, more "complex and challenging," phenomenon. The movement of a single clump of dirt down a slope is one thing; an avalanche, though it is nothing more than the movement of lots of individual pieces of dirt down a slope, is another, more "complex and challenging," event. The motion of a single pendulum — which has been understood with great precision since Galileo's day — is one thing; connect a number of pendulums together and you have a much more "complex and challenging" phenomenon.

Post 2002 *Berkeley Technology Law Journal* 1377.

69 *Religious Tech Center v Netcom On-line Comm* 907 F Supp 1361 (N D Cal 1995).

70 Post 2002 *Berkeley Technology Law Journal* 1380.

71 *Religious Tech Center v Netcom On-line Comm* 907 F Supp 1361 (ND Cal 1995) 1372.

tóg onwerkbare gevolge op geykte regsbeginsels kan hê as dit sonder meer toegepas word.[72]

Tweedens maak Post die punt dat die *effek* van die Internet heel anders as die "real-space" is. Hy verduidelik dat as daar na die gevolge van aktiwiteite van 'n gebied, soos Singapore, in die 1450's beskou sou word, dit waarskynlik tot 'n klein geografiese gebied rondom Singapore beperk sou wees. Indien mens die gevolge van aktiwiteite in die Internet-era beskou, sal dit blyk dat dit globaal verspreid is weens die omvang van die Internet.[73]

Dus, sê Post, is die Internet tóg fundamenteel anders, en behoort geykte regsbeginsels getemper te word wanneer dit op die Internet toegepas word.[74]

Selfregulering het inderdaad in die negentigerjare 'n groot reguleringsrol gespeel. Die beste voorbeeld hiervan is sekerlik die selfreguleringsisteme van gemeenskaplike belangegroepe, en daarom word sosiale regulering vervolgens hanteer.

4.2.2.2.6 Samevatting

Omdat die Internet in die 1990's 'n eenheidsnetwerk was, het toonaangewende akademici gemeen dat dit nie deur enige soewereine staat gereguleer kan word nie, en het aangevoer dat selfregulering die aangewese wyse is om dit te reguleer.[75] Hierdie vorm van regulering is deur Johnson en Post verkies bo ander alternatiewe, soos die regulering deur 'n soewereine

---

72 Post verduidelik dat:

> After all, whether you are operating a photocopying machine, a CD-burner, or a Usenet server, you are making a copy of a document, hardly an unfamiliar activity. But the system within which those acts were embedded had changed, and application of the settled law to the *aggregate* of those individual actions somehow needed to change along with it.

Post 2002 *Berkeley Technology Law Journal* 1380.

73 Post 2002 *Berkeley Technology Law Journal* 1380.

74 Post 2002 *Berkeley Technology Law Journal* 1387.

75 Afd 4.2.2.2.

staat,[76] regulering deur multilaterale ooreenkoms,[77] of regulering deur 'n internasionale organisasie.[78]

Die rede waarom Johnson en Post gemeen het dat selfregulering die enigste werkbare opsie is om die Internet te beheers, is omdat dit ontstaan het sonder enige regeringsinmenging.[79] Hierdie siening is versterk toe die saak van *Reno v American Civil Liberties Union* dele van die Communications Decency Act ongeldig verklaar het.[80]

Ander kommentators soos Goldsmith het egter aangetoon dat die Internet nie werklik buite die bereik van regerings was nie, aangesien tussengangers gebruik kan word om regulering te bewerkstellig.[81] In terugskou is dit duidelik dat Goldsmith reg was.[82]

4.2.2.3 Sosiale Regulering

Sosiale regulering verwys na 'n beweging om individuele regsfere, wat territorialiteit verontagsaam, te skep. Die beginsels wat hierdie tipe ontwikkeling onderlê, is gegrond in menslike gemeenskaplikhede en -belange.[83] Hierdie tipe ontwikkeling kom veral voor in die kommersiële sfeer, soos byvoorbeeld *eBay*[84] en die sosiale sfeer, soos speletjies-gemeenskappe.[85]

Murray verduidelik hoe hierdie sosiale gemeenskappe funksioneer, en het selfs sover gegaan om gemeenskappe op die Internet te klassifiseer.[86] Hy meen dat daar in wese ses verskillende kategorieë aanlyn-gemeenskappe

76 Afd 4.2.2.2.2.

77 Afd 4.2.2.2.3.

78 Afd 4.2.2.2.4.

79 Afd 4.2.2.2.5.

80 Afd 4.2.2.2.5.

81 Afd 4.2.2.2.5.

82 Hfst 6 en 7.

83 Murray A D *The Regulation of Cyberspace: Control in the Online Environment* (2007) 148 noem: "As there is no physical glue to hold people together in cyberspace, what draws individuals together to form a community is a shared set of values and goals".

84 Murray *The Regulation of Cyberspace* 151–152.

85 Afd 3.3.1.

86 Murray *The Regulation of Cyberspace* 148.

is,[87] elkeen met sy eie gespesialiseerde fokus. Aangesien mense verskillende belange het, is dit algemeen dat lidmaatskap van meer as een gemeenskap verkry word.[88] Wat veral interessant is, is hoe die betrokke gemeenskappe hulself gereguleer het om die gemeenskaplike forum te kan laat voortbestaan. Kommersiële gemeenskappe soos *eBay* het byvoorbeeld gespesialiseerde betaalstelsels ontwikkel om handel tussen mense op verskillende kontinente moontlik te maak.[89] Net so het speletjiesgemeenskappe hulle eie reëls geskep om onderlinge respek te kweek.[90]

Sosiale gemeenskappe het die fragmentering van die Internet grotendeels oorleef. Gemeenskappe soos *eBay* bestaan vandag nog, alhoewel dit nie wêreldwyd beskikbaar is nie.[91] Die fenomeen van sosiale gemeenskappe het egter in die 21ste eeu 'n reuse transformasie ondergaan met die ontwikkeling van sosiale media soos *Facebook* en *Twitter*.[92]

***

In hierdie afdeling is daar aangetoon hoe selfregulering die gewildste model van Internetregulering in die negentigerjare was. Gedurende hierdie tyd het Lawrence Lessig, wat uiteindelik 'n groot invloed op Internetregulering uitgeoefen het, 'n reeks artikels geskryf wat verduidelik wat die aard van die kuberruim is — en hoe regulering daarvan kan geskied.[93] Dit word vervolgens onder die loep geneem.

---

87 Murray *The Regulation of Cyberspace* 148. Dit is: (1) Kommersiële gemeenskappe — gewoonlik handel; (2) "Online/offline"-gemeenskappe — aanlyn-bespreking van onderwerpe in die fisiese wêreld; (3) Speletjie-gemeenskappe — gemeenskaplike speletjies word gespeel; (4) Kafee-gemeenskappe — sosiale besprekings; (5) Kennisgemeenskappe — hulp en advies; (6) Kreatiewe gemeenskappe — samewerking om produkte of dienste te skep.

88 Murray *The Regulation of Cyberspace* 149.

89 Murray *The Regulation of Cyberspace* 151-152 bespreek in besonderhede die stappe wat die *eBay*-gemeenskap geneem het om aankoop- en betaalsisteme te ontwikkel.

90 Murray *The Regulation of Cyberspace* 149.

91 *eBay* is bv nie in Sjina beskikbaar nie. So S en Westland J *Red Wired: China's Internet Revolution* (2010) 98–100 verduidelik hoe *eBay* in Sjina gefaal het. *Ebay* se bedieners was buite Sjina gestasioneer, en dit het veroorsaak dat die *eBay*-diens gereeld nie beskikbaar was nie. Die Sjinese ekwivalent van *Ebay, Taobao* het die grootste markaandeel verkry en dit behou.

92 Van Dijk J *The Culture of Connectivity: A Critical History of Social Media* (2013) 45–67 verduidelik hoe Facebook ontstaan het, en 68–88 toon aan hoe Twitter ontwikkel het.

93 Lessig 1999 *Harvard Law Review* 506; Lessig 1998 *Journal of Legal Studies* 662.

4.2.2.4 Die Vier Modaliteite van Regulering

4.2.2.4.1 Inleiding

Lawrence Lessig illustreer in sy artikel *The Law of the Horse: What Cyberlaw might teach*[94] dat die Internet, net soos die fisiese wêreld, nie net deur regsbeginsels gereguleer word nie, maar dat ander faktore ook 'n rol speel om 'n samelewing te reguleer. Hy identifiseer vier groot "groepe" beginsels wat hy *modaliteite* noem wat saamwerk om regulering te bewerkstellig. Dit is regsbeginsels, sosiale norme, markte en fisiese argitektuur.[95] Die som van hierdie vier modaliteite stel dan regulering daar. Dit beteken dat dit dikwels nie net een rolspeler is wat reguleer nie, maar 'n verskeidenheid entiteite wat dikwels heel verskillende doelwitte het. Hieronder word die vier modaliteite kortliks uiteengesit, en sal dit ook in die konteks van die Internet bespreek word.

4.2.2.4.2 Die Vier Modaliteite

In die eerste plek reguleer *regsbeginsels* 'n samelewing, deurdat daar sekere wette en regsreëls uiteengesit word wat spesifiek in daardie staat geld.[96] Sedert die ontstaan van state is dit die primêre wyse waarop hulle die sake van hulle onderdane reguleer. Dit is ook 'n baie omvangryke metode van regulering, aangesien dit 'n verskeidenheid verskillende sake kan reguleer.[97]

Tweedens word 'n samelewing deur *sosiale norme* gereguleer. Dit word nie vanuit regsweë afgedwing nie, maar eerder die samelewing as geheel.[98] Voorbeelde hiervan uit die alledaagse lewe is wat as gepaste kleredrag vir mans en vrouens beskou sou word, of waar en wanneer dit gepas sou wees om in die publiek te rook.[99]

94 Lessig 1999 *Harvard Law Review* 662.

95 Lessig 1999 *Harvard Law Review* 506 asook Lessig L *Code Version 2.0* (2006) 122.

96 Lessig 1999 *Harvard Law Review* 506.

97 Lessig 1999 *Harvard Law Review* 507.

98 Lessig 1999 *Harvard Law Review* 507.

99 Lessig 1999 *Harvard Law Review* 507.

In die derde plek reguleer *markte* 'n samelewing — byvoorbeeld, die brandstofprys reguleer in hoe 'n mate mense bereid is om rond te beweeg.[100]

Vierdens word mense deur die fisiese wêreld — of *argitektuur*, soos Lessig dit postuleer — gereguleer.[101] 'n Eenvoudige voorbeeld hiervan is hoe die wêreld gestruktureer is, soos verskillende woonbuurte waar die een meer gegoed is as die ander. Huispryse en 'n persoon se finansiële posisie sal bepaal waar 'n huis aangekoop word.[102]

4.2.2.4.3 Onderlinge Verband

Lessig voer aan dat die vier modaliteite elkeen 'n komplekse aard het, en dat dit in wisselwerking met mekaar is om regulering in 'n gemeenskap te bewerkstellig.[103] Aan die een kant kan die vier modaliteite saam werk om regulering daar te stel, maar aan die ander kant kan dit ook mekaar negatief beïnvloed, soos waar norme die landswette kan afwater,[104] byvoorbeeld waar korrupsie algemeen in 'n staat voorkom sal dit wetgewing oor korrupsie ondermyn. Dus, die vier modaliteit moet altyd in samewerking met mekaar beskou word om die volle reguleringsprentjie te beskou.[105]

Die reg is 'n ingewikkelde modaliteit aangesien dit meerdere funksies kan verrig. Die basis van die reg is 'n bevel wat met 'n sanksie opgevolg word, soos regsreëls wat bepaal dat as 'n dader 'n sekere optrede verrig, daar strafmaatreëls sal wees.[106] Aan die ander kant is regsreëls baie meer as bloot net bevele wat aan sanksies gekoppel is. Dit bevat ook reëls wat gemeenskapswaardes vergestalt, soos wette oor watter vakansiedae in 'n

100 Lessig 1999 *Harvard Law Review* 507.

101 Lessig 1999 *Harvard Law Review* 507.

102 Lessig 1999 *Harvard Law Review* 507.

103 Lessig *Code Version 2.0* 123.

104 Lessig *Code Version 2.0* 123.

105 Lessig *Code Version 2.0* 123.

106 Lessig *Code Version 2.0* 340.

land sal geld.[107] Net so vervat dit ook konstitusionele aangeleenthede, soos hoe die staat se regering of howe saamgestel word of watter regte in 'n handves van menseregte vervat sal word.[108] Tóg, in sy mees basiese vorm, bly die reg eenvoudig 'n bevel wat aan 'n strafsanksie gekoppel word.[109]

Net so is sosiale norme ook van 'n komplekse aard, en funksioneer heel verskillend van regsreëls. Dit is die gemeenskap — en nie die reg nie — wat hierdie norme afdwing deurdat daar sosiale strafmaatreëls is vir die oortreding van sosiale norme.[110] Deur die toepassing van sosiale norme sal mans wat rokke dra, byvoorbeeld in 'n gemeenskap geïsoleer word. Sosiale norme en regsreëls deel egter die gemeenskaplike faktor dat beide slegs tot 'n sanksie lei indien die reël of norm verbreek word, en beide word *ex post facto* afgedwing.[111]

Markte reguleer op 'n relatief eenvoudige manier — met pryse. 'n Prys is bloot die ooreengekome bedrag waarvolgens die verkoper bereid is om die saak van die hand te sit.[112] Wanneer die koper hierdie prys aanvaar, tree regulering onmiddellik in. Die verkoper moet dan die saak oorhandig, en die koper moet die ooreengekome prys betaal. Die mark as reguleringsvorm verskil dan juis van die twee vorige vorms van regulering deurdat die sanksie nie *ná* die optrede in werking tree nie, maar reeds tydens die totstandkoming van die transaksie.[113]

Die vierde modaliteit — argitektuur — is in 'n sekere sin die vreemdste vorm van regulering, aangesien dit dikwels nie eers as 'n reguleringsmetode beskou word nie. Tog is dit waarskynlik die mees effektiewe wyse van regulering.[114] Op 'n fisiese vlak is elke persoon op aarde aan sekere absolute argitektuur-reëls onderworpe. Natuurwette reguleer byvoorbeeld

107 Lessig *Code Version 2.0* 340.

108 Lessig *Code Version 2.0* 340.

109 Lessig *Code Version 2.0* 340.

110 Lessig *Code Version 2.0* 340.

111 Lessig *Code Version 2.0* 340.

112 Lessig *Code Version 2.0* 341.

113 Lessig *Code Version 2.0* 340.

114 Lessig *Code Version 2.0* 342.

hoe vinnig die mens oor die aarde kan beweeg — en hierdie vorm van regulering geskied vanself en hoef geensins afgedwing te word nie. [115]

Benewens die fisiese beperkinge van die natuur lewe mense daagliks ook in 'n mensgemaakte argitektuur, wat baie effektief reguleer. In Suid-Afrika is die ooreengekome pad-argitektuur dat mense aan die linkerkant van die pad ry. In teenstelling met die natuurwette wat nie oortree kan word nie, kan hierdie mensgemaakte argitektuur-reëls wel oortree word, maar die verontagsaming daarvan sal vinnig rampspoedige gevolge inhou. Daarom is dit te verstane dat hierdie argitektuur-reëls nie sommer verontagsaam word nie.[116]

Soos hierbo genoem, verduidelik Lessig dat die vier modaliteite inmekaar verweef is, en gelyktydig op elke persoon op aarde van toepassing is. Sosiale norme kan in wetgewing vervat word.[117] Net so kan argitektuur regtens gekodifiseer word, soos die voorbeeld van die padreëls in die vorige paragraaf. Sosiale norme is ook in die markte aanwesig, soos die beginsel dat 'n kontraksparty met eerlikheid en integriteit behoort te kontrakteer. Dus, die vier modaliteite van regulering is interverweef in elke persoon se lewe.[118]

4.2.2.4.4 Modaliteite in die Kuberruim

Die werking van die vier modaliteite van regulering is hierbo verduidelik aan die hand van die fisiese wêreld, en hoe dit daar toepassing vind. Soos te verwag speel hierdie vier modaliteite ook 'n rol in die kuberruim, maar interessant genoeg is die werking van die modaliteite nie noodwendig in dieselfde verhouding as in die fisiese wêreld nie. Die praktiese voorbeeld van lêerverspreiding in Japan sal dié punt illustreer.

Lêerverspreiding[119] ("file-sharing" in Engels) is 'n fenomeen wat in die

115 Lessig *Code Version 2.0* 340.

116 Lessig *Code Version 2.0* 340.

117 Lessig *Code Version 2.0* 341.

118 Lessig *Code Version 2.0* 341.

119 Die Engelse term "file sharing" verduidelik die konsep ietwat beter. Hierdie is 'n geweldige omvangryke onderwerp wat nie in hierdie studie in besonderhede bespreek sal word nie. Die konsep van "file

laaste dekade regoor die wêreld geweldig veld gewen het. Kortliks behels dit dat 'n verskeidenheid media, wat kan wissel van die nuutste films tot rekenaarspeletjies, kosteloos tussen miljoene mense ("file sharers") versprei word.[120]

Japan is sover bekend die enigste staat wat uitdruklik lêerverspreiding as 'n misdaad verklaar het.[121] Die blote aflaai van 'n lêer vir eie gebruik is strafbaar met twee jaar gevangenisstraf of 'n boete van tweemiljoen Yen.[122]

Ten spyte hiervan word lêerverspreiding algemeen in Japan beoefen.[123] Trouens, statistiek toon dat een uit ses mense in Japan in onwettige

---

sharing" behels egter die volgende:

> File sharing networks are typically peer-to-peer networks that operate over an existing physical network such as the Internet, allowing participating computers to connect to each other so users can search for and transfer files, especially music and video files.

Editors of the American Heritage Dictionaries (red) *High Definition: An A to Z Guide to Personal Technology* (2006) 128.

Rutenbeck verduidelik hoe lêerverspreiding in die 21ste eeu eksponensiëel gegroei het:

> With the quantum leap of high-speed Internet connectivity and high-function peer-to-peer file sharing programs that essentially turned millions of personal computers into mini-servers around the world, the late 1990s and early 2000s saw a boom in file sharing among tens of millions of users around the world.

Rutenbeck J *Tech Terms: What Every Telecommunications and Digital Media Professional Should Know* (2012) 104.

120 Federal Trade Commission *Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues: A Federal Trade Commission Staff Workshop Report* (2005) 3 definieer lêerverspreiding so: "Broadly defined, P2P technology is a distributed computing software architecture that enables individual computers to connect to and communicate directly with other computers. Through this connection, computer users (known as 'peers') can share communications, processing power, and data files."

121 Art 30(iii), art 113 en art 119 van die Chosakuken Hõ (Japanese wet op Kopiereg) 48 van 1970. Die Engelse weergawe van dié wet is beskikbaar by Oyama Y "Copyright Law of Japan" http://www.cric.or.jp/english/clj/index.html (besoek op 9 Desember 2014). Art 30(iii) beskryf die omstandighede waaronder 'n wettige kopie van 'n gekopieërde werk vir eie gebruik gemaak mag word, en lêerverspreiding word spesifiek hieronder *uitgesluit*. Art 119 lê die strafbepalings neer, en art 119(2)(ii) bepaal dat indien 'n lêer van die Internet afgelaai word met die doel om dit verder te versprei, 'n straf van tot vyf jaar of 'n boete van vyfmiljoen Yen opgelê mag word. Hierteenoor word die blote aflaai van 'n lêer vir eie gebruik in art 119(3) strafbaar gestel, maar die straf hiervoor mag hoogstens twee jaar gevangenisskap of tweemiljoen Yen wees. Sien Mehra S K "Keep America Exceptional! Against Adopting Japanese and European-Style Criminalization of Contributory Copyright Infringement" 2011 *Vanderbilt Journal of Entertainment and Technology Law* 811 816 vir 'n bespreking van *Japan v Kaneko* Kyõtõ Chihõ [Kyõtõ Dist Ct] Dec 13 2006 Hei 16 (wa) no 726 1229 (Japan) waar 'n skrywer van 'n lêerverspreidingsprogram strafregtelik vervolg is. Die skuldigbevinding is op appèl in Osaka Kõtõ Saibansho [Osaka High Ct] Oct 8 2009 Hei 19 (wa) no 461 (Japan) in die hoë hof omvergewerp.

122 Vn 121.

123 Oxford Economics *Economic Consequences of Movie Piracy: Japan* (2011) 3.

lêerverspreiding meedoen.[124] Dit is dus duidelik dat die reg in hierdie verband nie effektief is nie, ten spyte daarvan dat sulke gedrag 'n misdaad is en boetes of gevangenisstraf as afskrikmiddel gebruik word.[125]

Die vraag wat ontstaan is waarom is die reg so oneffektief in hierdie geval? Die antwoord is te vinde in Japan se hantering van CD-kopiëring. In Japan bestaan daar reeds vir dekades lank 'n sisteem waarvolgens plaaslike musikante se musiek-CD's binne drie weke ná vrystelling in winkels verhuur kan word teen 'n fraksie van die aankoopprys van die CD.[126] Dieselfde winkels verhuur ook kopieërmasjiene om huurders in staat te stel om eie kopieë van die CD's te maak. Trouens, "the practice of copying CD-Rs is so rampant that teenagers no longer refer to a purchased CD as a "CD" *(shii dee)* but instead use the term "master" *(masutaa)*, as in the master copy which is best for dubbing".[127] Kortom, die kopiëring van CD's is deel van die Japanese normsisteem, en platemaatskappye poog nie eers om hierdie toedrag van sake te verander nie.[128]

Met hierdie inligting word die prentjie duideliker: daar bestaan 'n norm van CD-kopiëring wat nie net deur die reg erken word nie, maar geheel en al sosiaal aanvaarbaar is. Om 'n CD by 'n winkel te huur en dit te kopieer is nie veel verskillend van om musiek van die Internet af te laai en dit vir eie gebruik aan te wend nie. Tog is daar wél 'n verskil tussen die twee, aangesien CD's in Japan 'n spesifieke belasting dra wat aan die "Japanese Society for Rights of Authors" oorbetaal word, en dié dit proporsioneel aan kopiereghouers uitbetaal.[129] Hierdie proses gebeur nie met lêerverspreiding nie, wat tot gevolg het dat kopiereghouers van inkomste ontneem word.

---

124 Oxford Economics *Economic Consequences of Movie Piracy: Japan* 3.

125 Field S G *Internet Piracy in Japan* (2010) 25.

126 Condry I "Cultures of Music Piracy: An Ethnographic Comparison of the US and Japan" 2004 *International Journal of Cultural Studies* 343 352.

127 Condry 2004 *International Journal of Cultural Studies* 352.

128 'n Volledige verduideliking van die Japanese bevolking se waardes ten opsigte van kopieregskending — van CD's tot strokiesprente — word volledig verduidelik in Condry 2004 *International Journal of Cultural Studies* op 352–355.

129 Leitner J "A Legal and Cultural Comparison of File-sharing Disputes in Japan and the Republic of Korea and Implications for Future Cyber-regulation" 2008 *Columbia Journal of Asian Law* 3 12.

Die punt wat egter begryp moet word, is dat wettige kopiëring so in die normsisteem van Japan ingeburger is dat dit die reg ondermyn in die geval van onwettige lêerverspreiding.

Die rol van argitektuursveranderinge van die Internet kan ook in die voorbeeld van lêerverspreiding in Japan gevind word. In die vroeë 2000's het lêerverspreiding wêreldwyd geweldig toegeneem.[130] Dit was ook die geval in Japan, maar die toename was nie so drasties soos in ander lande nie.[131] In die lig van wat sopas oor CD-kopiëring verduidelik is, is hierdie tendens eienaardig. Tog is die verklaring redelik eenvoudig — die grootste deel van die Japanese publiek het met die Internet kennis gemaak deur die gebruik van gespesialiseerde apparate waarmee hulle e-pos en beperkte Internet kon lees (in Japanees).[132] Dit alles het plaasgevind voor die ontwikkeling van die moderne slimfone.[133] Met die ontwikkeling van hoëspoed-Internet het dit alles verander, en die Japanese publiek het met slimfone films en musiek van die Internet begin aflaai.[134] Dus, toe die aflaai van musiek en video's moontlik geword het op die platform waaraan die algemene Japanese gebruiker gewoond was, het dit vinnig toegeneem. Dit illustreer treffend hoe die verandering van Internet-argitektuur 'n vinnige verandering van gedrag in 'n groot gedeelte van 'n bevolking kan meebring.

Hierdie illustrasie toon aan hoe die modaliteite van regulering in die geval van die Internet kan uitspeel. Elke gevallestudie sal ander resultate oplewer, maar dit is seker dat regsreëls alleen nie die antwoord is tot effektiewe regulering van die Internet nie. Al die modaliteite speel 'n rol — en hoe vinniger die wetgewers van die wêreld hierdie beginsel verstaan, hoe vinniger sal 'n effektiewe Internetreguleringsmodel saamgestel kan word.

---

130 Schell B H *The Internet and Society: A Reference Handbook* (2007) 18.

131 Field *Internet Piracy in Japan* 36.

132 Field *Internet Piracy in Japan* 36.

133 Field *Internet Piracy in Japan* 37.

134 Field *Internet Piracy in Japan* 38. Marsden C T *Net Neutrality: Towards a Co-regulatory Solution* (2010) 12 verduidelik die fenomenale groei van hoëspoed-Internet in Japan.

4.2.2.5 Samevatting

Die negentigerjare van die vorige eeu het tot verskeie interessante en somtyds vreemde teorieë aanleiding gegee om Internetregulering te probeer verklaar.[135] Aangesien die Internet op daardie stadium 'n wêreldwye eenheidsnetwerk was, was dit nie vreemd dat daar akademici was wat die Internet as 'n afsonderlike internasionale ruimte wou beskou nie.[136] Artikels soos dié van Menthe het aangetoon hoe die konsep van nasionaliteit in die kuberruim aangewend kon word.[137] Ander skrywers soos Johnson en Post het breedvoerig aangevoer hoe selfregulering die voorkeurmetode vir Internetregulering as afsonderlike ruimte sou wees.[138] Ál hierdie teorieë het op niks uitgeloop nie, aangesien nuwe tegnologieë teen die draai van die eeu ontwikkel is om die Internet te fragmenteer.[139]

Hierteenoor het Lessig se verklaring van regulering deur die vier modaliteite die toets van die tyd deurstaan. Die menslike bestaan is kompleks, en die reg alleen kan nie as enigste reguleerder dien nie.[140] Sosiale norme, markte en argitektuur speel ook 'n integrale rol in menslike regulering — in die fisiese wêreld en ook op die Internet.[141] Die vier modaliteite van regulering is iets wat praktiese aanwending geniet, soos wat aangetoon is in die bespreking oor lêerverspreiding op die Internet in Japan.[142]

Met hierdie verduidelikings word daar volstaan met akademiese verklarings van Internetregulering in die negentigerjare. Daar word vervolgens gefokus op tegniese regulering, waar geo-plasing[143] en plaaslike

135 Afd 4.2.2.
136 Afd 4.2.2.1.
137 Afd 4.2.2.1.
138 Afd 4.2.2.2.
139 Afd 2.3.6.
140 Afd 4.2.2.4.2.
141 Afd 4.2.2.4.2.
142 Afd 4.2.2.4.4.
143 Afd 2.3.6.2.1.

netwerkbeheer[144] die norm geword het. Die eerste bespreking sal fokus op Netwerk Neutraliteit — wat vandag nog 'n tameletjie vir reguleerders, Internetdiensverskaffers én verbruikers is.[145]

4.2.3 Tegniese Regulering

4.2.3.1 Netwerk Neutraliteit

Netwerk neutraliteit is 'n term wat deur Timothy Wu geskep is om 'n teorie van netwerkregulering voor te stel.[146] Soos nuwe tegnologieë in die beginjare van die 21ste eeu ontwikkel het, het dit geblyk dat Internetdiensverskaffers by magte is om hulle netwerke so te manipuleer dat hulle finansiële voordele vermeerder terwyl dit ten koste van verbruikers geskied.[147] ISP's kan sekere webdienste óf verbied óf so erg smoor dat dit onbruikbaar word. Byvoorbeeld, sommige Internet-speletjies wat intyds tussen verskillende groepe gespeel word neem geweldig baie bandwydte op. Die aanhoudende aflaai van data deur die gebruiker is dikwels nie proporsioneel tot Internetgebruik van ander gebruikers nie. Daarom het ISP's in die vroeë 2000's begin om sulke speletjies óf af te sny, wat beteken dat die gebruiker nie die speletjie kon speel nie, óf so te smoor dat data nie behoorlik tussen die bediener en die gebruiker kon vloei nie, en die speletjie

144 Afd 5.5.1.

145 Netwerk Neutraliteit het baie praktiese gevolge vir al drie hierdie rolspelers. Reguleerders is op soek na die beste wyse waarop netwerke gereguleer kan word, aangesien dit óf ekonomiese groei kan bevorder, óf dit kan laat inkrimp. Internetdiensverskaffers sal netwerk neutraliteit (of eerder sy teëkant — breëband diskriminasie) in hul guns wil swaai vir groter winste, en gebruikers sal ten gunste wees van netwerk neutraliteit vir 'n groter verskeidenheid Internetdienste. Afd 4.2.3.1 en afd 5.5.1 sal hierdie beginsels volledig illustreer. De Beer J en Clemmer C D "Global Trends in Online Copyright Enforcement: A Non-neutral Role for Network Intermediaries?" 2009 *Jurimetrics* 375 408 verduidelik hoe netwerk neutraliteit onder verskeie rolspelers gedebatteer word. In *Verizon v FCC* 740 F 3d 623 — Court of Appeals Dist of Columbia Circuit 2014 meld die hof op 634 dat "net neutrality implicates serious policy questions, which have engaged lawmakers, regulators, businesses, and other members of the public for years".

146 Wu T "Network Neutrality, Broadband Discrimination" 2003 *Journal on Telecommunications and High Technology Law* 141 141. Die volledige aanloop tot die netwerk neutraliteit-debat word geskets in Marsden *Net Neutrality* 4.

147 Wu 2003 *Journal on Telecommunications and High Technology Law* 143.

te stadig was dat dit eenvoudig nie gespeel kan word nie.[148] Daar is vele ander voorbeelde van soortgelyke probleme wat ontstaan, soos onderlinge lêerverspreiding[149] en video-stroming tydens Internet-spitstye.[150]

Die konsep van netwerk neutraliteit poog om sinvolle beginsels neer te lê vir hierdie probleme. Wu verduidelik die doelwitte van netwerk neutraliteit:

> What follows is a proposed antidiscrimination principle (a rule, only if necessary). The effort is to strike a balance: to forbid broadband operators, absent a showing of harm, from restricting what users do with their Internet connection, while giving the operator general freedom to manage bandwidth consumption and other matters of local concern.[151]

Die oogmerk van netwerk neutraliteit is om dus die speelveld as't ware gelyk te maak sodat ISP's aan die een kant by magte is om hulle netwerke so te struktureer dat dit sy integriteit behou en gelyke kwaliteit diens aan ál sy gebruikers verleen terwyl dit ook verbruikers magtig om alle dienste van die Internet sonder beperkings te gebruik.[152] 'n Uitstekende definisie van netwerk neutraliteit is te vinde by 'n Verenigde Koninkryk-verslag oor EU-netwerkstrukturering:

> Net neutrality is the principle that Internet service providers and governments should treat all data on the Internet equally, not discriminating or

148 Heckmann O M *The Competitive Internet Service Provider: Network Architecture, Interconnection, Traffic Engineering and Network Design* (2007) 73 verduidelik die bandwydte-implikasies van intydse Internet-speletjies. Sien ook Savin A en Trzaskowski J *Research Handbook on EU Internet Law* (2014) 45 waar die Europese Unie dit regverdig beskou om lêerverspreiding tydens spitstye te smoor:

> The European regulators group BEREC has also analysed "reasonable" and concluded it is "more reasonable to simply throttle P2P applications in times of congestion to the benefit of, for example, time-sensitive applications. Those practices would be considered more reasonable than totally blocking special applications because they induce fewer side effects".

149 Vn 119 en vn 120. Sien ook Newman J "Keeping the Internet Neutral: Net Neutrality and it's Role in Protecting Political Expression on the Internet" 2008 *Hastings Communications and Entertainment Journal* 153 162 en Kohl U "The Rise and Rise of Online Intermediaries in the Governance of the Internet and Beyond — Connectivity Intermediaries" 2012 *International Review of Law, Computers and Technology* 185 198 vir 'n bespreking van die VSA Internetdiensverskaffer *Comcast* wat in 2007 lêerverspreiding eensydig op sy netwerk afgesny het.

150 Bing B *3D and HD Broadband Video Networking* (2010) 219 toon hoe intydse video-dienste gewoonlik nie gesmoor word nie, tensy dit op sekere spitstye afgelaai word — in sulke gevalle word smoring wel toegepas.

151 Wu 2003 *Journal on Telecommunications and High Technology Law* 165.

152 Kurbalija J *An Introduction to Internet Governance* (2012) 53.

> charging differentially by user, content, site, platform, application, type of attached equipment, and modes of communication.[153]

Wu verduidelik dat netwerk neutraliteit eintlik die einddoel is, maar dat 'n verskeidenheid ander konsepte 'n rol speel om dit te bereik.[154] Breëband diskriminasie ("broadband discrimination") en vrye toegang ("open access") is die twee belangrikstes.[155]

Breëband diskriminasie beteken dat 'n ISP sekere gedrag op sy netwerk verbied.[156] Dit word soms gedoen om die netwerk te beskerm, soos in die geval van virusprogramme wat verwyder word,[157] maar dit kan ook meer subtiel wees, byvoorbeeld waar 'n ISP sekere pakkette aanbied wat verskillende dienste lewer.[158] Die probleem met prysdiskriminasie is dat dit dikwels geforseerd is — die ISP verdeel die dienste op sy netwerk en bied dan 'n afgewaterde diens teen 'n laer koste aan terwyl die beter diens teen 'n baie hoër premie verskaf word.[159] 'n Ander wyse waarop prysdiskriminasie kan plaasvind, is waar sekere gedrag of webdienste by sekere pakkette verbied word, soos om nie VPN-dienste[160] te kan gebruik nie.[161] Wu meen hierdie tipe diskriminasie is teenproduktief, aangesien dit nuwe ontwikkelings op die Internet verhinder.[162]

Internetdiensverskaffers bondel soms 'n verskeidenheid web- en ander dienste saam met 'n Internet-toegangspakket. Wu is van mening dat

---

153 Great Britain Parliament House of Commons European Scrutiny Committee *HC 219-ix — House of Commons European Scrutiny Committee Ninth Report of Session 2014-15* (2014) 62 vn 37.

154 Wu 2003 *Journal on Telecommunications and High Technology Law* 145.

155 Wu 2003 *Journal on Telecommunications and High Technology Law* 145.

156 Wu 2003 *Journal on Telecommunications and High Technology Law* 150.

157 Wu 2003 *Journal on Telecommunications and High Technology Law* 150.

158 Wu 2003 *Journal on Telecommunications and High Technology Law* 151.

159 Wu 2003 *Journal on Telecommunications and High Technology Law* 152.

160 Barnes M *An Infinite Number of Monkeys: A Guide to Effective Business Communications* (2013) 115 definieer "Virtual Private Network"-dienste as: "basically a means to securely connect two private networks over the internet, with encryption and strong authentication". Riggs C *Network Perimeter Security: Building Defense In-Depth* (2003) 275 beskou dit eenvoudig as: "using encryption over a public IP network to make sure nobody can read my data".

161 Wu 2003 *Journal on Telecommunications and High Technology Law* 153.

162 Wu 2003 *Journal on Telecommunications and High Technology Law* 153.

hierdie gebruik so ver moontlik beperk moet word, en meen dat dit nie "vrye toegang" bevorder nie. Meer spesifiek beperk dit kompetisie op die Internet.[163] In die onlangse verlede het 'n nuanse van hierdie beginsel wye opspraak gemaak toe die onjuiste gevolge van so 'n sisteem openbaar gemaak is: *Comcast*, die VSA se grootste Internetdiensverskaffer, en *Netflix*, 'n reuse filmstromingsmaatskappy, het 'n ooreenkoms bereik waarvolgens *Comcast* vinniger stromingsdienste aan *Netflix* sal lewer as aan ander kompetisie (ander filmstromingsmaatskappye se films word dus gesmoor).[164] Die gevolge is baie duidelik: as 'n fliekflooi gereeld van *Netflix* gebruik maak, sal dit hom baat om *Comcast* as ISP te gebruik; en *Netflix* kan films vinniger aan meeste van sy gebruikers stroom, aangesien *Comcast* die grootste ISP in die VSA is en noodwendig die ISP van meeste van *Netflix* se kliëntebasis vorm. Deur die saambondeling van ISP-dienste met vinniger *Netflix*-videostroming, verkry *Comcast* 'n onregverdige voordeel bo sy kompetisie.

Wu verduidelik dat die oplossing van hierdie probleem te vinde is in die beginsel dat elke ISP moet verstaan dat hy deel is van twee netwerke: die een is sy eie kommersiële netwerk, en die tweede is die skakeling tussen verskillende ISP's om 'n groter netwerk te vorm, oftewel 'n *internetwerk*.[165] Die beginsel van netwerk neutraliteit is dan dat:

> by adopting the basic principle that broadband operators should have full freedom to "police what they own" (the local network) while restrictions based on inter-network *indicia* should be viewed with suspicion.[166]

Hierdie beginsel is van uiterste belang, en vorm die kern van netwerk neutraliteit: ISP's mag hulle eie netwerke beheer en administreer, maar

163 Wu 2003 *Journal on Telecommunications and High Technology Law* 147; Werbach K "The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart" 2008 *University of California Davis Law Review* 343 375; Balkin J M "The Future of Free Expression in a Digital Age" 2009 *Pepperdine Law Review* 427 431.

164 New York Times "Comcast and Netflix Reach Deal on Service" http://www.nytimes.com/2014/02/24/business/media/comcast-and-netflix-reach-a-streaming-agreement.html?_r=0 (besoek op 12 April 2016).

165 Wu 2003 *Journal on Telecommunications and High Technology Law* 165.

166 Wu 2003 *Journal on Telecommunications and High Technology Law* 165.

indien enige netwerkmanipulering die gevolg gaan hê dat die *internetwerk* daardeur beïnvloed gaan word, moet die veranderinge op die plaaslike netwerk nie toegelaat word nie.[167]

Dit is dus verkeerd om te beweer dat netwerk neutraliteit te doen het met 'n gebrek aan beheer, en dat ISP's se netwerke totaal ongereguleerd moet wees.[168] Wat Wu aanvoer is dat die *internetwerk* ongeaffekteer moet bly van enige regulering deur individuele ISP's.[169] Dit beteken dan dat 'n ISP wél sy netwerk kan manipuleer om 'n kwaliteit diens ("Quality of Service", of QoS) aan sy gebruikers te lewer *solank daardie manipulasie nie die groter internetwerk beïnvloed nie.*

Indien hierdie beginsel op die *Comcast*-geval soos hierbo bespreek, toegepas word, is dit duidelik dat die *Comcast/Netflix*-ooreenkoms die beginsel van netwerk neutraliteit ondermyn deurdat nie slegs *Comcast* se privaatnetwerk deur die ooreenkoms beïnvloed word nie, maar dit ook wyer na die *internetwerk* deurfiltreer — ander ISP's verkry "gewone" stromingspoed terwyl *Comcast* "vinniger" stromingspoed verkry. In kort — *Comcast* en *Netflix* word bevoordeel ten koste van die *internetwerk*.

Wu voer aan dat die korrekte wyse waarop ISP's op hulle netwerke behoort te diskrimineer, nie moet wees om webdienste te smoor of saamgebondelde pakkette te verskaf nie, maar eerder om verskillende bandwydte-pakkette aan te bied.[170] Sodoende kan die gebruiker kies watter spoed hy op die Internet verlang, en ISP-pakkette dienooreenkomstig kies.

In sy artikel maak Wu 'n verskeidenheid voorstelle van hoe die beginsel

---

167 Wu 2003 *Journal on Telecommunications and High Technology Law* 165.

168 Land M "Toward an International Law of the Internet" 2013 *Harvard International Law Journal* 423 meld dat die doel van ISP's moet wees "to treat all content, sites, and platforms equally". Dit is nie wat Wu in sy artikel aanvoer nie.

169 Wu T 2003 *Journal on Telecommunications and High Technology Law* 165; Sylvain O "Internet Governance and Democratic Legitimacy" 2010 *Federal Communication Law Journal* 205 207.

170 Wu 2003 *Journal on Telecommunications and High Technology Law* 168 meld:

> ... a carrier concerned about bandwidth consumption would need to invest in policing bandwidth usage, not blocking individual applications. Users interested in a better gaming experience would then need to buy more bandwidth — not permission to use a given application.

van netwerk neutraliteit in wetgewing vervat kan word.[171] Die beginsel van netwerk neutraliteit word geformuleer as dat 'n ISP "shall impose no restrictions on the use of an Internet connection", maar dat sekere uitsonderings wél gemaak kan word. Voorbeelde van die uitsonderings is (a) om aan 'n statuut of hofbevel te voldoen, (b) om die netwerk se integriteit te verseker, en (c) om aan alle gebruikers dieselfde kwaliteit van diens te verskaf.[172]

Die beginsels van netwerk neutraliteit is iets wat reeds tot verskeie hoëprofiel hofsake aanleiding gegee het.[173] Dit is belangrik om daarop te let dat die teoretiese beginsels van netwerk neutraliteit hierbo bespreek is, terwyl die praktiese gevolge van netwerk neutraliteit in afdeling 5.5 bespreek word.[174] Die rede vir die skeiding is dat hierdie hoofstuk die teoretiese fundering van reguleringsteorieë hanteer, terwyl afdeling 5.5 aantoon hoe Internet-diensverskaffers reguleringsrolspelers in eie reg is.

4.2.3.2 Regulering op grond van Netwerk Argitektuur

Lawrence Lessig het reeds in 1999 gesê dat: "Cyberspace has no nature; it has no particular architecture that cannot be changed. Its architecture is a function of its design".[175] Dit is 'n kritiese konsep wat van die Internet begryp moet word, en dit is al by verskeie geleenthede in hierdie studie aangetoon: die Internet was aanvanklik ontwerp om een netwerk te vorm;[176] deur gebruikmaking van tegnologie is die argitektuur van die Internet verander in 'n gefragmenteerde netwerk;[177] die vierde modaliteit van Lessig se modaliteite van regulering is juis argitektuur,[178] en netwerk neutraliteit

171 Wu 2003 *Journal on Telecommunications and High Technology Law* 166–167.

172 Wu 2003 *Journal on Telecommunications and High Technology Law* 166–167.

173 Afd 5.5.

174 Bl 247.

175 Lessig 1999 *Harvard Law Review* 505.

176 Afd 2.3.2.4.

177 Afd 2.3.6.

178 Afd 4.2.2.4.

poog juis om die argitektuur-speelveld van die Internet so gelyk moontlik te hou.[179] Daarom is regulering op grond van netwerk argitektuur nie 'n nuwe teorie nie, maar eerder 'n ou realiteit wat steeds 'n geweldige rol in 'n veranderde Internet speel.[180]

Wanneer regulering op grond van argitektuur bespreek word, is een van die belangrikste konsepte die sogenaamde "end-to-end"-beginsel. Dit is reeds in 1984 geformuleer, en bepaal dat in 'n gewone netwerk behoort programme wat spesifieke funksies verrig, aan die punte van die netwerk by die laaste gasheer-rekenaars geplaas te word, met dien verstande dat hulle korrek in die gasheerrekenaars geïmplementeer word.[181] Met ander woorde, enige gespesialiseerde sagteware behoort slegs aan die punte van die netwerk geplaas te word, en nie binne-in die nodes daarvan nie.[182] Die *rationale* is dat indien gespesialiseerde sagteware in die nodes geplaas word, sal daardie selfde sagteware ook verder-aan geplaas moet word vir die netwerk om korrek te funksioneer en die boodskap na die ander kant van die netwerk te roeteer. Die kort en lank van die beginsel is dat die netwerk self 'n "dom netwerk" moet wees wat bloot inligting van een punt na 'n ander roeteer.[183]

Die voordeel van 'n "end-to-end"-netwerk is dat dit maklik is om te administreer, en in die konteks van regulering verseker dit dat niemand die groter netwerk manipuleer nie — enige gespesialiseerde programmatuur word op die eind-rekenaar geplaas, wat uiteraard die eiendom van die eindgebruiker is.[184]

---

179 Afd 4.2.3.1.

180 Afd 2.3.6.

181 Saltzer J H, Reed D P en Clark D "End-to-End Arguments in System Design" 1984 *ACM Transactions on Computer Systems (TOCS)* 277 278: "The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the endpoints of the communication system"; Lessig L "The Internet Under Siege" 2001 *Foreign Policy* 56 58.

182 Werbach 2008 *University of California Davis Law Review* 399.

183 Marsden *Net Neutrality* 19.

184 Lessig 2001 *Foreign Policy* 61 stel dit eenvoudig as: "The end-to-end design assured that no network owner could exercise control over the network". Werbach 2008 *University of California Davis Law Review* 401.

Die Internet voldoen huidig nie meer aan hierdie vereiste nie. Deur diep-pakket-inspeksie te gebruik, installeer ISP's gespesialiseerde sagteware (wat die monitering van die pakkette behartig) in roeteerders, wat nodes van die groter Internet vorm.[185] Net so is die gebruikmaking van die *Border gateway protocol* 'n kragtige gespesialiseerde sisteem wat in die node geplaas word wat die land se intranet van die groter Internet afskei.[186]

Regulering op grond van netwerk argitektuur kan op twee wyses toepassing vind: in die eerste plek kan die fisiese struktuur van die Internet verander word. Die Sjinese regering het reeds sedert sy koppeling aan die groter Internet besluit om hulle intranet onafhanklik van die groter Internet te ontwikkel.[187] Reguleringsreëls is neergelê om netwerke te beheer, asook die skakeling tussen netwerke om die internetwerk te vorm. Die omvangryke *Golden Shield*-sisteem[188] word dan gebruik om beperkte skakeling met die groter Internet te bewerkstellig — alles geskoei op die reëls van die Sjinese regering.

In die tweede plek kan die *kode* van die Internet verander word.[189] Die beginsel van netwerk neutraliteit is 'n voorbeeld hiervan, en ISP's voer geweldige beheer uit deur byvoorbeeld van diep-pakket-inspeksie gebruik te maak om regulering op hulle eie netwerke deur te voer.[190]

Die interessantheid van regulering op grond van Netwerk argitektuur is dat dit grotendeels onsigbaar vir gebruikers is. Diep-pakket-inspeksie kan byvoorbeeld glad nie opgespoor word nie, en slegs as die ISP spesifieke protokolle in plek sit om sekere gedrag of dienste te beperk of te smoor, sal

185 Mueller M L en Hadi A "Deep Packet Inspection and Bandwidth Management: Battles Over BitTorrent in Canada and the United States" 2012 *Telecommunications Policy* 462 463.

186 Dong J *Network Dictionary* (2007) 73 definieer "Border Gateway Protocol" soos volg: "The Border Gateway Protocol (BGP) runs over TCP and is an inter-Autonomous System routing protocol. BGP is the only protocol that is designed to deal with a network of the Internet's size and the only protocol that can deal well with having multiple connections to unrelated routing domains".

187 Afd 6.4.2.2.1.

188 Hagestad W *21st Century Chinese Cyberwarfare* (2012) 253. Dit word ook spottenderwys die "Great Firewall of China" genoem.

189 Lessig L *Code 2.0* (2006) 62; Lessig 1999 *Harvard Law Review* 508.

190 Afd 5.5.1.

die gebruiker daarvan bewus word.[191]

Die reg het ook vroeg reeds daarvan bewus geword dat argitektuur van die Internet 'n kragtige reguleerder kan wees. In die oorspronklike *Licra v Yahoo*-saak het die hof aangevoer dat regulering op grond van argitektuur die oplossing is om Nazi-memorabilia in Frankryk van die Internet te verwyder.[192] Interessant genoeg was dit een van die min gevalle waar 'n hof 'n bevel gemaak het wat tegnologies sy tyd vooruit was, ten spyte van die kritiek wat dit op daardie stadium ontlok het.[193]

'n Ander kritiese aangeleentheid wat die toekoms van die Internet radikaal sal beïnvloed, is *modulariteit.*[194] Die beginsels daarvan is reeds in afdeling 2.2.4 bespreek,[195] en dit behels eenvoudig dat die Internet aanvanklik as 'n verspreide netwerk ontwerp is, maar deur kommersiële- en politieke oorwegings al hoe meer die eienskappe van 'n sentrale netwerk vertoon. Indien die nodes (en dus modules) vermeerder word, sal dit 'n meer robuuste netwerk vorm.[196] Die teendeel is ook waar — as die nodes verminder word (en dus die modulariteit), sal dit makliker beskadig kan word.

Farrel en Weiser toon aan hoe modulariteit 'n regsdilemma vir reguleerders skep deurdat hulle moet bepaal watter mate van modulariteit in regeringsbeleid geïnkorporeer moet word.[197] Hulle toon aan hoe beleid wat modulariteit bevoordeel, tot innovasie in verskeie gevalle gelei het, en dat die konsep van modulariteit selfs vir die ontstaan van die Wêreldwye

---

191 Afd 5.5.1.

192 Afd 2.3.6.2.1. Greenberg 2003 *Berkeley Technology Law Journal* 1209–1213 verduidelik in besonderhede hoe die Franse hof van mening was dat *Yahoo* oor die vermoë beskik het om inligting aangaande Nazi-memorabilia aan Franse burgers te blokkeer. *Yahoo* het aangevoer dat hulle nie in staat was om dit te doen nie, maar het tóg na die hofbevel sulke filtreringsisteme geïnstalleer.

193 Afd 2.3.6.2.1.

194 Massachusetts Institute of Technology Computer Science and AI Lab *New Arch: Future Generation Internet Architecture* (2004) 14.

195 Bl 29.

196 Cooper M N (red) *Open Architecture v Communications Policy: Preserving Internet Freedom in the Broadband Era* (2004) 118.

197 Farrel J en Weiser P J "Modularity, Vertical Integration, and Open Access Policies: Towards A Convergence of Antitrust and Regulation in the Internet Age" 2003 *Harvard Journal of Law & Technology* 86 96.

web verantwoordelik was, omdat dit innovasie voor ekonomiese groei gestel het.[198] Beleid wat modulariteit bevoordeel kan ongelukkig die effek hê dat dit maatskappye kan oor-reguleer, wat ekonomiese skade kan veroorsaak.[199]

4.2.3.3 Samevatting

Netwerk Neutraliteit is 'n belangrike konsep by die regulering van die Internet.[200] Dit behels in wese dat netwerk-eienaars hulle netwerke só mag bestuur dat dit nie beskadig word nie, máár dit mag nie gepaard gaan met die uitbuiting van gebruikers of benadeling van die groter netwerk nie.[201] Ongelukkig gee groot netwerk-eienaars (veral Internet-diensverskaffers) nie veel aandag aan die beginsel van netwerk neutraliteit nie, en manipuleer hulle netwerke ten einde groter profyte te maak. Dit is uiteindelik tot nadeel van gebruikers asook die groter Internet.[202]

Regulering op grond van netwerk argitektuur is so vroeg as 1999 deur Lessig beskryf, en dit wys dat die Internet anders as die fisiese wêreld is deurdat die Internet se argitektuur gemanipuleer kan word om makliker regulering daar te stel.[203] Dit is in wese 'n deel van netwerk neutraliteit, aangesien beide te make het met die manipulering van die Internet om 'n sekere gevolg te bewerkstellig.

Die "end-to-end"-beginsel is 'n belangrike konsep in netwerkbestuur. Dit verduidelik dat rekenaars met spesifieke sagteware aan die einde van die netwerk geplaas moet word ten einde die integriteit en goeie werking van die netwerk te verseker.[204] Die moderne Internet voldoen nie meer aan hierdie vereiste nie.[205]

198 Farrel 2003 *Harvard Journal of Law & Technology* 96.

199 Farrel 2003 *Harvard Journal of Law & Technology* 121 noem bv dat "it is difficult to know whether ... a particular approach will outweigh the efficiencies it generates; [it] also risks greater collateral damage".

200 Afd 4.2.3.1.

201 Afd 4.2.3.1.

202 Afd 4.2.3.1.

203 Afd 4.2.3.2.

204 Afd 4.2.3.2.

205 Afd 4.2.3.2.

Regulering op grond van netwerk argitektuur kan op twee wyses deurgevoer word: deur die fisiese struktuur van die Internet te verander, of deur die kode (rekenaarprogrammatuur) van die Internet te manipuleer.[206] Beide hierdie vorms van regulering is onsigbaar vir gebruikers.[207]

4.2.4 Moderne reguleringsteorieë

Sedert ten minste 2005 het daar twee teenstrydige hoofstromings ontstaan van hoe die Internet gereguleer moet word.[208] Aan die een kant was daar state wat 'n multi-belangegroepreguleringsmodel[209] voorstaan, terwyl daar ook 'n reeks state is wat 'n regeringsbeheerde reguleringsmodel[210] aanbeveel het. Voorstanders van die multi-belangegroepreguleringsmodel is die VSA en hulle skepping ICANN, sowel as die groter Europese Unie, en aan die ander kant is daar die Internasionale Telekommunikasie Unie (hierna ITU) met ondersteuners soos Sjina, Brasilië en Rusland wat die regeringsbeheerde reguleringsmodel voorstaan.[211] Die verskil in ideologie is tydens die *World Conference on International Telecommunications 2012* (hierna WCIT-12)[212] op die spits gedryf toe 'n stemming daaroor gehou is: 55 state was ten gunste van die multi-belangegroepreguleringsmodel terwyl 89 state die regeringsbeheerde reguleringsmodel voorgestaan het.[213] Die *Economist* het dit as 'n "digital cold war" voorgestel.[214]

Tydens die NETmundial-2014-konferensie[215] het hierdie verskil in

---

206 Afd 4.2.3.2.

207 Afd 4.2.3.2.

208 Afd 4.2.4.

209 Afd 4.2.4.1.

210 Afd 4.2.4.3.

211 Radu R, Chenou J en Weber R (red) *The Evolution of Global Internet Governance: Principles and Policies in the Making* (2014) 14; Hill R *The New International Telecommunication Regulations and the Internet: A Commentary and Legislative History* (2014) xi.

212 Afd 5.3.3.3.

213 Radu *The Evolution of Global Internet Governance* 13.

214 The Economist "A Digital Cold War?" http://www.economist.com/blogs/babbage/2012/12/internet-regulation (besoek op 14 April 2016).

215 Dit is die verkorte naam van die *Global Multistakeholder Meeting on the Future of Internet Governance*

reguleringsisteme weer opgeduik toe daar state was wat aangetoon het dat hulle die regeringsbeheerde reguleringsmodel voorstaan, maar na intense onderhandelinge is dié siening nie in die finale verklaring ingewerk nie.[216]

In 2015 het die Verenigde Nasies 'n *World Summit on the Information Society +10* (hierna WSIS+10) inisiatief deurgevoer waar daar beoordeel moes word wat die suksesse van die WSIS-proses oor die laaste tien jaar was.[217] Net soos by ander wêreldkonferensies is amptelike voorleggings versoek om probleme voor die konferensie grotendeels uit te stryk. Hier het Rusland weer bevestig dat dit van mening is dat Internetbeheer binne die reg van state val deur uitlatings soos "We reaffirm that policy authority for Internet-related public policy issues is the sovereign right of States".[218]

Tot op hede is daar nog geen aanduiding watter ideologie sal seëvier nie. Beide modelle word bespreek.

4.2.4.1 Multi-belangegroepreguleringsmodel

Die multi-belangegroepreguleringsmodel ("multi-stakeholder model") is — soos sy naam aandui — 'n model wat bepaal dat die Internet deur 'n belangegroep van multidimensionele organisasies gereguleer moet word.[219]

---

wat in São Paulo, Brasilië in April 2014 gehou is. Die organiseerders van die konferensie verwys self na die konferensie as NETmundial — "mundial" beteken "wêreldwyd" in Spaans. NETmundial "Global Multistakeholder Meeting on the Future of Internet Governance" http://netmundial.br/ (besoek op 27 April 2016); Mirriam Webster "Spanish Central" http://www.spanishcentral.com/translate/mundial (besoek op 27 April 2016).

216 Vn 215. Verskeie lande, soos Rusland en Indië het geweier om die finale dokument te teken aangesien dit nie aantoon dat regerings 'n groter rol in Internetregulering behoort te speel nie — dus insluiting van die regeringsbeheerde reguleringsmodel. Shackleford S J "Spotlight on Cyber V: Back to the Future of Internet Governance?" 2015 *Georgetown Journal of International Affairs (Cyber)* http://journal.georgetown.edu/back-to-the-future-of-internet-governance/ (besoek op 16 April 2016); Intellectual Property Watch "NETmundial Internet Governance Meeting Closes With Less Than 'Rough Consensus'" http://www.ip-watch.org/2014/04/25/netmundial-internet-governance-meeting-closes-with-less-than-rough-consensus/ (besoek op 16 April 2016).

217 World Summit on the Information Society *Implementing WSIS Outcomes: A Ten-year Review* (2015). Verkrygbaar by World Summit on the Information Society "Implementing WSIS Outcomes: A Ten-year Review" http://unctad.org/en/PublicationsLibrary/dtlstict2015d3_en.pdf (besoek op 8 Mei 2016).

218 Russian Federation *Written Submission of the Russian Federation to the Draft Final Document of the UNGA High-level Meeting on the Implementation of WSIS Outcomes* (2015) 2.

219 Radu *The Evolution of Global Internet Governance* 9.

Daar bestaan egter geen algemeen aanvaarde definisie van die multi-belangegroepreguleringsmodel nie, maar Banks beskou dit as:

> the coming together of different interest groups on an equal footing, to identify problems, define solutions and agree on roles and responsibilities for policy development, implementation, monitoring and evaluation.[220]

Wentworth definieer die multi-belangegroepreguleringsmodel as 'n:

> model [that] engages technologists, the private sector and civil society in a bottom-up, consensus driven approach to standards setting, Internet development, and management.[221]

Uit hierdie twee definisies blyk dit dat die multi-belangegroepreguleringsmodel 'n model is waar die rolspelers uit verskeie uiteenlopende groepe bestaan wat almal bymekaar kom om Internet-aangeleenthede van gemeenskaplike belang te bespreek. Wanneer dit gedoen word, word daar veronderstel dat die verskeie groepe as gelykes bymekaar kom en die doel is om probleme te identifiseer, oplossings te vind, en rolverdelings uit te klaar (vanuit Banks se definisie).[222] Die groepe word aldus Wentworth se definisie uit die privaat sektor asook die burgerlike gemeenskap opgemaak.

Die definisies gee 'n algemene oorsig wat met die multi-belangegroepreguleringsmodel bedoel word, maar dit is duidelik dat hierdie definisies ook te kort skiet: van die grootste rolspelers in hierdie model is state, waarvan die VSA waarskynlik die prominentste is.[223] Die multi-belangegroepreguleringsmodel het ook vanuit die *World Summit on the Information Society II* (hierna WSIS-II) proses voortgespruit, en daardie beraad was 'n inisiatief van die Verenigde Nasies.[224] Dit is dus duidelik dat

---

220 Banks K "Summitry and Strategies" 2005 *Index on Censorship* 85 85.

221 Wentworth S "Hearing: Fighting for Internet Freedom, Dubai and Beyond" 2013 *US House of Representatives Committee on Energy and Commerce's Subcommittee on Communications and Technology* 3.

222 Kleinwächter W (red) *The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment* (2007) 261 beskou dit as "the basic principle of multi-stakeholderism is the fundamental right of any actor to participate, in an appropriate manner".

223 Winter J en Ono R *The Future Internet: Alternative Visions* (2016) 29 verduidelik die belang van die VSA by die multi-belangegroepreguleringsmodel, veral ten aansien van die oordrag van die IANA-funksie.

224 Afd 5.3.2.1.

hierdie definisies ten minste uitgebrei moet word om state ook as rolspelers te identifiseer. Daarom wil dit voorkom asof Lawrence Strickling — wat die VSA se assistent-sekretaris vir Kommunikasie is — se definisie meer water dra:

> Known as the multistakeholder process, it involves the full involvement of all stakeholders, consensus-based decision-making and operating in an open, transparent and accountable manner.[225]

Ten spyte van die definisies se tekortkominge kan die algemene aard van die multi-belangegroepreguleringsmodel tog afgelei word: 'n verskeidenheid uiteenlopende rolspelers werk almal saam om gemeenskaplike belange te soek en dit te bevorder.[226]

Wanneer sulke uiteenlopende groepe soos state en individue bymekaar kom om sake te bespreek, is dit voor-die-hand-liggend dat dit uiters moeilik sal wees om tot enige vergelyk te kom. Die rolspelers se belange is geweldig uiteenlopend, en elkeen kom na die tafel met sy eie agenda. Dit is daarom nie vreemd dat die *forums* van die multi-belangegroepreguleringsmodel — meerendeels die verskeie WSIS-konferensies — nie veel uitgerig het nie en grotendeels as "talk shops" beskou is.[227]

Die multi-belangegroepreguleringsmodel is baie interessant wanneer dit uit 'n Internasionaalregtelike hoek beoordeel word. Daar is reeds aangetoon dat die tradisionele siening van die volkereg[228] is die regulering van verhoudings tussen state.[229] Met die ontwikkeling van die Verenigde Nasies is hierdie siening uitgebrei om ook internasionale organisasies te omvat — en dat hulle sekere aangeleenthede namens state mag bereg.[230]

---

225 National Telecommunications and Information Administration "Moving Together Beyond Dubai" https://www.ntia.doc.gov/blog/2013/moving-together-beyond-dubai (besoek op 27 April 2016).

226 Malcolm J *Multi-Stakeholder Governance and the Internet Governance Forum* (2008) 112.

227 Afd 5.3.2.5.

228 Die term "volkereg" is die meer tradisionele term van die Internasionale publiekreg. Kleyn D en Viljoen F *Beginnersgids vir Regstudente* (2010) 97 merk heel bondig op: "Internasionale reg staan ook as volkereg bekend". Wikipedia "Internasionale Reg" https://af.wikipedia.org/wiki/Internasionale_reg (besoek op 27 April 2016).

229 Afd 1.5.

230 Afd 1.5.

Met die ontwikkeling van die multi-belangegroepreguleringsmodel wil dit voorkom asof hierdie definisie weer eens aangepas sal moet word, aangesien die privaat sektor 'n al-hoe-groterwordende rol in die volkereg speel.[231] Brölmann noem dit "transnational 'private' regulation", en meld dat dit die konsep van die volkereg herskep:

> [T]ransnational 'private' regulation (TPR) represents a distinct phenomenon. Of interest in this regard are the ways in which the private sphere has become a source of normativity for regulation. Inverting the traditional Westphalian picture of the State as the source of regulation, TPR represents a new development...[232]

As voorbeeld van hierdie nuwe vorm van transnasionale privaatregulering gebruik Brölmann die voorbeeld van die multi-belangegroepreguleringsmodel, en meld dat ICANN as privaat entiteit 'n rol in die Internasionale publiekreg speel[233] — dit alles ten spyte daarvan dat dit nie 'n internasionale organisasie volgens die definisie van die Verenigde Nasies is nie.[234]

Hierdie nuwe verwikkeling is tot hede nog ongekend in die Internasionale reg. Dit is nog onbekend in watter mate die multi-belangegroepreguleringsmodel 'n blywende rol in die wêreld se Internasionaalregtelike sfeer kan speel. Gurumurthy stel dit raak wanneer sy meld dat: "Multistakeholderism is a framework and means of engagement, it is not a means of legitimization".[235] Die multi-belangegroepreguleringsmodel is bloot 'n meganisme vir groepe om tot 'n vergelyk te kom, maar in wese stel dit nie 'n omvattende reguleringsmodel *per se* daar nie.

Ten spyte van dit wat reeds gesê is, het die NETmundial-

231 Brölmann C en Radi Y *Research Handbook on the Theory and Practice of International Lawmaking* (2016) 58.

232 Brölmann *Research Handbook on the Theory and Practice of International Lawmaking* 58.

233 Brölmann *Research Handbook on the Theory and Practice of International Lawmaking* 59.

234 Afd 5.4.1.

235 Gurumurthy A *Statement by Anita Gurumurthy, Executive Director, IT for Change 1 at the Closing Ceremony of WSIS Plus 10 Review held by UNESCO from 25th to 27th February, 2013* (2013) 3.

2014-konferensie[236] probeer om die beginsels van die multi-belangegroepreguleringsmodel uiteen te sit.[237] Uit die verklaringsdokument van die konferensie blyk dit dat algemene beginsels neergelê word, soos die beskerming van menseregte, vryheid van Internet-tussengangers, kulturele en linguistieke verskeidenheid, 'n eenheids-Internet en 'n oop- en verspreide-Internet-netwerk.[238] Die optrede van die VSA met hulle metadata-program, (wat elders bespreek word),[239] word ook indirek aangespreek en ten sterkste veroordeel.[240] Ongelukkig lees die verklaring in algemene stellings, en is daar geen konkrete beginsels wat neergelê word nie. Ironies genoeg is al die waardes wat voorgehou word, dit wat reeds in die era van die Internet bestaan het voordat dit in die vroeë 2000's gefragmenteer geword het.

Uit alles wat hierbo bespreek is, blyk dit dat die multi-belangegroepreguleringsmodel steeds na meer as tien jaar van onderhandelinge steeds in sy kinderskoene is.[241]

Dit is die skrywer se mening dat die rede waarom die multi-belangegroepreguleringsmodel steeds so 'n prominente rol by Internetregulering speel, te vinde is in die feit dat die regering van die VSA duidelik aangetoon het dat hulle nie bereid is om die IANA-funksie te delegeer tensy die nuwe liggaam 'n multi-belangegroepreguleringsmodel voorstaan nie.[242] Dit is dan ook waarom ICANN se hele struktuur op

---

236 Vn 215.

237 NETmundial *NETmundial Multistakeholder Statement* (2014). Hierdie is bloot 'n dokument wat die uitkoms van die verrigtinge tydens die konferensie *ex post facto* uiteengesit het, en dra nie enige vorm van regskrag in die Internasionale reg nie. NETmundial "NETmundial Multistakeholder Statement" http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf (besoek op 28 April 2016).

238 NETmundial *NETmundial Multistakeholder Statement* (2014) 4–5.

239 Afd 6.4.1.5.2.

240 NETmundial *NETmundial Multistakeholder Statement* (2014) par III(2) op 11.

241 United Nations *Implementing WSIS Outcomes: A Ten-year Review* (2015) 175 meld bv: "Experience of multi-stakeholder cooperation and dialogue in the Information Society is still relatively new". Daar sou gehoop word dat met tien jaar se onderhandelinge en onbepaalbare bedrae geld wat in hierdie proses ingestoot is, daar meer vordering sou wees.

242 National Telecommunications and Information Administration "NTIA Announces Intent to Transition Key Internet Domain Name Functions" https://www.ntia.doc.gov/press-release/2014/ntia-announces-

hierdie model gebaseer is.[243] Na verwagting behoort delegering van die IANA-funksie binne een tot drie jaar plaas te vind.[244] Die toekoms van die multi-belangegroepreguleringsmodel by Internetregulering sal dan eers duidelik word.

4.2.4.2 Regulatoriese Matriks

In sy boek, *The Regulation of Cyberspace*,[245] verduidelik Andrew Murray dat die aanvanklike siening dat daar 'n model ontwikkel kan word wat die Internet sinvol kan reguleer, 'n blote lugkasteel is en dat Internetregulering eerder vanuit 'n regulatoriese matriks beskou behoort te word.[246] Die voorstelling van sy matriks word in figuur 4.1 weergegee.

Murray verduidelik sy matriks deur te sê dat verskeie rolspelers almal in wisselwerking met mekaar staan, en dat elke rolspeler se optrede 'n uitwerking op die ander het. Hy gebruik die voorbeeld van die sogenaamde "butterfly effect" wat illustreer dat selfs die kleinste werking van een van die rolspelers 'n geweldige uitwerking op die groter matriks kan hê.[247] Die gevolg hiervan is dat wanneer 'n rolspeler die matriks met sy optrede beïnvloed, dit 'n ingewikkeldheid ontketen wat veroorsaak dat die veranderinge in die matriks nie vooraf voorspel kan word nie.[248]

---

intent-transition-key-internet-domain-name-functions (besoek op 28 April 2016); Kruger L G *Internet Governance and the Domain Name System: Issues for Congress* (2014) 6.

243 Afd 5.4.1.

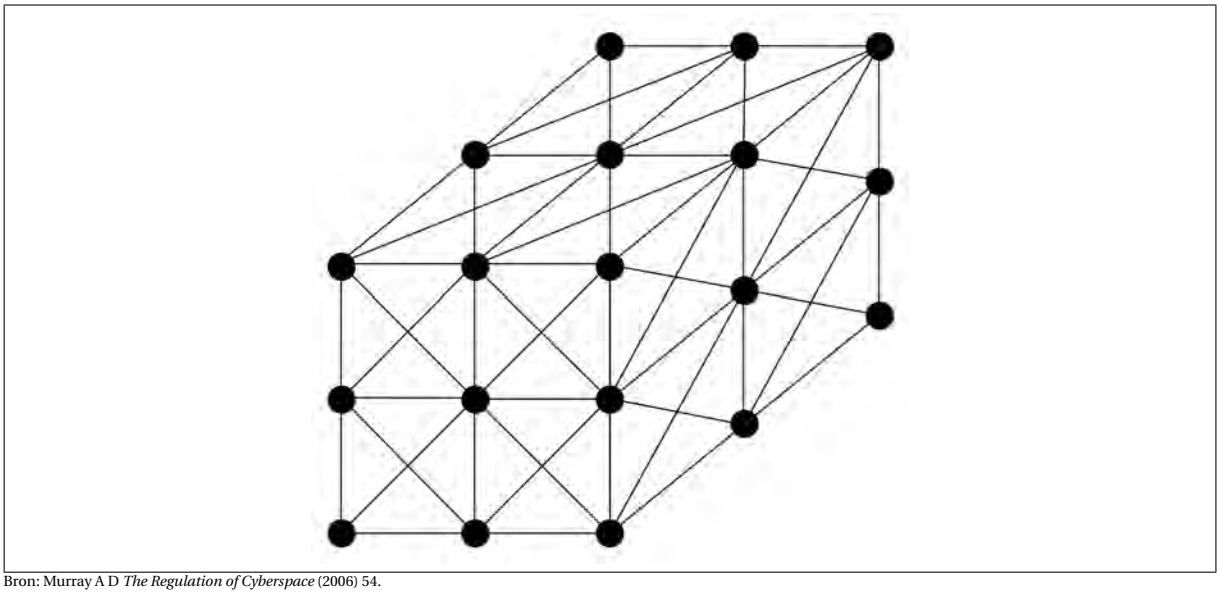
244 In Maart 2014 is die IANA-funksie-delegering deur 'n persverklaring aangekondig. Vn 242. Op 17 Augustus 2015 het die assistent-sekretaris van Kommunikasie in die VSA aangetoon dat onderhandelinge steeds aan die gang is om die IANA-funksie te delegeer, en dat dit na verwagting teen 30 September 2016 afgehandel behoort te wees. Tog meld Strickling ook: "Beyond 2016, we have options to extend the contract for up to three additional years if needed". National Telecommunications and Information Administration "An Update on the IANA Transition" https://www.ntia.doc.gov/blog/2015/update-IANA-transition (besoek op 28 April 2016).

245 Murray *The Regulation of Cyberspace* 52–54 en 234–240.

246 Murray *The Regulation of Cyberspace* 52.

247 Murray *The Regulation of Cyberspace* 52 meld effe sensasioneel dat "any change at any point in the regulatory web can have immeasurable repercussions".

248 Murray *The Regulation of Cyberspace* 53 meld: "At each point in the matrix, a regulatory intervention may be made, but the complexity of the matrix means that it is impossible to predict the response of any other point in the matrix".



Bron: Murray A D *The Regulation of Cyberspace* (2006) 54.

Figuur 4.1: Murray se Regulatoriese Matriks

Daar word aan die hand gedoen dat Murray se regulatoriese matriks geensins 'n nuwe Internetreguleringsmodel is nie, maar dat dit bloot 'n visuele wyse is waarop die multi-belangegroepreguleringsmodel voorgestel kan word. Murray se rolspelers is identies aan dié van die multi-belangegroepreguleringsmodel, en die wisselwerking tussen rolspelers in die multi-belangegroepreguleringsmodel is ook soos Murray in sý model aantoon.[249] Sy "butterfly effect" is waarskynlik effe oordrewe aangesien dit bevraagteken kan word in watter mate klein rolspelers so 'n geweldige effek op die multi-belangegroep-proses kan hê, maar dit doen nie afbreuk aan die gedagte dat hierdie nie 'n nuwe model in die Internetreguleringsdebat vorm nie.

4.2.4.3 Regeringsbeheerde Reguleringsmodel

'n Regeringsbeheerde reguleringsmodel is eenvoudig 'n model van regulering waar regerings van die wêreld die sentrale funksie van regulering verrig. King definieer dit soos volg:

[249] Murray *The Regulation of Cyberspace* 234–238. Hier bespreek hy verskeie rolspelers, soos die ICANN en deelnemers aan die WSIS-proses. Hierdie is almal rolspelers in die multi-belangegroepreguleringsmodel.

> "Intergovernmental" is defined to mean that several governments agree common rules to deal with specific governance aspects, and the implication is that certain aspects of Internet governance will be committed to some international structure.[250]

Hierdie struktuur is nie eie aan die Internet nie. Met die ontwikkeling van die Verenigde Nasies het internasionale organisasies 'n prominente reguleringsfunksie van state se gemeenskaplike belange begin vertolk.[251] Byvoorbeeld, die Internasionale Telekommunikasie Unie is 'n amptelike internasionale organisasie volgens die vereistes van die Verenigde Nasies, en hanteer internasionale telekommunikasie-aangeleenthede namens state. [252] Die gedagte van 'n regeringsbeheerde reguleringsmodel is dus bloot dat 'n internasionale organisasie Internet-aangeleenthede namens state van die wêreld hanteer.

Die regeringsbeheerde reguleringsmodel vir die Internet het — eienaardig genoeg — net soos die multi-belangegroepreguleringsmodel uit die WSIS-proses voortgespruit.[253] Op daardie stadium is die WGIG-vergadering aangesê om moontlike modelle te identifiseer wat gepas kan wees om die Internet op 'n globale vlak te reguleer.[254] Die verslag het verskeie modelle voorgehou, waarvan die multi-belangegroepreguleringsmodel en die regeringsbeheerde reguleringsmodel uiteindelik die belangrikstes was.

Voordat die regeringsbeheerde reguleringsmodel bespreek word, moet dit duidelik gestel word dat verwarring maklik kan voorkom wanneer veral die WGIG-verslag gelees word. Toe die multi-belangegroepreguleringsmodel deur die WGIG-vergadering in 2005 voorgestel is, was daar nog geensins enige eenstemmigheid oor wat met

---

250 King I "Internationalising Internet Governance: Does ICANN Have a Role to Play?" 2004 *Information and Communications Technology Law* 243 253.

251 Afd 1.5.

252 Afd 1.5.

253 Internet Governance Forum "Report of the Working Group on Internet Governance" http://www.wgig.org/docs/WGIGREPORT.pdf (besoek op 28 April 2016).

254 Afd 5.3.2.1.

"multi-belangegroepreguleringsmodel" bedoel word nie. Die verduideliking soos hierbo uiteengesit het oor 'n tien jaar tydperk uitgekristalliseer.[255] Die wortels van die regeringsbeheerde reguleringsmodel het gespruit uit die multi-belangegroepreguleringsmodel deurdat regerings van die wêreld gemeen het dat hulle die prominentste rol in die multi-belangegroepreguleringsmodel sal speel.[256] Trouens, die WGIG-verslag het dit baie duidelik so uiteengesit, soos direk hieronder aangetoon sal word.

Die WGIG-verslag het in hoofstuk IV uiteengesit dat daar drie groepe is wat die multi-belangegroepreguleringsmodel sal uitmaak, te wete regerings, die privaat sektor, en die burgerlike gemeenskap ("civil society").[257] Paragraaf 30 van die dokument bevat 'n lys funksies wat onder die uitsluitlike beheer van regerings sou wees. Dit sluit aspekte in soos die skepping van beleid oor nasionale en internasionale Internet-aangeleenthede; oorsigfunksies; aanvaarding van wetgewing en standaarde; sluiting van verdrae en ontwikkeling van beste gebruike om die Internet glad te laat funksioneer.[258]

Uit hierdie lys is dit baie duidelik dat die rol van regerings beskou is as die rolspelers wat makro-besluite aangaande hulle state se intranet- sowel as Internet-aangeleenthede sal maak. Dit is trouens die funksie van regerings in die fisiese wêreld. Die WSIS-verslag maak geen geheim van die leidende

255 Die WSIS+10-konferensie is in 2015 gehou om die vordering van die WSIS-proses oor die laaste 10 jaar te beoordeel. United Nations "WSIS+10 United Nations General Assembly High Level Meeting" https://publicadministration.un.org/WSIS10/ (besoek op 28 April 2016).

256 Internet Governance Forum "Report of the Working Group on Internet Governance" http://www.wgig.org/docs/WGIGREPORT.pdf (besoek op 28 April 2016) par 30.

257 Par 29–32 van die verslag.

258 Die volledige lys van par 30 is soos volg: "Public policymaking and coordination and implementation, as appropriate, at the national level, and policy development and coordination at the regional and international levels; Creating an enabling environment for information and communication technology (ICT) development; Oversight functions; Development and adoption of laws, regulations and standards; Treaty-making; Development of best practices; Fostering capacity-building in and through ICTs; Promoting research and development of technologies and standards; Promoting access to ICT services; Combating cybercrime; Fostering international and regional cooperation; Promoting the development of infrastructure and ICT applications; Addressing general developmental issues; Promoting multilingualism and cultural diversity; Dispute resolution and arbitration".

rol wat regerings behoort te speel nie.

Volledigheidshalwe behoort die funksies van die ander twee rolspelers ook genoem te word. Die WSIS-verslag bepaal in paragraaf 31 dat die rol van die privaat sektor die volgende funksies insluit: self-regulering van die industrie; ontwikkeling van beleidsvoorstelle wat aan beleidsmakers voorgelê kan word; navorsing en ontwikkeling van nuwe tegnologieë en hantering van arbitrasie en dispute.[259]

Op dieselfde wyse word die funksies van die burgerlike gemeenskap uiteengesit as onder andere: die mobilisering van burgers in demokratiese prosesse; voorstelling van minderheidsgroepe; aanbied van kundigheid en die ontwikkeling van mens-gesentreerde gemeenskappe wat menseregte voor oë hou.[260]

Uit die bespreking tot dusvêr is dit duidelik dat regerings van die dag nie verkeerd sou wees om die WSIS-verslag te interpreteer as dat hulle die leidende rol ten aansien van Internetregulering behoort te neem nie. Dit is vanuit hierdie siening dat die regeringsbeheerde reguleringsmodel gebore is.

Nadat hierdie verskillende funksies uiteengesit is, beskryf die WSIS-verslag vier moontlike modelle vir Internetregulering.[261] Die vier modelle sal hier slegs oorsigtelik genoem word aangesien dit op hierdie stadium slegs

259 Die volledige lys van par 31 is soos volg: "Industry self-regulation; Development of best practices; Development of policy proposals; guidelines and tools for policymakers and other stakeholders; Research and development of technologies, standards and processes; Contribution to the drafting of national law and participation in national and international policy development; Fostering innovation; Arbitration and dispute resolution; Promoting capacity-building".

260 Die volledige lys van par 32 is soos volg: "Awareness-raising and capacity-building (knowledge, training, skills sharing); Promoting various public interest objectives; Facilitating network-building; Mobilizing citizens in democratic processes; Bringing perspectives of marginalized groups, including, for example, excluded communities and grass-roots activists; Engaging in policy processes; Contributing expertise, skills, experience and knowledge in a range of ICT policy areas; Contributing to policy processes and policies that are more bottom-up, people-centred and inclusive; Research and development of technologies and standards; Development and dissemination of best practices; Helping to ensure that political and market forces are accountable to the needs of all members of society; Encouraging social responsibility and good governance practice; Advocating for the development of social projects and activities that are critical but may not be 'fashionable' or profitable; Contributing to shaping visions of human-centred information societies based on human rights, sustainable development, social justice and empowerment".

261 13-16 van die verslag.

historiese waarde het.

Die eerste model behels dat 'n sogenaamde "Global Internet Council" geskep moet word om volledige beheer oor die Internet te neem. Dit sou bestaan uit verteenwoordigers van state van die wêreld, en daar sou toegesien moet word dat verteenwoordiging vanuit alle streke verkry word. Hierdie raad sou dan die IANA-funksie oorneem en alle beleid aangaande die Internet maak. Enige nie-regeringsrolspelers sou slegs in 'n adviserende hoedanigheid tot diens kan wees.[262]

Die tweede model behels dat geen oorsigstrukture geskep hoef te word nie, maar dat ICANN se "Governmental Advisory Committee" versterk word om regerings-aangeleenthede aan te spreek.[263]

Die derde model wat voorgestel is, is dat 'n "International Internet Council" geskep moet word wat spesifiek die IANA-funksie hanteer. Dit is soortgelyk aan ander internasionale organisasies wat geskep word om internasionale gemeenskaplike belange te beheers, soos die "International Civil Aviation Authority" wat alle sake rakende die internasionale lugruim reguleer.[264]

Die vierde en laaste model wat deur die WSIS-verslag voorgestel is, bestaan uit die skepping van drie organisasies wat elkeen 'n eie funksie verrig, maar saam die Internet reguleer.[265] Die eerste organisasie het die funksie om internasionale beleid te skep, en word verteenwoordig deur regerings van die wêreld, terwyl die privaat sektor en die burgerlike gemeenskap waarnemer status het. Die tweede organisasie word geïdentifiseer as 'n wêreldgebaseerde ICANN (genaamd WICANN), wat eweneens deur state van die wêreld verteenwoordig word, maar die taak het om oorsig- en die IANA-funksie te verrig. Hier het die privaat sektor en die burgerlike gemeenskap eweneens waarnemer status. Die derde organisasie

262 13 van die verslag.

263 14 van die verslag.

264 14 van die verslag.

265 15 van die verslag.

is ’n gespreksforum tussen regerings, die privaat sektor, en die burgerlike gemeenskap om beleidsake rakende die Internet te bespreek.[266]

Nie een van hierdie modelle is tot op hede gevolg nie. Die belangrikheid daarvan vir die konteks van die huidige onderwerp is dat twee van die vier modelle ’n beherende rol vir state van die wêreld skep (modelle 1 en 4). Daar is dus reeds sedert die vroegste gesprekke oor Internetregulering ’n sterk aanspraak deur state gemaak dat hulle die beherende rol daarin moet speel. Of dit die korrekte roete is om te volg, is nie tans onder bespreking nie — daar word bloot aangetoon dat hierdie siening van regerings om die sentrale rol by Internetregulering te speel reeds tydens die aanvanklike gesprekke na vore gekom het.

Uit hierdie modelle blyk dit ook dat daar verskillende wyses bestaan waarop strukture in plek gestel kan word om regerings die beherende rol oor Internetregulering te gee. Tot op hede is daar nog geensins ooreengekom oor wat dit sal wees nie, aangesien daar nog geen aanduiding is of die regeringsbeheerde reguleringsmodel gevolg sal word nie. Daar is egter wel aanduidings dat sommige regerings begin om hul stemme dik te maak om hierdie reguleringsisteem ’n werklikheid te maak.[267]

Wanneer daar begryp word dat daar steeds baie konflik oor die regeringsbeheerde reguleringsisteem heers, word dit duidelik dat dit baie moeilik is om enige konkrete beginsels aangaande hierdie sisteem neer te lê. Al wat eintlik gesê kan word is dat sommige regerings van die dag van mening is dat hierdie roete gevolg moet word — en dat hulle die mag het om dit deur te voer.[268] Sekere aspekte hiervan word in hoofstuk 7 — wat oor kubersoewereiniteit handel — hanteer.

Wat egter in hierdie konteks genoem moet word is dat ten spyte daarvan dat die multi-belangegroepreguleringsmodel die meeste in die nuus is, die regeringsbeheerde reguleringsmodel geensins dood

266 15 van die verslag.

267 Hfst 7.

268 Lande soos Sjina, Brasilië, Suid-Afrika en Indië is groot ITU-ondersteuners. Balleste *Internet Governance* 51.

is nie. Tydens die WCIT-12-verrigtinge is die konflik tussen die multi-belangegroepreguleringsmodel en die regeringsbeheerde reguleringsmodel op die spits gedryf toe die ITU se nuwe regulasies aanvaar moes word. Die regeringsbeheerde reguleringsmodel is met 'n stemming van 89 teenoor 55 verkies.[269] Rusland se voorstel het sy standpunt baie duidelik verwoord:

> Member States shall have equal rights to manage the Internet, including in regard to the allotment, assignment and reclamation of Internet numbering, naming, addressing and identification resources and to support for the operation and development of the basic Internet infrastructure.[270]

Aan die begin van hierdie afdeling het die definisie van "intergovernmental" aangetoon dat die regeringsbeheerde reguleringsmodel veronderstel dat 'n internasionale organisasie gemeenskaplike Internet-belange kan reguleer. Uit verskeie bronne is dit duidelik dat die ITU poog om hierdie rolspeler te wees.[271] Dit was die ITU wat die eerste WSIS-proses begin het waar daar aanbevelings gemaak is om regerings meer magte te gee met Internetregulerings-aangeleenthede.[272] Dit was ook die ITU wat die WCIT-12-verrigtinge van stapel gestuur het, en waar die uiteindelike stemming daartoe gelei het dat die regeringsbeheerde reguleringsmodel as die voorkeurmodel aangewys is.[273] Indien so 'n model in werking gestel word, is die ITU inderdaad die organisasie om so 'n funksie te verrig. Soos hierbo genoem is daar egter nog geensins enige ooreenstemming oor hoe 'n finale regeringsbeheerde reguleringsisteem sou lyk nie. Dit is selfs moontlik dat state 'n meer "hands-on"-benadering volg, soos wat in hoofstuk 7 aangetoon word. Die verloop van tyd sal uiteindelik die antwoord verskaf.

---

269 Radu *The Evolution of Global Internet Governance* 13.

270 Radu *The Evolution of Global Internet Governance* 12.

271 Balleste *Internet Governance* 45; Yeo S "Book Review: Networks and States: The Global Politics of Internet Governance" (2011) *Journal of the American Society for Information Science and Technology* 1648; Zekos G I "Demolishing State's Sole Power Over Sovereignty and Territory Via Electronic Technology and Cyberspace" *Journal Of Internet Law* 3 5; Ibrahim Y "Global Governance and the Local Internet" 2007 *Linguistic and Cultural Online Communication Issues in the Global Age* 177 184; Hill R "The Internet, its Governance, and the Multi-stakeholder Model" 2014 *Info* 16 36.

272 Segura-Serrano A "Internet Regulation and the Role of International Law" 2006 *Max Planck Yearbook of United Nations Law* 192 193; Balleste *Internet Governance* 46.

273 Balleste *Internet Governance* 45.

Oor die algemeen word die regeringsbeheerde reguleringsmodel deur die privaat sektor en die burgerlike samelewing in twyfel getrek. Fidler noem byvoorbeeld dat die Internet ontwikkel het sonder enige Internasionaalregtelike reëls, en dat dit beter sal wees indien regerings nie te veel betrokke raak nie.[274] Vinton Cerf het opgemerk dat die WCIT-12-proses het die "potential to put government handcuffs on the Net".[275] Van Eeten en Mueller meen dat regeringsbeheer op die Internet is "myopic" — met ander woorde dat dit 'n engheid sal meebring wat Internetgroei onderdruk,[276] en King meen dat so 'n model enige invloed wat privaat individue op regulering sou kon uitoefen, geheel en al tot niet gemaak word.[277] In wese wil dit voorkom asof die enigste voorstanders van die regeringsbeheerde reguleringsisteem regerings sélf is.

King stel dit moontlik akkuraat wanneer hy sê:

> [T]he unavoidable truth [is] that once governments recognise the importance of an issue such as Internet governance, they inevitably wish to take control of it. Some form of intergovernmental coordination is inevitable.[278]

Regerings van die wêreld het inderdaad reeds kennis geneem van die belang van Internetregulering. Dit word volledig in hoofstukke 6 en 7 hieronder bespreek.

4.2.4.4 Samevatting

Moderne Internetreguleringsmodelle kan in twee kampe verdeel word. Aan die een kant is daar die multi-belangegroepreguleringsmodel, en aan die ander kant is daar die regeringsbeheerde reguleringsmodel.[279] Aanhangers

---

274 Fidler D P "Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations" 2013 *Insights* 1 1.

275 New York Times "Keep the Internet Open" http://www.nytimes.com/2012/05/25/opinion/keep-the-internet-open.html?_r=0 (besoek op 28 April 2016).

276 Van Eeten M J G en Mueller M L "Where is the Governance in Internet Governance?" 2012 *New Media and Society* 720 729.

277 King 2004 *Information and Communications Technology Law* 254.

278 King 2004 *Information and Communications Technology Law* 255.

279 Afd 4.2.4.

van die multi-belangegroepreguleringsmodel is hoofsaaklik die VSA en ICANN, sowel as meeste Europese-Unie-lande, terwyl state soos Sjina, Brasilië en Rusland die regeringsbeheerde reguleringsmodel voorstaan.[280]

Die multi-belangegroepreguleringsmodel bepaal dat 'n groot groep uiteenlopende entiteite — wat kan wissel van individue tot organisasies en state — almal as gelyke rolspelers saam kom om sake van gemeenskaplike belang te bespreek en om oplossings tot probleme te vind.[281] Hierdie tipe samewerking is relatief nuut in die Internasionaalregtelike sfeer, aangesien die Internasionale reg hom grotendeels besig hou met die regulering van verhoudings tussen state, en die privaat sektor vorm nie deel hiervan nie.[282]

Ten spyte van tien-jaar lange onderhandelings is die multi-belangegroepreguleringsmodel steeds onontwikkeld.[283]

Murray se konsep van 'n regulatoriese matriks is onder die loep geneem, en daar is aangetoon dat dit niks anders is as 'n visuele voorstelling van die multi-belangegroepreguleringsmodel nie.[284]

Die regeringsbeheerde reguleringsmodel is eenvoudig 'n model van regulering waar regerings van die wêreld die sentrale funksie van regulering verrig — gewoonlik deur die gebruikmaking van 'n internasionale organisasie wat sake van gemeenskaplike belang behartig.[285]

Die oorsprong van die regeringsbeheerde reguleringsmodel lê in die multi-belangegroepreguleringsmodel.[286] Tydens die WSIS-proses het dit geblyk dat regerings die prominente rol by die multi-belangegroepreguleringsmodel sou speel, maar hierdie gedagte het in latere jare in onguns verval soos wat gesprekke die aard van die multi-belangegroepreguleringsmodel probeer bepaal het.[287] Tog het regerings van

280 Afd 4.2.4.

281 Afd 4.2.4.1.

282 Afd 4.2.4.1.

283 Afd 4.2.4.1.

284 Afd 4.2.4.2.

285 Afd 4.2.4.3.

286 Afd 4.2.4.3.

287 Afd 4.2.4.3.

die dag nog nooit die gedagte van 'n regeringsbeheerde reguleringsmodel laat vaar nie.[288]

Die ITU het sedert die begin van die 21ste eeu 'n prominente rol gespeel in die bevordering van 'n regeringsbeheerde reguleringsmodel. Indien regerings van hierdie model gebruik maak en 'n internasionale organisasie gebruik om Internetregulering te behartig, sal die ITU waarskynlik die beste kandidaat wees om hierdie rol te vervul.[289]

Tot op hede is daar nog geen aanduiding van watter een van die twee reguleringsmodelle in die internasionale sfeer gebruik sal word nie.[290]

4.3 Gevolgtrekking

In hierdie hoofstuk is verskeie konsepte en modelle bespreek wat die regulering van die Internet onderlê. Daar is aangetoon dat die Internet anders as die fisiese wêreld is, in die mate dat die argitektuur van die Internet gemanipuleer kan word, terwyl dit grotendeels nie moontlik in die fisiese wêreld is nie.[291]

Die negentigerjare van die vorige eeu het tot 'n verskeidenheid opinies gelei oor wat die beste meganisme sou wees om die Internet te reguleer.[292] Sommige akademici het gemeen dat die Internet as 'n afsonderlike internasionale ruimte gereguleer moet word,[293] terwyl ander metodes soos selfregulering,[294] regulering deur 'n soewereine staat,[295] regulering deur multilaterale ooreenkomste[296] en regulering deur 'n internasionale

288 Afd 4.2.4.3.
289 Afd 4.2.4.3.
290 Afd 4.2.4.
291 Afd 4.2.1.
292 Afd 4.2.2.
293 Afd 4.2.2.1.
294 Afd 4.2.2.2.
295 Afd 4.2.2.2.2.
296 Afd 4.2.2.2.3.

organisasie[297] ook oorweeg is. Die gewildste vorm van regulering wat vir die Internet uitgewys is, is selfregulering.[298]

Met die ontwikkeling van sosiale media en -belangegroepe soos *Facebook* het die Internet 'n transformasie ondergaan, en het die gedagte van sosiale regulering gewild geword.[299] Sosiale gemeenskappe met gemeenskaplike belange gebruik selfregulering om hulle gemeenskappe te reguleer, en skep meganismes om hulle gemeenskap beter te laat funksioneer, soos byvoorbeeld betaalstelsels wat geskep word om ekonomiese gemeenskappe in staat te stel om met mekaar handel te dryf ten spyte daarvan dat hulle dalk op verskillende kontinente mag wees.[300]

Daar is ook in hierdie hoofstuk aangetoon dat regsbeginsels nie die enigste manier is waarop regulering kan geskied nie.[301] Dit kan ook geskied deur sosiale norme, markte, en argitektuur.[302] Daar bestaan 'n onderlinge verband tussen hierdie modaliteite, en een modaliteit wat meer gewig in 'n betrokke samelewing dra sal ander modaliteite se effektiwiteit ondermyn.[303] Lêerverspreiding in Japan is as voorbeeld voorgehou om hierdie fenomeen te illustreer.[304]

Tegniese regulering van die Internet is 'n baie effektiewe wyse van regulering, aangesien dit die onderliggende argitektuur van die Internet manipuleer om 'n sekere regulatoriese gevolg tot stand te bring.[305] 'n Krities belangrike konsep in hierdie verband is netwerk neutraliteit.[306] Dit behels dat data op 'n netwerk gelyk behandel moet word, en dat een soort data dus nie voorkeur bo 'n ander soort geniet nie.[307] Deur dit te

297 Afd 4.2.2.2.4.
298 Afd 4.2.2.2.5.
299 Afd 4.2.2.3.
300 Afd 4.2.2.3.
301 Afd 4.2.2.4.
302 Afd 4.2.2.4.2.
303 Afd 4.2.2.4.3.
304 Afd 4.2.2.4.4.
305 Afd 4.2.3
306 Afd 4.2.3.1.
307 Afd 4.2.3.1.

doen word gebruikers nie benadeel nie, en verseker dit die strukturele integriteit van die groter Internet.[308] Ongelukkig wil dit voorkom asof groot kommersiële rolspelers hierdie beginsel verontagsaam ten einde groter profyte te bewerkstellig.[309] Wu — die skepper van die term "netwerk neutraliteit" — voer aan dat elke netwerk eienaar moet begryp dat sy netwerk deel is van 'n groter netwerk, en dat 'n manipulering van die eienaar se netwerk tot die groter netwerk se nadeel kan lei. Dit sal uiteindelik tot die nadeel van die netwerk-eienaar ook wees.[310]

'n Basisbeginsel in netwerkbestuur is die konsep van "end-to-end".[311] Dit behels dat enige gespesialiseerde sagteware aan die einde van die netwerk geplaas moet word om die behoorlike funksionering van die hele netwerk te verseker.[312] Ongelukkig voldoen die moderne Internet nie aan hierdie vereistes nie, aangesien verskeie argitektuursveranderinge — soos die gebruik van dieppakketinspeksie — in die nodes van die Internet geplaas word. Hierdie is gespesialiseerde rekenaars, en verontagsaam die "end-to-end"-beginsel.[313] Dit kan potensieel ernstige negatiewe gevolge vir die groter Internet inhou.[314]

Ten slotte is moderne reguleringsteorieë bespreek.[315] Hierdie is meerendeels 'n politieke speelbal tussen twee groepe wat verskillende ideologieë voorstaan. Enersyds is daar state soos die VSA, met hulle skepping ICANN, asook die groter Europese Unie wat die multi-belangegroepreguleringsmodel voorstaan.[316] Andersyds is daar state soos Sjina, Rusland, Brasilië en Indië wat die regeringsbeheerde

308 Afd 4.2.3.1.
309 Afd 4.2.3.1.
310 Afd 4.2.3.1.
311 Afd 4.2.3.2.
312 Afd 4.2.3.2.
313 Afd 4.2.3.2.
314 Afd 4.2.3.2.
315 Afd 4.2.4.
316 Afd 4.2.4.1.

reguleringsmodel ondersteun.[317]

Die multi-belangegroepreguleringsmodel veronderstel dat verskillende rolspelers saam optree om regulering van die Internet te bewerkstellig.[318] Alle partye tree op as gelykes, ten spyte daarvan dat hulle uit verskeie groepe bestaan wat so uiteenlopend soos state, internasionale organisasies en individue kan wees.[319] Ten spyte van meer as tien jaar se onderhandelinge het die beginsels van die multi-belangegroepreguleringsmodel steeds nie uitgekristalliseer nie. Dit wil voorkom asof die belangrikheid van hierdie model daarin lê dat die regering van die VSA vasbeslote is om die IANA-funksie aan ’n multi-belangegroep oor te dra.[320]

Die regeringsbeheerde reguleringsmodel behels dat state van die wêreld die regulering van die Internet behartig.[321] Dit kan gestruktureer word op ’n verskeidenheid van wyses, soos om van ’n internasionale organisasie gebruik te maak om Internetsake van gemeenskaplike belang te bestuur,[322] of dit kan ook deur state self behartig word.[323] Die privaat sektor staan krities teenoor die regeringsbeheerde reguleringsmodel.[324]

Ongelukkig wil dit voorkom asof die moderne reguleringsmodelle vir die Internet nie bevredigende antwoorde lewer nie. Dit blyk uit die bespreking in hierdie hoofstuk dat die multi-belangegroepreguleringsmodel sowel as die regeringsbeheerde reguleringsmodel nie behoorlik gestruktureerde modelle vorm wat “checks and balances” inhou om verskillende rolspelers se magte te beperk nie. Dit het eerder in ’n politieke manipulering-spel ontaard wat uiteindelik nie goeie gevolge vir die groter Internet kan inhou nie.

***

317 Afd 4.2.4.3.

318 Afd 4.2.4.1.

319 Afd 4.2.4.1.

320 Afd 4.2.4.1.

321 Afd 4.2.4.3.

322 Afd 4.2.4.3.

323 Hfst 6 en 7.

324 Afd 4.2.4.3.

Die basisbeginsels van Internetregulering is nou neergelê. Dit is duidelik dat daar verskeie belangrike rolspelers is wat elkeen 'n funksie verrig om die Internet na wense te bestuur en te sorg dat dit effektief op internasionale vlak gereguleer word. Aan die een kant is daar verskeie prominente internasionale organisasies wat reguleringsfunksies uitoefen, en aan die ander kant is daar state van die wêreld wat hoofsaaklik deur wetgewing reguleringsbeleid deurvoer. In hoofstuk 5 sal die belangrikste nie-regeringsorganisasies wat Internetregulering verrig, geïdentifiseer en bespreek word. Daarna — in hoofstuk 6 — sal prominente state van die wêreld se reguleringspogings onder die vergrootglas geplaas word.

Hoofstuk 5

Nie-regeringreguleringrolspelers

> *It is now also increasingly acknowledged that effective business regulation is beyond the capacity of governments alone, and regulation requires the involvement of many other institutions.*[1]
>
> Peter Grabosky

5.1 Inleiding

DIE INTERNET IS reeds meer as vier dekades oud, en in hierdie tyd het vele reguleringsrolspelers gekom en gegaan. Verskillende fasette van die Internet is deur uiteenlopende groepe hanteer. Internetbaanbrekers het byvoorbeeld tegniese besluite oor argitektuur en netwerk-ontwikkeling geneem,[2] terwyl academici en organisasies soos die *Internet Engineering Task Force* (hierna IETF)[3] besluite oor die stel van standaarde uiteengesit het.

---

1 Grabosky P N en Smith R G "Telecommunications and Crime: Regulatory Dilemmas" 1997 *Law and Policy* 317 318.

2 Afd 2.3.

3 Afd 5.4.3.

In hoofstuk 4 is fundamentele beginsels bespreek wat die regulering van die Internet onderlê. In die volgende twee hoofstukke word daar verduidelik watter reguleringsrolspelers na vore getree het om die Internet te vorm soos dit vandag vertoon. Enersyds is daar internasionale organisasies en multinasionale maatskappye wat reeds sedert die vroegste jare van die Internet aan die werk is.[4] Andersyds is daar state wat besef het dat die Internet 'n krities belangrike hulpbron vir ekonomiese groei geword het, en dat dit gereguleer behoort te word.[5]

Hierdie hoofstuk word beperk tot internasionale nie-regeringsrolspelers wat die Internet help vorm het. Dit wissel van internasionale organisasies en nie-regeringsorganisasies tot multinasionale maatskappye.

Daar moet uit die staanspoor duidelik gemaak word dat hierdie rolspelers tydens die hele bestaan van die Internet aktief was. Nie-regeringsrolspelers was reeds hard aan die werk met die struktuur van die Internet nog voor regerings op die toneel verskyn het.[6] Eweneens is dit hierdie rolspelers wat steeds 'n fundamentele rol speel om die Internet deurlopend te vorm.

5.2 Internasionale Organisasies in die Internasionale Publiekreg

Internasionale organisasies as rolspelers in die Internasionale publiekreg is 'n relatief onlangse verskynsel. Wanneer definisies van die Internasionale reg van minder as twee eeue gelede bestudeer word, is die melding van internasionale organisasies nêrens te vinde nie. Reddie beskou byvoorbeeld in 1851 die Internasionale reg as "the collection of the rules, which regulate, or ought to regulate, the external intercourse, with each other, of separate,

4 Afd 5.3 en afd 5.4.

5 Afd 6.4.

6 Afd 2.3.

and independent states".[7] Net so definieer Wheaton in 1836 internasionale reg as:

> The law of nations, or international law, as understood among civilized, christian nations, may be defined as consisting of those rules of conduct which reason deduces, as consonant to justice, from the nature of the society existing among independent nations; with such definitions and modifications as may be established by general consent.[8]

Hierdie beskouing van die Internasionale reg is natuurlik te verstane vir die tydperk waarin dit geskryf is, aangesien die eerste internasionale organisasie wat werklik internasionaal van aard was, in 1865 eers geskep is.[9] Dit het 'n tydperk ingelui waar internasionale organisasies 'n groterwordende rol in die Internasionale reg begin speel het.

Die skepping van die Verenigde Nasies word allerweë as die uitnemendste voorbeeld van 'n internasionale organisasie beskou.[10] Dit is in 1945 gestig.[11] In 1949 het dit 'n opinie van die Internasionale Geregshof versoek om te bepaal wat die regstatus van die Verenigde Nasies is.[12] 'n Diplomaat is vermoor in sy hoedanigheid as VN-mediator, en die Verenigde nasies wou bepaal of dit in staat is om 'n staat te dagvaar vir skadevergoeding (en natuurlik 'n presedent te skep om toekomstige veiligheid van sy werknemers

---

7 Reddie J *Inquiries in International Law, Public and Private* (1851) 4.

8 Wheaton H *Elements of International Law: With a Sketch of the History of the Science* (1836) 46.

9 Wallace M J en Singer D "Intergovernmental Organization in the Global System, 1815–1964" 1970 *International Organization* 239 250 verskaf 'n lys van die oudste inter-regeringsorganisasies. Hiervolgens is die Internasionale Telekommunikasie Unie in 1865 gestig. Dit word egter nie as die oudste internasionale organisasie *per se* beskou nie, aangesien die "Central Commission for the Navigation of the Rhine" in 1815 reeds gestig is. Laasgenoemde was egter nie 'n *globale* inter-regeringsorganisasie nie, en hierdie posisie word aan die ITU toegedig.

10 Martens K *NGOs and the United Nations: Institutionalization, Professionalization and Adaptation* (2005) xiv noem byvoorbeeld: "And this even includes the United Nations (UN) system, the quintessential inter-governmental organization on the global level". Moore J A en Pubantz J *The New United Nations: International Organization in the Twenty-First Century* (2015) 2 is van soortgelyke mening: "The extensive UN System ... is the quintessential international organization of current times".

11 Die Verenigde Nasies is in 1945 gestig met die doel om 'n verdere wêreldoorlog te verhoed. Vyftig state het by die *United Nations Conference on International Organization,* wat tussen 25 April tot 26 Junie 1945 in San Francisco gehou is, besluit dat so 'n internasionale organisasie gestig moet word. Dit het op 24 Oktober 1945 amptelik tot stand gekom. Leonard B *Basic Facts about the United Nations* (1999) 3.

12 *Reparation for Injuries Suffered in the Service of the United Nations* International Court of Justice Reports 1949 174.

te verseker).[13] In die saak van *Reparation for Injuries Suffered in the Service of the United Nations*[14] het die Internasionale Geregshof aangedui dat die kern van die aansoek voor hom "relate to the 'capacity to bring an international claim'".[15] Die hof verduidelik dan:

> This capacity certainly belongs to the State; a State can bring an international claim against another State. Such a claim takes the form of a claim between two political entitities, equal in law, similar in form, and both the direct subjects of international law.[16]

Die hof verduidelik dan verder dat state van die wêreld die Verenigde Nasies tot stand gebring het.[17] Die organisasie se bevoegdhede kan slegs sover strek as dit wat state aan die organisasie toegedig het. Ongelukkig is die saak van regspersoonlikheid nie in die Verenigde Nasies se grondwet vervat nie, en die hof noem dat dit slegs die vraag na regspersoonlikheid sal kan antwoord as die karaktereienskappe beoordeel word wat state aan die Verenigde Nasies *wou laat toekom* om dit in staat te stel om sy mandaat te verrig.[18] Die hof kom vinnig tot die gevolgtrekking dat die Verenigde Nasies nie sy mandaat sal kan uitoefen as dit nie met regspersoonlikheid beklee word nie:

> But to achieve these ends the attribution of international personality is indispensable. The Charter has not been content to make the Organization created by it merely a centre 'for harmonizing the actions of nations in the attainment of these common ends' (Article 1, para. 3). It has equipped that centre with organs, and has given it special tasks. It has defined the position of the Members in relation to the Organization by requiring them to give it every assistance in any action undertaken by it (Article 2, para. 5), and to

13 *Reparation for Injuries Suffered in the Service of the United Nations* International Court of Justice Reports 1949 174 175 meld dat die opinie se doel was: "with a view to ensuring to its agents the fullest measure of protection in the future and ensuring that reparation be made for the injuries suffered".

14 *Reparation for Injuries Suffered in the Service of the United Nations* International Court of Justice Reports 1949 174.

15 177.

16 177-178.

17 178.

18 Die hof stel dit so op 178: "To answer this question, which is not settled by the actual terms of the Charter, we must consider what characteristics it was *intended* thereby to give to the Organization." My kursivering.

> accept and carry out the decisions of the Security Council; by authorizing the General Assembly to make recommendations to the Members; by giving the Organization legal capacity and privileges and immunities in the territory of each of its Members; and by providing for the conclusion of agreements between the Organization and its Members.[19]

Die hof maak dit dus baie duidelik dat die Verenigde Nasies 'n regspersoon moet wees om enigsins die rol wat dit gegee is in die Internasionale reg, uit te speel. Met hierdie uitspraak het die Internasionale Geregshof 'n nuwe era vir die Internasionale publiekreg ingelui. Die siening van akademici soos Reddie en Wheaton, wat 'n eeu vantevore aangedui het dat state die enigste rolspelers in die Internasionale publiekreg is, is nie meer van krag nie. In hierdie konteks is Lauterpacht se definisie van die Internasionale reg, wat in 1970 geformuleer is, baie insiggewend:

> International law is the body of rules of conduct, enforceable by external sanction, which confer rights and impose obligations primarily, *though not exclusively*, upon sovereign States and which owe their validity both to the consent of States as expressed in custom and treaties and to the fact of the existence of an international community of States *and individuals*. In that sense international law may be defined, more briefly (though perhaps less usefully), as the *law of the international community*.[20]

Let daarop hoe die klem verskuif het van state as die alleenrolspelers tot die Internasionale reg wat beskou word as 'n "internasionale gemeenskap". Sedert hierdie woorde geskryf is, het die rol van internasionale organisasies geweldig uitgebrei. Foltea verduidelik byvoorbeeld dat daar in 1909 slegs sewe-en-dertig internasionale organisasies was.[21] In 1956 was daar 132 sulke organisasies, en teen 1985 was daar reeds 378 internasionale organisasies.[22] Trouens, hierdie tipes organisasies het so geweldig uitgebrei dat daar in die moderne era onderskei word tussen twee soorte internasionale organisasies: die eerste is inter-regeringsorganisasies

19 178-179.

20 Lauterpacht H *International Law: Volume 1, The General Works: Being the Collected Papers of Hersch Lauterpacht* (1970) 9. My kursivering.

21 Foltea M *International Organizations in WTO Dispute Settlement: How Much Institutional Sensitivity?* (2012) 2 vn 8.

22 Foltea *International Organizations in WTO Dispute Settlement* 2 vn 8.

(IGOs), en die tweede is internasionale nie-regeringsorganisasies (INGOs).[23] Inter-regeringsorganisasies is die "tradisionele" vorm van internasionale organisasie, en dit korrespondeer met die term "internasionale organisasie" soos wat dit tot dusver in hierdie studie en hoofstuk gebruik is. Hierdie tipe organisasie het van 378 in getal in 1985 gedaal na ongeveer 251 in 1999.[24] Hierteenoor het die getal internasionale nie-regeringsorganisasies toegeneem na 'n verbysterende 27 000 in 2010.[25] Dit wil voorkom asof Lauterpacht met sy definisie van 'n "internasionale gemeenskap" dit waarlik korrek weergegee het.

In 1992 het die Verenigde Nasies 'n "Commission on Global Governance" tot stand gebring.[26] In 'n verslag word die term "global governance" soos volg gedefinieer:

> At the global level, governance has been viewed primarily as intergovernmental relationships, but it must now be understood as also involving non-governmental organizations (NGOs), citizens' movements, multinational corporations, and the global capital market. Interacting with these are global mass media of dramatically enlarged influence.[27]

Alhoewel die definisie handel oor "global governance", is die algemene trant van ontwikkeling baie duidelik: waar state eers die enigste rolspelers in die internasionale sfeer was, het dit in die laaste eeu verskuif na state in samewerking met internasionale organisasies. In die eeu wat voorlê wil dit voorkom asof hierdie verskuiwing verder sal ontvou tot die insluiting van nóg rolspelers, te wete internasionale nie-regeringsrolspelers, multinasionale maatskappye, en moontlik selfs individue.

Die definisie wat hierbo deur die "Commission on Global Governance" voorgehou is, is uiteraard nie die meer algemene, konserwatiewe siening van die rolspelers in die Internasionale reg nie. Lederer kritiseer die

23 Archer C *International Organizations* (2014) 114.

24 Archer *International Organizations* 114.

25 Archer *International Organizations* 114.

26 Hierdie kommissie is intussen ontbind. Wikipedia "Commission on Global Governance" https://en.wikipedia.org/wiki/Commission_on_Global_Governance (besoek op 16 Mei 2016).

27 Archer *International Organizations* 150.

verslag as "wensdenkery",[28] en Harris het 'n bundel van nege artikels gepubliseer om die foute van hierdie verslag uit te wys.[29] Dit is daarom nodig om die beskrywing van 'n internasionale organisasie weer na suiwerder regsbeginsels te swaai.

Die Internasionale Regskommissie[30] definieer 'n internasionale organisasie soos volg:

> "International organization" means an organization established by a treaty or other instrument governed by international law and possessing its own international legal personality. International organizations may include as members, in addition to States, other entities.[31]

Hierdie definisie hanteer drie aangeleenthede wat by 'n internasionale organisasie aangetref moet word, te wete (a) dit moet in die lewe geroep word deur 'n verdrag of ander instrument; (b) dit behoort sy eie regspersoonlikheid te geniet, en (c) lede van die internasionale organisasie is hoofsaaklik state, alhoewel ander entiteite ook as lede aanvaar kan word.

1. **Met verwysing na die metode van ontstaan**

   Meeste internasionale organisasies word steeds deur verdrae geskep.[32] Hiervan is daar talle voorbeelde, soos die Verenigde Nasies[33]

---

28 Lederer M en Muller P *Criticizing Global Governance* (2005) 145.

29 Harris E E en Yunker J A (red) *Toward Genuine Global Governance: Critical Reactions to "Our Global Neighborhood"* (1999) 1.

30 Die Internasionale Regskommissie is kort na die ontstaan van die Verenigde Volke Organisasie (VVO) in die lewe geroep.

Op 11 Desember 1946 het die Algemene Vergadering van die VVO Resolusie 94 aanvaar waarin daar bepaal is dat 'n komitee van regskenners gevestig moet word om aanbevelings te maak aan die Verenigde Nasies oor die ontwikkeling van die internasionale reg en die kodifisering daarvan. Hierdie komitee het uit 17 lede bestaan.

Op 21 November 1947 het die Verenigde Nasies se Algemene Vergadering Resolusie 174 aanvaar wat die skepping van 'n Internasionale Regskommissie daargestel het ten einde aan die verpligtinge van die Handves te voldoen. Sien die Statuut van die Internasionale Regskommissie, Wood M "Statute of the International Law Commission" http://legal.un.org/avl/pdf/ha/silc/silc_e.pdf (besoek op 3 September 2014).

31 Konsep-artikel 2(a) van die "Draft Articles on the Responsibility of International Organizations" Report of the International Law Commission (2011) GAOR 66th Session, Supplement No 10 (A/66/10 en Addendum 1) Par 87.

32 Schermers H G en Blokker N M *International Institutional Law: Unity Within Diversity* (2011) 45.

33 Vn 11.

en die Afrika-unie.[34] Tóg word internasionale organisasies ook geskep deur ander internasionaalregtelike instrumente, soos resolusies wat by regeringskonferensie geneem word. Die beste voorbeeld hiervan is sekerlik die Organisasie van Petroleum Uitvoerlande (OPEC).[35]

2. **Afsonderlike regspersoon**

   Die definisie hierbo bepaal dat 'n internasionale organisasie sy eie "international legal personality" moet hê. Hierdie vereiste is problematies, aangesien verskeie internasionale organisasies *nie* eie regspersoonlikheid beklee nie en steeds as internasionale organisasies beskou word. Brownlie meen dat die definisie van die Internasionale Regskommissie geformuleer is in die konteks van internasionale verantwoordelikheid, wat regspersoonlikheid veronderstel.[36] Dit beteken dan — volgens Brownlie — dat 'n organisasie as 'n internasionale organisasie beskou kan word indien dit deur 'n verdrag gestig is en 'n "interstaatlike funksie" verrig.[37] Die *Reparation for Injuries Suffered in the Service of the United Nations*-beslissing[38] van die Internasionale Geregshof bevestig hierdie siening.

3. **Samestelling**

   Die tradisionele siening van 'n internasionale organisasie is eintlik

---

34 Die Afrika-unie is die opvolger van die Organisasie vir Afrika-eenheid (OAE) wat reeds in 1963 gestig is. Die Afrika-unie is deur die Sirte-deklarasie van die OAE van September 1999 gestig, en het amptelik op 9 Julie 2002 tot stand gekom. Viljoen F *International Human Rights Law in Africa* (2012) 164; Wikipedia "History of the African Union" https://en.wikipedia.org/wiki/History_of_the_African_Union#Organisation_of_African_Unity (besoek op 15 Mei 2016).

35 Die Organisasie van Petroleum Uitvoerlande (OPEC) is in 1961 deur die Baghdad Konferensie gestig. Skeet I *Opec: Twenty-Five Years of Prices and Politics* (1991) 23.

36 Brownlie I en Crawford J *Brownlie's Principles of Public International Law* (2012) 167 se verduideliking is soos volg: "Whilst useful, this definition was developed in the context of international responsibility, which presupposes legal personality. It is possible for an international organization to have no such personality but still — by virtue of its treaty-based, interstate character and activity — be considered an international organization".

37 Brownlie *Brownlie's Principles of Public International Law* 167.

38 *Reparation for Injuries Suffered in the Service of the United Nations* International Court of Justice Reports 1949 174.

> maar 'n inter-regeringsorganisasie, soos die Verenigde Nasies sélf.[39] Dit is 'n tussenganger in regeringsonderhandelinge, word deur individuele state geskep en state is lede daarvan.[40] In die meerderheid van gevalle sal die internasionale organisasie dus state as lede hê, maar die definisie van die Internasionale Regskommissie maak ook voorsiening vir gevalle waar nie slegs state nie, maar ook ander entiteite lidmaatskap van 'n internasionale organisasie mag verkry. Die *Internet Governance Forum* is sekerlik 'n voorbeeld hiervan: lidmaatskap van hierdie organisasie is nie beperk tot state nie.[41] Die definisie van die Internasionale Regskommissie is egter so geformuleer dat dit die duidelike indruk skep dat 'n internasionale organisasie *ten minste* state as lede moet hê, maar dat lidmaatskap nie beperk is tot state nie. In hierdie geval is die voorbeeld van die Internasionale Telekommunikasie Unie moontlik gepas, aangesien dit state as lede het, maar internasionale organisasies mag lidmaatskap as waarnemers verkry.[42]

Wanneer hierdie drie vereistes vir 'n internasionale organisasie in ag geneem word, skep dit heelwat probleme wanneer Internet-rolspelers beskou word. Daar is vele kern-rolspelers in die Internet-arena wat tegnies nie volgens hierdie definisie as internasionale organisasies beskou sal kan word nie. Die voor-die-hand-liggendste voorbeeld hiervan is sekerlik die *Internet Corporation for Assigned Names and Numbers (*ICANN). Dit kan as die Internet se belangrikste internasionale rolspeler beskou word omdat dit die IANA-funksie verrig (waarsonder die Internet nie kan funksioneer nie).[43] Dit is egter nie deur enige verdrag in die lewe geroep nie, maar is eensydig

---

39 Moore *The New United Nations* 2 noem: "The extensive UN System ... is the quintessential international organization of current times.".

40 Artikel 2(i) van die Vienna Convention on the Law of Treaties between States and International Organizations or between International Organizations van 1986 definieer internasionale organisasie as "intergovernmental organization".

41 Afd 5.3.2.

42 Afd 5.3.3.

43 Afd 3.4.2 verskaf meer inligting oor die IANA-funksie.

deur die Amerikaanse regering gestig om die skyn te skep dat die IANA-funksie deur die internasionale gemeenskap beheer word.[44] Regerings van die wêreld het wél seggenskap in ICANN, maar dit is nie 'n internasionale organisasie in die konteks van die Internasionale reg nie.

Op dieselfde wyse bestaan daar ook ander organisasies wat belangrike funksies verrig om die Internet goed te laat funksioneer wat nie noodwendig aan die strenger vereistes van "internasionale organisasie" volgens die Internasionale reg voldoen nie (en wat hieronder bespreek word). Wat sou hulle status in die Internasionale reg wees? Dit is dan ook algemeen bekend dat meeste van hierdie organisasies en forums besluite neem en dikwels verklarings uitreik. Wat sou die status van sulke dokumente wees? Het dit enige regswaarde? Drake verklaar dit aan die hand van die "soft law"-beginsel in die Internasionale reg:

> Soft law instruments contain principles and norms rather than specific rules. It is usually found in international documents such as declarations, guidelines, and model laws.
>
> Why are some international documents considered to be soft law while others are not? For example, the Rio Declaration (1992) is soft law, but hundreds of other declarations adopted by the United Nations are not. The "legality" of soft law instruments is supported by the evidence that their norms are usually observed by many countries. Soft law could fall under the umbrella of Louis Henkin's statement that, "Almost all nations observe almost all of their obligations almost all of the time." When countries adopt a particular document, even if it is not legally binding, they express a certain commitment and moral obligation to observe it. The more negotiating energy put into reaching consensus and drafting a particular instrument, the more nation states are ready to support and observe such an instrument. This is one of the main elements that lead to the categorization of particular international documents as soft law.
>
> As we can see, the difference between hard and soft law is not binary. Moreover, some situations are *prima facie* paradoxical, where hard law conventions contain soft law rules and *vice versa.*[45]

Verskeie "soft law"-dokumente waarna Drake verwys, sal in die bespreking

---

44 Afd 3.4.2.

45 Drake W J *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance* (2005) 113.

wat volg, gevind word.[46] Die leser word versoek om Drake se beskouing in gedagte te hou wanneer sulke dokumente voorgehou word.

***

Om die globale beeld van Internetregulering te begryp, is dit nodig om te bepaal watter rolspelers aan die werk is, en watter funksie hulle verrig. Die belangrikste nie-regeringsrolspelers word vervolgens bespreek.

5.3 Internasionale Organisasies Geskep deur Verdrae

5.3.1 Inleiding

Die lys van organisasies wat volg is almal geskep deur internasionale verdrae, en kan dus as "internasionale organisasies" volgens die tradisionele siening van die internasionale reg beskou word.[47] 'n Studie wat Internetregulering binne die internasionale sfeer beskou, moet soms ook die politieke landskap waarbinne die gebeure afspeel, skets. Dit sal baie kortliks gedoen word waar nodig, aangesien die weglating daarvan nie die hele Internetreguleringsprentjie sal skets nie.

5.3.2 *Internet Governance Forum* (IGF)

5.3.2.1 Die IGF se Voorloper — WGIG

Gedurende die draai na die 21e eeu het state van die wêreld reeds besef dat Internetregulering op 'n globale vlak aandag behoort te kry.[48] Die Internet

46 Drake is nie die enigste skrywer wat hierdie standpunt oor "soft law" ten aansien van die Internet huldig nie. Maclean D F (red) *Internet Governance: A Grand Collaboration* (2004) 156 meld byvoorbeeld dat by Internasionale Internet-reg maak vele rolspelers gebruik van "'soft law' instruments such as declarations, recommendations, and guidelines. A soft law approach might frequently be appropriate in a rapidly changing environment like Internet governance, where 'hard' instruments like treaties can quickly be rendered problematic or obsolete".

47 Afd 5.2.

48 Afd 3.4.2.

was reeds 'n internasionale verskynsel wat 'n geweldige potensiaal vir wêreldwye ekonomiese groei ingehou het, en state het bekommerd geword dat hierdie bron alleen deur die VSA beheer word.[49] Die stigting van ICANN het hierdie vrese versterk, aangesien dit geblyk het dat die VSA nie van voorneme was om beheer oor die Internet te laat vaar nie.[50]Die Verenigde Nasies het deur gebruikmaking van die ITU besluit om in te gryp, en het besluit om 'n wêreldkonferensie te hou om hierdie saak op die spits te dryf. Die gevolg was die *World Summit on the Information Society* (hierna WSIS-I) wat in Desember 2003 in Genève gehou is.[51]

Die doel van die beraad was:

> to formulate a common Vision and understanding of the global information society" en "to harness the potential of knowledge and technology to promote the development goals of the Millennium Declaration.[52]

Een van die besprekingspunte was die wyse waarop die Internet bestuur behoort te word.[53] Tydens die WSIS-I is daar besluit dat die *Working Group on Internet Governance* (hierna WGIG) in die lewe geroep moes word.[54] Die taak van die WGIG was om globale Internetregulering op die been te kry, asook prosedures in plek te stel om hierdie doelwit te bereik.[55] Befondsing is van 'n verskeidenheid bronne gekry, soos die Switserse regering en die Foundation for Multimedia Communications.[56] Dit was ongekend in die konteks van die Verenigde Nasies, want nou het 'n multi-belangegroep soos die WGIG befondsing van ander multi-belangegroepe gekry, en nie net regerings, soos in die verlede nie.[57]

Die eerste WGIG-vergadering was in Genève van 20 tot 21 September

49 Mathiason J *Internet Governance: The New Frontier of Global Institutions* (2009) 53.

50 Mathiason *Internet Governance* 53.

51 Mathiason *Internet Governance* 97.

52 United Nations *General Assembly Resolution 56/183* (21 Desember 2001).

53 Mathiason *Internet Governance* 111.

54 Mathiason *Internet Governance* 111.

55 Mathiason *Internet Governance* 111.

56 Mathiason *Internet Governance* 116.

57 Mathiason *Internet Governance* 116.

2004. Die bywoningsyfer was indrukwekkend: 165 regeringsorganisasies, 52 inter-regeringsorganisasies, 44 nie-regeringsorganisasies en 19 besighede.[58] Die doel van die vergadering was bloot om te bepaal hoe die WGIG sal funksioneer, en watter belangegroepe op die vergaderings insette sal lewer.

Nadat die WGIG saamgestel is, was dit tyd om te begin werk aan 'n omvattende verslag om die toekoms van Internetregulering uit te stippel. Vier vergaderings is gehou[59] om die volgende vrae te beantwoord:

- wat is Internetregulering
- watter openbare beleidsake behoort hanteer te word binne die sfeer van Internetregulering, en
- watter roete moet in die toekoms ingeslaan word, met ander woorde wat sou besprekingspunte op die pad vorentoe kon wees.[60]

Die WGIG se finale verslag sou by die tweede *World Summit on the Information Society* in Tunisië in November 2005 voorgelê word. Die aanbevelings is in 'n vier-en-twintig bladsy-verslag vervat. Ten eerste is 'n definisie van Internetregulering uiteengesit:

> Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.[61]

Hieruit blyk dit duidelik dat die WGIG se beskouing van Internetregulering 'n multi-belangegroep in gedagte gehad het. Regerings, die privaat sektor, en die burgerlike samelewing het elkeen 'n rol te speel om die Internet behoorlik te reguleer.

---

58 Mathiason *Internet Governance* 116.

59 Die eerste vergadering was op 23–25 November 2004, die tweede op 14–18 Februarie 2005, die derde op 18–20 April 2005, en die finale ontmoeting van 14–17 Junie 2005. Mathiason *Internet Governance* 116–120. Sien ook die finale verslag van die WGIG, getiteld Anoniem "Report of the Working Group on Internet Governance 2005" http://www.wgig.org/docs/WGIGREPORT.pdf (besoek op 11 September 2014) par 3.

60 Mathiason *Internet Governance* 119 en Working Group on Internet Governance *Report of the Working Group on Internet Governance* (2005) par 5.

61 Working Group on Internet Governance *Report of the Working Group on Internet Governance* (2005) 4.

Verskeie beleidsake is deur die WGIG geïdentifiseer, soos die gebrek aan internasionale samewerking rakende kubermisdaad,[62] ongevraagde e-pos ("*spam*"),[63] en hoë internasionale interkonneksiekostes, veral in die derde wêreld.[64]

Wat betref die internasionale regulering van die Internet het die WGIG-verslag vier moontlike modelle voorgehou.[65] Ten eerste was daar die model van 'n *Global Internet Council (GIC)*, wat sou bestaan uit lede van regerings van die wêreld, en wat ICANN (en dus ook die VSA) se beheer oor die IANA-funksie sou oorneem.[66] Tweedens was daar die model dat géén oorsig nodig is nie,[67] en derdens was daar die model van 'n *International Internet Council*, wat sou bestaan uit state van die wêreld wat 'n leidende rol in die regulering van die IANA-funksie sou speel, en ander belangegroepe uit die privaat sektor en burgerlike samelewing wat in 'n adviserende hoedanigheid sou optree.[68] Vierdens het die WGIG 'n uitgebreide model van Internetregulering voorgestel waar die drie areas van Internet-beleidsbestuur, oorsig en globale koördinering op 'n samewerkingsbasis deur regerings, die privaat sektor en burgerlike gemeenskappe (*civil society*) hanteer kon word. Regerings van die dag sou verantwoordelik wees vir Internet-beleidsbestuur, die privaat sektor sou vir die oorsigfunksie verantwoordelik wees, en regerings, die privaat sektor en burgerlike gemeenskappe sou sáám vir globale koördinering verantwoordelik wees.[69]

Nodeloos om te sê was die VSA-regering glad nie te vinde vir hierdie modelle nie aangesien dit sy greep op die IANA-funksie sou laat los en in

62 Par 17 van die finale WGIG-verslag.

63 Par 18 van die finale WGIG-verslag.

64 Par 16 van die finale WGIG-verslag.

65 Par 52–71 van die finale WGIG-verslag.

66 Par 52–56 van die finale WGIG-verslag.

67 Par 57–61 van die finale WGIG-verslag.

68 Par 62–67 van die finale WGIG-verslag. Par 64 vorm die kern van hierdie model: "...the governmental component of the International Internet Council will take a leading role, with the private sector and civil society providing advice".

69 Par 68–70 van die finale WGIG-verslag.

die hande van ander regerings plaas.[70] ICANN was te vinde vir die tweede model van géén oorsig, aangesien dit hulle posisie sou verstewig.[71] Met die *World Summit on the Information Society II* (WSIS-II) voor die deur was dit duidelik dat daar nie sommer tot 'n vergelyk oor hierdie aangeleenthede gekom sou word nie. In 'n laaste poging tot bereddering van die saak het die voorsitter van die WGIG 'n voorstel gemaak dat 'n nuwe forum tot stand gebring word om die WGIG se bedrywighede voort te sit, en dat dit vir 'n tydperk van vyf jaar moet geld.[72] Hierdie gedagte van 'n *Internet Governance Forum* het byval gevind — veral vir die VSA — wat nog nie reg was om beheer oor die IANA-funksie te laat vaar nie.[73]

Die Agenda van die WSIS-II in Tunisië in 2005 het die amptelike voorstel vir die *Internet Governance Forum* vervat, en die samestelling daarvan is voorgehou as "The Internet Governance Forum, in its working and function, will be multilateral, multi-stakeholder, democratic and transparent."[74]

By die WSIS-II is die voorstel van die *Internet Governance Forum* amptelik aanvaar, en dit is gestig vir 'n tydperk van vyf jaar.[75]

5.3.2.2 Internet Governance Forum word Gevorm

Alhoewel dit nie so op sigwaarde mag voorkom nie, was die totstandkoming van die IGF 'n stukkie baanbrekerswerk binne die konteks van die Verenigde Nasies. Die hooffokus van die Verenigde Nasies was — en is steeds — die regulering van verhoudinge tussen state.[76] Met die totstandkoming van die

70 Mathiason *Internet Governance* 122.

71 Mathiason *Internet Governance* 122.

72 Sien Mueller M L *Networks and States: The Global Politics of Internet Governance* (2010) 108 vir meer inligting oor die verskillende state se onderhandelinge tydens die WSIS.

73 Mathiason *Internet Governance* 124.

74 World Summit on the Information Society "Tunis Agenda for the Information Society" http://www.itu.int/net/WSIS/docs2/tunis/off/6rev1.html (besoek op 11 September 2014) par 73.

75 Malcolm J *Multi-Stakeholder Governance and the Internet Governance Forum* (2008) 351.

76 Art 2 van die Handves van die Verenigde Nasies meld uitdruklik: "To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples...". United Nations Treaty Collection "Charter of the United Nations" https://treaties.un.org/doc/publication/ctc/uncharter.pdf (besoek op 17 Mei 2016).

IGF is daar aanvaar dat 'n multi-belangegroep gedien moet word, te wete state, nie-regeringsorganisasies, en burgerlike samelewing (*civil society*).[77] Waar state in die verlede bo-aan die hiërargie van belangegroepe was, was dit nie die geval met die IGF nie. Hier was alle rolspelers op dieselfde vlak.[78]

Aangesien die IGF — net soos die WGIG voor hom — nie volledige befondsing van die Verenigde Nasies ontvang het nie, is daar ná die WSIS besluit om die WGIG nét so in die IGF te omskep.[79] Die personeel van die WGIG is direk na die IGF verskuif.[80] Om die IGF op 'n gesonde finansiële voet te plaas, is daar befondsing uit verskeie oorde gekry.[81] Die multi-belangegroep-gedagte het ook by die befondsing gestalte gekry deurdat dit nie nét die regerings van Switserland, Nederland en Noorweë was wat fondse verskaf het nie, maar ook nie-regerings, soos ICANN, sommige Internetregistrateurs, en selfs privaatmaatskappye, soos Siemens en die Verizon-stigting.[82]

5.3.2.3 Doel van die IGF

Die IGF is bloot 'n forum vir gesprekvoering, en het geen mag om enige besluite te neem of af te dwing nie. Die inligtingsblad van die IGF stel dit so:

> The Internet Governance Forum (IGF) serves to bring people together from various stakeholder groups as equals, in discussions on public policy issues relating to the Internet. While there is no negotiated outcome, the IGF informs and inspires those with policy-making power in both the public and private sectors. At their annual meeting delegates discuss, exchange information and share good practices with each other.[83]

77 United Nations Treaty Collection "Charter of the United Nations" https://treaties.un.org/doc/publication/-ctc/uncharter.pdf (besoek op 17 Mei 2016).

78 Mathiason *Internet Governance* 127.

79 Mathiason *Internet Governance* 126.

80 Mathiason *Internet Governance* 127.

81 Mathiason *Internet Governance* 127.

82 Mathiason *Internet Governance* 127.

83 Internet Governance Forum "Internet Governance Forum Background Note Nairobi 27–30 September 2011" http://www.intgovforum.org/cms/2011/press/Backgrounder_What_is_IGF_final.doc (besoek op 3 September 2014).

Dus, alhoewel die IGF as een van die Internet se belangrikste reguleringsorgane beskou word, is dit eintlik maar bloot 'n forum wat gespreksvoering oor reguleringskwessies op die Internet genereer. So 'n posisie is geensins ideaal nie, aangesien dit baie moeilik is om enige vooruitgang ten opsigte van Internetregulering te maak indien enige van die rolspelers huiwerig is om aanbevelings van die IGF te aanvaar.[84]

5.3.2.4 Vergaderings van die IGF

Die IGF het sedert 2006 jaarliks vergader om aspekte van Internetregulering te bespreek. Die verskillende vergaderings tot op hede sal kortliks bespreek word, aangesien dit 'n sinvolle bydrae lewer oor hoe die IGF en Internetreguleringskwessies sedertdien die laaste agt jaar ontwikkel het.

IGF I: Athene, Griekeland, 2006 Die eerste vergadering van die IGF is in Oktober 2006 in Griekeland gehou.[85] Uit die staanspoor was dit duidelik dat die IGF nie die tradisionele Verenigde Nasies-protokol sou volg nie. Mathiason verduidelik:

> The plenary sessions had a common, and somewhat unusual, format. For each session there was a panel of up to 10 experts, drawn from all of the stakeholder groups. Rather than the usual format at the UN of having each panelist make a presentation, the sessions were moderated by media professionals who used the format of a television program in which the moderator tries to maintain a flow of discussion by calling on different panelists, allowing them to cross-comment, and inviting the audience to join in the debate.[86]

Benewens die volle vergaderings was daar ook 36 werkswinkels wat 'n verskeidenheid aangeleenthede bespreek het. Die gedagte was dat rolspelers wat saamstem oor sake, sogenaamde "dynamic coalitions" sou stig.[87] Dit sou dan terugvoering na die volle vergadering makliker maak.

---

84 Franklin M I *Digital Dilemmas: Power, Resistance, and the Internet* (2013) 152 noem byvoorbeeld: "While it may not be more than a paper tiger, a 'talk-shop' to its detractors, the Internet Governance Forum is, like the internet itself, in a state of flux".

85 Mathiason *Internet Governance* 132.

86 Mathiason *Internet Governance* 132.

87 Mathiason *Internet Governance* 133.

Trouens, dit wil voorkom asof die vorming van "dynamic coalitions" die mees tasbare uitkoms by die eerste IGF-vergadering was.[88] Volgens die IGF behoort dinamiese koalisies nie werkswinkels te wees nie, maar eerder aksie-georiënteerde *fora* waar 'n breë groep persone hulle kundigheid kan gebruik om die gespreksvoering meer sinvol te maak.[89]

Malcolm is van mening dat "dynamic coalitions" geensins 'n sinvolle wyse is om enige regulatoriese ingrepe teweeg te bring nie.[90] Enersyds bestaan daar geen wyse vir die IGF om te bepaal of reeds gevormde "dynamic coalitions" demokraties en van 'n multi-belangegroep bly nie, en andersyds bestaan daar geen formele proses waarvolgens "dynamic coalitions" hul insette aan die groter IGF kan lewer nie.[91]

Geen formele aanbevelings is tydens die IGF I in Athene gemaak nie. Daar was bloot twee sessies aan die einde van die vergadering wat die verrigtinge van die vorige paar dae saamgevat het.[92]

IGF II: Rio de Janeiro, Brazilië 2007 Tydens die tweede IGF-vergadering het die Verenigde Nasies se hoofsekretaris, M Ban Ki Moon, deur 'n afgevaardigde laat blyk dat hy graag sou wou hê dat die IGF ontwikkel in 'n forum wat geleenthede op die Internet kan vergroot, asook geleenthede skep vir alle volke en nasies.[93] Dit is uiteraard wat die IGF die heel tyd

---

88 Kleinwächter W (red) *The Power of Ideas: Internet Governance in a Global Multi-stakeholder Environment* (2007) 10 en 79; Padovani C en Pavan E *Diversity Reconsidered in a Global Multi-stakeholder Environment: Insights From the Online World"* in Kleinwächter *The Power of Ideas* (2007) 99–109, en veral 102–105. Volgens Wikipedia is "The most tangible result of the first IGF in Athens was the establishment of a number of so-called Dynamic Coalitions. These coalitions are relatively informal, issue-specific groups consisting of stakeholders that are interested in the particular issue." Wikipedia "Internet Governance Forum" http://en.wikipedia.org/wiki/Internet_Governance_Forum (besoek op 11 September 2014). Sien ook laasgenoemde vir voorbeelde van dinamiese koalisies wat steeds bestaan.

89 Weber R H *Shaping Internet Governance: Regulatory Challenges* (2010) 70. Gutterman meen dat: "Meetings of Dynamic Coalition should not be workshops. They should be action oriented and make an effort to ensure that a broad range of stakeholders can bring their expertise to the discussions". Gutterman B "IGF 2010 — Developing the Future Together" http://www.intgovforum.org/cms/documents/publications/175-developing-the-future-together/file (besoek op 11 September 2014) 11.

90 Malcolm *Multi-Stakeholder Governance and the Internet Governance Forum* 459.

91 Malcolm *Multi-Stakeholder Governance and the Internet Governance Forum* 459.

92 Mathiason *Internet Governance* 134.

93 Chairman's Summary *Second Meeting of the Internet Governance Forum* (2007) 1.

nastreef.

Verskeie aangeleenthede is tydens hierdie vergadering bespreek, soos:

- diversiteit — veeltaligheid van die Internet sou meer mense toegang daartoe gee;[94]
- sekuriteit — kubermisdaad en kuberterrorisme is 'n globale probleem wat globale antwoorde nodig het. Die vergadering het versoek dat internasionale samewerking 'n groter prioriteit moet wees.[95]
- oop standaarde — te veel regerings gebruik sagteware van kommersiële maatskappye. Dit veroorsaak dat regeringsdokumente nie op oop standaarde gebaseer is nie. Die gebruik van sagteware wat oop standaarde bevorder, behoort deur regerings oorweeg te word.[96]

Een van die kernpunte wat tydens dié vergadering aanvaar is, is dat die multi-belangegroepreguleringsmodel ("multi-stakeholder model") van Internetregulering die een is wat nagevolg behoort te word.[97]

IGF III: Hyderabad, Indië 2008 Die tema van hierdie vergadering was "Internet for All".[98] Meeste van die sake wat tydens die vorige IGF in Rio de Janeiro bespreek is, is weer eens opgehaal, soos die veeltaligheid van die Internet,[99] sekuriteit en kubermisdaad.[100] Die belangrike saak van die verskuiwing van IPv4 na IPv6 is bespreek, aangesien die geweldige uitbreiding van die Internet meegebring het dat IPv4 adresse nie meer beskikbaar was nie.[101] Interessant genoeg het die IGF sélf erken dat die privaat sektor die IPv4 na IPv6 aangeleentheid bestuur het, aangesien dit 'n kwessie was wat opgelos moet word om die suksesvolle werking van die

94 Kurbalija J *An Introduction to Internet Governance* (2012) 27.

95 Kurbalija *An Introduction to Internet Governance* 27.

96 Kurbalija *An Introduction to Internet Governance* 27.

97 Mathiason *Internet Governance* 140.

98 Chairman's Summary *Third Meeting of the Internet Governance Forum* (2008) 1.

99 Chairman's Summary *Third Meeting of the Internet Governance Forum* 3.

100 Chairman's Summary *Third Meeting of the Internet Governance Forum* 6.

101 Chairman's Summary *Third Meeting of the Internet Governance Forum* 11–16.

Internet te verseker.[102] Hierdie is 'n sprekende voorbeeld van hoe die IGF as 'n globale beleidmaker in die sfeer van die Internet beskou word, maar tog geen uitvoering van enige beleid kan magtig nie.

IGF IV: Sharm El Sheikh, Egipte 2009 Tydens die vierde vergadering van die IGF is twee verslae voorberei. Die eerste verslag het die IGF se jaarverslag vervat, terwyl die tweede verslag gehandel het oor die verlenging van die IGF se mandaat.[103] Soos hierbo uiteengesit[104] het die WSIS aangedui dat die IGF vir vyf jaar sou voortbestaan, en indien dit suksesvol sou wees, kon 'n verdere vyfjaar-verlenging deur die Verenigde Nasies toegestaan word. In die verslag oor die voortbestaan van die IGF was meeste rolspelers ten gunste daarvan.[105] Sommige kommentators het gemeen dat:

> a "tremendous positive change" was noted to have taken place among stakeholders since 2005. Topics that had caused a complete gridlock in the dialogue then were since being discussed in a "calm and matter-of-fact way".[106]

Ander kommentators het egter gemeen dat die IGF geen impak in sy bestaan gemaak het nie, "except that the proceedings are observed with a sense of curiosity by those who have the powers to cause changes to the fabric of the Internet",[107] en dat werklike Internetbeleid elders sonder enige insette van die IGF gemaak word.[108]

---

102 "The view was held that there was no need to impose a deadline to forestall the inevitable, because the market was dictating the IPv6 deployment." Chairman's Summary *Third Meeting of the Internet Governance Forum* 11.

103 Internet Governance Forum "The IGF 2009 Meeting" http://www.intgovforum.org/cms/2009-igf-sharm-el-sheikh (besoek op 17 Mei 2016).

104 Afd 5.3.2.1.

105 "The view was expressed that the Forum had achieved real progress in meeting the objectives of the Tunis Agenda on greater involvement, especially by participants from developing countries." IGF Secretariat *The Internet Governance Forum on the Desirability of the Continuation of the Forum* (2009) par 20 5.

106 IGF Secretariat *The Internet Governance Forum on the Desirability of the Continuation of the Forum* par 42 8.

107 IGF Secretariat *The Internet Governance Forum on the Desirability of the Continuation of the Forum* par 43 8.

108 IGF Secretariat *The Internet Governance Forum on the Desirability of the Continuation of the Forum* par 43 8.

Wat die verslag van IGF-bedrywighede betref, is bekende onderwerpe soos sekuriteit, openheid en privaatheid bespreek. 'n Nuwe interessante aangeleentheid wat aangespreek is, was die ontwikkeling van die verskynsel van sosiale netwerke.[109] Veral jong mense het die konsep van sosiale netwerke vinnig aanvaar, en dit is juis hierdie persone wat nie bewus is van die gevaar van privaatheidskending nie — en dit is juis op sosiale netwerke dat privaatheid so maklik geskend kan word.[110] Weer eens is verskeie probleme binne die sfeer van sosiale netwerke uitgelig sonder om enige konkrete voorstelle tot die regulering daarvan te formuleer.[111]

IGF V: Vilnius, Lithuania 2010 Sekere onderwerpe het teen hierdie tyd 'n algemene verskynsel by IGF vergaderings geword. Die bestuur van kritiese Internet-hulpbronne, en spesifiek die IPv4 na IPv6 aangeleentheid is weer eens bespreek,[112] en so ook sekuriteit, openheid en privaatheid.[113] Daar is ook 'n groot gewag gemaak van die ontwikkeling van Internet-tegnologie in ontwikkelende lande, want dit het geblyk dat die ontwikkelde wêreld vinniger vooruitgang maak as die ontwikkelende wêreld, met ander woorde die digitale skeiding (*digital divide*) was besig om groter te word in plaas daarvan om te krimp.[114] Die ontwikkeling van sosiale netwerke, en die gebruik daarvan deur veral jongmense, is weer eens bespreek.[115]

'n Nuwe aangeleentheid wat tydens hierdie IGF-vergadering bespreek was, was die nuwe tegnologie van "cloud-computing", en hoe dit die Internet kan omvorm van 'n netwerk-gebaseerde infrastruktuur na 'n diensgedrewe netwerk, met ander woorde dat 'n gebruiker nou in staat is om sy lêers en sagteware in die *cloud* te plaas met die wete dat dit altyd beskikbaar sal wees.[116] Hierdie nuwe tegnologie is geloof, maar daar is terselfdertyd

109 Chairman's Summary *Fourth Meeting of the Internet Governance Forum* (2009) 7.

110 Chairman's Summary *Fourth Meeting of the Internet Governance Forum* 7.

111 Chairman's Summary *Fourth Meeting of the Internet Governance Forum* 8-9.

112 Chairman's Summary *Fifth Meeting of the Internet Governance Forum (Final Version)* 9.

113 Chairman's Summary *Fifth Meeting of the Internet Governance Forum (Final Version)* 5.

114 Chairman's Summary *Fifth Meeting of the Internet Governance Forum (Final Version)* 1.

115 Chairman's Summary *Fifth Meeting of the Internet Governance Forum (Final Version)* 6.

116 Chairman's Summary *Fifth Meeting of the Internet Governance Forum (Final Version)* 8.

gemaan dat *cloud computing* potensieël ernstige sekuriteitsrisiko's inhou.[117]

Die gebruiklike samevatting van die verrigtinge het gefokus op hoe die IGF in die voorafgaande vyf jaar van Athene tot Vilnius verander het. Daar is aangevoer dat:

> ...as the context of the Internet had changed, so had the discussion in the IGF. It was pointed out that the Internet had grown in the last five years and that the Internet of 2010 was not the same as the Internet in 2005. The IGF was seen as having grown alongside the Internet.[118]

Tog was daar ook nog steeds 'n groep wat gemeen het dat die IGF meer uitkomsgerig moet wees.[119] Daarteenoor het ander afgevaardigdes geargumenteer dat die gespreks-aard van die IGF júís sy sterkte was, aangesien daar nie die spanning van onderhandelinge was wat gewoonlik tydens Verenigde Nasies-vergaderings teenwoordig was nie.[120]

Die sluitingseremonie het gefokus op die multi-belangegroepregulerings-model, en die nodigheid dat hierdie model ook verder in die toekoms verstewig behoort te word.[121]

IGF VI: Nairobi, Kenia 2011 Die sesde vergadering van die IGF is vir die eerste keer op Afrika-bodem gehou. Dit was ook die sesde vergadering, wat beteken dat die IGF sy mandaat vir vyf jaar kon verleng (by die WSIS is die IGF aanvanklik vir vyf jaar belê, maar dit is na vurige debatvoering vir 'n verdere vyf jaar verleng).[122]

Tydens die openingstoesprake is die steun vir die multi-belangegroepreguleringsmodel wat by Vilnius bevestig is, weer opgehaal.[123] Volgens die IGF was dít die voorkeurmodel van Internetregulering.[124]

---

117 Chairman's Summary *Fifth Meeting of the Internet Governance Forum (Final Version)* 8.

118 Chairman's Summary *Fifth Meeting of the Internet Governance Forum (Final Version)* 9.

119 Chairman's Summary *Fifth Meeting of the Internet Governance Forum (Final Version)* 10.

120 Chairman's Summary *Fifth Meeting of the Internet Governance Forum (Final Version)* (2010) 10.

121 Chairman's Summary *Fifth Meeting of the Internet Governance Forum (Final Version)* (2010) 10–11.

122 Radu R, Chenou J en Weber R (red) *The Evolution of Global Internet Governance: Principles and Policies in the Making* (2014) 11.

123 Chair's Summary *Sixth Meeting of the Internet Governance Forum* (2011) 2.

124 Chair's Summary *Sixth Meeting of the Internet Governance Forum* 2.

Die gebruiklike agenda-items van toegang tot die Internet — veral vir die derde wêreld — was weer 'n besprekingspunt,[125] asook die aangeleentheid van sekuriteit, openheid en privaatheid.[126] Alhoewel laasgenoemde 'n langstaande agendapunt was, het dit in Nairobi nuwe lewe gekry omdat die sogenaamde Arabiese lente[127] gedurende die voorafgaande jaar plaasgevind het, en hierdie gebeure aangetoon het hoe broos die Internet kan wees.[128] Dit was 'n tydperk van ongekende menseregte-skendings in die konteks van die Internet.

IGF VII: Baku, Azerbaijan 2012 Tydens die sewende vergadering van die IGF het dit duidelik geword hoe sentraal die Internet in die moderne wêreld geword het. Slimfone het begin om 'n rol te speel om die Internet te verander van 'n hulpmiddel wat net met 'n rekenaar bereik kon word, tot iets wat deel van die daaglikse bestaan is.[129] Gebeure kort voor hierdie vergadering, soos die storm Sandy wat groot skade aan die oostelike deel van die VSA aangebring het, asook 'n aardskudding in Japan, het aangetoon hoe die Internet onmisbaar geword het om mense op te spoor, reddingstogte te reël, en huislose mense te huisves.[130]

Die Internet het as't ware die mens se hele bestaan binnegedring, en daarom het hierdie IGF-vergadering dit ook nodig geag om maniere te beoordeel waarop die Internet na die ontwikkelende wêreld — en veral Afrika — gebring kon word.[131] Kenia is as 'n voorbeeld uitgesonder waar die regering besondere sukses behaal het om Internet-penetrasie te verhoog.[132]

Soos gebruiklik by IGF-vergaderings was sekuriteit, openheid en privaatheid weer 'n staande punt op die agenda. Kommer is uitgespreek oor die ontwikkeling van 'n fenomeen genaamd *big data*, waar groot maatskappye

125 Chair's Summary *Sixth Meeting of the Internet Governance Forum* 4.

126 Chair's Summary *Sixth Meeting of the Internet Governance Forum* 9.

127 "Arab spring" in Engels. Vir 'n verduideliking van die gebeure van die Arabiese lente, sien afd 6.3.5.2.

128 Chair's Summary *Sixth Meeting of the Internet Governance Forum* 9–10.

129 Hajiyev Y *Seventh Meeting of the Internet Governance Forum* (2012) 14.

130 Hajiyev *Seventh Meeting of the Internet Governance Forum* 4.

131 Hajiyev *Seventh Meeting of the Internet Governance Forum* 11.

132 Hajiyev *Seventh Meeting of the Internet Governance Forum* 11.

soveel inligting oor individue begin insamel het dat individuele profiele van mense saamgestel kon word sonder hul medewete. Daar is ernstig gemaan teen hierdie verskynsel.[133]

Tydens die samevatting- en sluiting-sessies van die vergadering was die sinvolheid van die multi-belangegroepreguleringsmodel weer beklemtoon.[134]

IGF VIII: Bali, Indonesië 2013 Twee belangrike gebeure tydens die verloop van 2013 het die IGF-vergadering in Bali se agenda oorheers. Die eerste hiervan was 'n formele opinie wat die regering van Brasilië by die *World Telecommunications Policy Forum* (WTPF) in Mei 2013 voorgelê het. Laasgenoemde is 'n forum waar lede van die *International Telecommunications Union* (ITU) bymekaarkom om internasionale aangeleenthede rakende telekommunikasie te bespreek. Die opinie van Brasilië — wat 'n multi-belangegroepreguleringsmodel voorgehou het — is met teëkanting begroet omdat dit so laat in die besluitnemingsproses by die WTPF ingevoer is.[135] Dit was egter 'n handige verskoning, want die ITU en meeste van sy lidlande (veral die VSA) was nog nooit ten gunste van die multi-belangegroepreguleringsmodel nie.[136]

Die tweede gebeurtenis wat Bali se IGF-vergadering oorheers het, was die spioenasie-lekkasie van Edward Snowden. Hy het 'n wêreldwye Internetmoniteringsprogram blootgelê waar dit geblyk het dat 'n groep lande regoor die wêreld saamgespan het om 'n enorme multinasionale spioenasieprogram te bedryf.[137] Hierdie gebeurtenis het die Internet-

133 Hajiyev *Seventh Meeting of the Internet Governance Forum* 13–14.

134 "Representatives of the Internet and business communities emphasized the importance of the multi-stakeholder, bottom-up Internet governance model championed by the IGF to ensure that the Internet fairly advances social and economic development around the world." Hajiyev *Seventh Meeting of the Internet Governance Forum* 18.

135 Dickinson S "WTPF-13 Day 3: Brazil's Draft Opinion, Informally Known as Opinion 7" http://linguasynaptica.com/wtpf-13-part3/ (besoek op 7 September 2014); Ermert M "5th World Telecom Policy Forum — Stepping Stone to Changes in the Internet Governance Arena?" http://policyreview.info/articles/news/5th-world-telecom-policy-forum-%E2%80%93-stepping-stone-changes-internet-governance-arena/129 (besoek op 7 September 2014).

136 Afd 5.3.3.

137 Sien Farrell H en Finnemore M "The End of Hypocrisy: American Foreign Policy in the Age of Leaks"

gemeenskap onkant betrap, want een van die grootste rolspelers in die spioenasie was die VSA.[138]

Met hierdie gebeure as agtergrond was die gevoel van afgevaardigdes dat:

> ...governments should "practice what they preach" when talking about openness and transparency on the Internet. It was felt by many that we have seen trust in the Internet significantly eroded by recent events. This erosion of trust relates to government's role as protector of internationally recognized human rights and as stewards of the Internet policy processes.[139]

Dit is daarom nie vreemd nie dat die Bali-IGF vergadering grootliks gewy is aan die handhawing van menseregte op die Internet.[140] Die Raad van Europa het hieroor 'n voorlegging gemaak, en die IGF-koalisie van Internet-menseregte het selfs 'n konsep handves van menseregte voorgehou.[141] Die IGF-self was van mening dat regerings weer op die regte pad gestuur moet word, en dat daar 'n behoefte is "for an open multistakeholder discussion on how to find high-level principles which can guide governments in this sensitive policy area and re-establish trust".[142]

Ten spyte van al hierdie besprekingspunte, was die uitkoms van die IGF — soos in al die voorafgaande vergaderings — bloot 'n verslag van die voorsitter van die IGF.

IGF IX: Istanbul, Turkye 2014 Uit die voorsitter se verslag is dit duidelik dat die IGF-vergadering in Istanbul gepoog het om die IGF op 'n nuwe weg te plaas waar gesprekke in meer konkrete besluite kan uitloop.[143] Die dokument vertoon 'n glans en uiteensetting wat nie by enige vorige IGF-voorsittersverslag te vinde is nie. Daar is selfs 'n opskrif wat lui: "Why

2013 *Foreign Aff* airs 22 22 vir meer inligting oor die Snowden-spioenasieblootlegging.

138 Farrell 2013 *Foreign Aff* airs 22.

139 Chair's Summary *8th Meeting of the Internet Governance Forum* (2013) 4.

140 Chair's Summary *8th Meeting of the Internet Governance Forum* 8.

141 Chair's Summary *8th Meeting of the Internet Governance Forum* 8.

142 Chair's Summary *8th Meeting of the Internet Governance Forum* 22.

143 Chair's Summary *IGF 2014: Connecting Continents for Enhanced Multistakeholder Internet Governance* (2014) 1.

IGF 2014 is Different from Past IGFs".[144] Daar word ook aangedui dat die doel is om meer uitkomsgebaseerde besluite te neem: "The ninth IGF aimed to actively link with other Internet governance processes ... by taking forward the suggested issues for further discussion and by improving its outcomes".[145]

Dit wil voorkom asof die opgewondenheid gespruit het uit die VSA-regering se aankondiging vroeër in 2014 dat dit uiteindelik die IANA-funksie gaan afwentel. (Hierdie aankondiging is in besonderhede in afd 3.4.3 bespreek.). Die IGF-vergadering in Istanbul het 'n hele dag aan die IANA-oordrag afgestaan, en die verslag verduidelik dat: "the Internet Assigned Numbers Authority (IANA) stewardship transition were noted as signs that Internet governance had reached a pivotal moment in its development".[146] Dit wou dus voorkom asof Internetregulering — en spesifiek die IANA-funksie — uiteindelik tot uitvoering gebring sou word.

Die vergadering het ook 'n groot gewag gemaak daarvan dat vyf gespreksforums gekies sou word omdat dit "best practices" beoefen, en dat hierdie subforums as voorbeelde vir ander gespreksforums kon dien.[147] Aangeleenthede wat in vorige IGF-vergaderings aangespreek is, soos menseregte[148] en die verskaffing van Internetdienste aan die derde wêreld is weereens bespreek,[149] maar ander aangeleenthede wat krities vir die voortbestaan van die Internet is, soos netwerk neutraliteit, is in diepte bespreek.[150] Kortom, dit wil voorkom asof hierdie IGF-vergadering van so 'n

144 Chair's Summary *IGF 2014: Connecting Continents for Enhanced Multistakeholder Internet Governance* 7.

145 Chair's Summary *IGF 2014: Connecting Continents for Enhanced Multistakeholder Internet Governance* 7.

146 Chair's Summary *IGF 2014: Connecting Continents for Enhanced Multistakeholder Internet Governance* 18.

147 Chair's Summary *IGF 2014: Connecting Continents for Enhanced Multistakeholder Internet Governance* 2.

148 Chair's Summary *IGF 2014: Connecting Continents for Enhanced Multistakeholder Internet Governance* 10.

149 Chair's Summary *IGF 2014: Connecting Continents for Enhanced Multistakeholder Internet Governance* 11.

150 Chair's Summary *IGF 2014: Connecting Continents for Enhanced Multistakeholder Internet Governance*

aard is dat konkrete besluite hieruit kon voortvloei. Ongelukkig is daar geen teken dat dit gebeur het nie.

IGF X: João Pessoa, Brasilië 2015 Die IGF-vergadering in Brasilië het gepoog om dieselfde uitkomsgedrewe fokus te behou as wat daar in Turkye geheers het. Die voorsitter se verslag meld uitdruklik dat: "... the IGF community was united this year in its willingness to address complex issues and work towards concrete solutions".[151] Dit wil voorkom asof hierdie IGF-vergadering ten doel gehad het om die IGF so te omvorm dat besluite wel tot uitvoering gebring kon word, want verskeie hooggeplaaste persone by Internetregulering was aanwesig.[152] Twee hoof-fasiliteerders van die belangrike WSIS+10-vergadering (wat ten doel het om die WSIS-I en WSIS-II prosesse te beoordeel) was daar, en die Verenigde Nasies se spesiale rapporteur op die bevordering van menseregte het ook aan die vergadering deelgeneem.[153]

Onderwerpe wat bespreek is, het weer eens die oue en nuwe ingesluit. Menseregte is in besonderhede aangespreek, en daar is veral gepoog om te bepaal hoe Internet-tussengangers gebruik kan word om menseregte te beskerm.[154] 'n "Internet Bill of Rights" is voorgehou.[155] "Big data" is, net soos by die IGF-vergadering in Baku, weer bespreek.[156] Nuwe aangeleenthede wat onder die loep geneem is, is die "Internet of Things", en 'n nuwe program wat spesifiek ontwerp is om die jonger geslag by Internetregulerings-aangeleenthede te betrek, is bekend gestel.[157]

Dit wil voorkom asof die voorsitter van mening was dat die uitkoms by die IGF-vergadering in Brasilië was dat skakeling tussen verskeie rolspelers versterk is: "The IGF once again served as a nexus for UN agencies,

10.

151 Chair's Summary *The 10th Internet Governance Forum* (2015) 3.

152 Chair's Summary *The 10th Internet Governance Forum* 4.

153 Chair's Summary *The 10th Internet Governance Forum* 4.

154 Chair's Summary *The 10th Internet Governance Forum* 5.

155 Chair's Summary *The 10th Internet Governance Forum* 5.

156 Chair's Summary *The 10th Internet Governance Forum* 5.

157 Chair's Summary *The 10th Internet Governance Forum* 5.

intergovernmental organizations and major institutions tackling challenges related to Internet public policy".[158] Dit wil voorkom asof gesprekke ook meer gemoedelik was, en onderlinge samewerking bevorder het: "As the IGF has matured, issues ... are now approached at a more practical level in main sessions and in both technical and non-technical workshops. Discussions have turned to focus more on sharing information and enhancing mutual education".[159]

Om een of ander konkrete bewys te lewer dat dit wat tydens die vergadering bespreek is, nie tevergeefs is nie, het die voorsitter aangedui dat sy verslag, asook verskeie geskrewe insette wat tydens die vergadering gemaak is, aan verskillende Verenigde Nasies-agentskappe gestuur sal word met die versoek dat dit wyer versprei word vir kennisname deur meer Internetreguleringsrolspelers.[160]

5.3.2.5 Die IGF in Perspektief

Wanneer die IGF in sy geheel beskou word, word dit duidelik dat hierdie organisasie nie werklik die dinamiese organisasie is wat reguleringsbeleid op die Internet bevorder nie. Dit is bloot 'n gespreksforum waar Internet-regulering bespreek word sonder om enige daadwerklike bydrae te maak. Zittrain noem dit dan ook bloot 'n "talk-shop initiative" wat slegs "bland consensus pronouncements" maak en nie tot die "nuts and bolts" uitkom om werklike verskille teweeg te bring nie.[161]

---

158 Chair's Summary *The 10th Internet Governance Forum* 4.

159 Chair's Summary *The 10th Internet Governance Forum* 4.

160 Die voorsitter se verslag stel dit so:

> This year's 'Policy Options for Connecting the Next Billion' process produced a tangible and community-driven, bottom-up IGF output. The compilation output document and the comprehensive collection of inputs and contributions to the process, available on the IGF website, will be forwarded to other related processes such as the UNGA 2nd Committee through UNDESA, the ITU Council and UNESCO through council meetings, and these agencies will be encouraged to disseminate this information as widely as possible to make public officials aware of the work.

Chair's Summary *The 10th Internet Governance Forum* 5.

161 Zittrain J *The Future of the Internet — And How to Stop It.* (2008) 242:

Van Eeten en Mueller is ewe krities op die IGF:

> The IGF has produced no collective resolutions, let alone binding agreements or decisions, and even if it did, these would have had no commitment power over the actors actually operating the Internet. More importantly, most of the stakeholders with actual control over Internet resources are not participating in the IGF.[162]

Volgens Mueller en Wagner is die doel van die IGF bloot om die voorstanders van die multi-belangegroepreguleringsmodel te anker in 'n internasionale organisasie waar hulle dié model kan promoveer en uitbou.[163]

Alhoewel die IGF 'n Verenigde Nasies-orgaan is, blyk dit dat hierdie forum nie die internasionale reguleringsrolspeler is wat dit voorgee om te wees nie. Daar sal dus verder gesoek moet word na rolspelers wat hierdie funksie effektief kan verrig. Die *International Telecommunications Union*, wat gestig is voordat die Internet eens bestaan het, blyk 'n moontlike kandidaat te wees, en sal vervolgens bespreek word.

5.3.3 Internasionale Telekommunikasie Unie

5.3.3.1 Inleiding

Die Internasionale Telekommunikasie Unie (hierna ITU) is die oudste internasionale organisasie in die wêreld.[164] Dit is in 1865 gestig as die

> The traditional approaches lead us in the direction of intergovernmental organizations and diplomatically styled talk-shop initiatives like the World Summit on the Information Society and its successor, the Internet Governance Forum, where "stakeholders" gather to express their views about Internet governance, which is now more fashionably known as "the creation of multi-stakeholder regimes" .... Their solution for the difficulties of individual state enforcement on the Net is a kind of negotiated intellectual harmony among participants at a self-concious summit ... at an endlessly long table.

162 Van Eeten M J G en Mueller M L "Where is the Governance in Internet Governance?" 2012 *New Media and Society* 720 728.

163 Mueller 2014 *Internet Policy Observatory* 8.

164 Codding G "The International Telecommunications Union: 130 Years of Telecommunications Regulation" 1994 *Denver Journal of International Law and Policy* 501 501. Sien vn 9 hierbo waar hierdie stelling in konteks geplaas word.

International Telegraph Union,[165] maar die naam is in Januarie 1934 verander na die "International Telecommunications Union".[166] In 1947 is dit as spesiale agentskap onder die vaandel van die nuutgestigte Verenigde Nasies ingeskuif.[167]

Die ITU is 'n indrukwekkende organisasie wat al reuse vordering in sy bestaan gemaak het. Na die tweede wêreldoorlog was radio-frekwensies in 'n chaotiese toestand omdat elke land sy eie sisteem tydens die oorlogsjare bedryf het. Dit was die ITU se taak om radio-frekewensiespektrums weer te orden, en dié organisasie het die taak met besondere onderskeiding deurgevoer.[168]

Die ITU se lidmaatskap bestaan uit regerings, en ál die state van die wêreld het lidmaatskap by die ITU verkry.[169] Privaat-entiteite soos maatskappye mag ook lidmaatskap verkry, maar hierdie "sektor-lede"[170] het nie stemreg by ITU-vergaderings nie.[171] Besluite word geneem by gevolmagtigde vergaderings, wat elke vier jaar gehou word.[172] Die ITU het

---

165 Die "International Telegraph Conference" van 1865 wat in Parys, Frankryk gehou is, het die ITU gestig. Codding 1994 *Denver Journal of International Law and Policy* 502.

166 Codding 1994 *Denver Journal of International Law and Policy* 501.

167 Codding 1994 *Denver Journal of International Law and Policy* 504.

168 Codding 1994 *Denver Journal of International Law and Policy* 504.

169 Daar is 193 lidlande van die ITU, waarvan 192 Verenigde Nasies-lidlande is. Palau is die enigste land wat nie 'n lid van die ITU is nie. Wikipedia "International Telecommunication Union" http://en.wikipedia.org/wiki/International_Telecommunication_Union#Membership (besoek op 22 Mei 2014); International Telecommunications Union "List of Member States" https://www.itu.int/online/mm/scripts/gensel8 (besoek op 22 Mei 2014).

170 Gutterman B "IGF 2010 — Developing the Future Together: The Fifth Meeting of the Internet Governance Forum Vilnius Lithuania 14–17 September 2010" http://www.intgovforum.org/cms/documents/publications/175-developing-the-future-together/file (besoek op 3 September 2014) 77.

171 McPhail T L *Global Communication: Theories, Stakeholders, and Trends* (2011) 115 meld dat 'n "ongemaklike" nuwe tendens by ITU-vergaderings is dat privaatmaatskappye die meeste tegniese insette lewer, maar steeds geen stemreg het nie: "The current situation in the ITU is becoming awkward, with the private sector members estimated to provide over 90 percent of the intellectual and technical contribution that underpin ITU's recommendations and technical standards. This new reality needs to be dealt with in order for ITU to retain its global technical decision-making role".

172 "Plenipotentiary meeting" in Engels. US Department of Commerce *Addressing the Challenges of International Bribery and Fair Competition 2001* (2001) 96. Sien ook International Telecommunications Union "Brief Guide to ITU Conferences, Assemblies and Events" https://www.itu.int/en/history/Documents/GuideToConferencesAssembliesEvents.pdf (besoek op 3 September 2014) vir meer inligting oor die besluitnemingsvermoëns by gevolmagtigde vergaderings.

ook 'n eie interne gespreksforum, te wete die "World Telecommunication Policy Forum" (WTPF),[173] en bied ook 'n eie "World Conference on International Telecommunications" (WCIT) aan.[174]

5.3.3.2 Die ITU en die Internet

Die ITU se belangstelling in die Internet het reeds begin toe Jon Postel en die NSI saam die IANA-funksie verrig het.[175] In hierdie tyd was die registrasie van domeinname uiters gewild, en die Internet het so uitgebrei dat probleme met domeinname spoedig gevolg het.[176] Daar was veral twee kwessies wat uiters problematies was: die eerste was dat handelsmerk-eienaars ongelukkig was dat hulle handelsmerke se ooreenstemmende domeinname deur privaat-entiteite geregistreer word, en tweedens was dit duidelik dat die VSA se monopolie om domeinname internasionaal te registreer, onredelik was.[177] Om die probleem te beredder, is 'n "International Ad Hoc Committee" gevorm, en dié het met 'n uitstekende oplossing vorendag gekom: die probleme met handelsmerke kon deur die "World Intellectual Property Organization" (hierna WIPO) beredder word, en die ITU is genader om domeinnaamregistrateurs regoor die wêreld te reguleer.[178] Beide hierdie organisasies val binne die kader van die Verenigde Nasies, en regulering van die probleemkwessies sou deur internasionaal-erkende organisasies hanteer word.[179] Om daad by die woord te voeg, is

---

173 United Nations Publications *International Geneva Yearbook: Organization and Activities of International Institutions in Geneva, Volume 16; Volumes 2002-2003* (2002) 267 beskryf die WTPF so: "In 1996 ITU initiated the World Telecommunication Policy Forum (WTPF), an informal international gathering convened on an *ad hoc* basis to harmonize telecommunication policies on issues which extend beyond the domain of any single country".

174 Schiavone G *International Organizations* (2015) 179 noem dat 'n "World Conference on International Telecommunications" byeengeroep word op versoek vanuit 'n gevolmagtigde vergadering wanneer dit nodig blyk te wees: "World conferences on international telecommunications are held at the request of plenipotentiary conferences".

175 Afd 3.4 bespreek hierdie gebeure in besonderhede.

176 Mathiason *Internet Governance* 51.

177 Mathiason *Internet Governance* 52.

178 Mathiason *Internet Governance* 52.

179 Mathiason *Internet Governance* 52.

'n "Memorandum of Understanding" deur die ITU opgestel, en is dit in Mei 1997 deur 215 rolspelers van regoor die wêreld onderteken.[180] Dit was inderdaad 'n verteenwoordigende groep, met ondertekenaars vanuit alle kontinente.[181]

Die ITU se "Memorandum of Understanding" is nie goed deur die VSA-regering ontvang nie.[182] Daar is geargumenter dat dit die VSA se regulatoriese invloed ten aansien van die Internet ondermyn.[183] Gevolglik is die ITU se "Memorandum of Understanding" deur die VSA verwerp, en die proses wat in afdeling 3.4.1 tot afdeling 3.4.3 bespreek is waar die VSA-regering die beheer oor die IANA-funksie oorgeneem het, het afgespeel. Die gevolg was dat die VSA se beheer oor die Internet versterk is, terwyl die invloed van die ITU ten aansien van die Internet gekwyn het.

Die ITU het tydens sy 1998-gevolmagtigde vergadering die kwessie oor die regulering van die Internet aangespreek.[184] Dit is die eerste keer dat enige vorm van regulering van die Internet op 'n wêreld-verhoog aangespreek is.[185] Die gevolg was dat die ITU resolusie 73 aanvaar het wat die Verenigde Nasies versoek om 'n "World Conference on the Information Society" (hierna WSIS) te belê om te bepaal hoe regulering van die Internet moet geskied.[186]

---

180 Mathiason *Internet Governance* 52–53.

181 Mathiason *Internet Governance* 53 Tabel 4.2.

182 Mathiason *Internet Governance* 53.

183 Mathiason *Internet Governance* 53.

184 Brousseau E, Marzouki M en Méadel C *Governance, Regulation and Powers on the Internet* (2012) 372.

185 Brousseau *Governance, Regulation and Powers on the Internet* 372.

186 Brousseau *Governance, Regulation and Powers on the Internet* 372. Die resolusie versoek die sekretaris-generaal van die Verenigde Nasies om:

> To consider and decide on the Union's contribution to the holding of a world summit on the information society, with a view to:
>
> 1. establishing an overall framework identifying, with the contribution of all partners, a joint and harmonized understanding of the information society;
> 2. drawing up a strategic plan of action for concerted development of the information society by defining an agenda covering the objectives to be achieved and the resources to be mobilized;
> 3. identifying the roles of the various partners to ensure smooth coordination of the establishment in practice of the information society in all Member States.

Die gevolmagdigde vergadering van 1998 het Internetregulering in die soeklig geplaas, en dit is op die gevolmagtigde vergadering in 2002 verder uitgebrei.[187] Hierdie konferensie het spesifiek aandag gegee aan meganismes wat die ITU in werking kon stel om die "digital divide" te verklein, en Internetdienste op 'n globale vlak moontlik te maak.[188] Die ITU het aangedui dat sy versoek om die WSIS-I aan te bied, deur die Verenigde Nasies goedgekeur is, en het op grond hiervan aanvaar dat dit 'n leidende rol tydens die WSIS-I-proses[189] sou speel.[190]

Die ITU het grootliks sy doel met die WSIS-I-proses bereik.[191] Die uitkoms van die WSIS-I is in afdeling 4.2.4.3 bespreek. Die aanbevelings was dat 'n "multi-belangegroep" die Internet moes reguleer, en die finale WSIS-I-verslag het aangevoer dat state die hoofrol sou speel.[192] Dit was eers tydens latere konferensies dat die multi-belangegroepreguleringsmodel alle rolspelers op 'n gelyke speelvlak probeer plaas het,[193] en die regeringsbeheerde reguleringsmodel as 'n afsonderlike model beskou is.[194]

5.3.3.3 World Conference on International Telecommunications 2012

Een van die ITU se basiese funksies was nog altyd om internasionale telekommunikasie-regulasies (hierna ITR's), uit te vaardig.[195] Hierdie ITR's vorm internasionale verdrae wat lidlande onderteken en later ratifiseer en in hul eie nasionale wetgewing inkorporeer.[196] ITR's word slegs opgedateer indien dit nodig is. Die laaste ITR's dateer uit 1988, en dit het duidelik geword

International Telecommunications Union *Final Acts of the Plenipotentiary Conference (Minneapolis, 1998)* (1998) 224

187 Weber *Shaping Internet Governance* 41.

188 Weber *Shaping Internet Governance* 41.

189 Afd 3.4.2 en afd 4.2.4.3 bevat meer inligting oor die inhoud van die WSIS-konferensies.

190 Weber *Shaping Internet Governance* 41.

191 Information Gatekeepers Inc *Telecom Standards Monthly Newsletter October 2010* (2010) 6.

192 Afd 4.2.4.3 vn 258.

193 Afd 4.2.4.1.

194 Afd 4.2.4.3.

195 Radu *The Evolution of Global Internet Governance* 12.

196 Radu *The Evolution of Global Internet Governance* 12.

dat hierdie ITR's opgeadteer moet word, veral in die nuwe konteks van die Internet.[197] Die ITU het daarom besluit om 'n wêreldkonferensie te hou om die ITR's op te dateer, maar ook sommer op dieselfde tyd sy greep op die Internet te probeer verstewig. Daarom is daar in 2012 'n "World Conference on International Telecommunications" (hierna WCIT-12*)* in Dubai gehou.[198]

Die ITU het voorgehou dat die doel van die konferensie spesifiek was om die 1988-ITR's op te dateer, maar state van die wêreld was nie oortuig dat die ITU se motiewe suiwer was nie. Etlike weke voor die konferensie sou begin, het die Europese parlement gewaarsku dat die voorgestelde ITR's die ITU in staat sal stel om te veel beheer oor die Internet uit te oefen.[199] Die Europese parlement het selfs 'n resolusie deurgevoer wat spesifiek genoem het dat "as a consequence of some of the proposals presented, the ITU itself could become the ruling power of the internet", en dat "the ITU, or any other single, centralised international institution ... is not the appropriate body to assert regulatory authority over the internet".[200] Twee dae nadat die twee-weke-konferensie begin het, het die VSA-kongres 'n resolusie aanvaar om die WCIT-12 teë te staan.[201] Selfs Google het 'n Internet-petisie gereël om sy misnoeë mat die WCIT-12 duidelik te maak.[202]

Hierteenoor het sommige state, soos Sjina en Rusland, besluit om die WCIT-12 te gebruik om Internetbeleid te probeer deurvoer.[203] Een van

197 Radu *The Evolution of Global Internet Governance* 12.

198 *World Conference on International Telecommunications 2012*. Die webblad van hierdie konferensie is verkrygbaar by: International Telecommunications Union "World Conference on International Telecommunications (WCIT-12)" http://www.itu.int/en/wcit-12/Pages/default.aspx (besoek op 17 Mei 2016).

199 British Broadcasting Corporation "European Parliament Warns Against UN Internet Control" http://www.bbc.com/news/technology-20445637 (besoek op 18 Mei 2016).

200 European Parliament *Motion for a Resolution: To Wind up the Debate on Statements by the Council and the Commission Pursuant to Rule 110(2) of the Rules of Procedure on the forthcoming World Conference on International Telecommunications (WCIT-12) of the International Telecommunication Union, and the Possible Expansion of the Scope of International Telecommunication Regulations* (2012/2881(RSP)).

201 The Hill "House Approves Resolution to Keep Internet Control Out of UN Hands" http://thehill.com/blogs/floor-action/house/271153-house-approves-resolution-to-keep-internet-control-out-of-un-hands (besoek op 18 Mei 2016).

202 British Broadcasting Corporation "Google Attacks UN's Internet Treaty Conference" http://www.bbc.com/news/technology-20429625 (besoek op 18 Mei 2016).

203 Radu *The Evolution of Global Internet Governance* 39.

die sensitiefste aangeleenthede met betrekking tot Internetregulering bly die VSA se beheer oor die IANA-funksie. By die 2012 WCIT (WCIT12) het Rusland byvoorbeeld probeer om die volgende bepaling by die nuwe ITR's te inkorporeer:

> Member States shall have equal rights to manage the Internet, including in regard to the allotment, assignment and reclamation of Internet numbering, naming, addressing and identification resources and to support for the operation and development of the basic Internet infrastructure.[204]

Hierdie, en ander bepalings het nie goed by lande soos die VSA afgegaan nie.[205] Die VSA het spesifiek aangevoer dat die ITU nie by magte is om sulke ITR's te skep nie aangesien dit buite sy mandaat is, en dat sulke ITR's die multi-belangegroepreguleringsmodel sou ondermyn.[206]

Die gevolg van die WCIT-12-konferensie is dat die Internet-wêreld in twee kampe verdeel is[207] — aan die een kant was daar die VSA, wat spesifiek téén die nuwe ITR's gestem het om ICANN te beskerm en as regmatige beheerder van die IANA-funksie te probeer voorhou.[208] Aan die ander kant was daar state wat wou toesien dat die DNS-funksie in die internasionale sfeer geplaas word — state soos Rusland, Sjina, Brasilië en bykans al die derdewêreldlande.[209] Ná die WCIT-12 skryf die vooraanstaande tydskrif *The Economist* dat die Internet-wêreld nou in 'n "koue-oorlog"-era van Internetregulering inbeweeg het.[210]

---

204 Russian Federation "World Conference on International Telecommunications (WCIT-12) Dubai 3–14 December 2012 Proposals for the Work of the Conference" http://www.soumu.go.jp/main_content/000188224.pdf (besoek op 4 September 2014) art 31B asook Radu *The Evolution of Global Internet Governance* 12.

205 Radu *The Evolution of Global Internet Governance* 13.

206 Radu *The Evolution of Global Internet Governance* 13.

207 Radu *The Evolution of Global Internet Governance* 14 tabel 1.

208 Radu *The Evolution of Global Internet Governance* 43.

209 Radu *The Evolution of Global Internet Governance* 14.

210 Dubai L S "A Digital Cold War? The Economist 14 Dec 2012" http://www.economist.com/blogs/babbage/2012/12/internet-regulation (besoek op 26 Mei 2014).

5.3.3.4 Die ITU se 5de Wêreld-Telekommunikasie Beleidsforum

Die volgende botsing tussen die voorstanders van die multi-belange-groepreguleringsmodel (die VSA) en regeringsbeheerde reguleringsmodel (Rusland, Sjina, Brasilië en ander) het ses maande na die WCIT-12 by die ITU se forum, genaamd die *5th World Telecommunications Policy Forum*, (hierna WTPF) plaasgevind.[211] Die WTPF was "designed to be high-level international events where ITU Members from government, industry and the global regulatory community exchange views on the key policy and regulatory issues and challenges emerging from the rapidly evolving information and communication technology environment."[212] Die WTPF is slegs 'n gespreksforum van die ITU, en maak dus nie formele besluite nie, maar die bespreking by dié forum beïnvloed dikwels latere ITU-vergaderings waar daar wél formele besluite geneem word.

By die WTPF is daar ses opinies aanvaar.[213] Al ses hierdie opinies het oor die Internet gehandel. Die vyfde opinie, getiteld "Supporting Multi-stakeholderism in Internet Governance"[214] behoort verdere aandag te geniet aangesien die titel daarvan effens verwarrend kan wees.

Met die eerste oogopslag wil dit voorkom asof opinie 5 wat deur die

---

211 Greenway C "Outcome of the 2013 World Telecommunications and Information and Communication Technology Forum." 2013 *Australian Journal of Telecommunications and the Digital Economy* 14.1.

212 Greenway 2013 *Australian Journal of Telecommunications and the Digital Economy* 14.1.

213 Die ses opinies het almal oor Internet aangeleenthede gehandel. Hier volg die lys van die opinies:

"Opinion 1: Promoting Internet Exchange Points (IXPs) as a long term solution to advance connectivity

Opinion 2: Fostering an enabling environment for the greater growth and development of broadband connectivity

Opinion 3: Supporting Capacity Building for the deployment of IPv6

Opinion 4: In Support of IPv6 Adoption and Transition from IPv4

Opinion 5: Supporting Multi-stakeholderism in Internet Governance

Opinion 6: On supporting operationalising the Enhanced Cooperation Process"

International Communications Union "WTPF 2013: Final Opinions" http://www.itu.int/en/wtpf-13/Pages/opinions.aspx (besoek op 22 Mei 2014).

214 Hierdie opinie kan besigtig word by Anoniem "World Telecommunication/ICT Policy Forum 2013: OPINION 5: Supporting Multi-stakeholderism in Internet Governance" http://www.itu.int/en/wtpf-13/Documents/WTPF-13-Opinion5.pdf. (besoek op 27 Mei 2014).

WTPF aanvaar is, 'n multi-belangegroepreguleringsmodel voorstaan, maar dit is nie die geval nie. Die opinie bepaal uitdruklik dat beleidsbesluite aangaande die Internet binne die soewereine reg van nasies val.[215] Daar word spesifiek gesê dat hierdie besluitnemingsvermoë oor Internetbeleid 'n staat se *reg* is.[216] Die privaat sektor word hierna geskets as rolspelers in die ontwikkeling van die Internet,[217] en die burgerlike samelewing as rolspelers op gemeenskapsvlak.[218] Inter-regerings-organisasies se taak word beskou as 'n fasiliteringsrol om die openbare beleid wat state vasgestel het, uit te rol.[219] Die rol van internasionale organisasies is om tegniese standaarde vir die Internet te ontwikkel.[220]

Hierdie opinie staan dus eerder die regeringsbeheerde reguleringsmodel voor.[221] Dit is te verstane, aangesien die ITU steeds 'n organisasie is waar state die enigste groep is wat stemgeregtig is. Radu stel dit so:

> In other words (the ITU) decided to remain a single stakeholder organization that had no intention of transforming into a genuinely multistakeholder

215 Par b(i) bepaal uitdruklik dat: "Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues". Anoniem "Opinion 5: Supporting multi-stakeholderism in Internet Governance" Anoniem "World Telecommunication/ICT Policy Forum 2013: OPINION 5: Supporting Multi-stakeholderism in Internet Governance" http://www.itu.int/en/wtpf-13/Documents/WTPF-13-Opinion5.pdf. (besoek op 27 Mei 2014). 1.

216 Art 7.1 van die Internasionale Telekommunikasie Regulasies bepaal soos volg: "If a Member State exercises its *right* in accordance with the Constitution and the Convention to suspend international telecommunication services partially or totally, that Member State shall immediately notify the Secretary-General of the suspension and of the subsequent return to normal conditions by the most appropriate means of communication". My kursivering. International Telecommunications Union *Final Acts of the World Conference on International Telecommunications* (2012) 7.

217 Anoniem "World Telecommunication/ICT Policy Forum 2013: OPINION 5: Supporting Multi-stakeholderism in Internet Governance" http://www.itu.int/en/wtpf-13/Documents/WTPF-13-Opinion5.pdf. (besoek op 27 Mei 2014). b(ii) 1.

218 Anoniem "World Telecommunication/ICT Policy Forum 2013: OPINION 5: Supporting Multi-stakeholderism in Internet Governance" http://www.itu.int/en/wtpf-13/Documents/WTPF-13-Opinion5.pdf. (besoek op 27 Mei 2014). b(iii) 1.

219 Anoniem "World Telecommunication/ICT Policy Forum 2013: OPINION 5: Supporting Multi-stakeholderism in Internet Governance" http://www.itu.int/en/wtpf-13/Documents/WTPF-13-Opinion5.pdf. (besoek op 27 Mei 2014). b(iv) 1.

220 Anoniem "World Telecommunication/ICT Policy Forum 2013: OPINION 5: Supporting Multi-stakeholderism in Internet Governance" http://www.itu.int/en/wtpf-13/Documents/WTPF-13-Opinion5.pdf. (besoek op 27 Mei 2014). b(v) 1.

221 Afd 4.2.4.3 verduidelik hoe die regeringsbeheerde reguleringsmodel uit die multi-belangegroepreguleringsmodel (soos in die finale verslag van die WSIS-I vervat), ontwikkel het.

> organization. While the nations of the ITU may on occasion permit non-governmental actors to offer comments and may even let them sit at the same table from time to time, there is no manner in which non-governmental actors are allowed to participate on anything resembling equal footing.[222]

Wanneer opinie 5, wat uiteindelik deur die WTPF aanvaar is, van naderby beskou word, vertoon dit merkwaardige ooreenkomste met hoofstuk IV van die finale verslag van die WGIG: in laasgenoemde verslag word daar uitvoerig bepaal dat regerings, die privaat sektor, en die burgerlike samelewing verskillende rolle het om te vervul by Internetregulering.[223] Die rol van regerings word primêr beskou as oorhoofse reguleerders van die Internet deur internasionale openbare beleid te maak, 'n oorsigfunksie te vervul, en om verdrae te skep.[224] Daarteenoor is die privaat sektor se funksie om te selfreguleer, beste praktyke te ontwikkel en riglyne en voorstelle in beleidsdokumente vir state te ontwikkel.[225] Die burgerlike samelewing se taak is om openbare belangstelling te kweek deur gebruikmaking van opleiding, asook minderheidsgroepe se standpunte aan regerings deur te gee.[226] Opinie 5 van die WTPF bepaal eweneens dat spesifieke take aan multi-belangegroepe gegee word.[227] Die gevolg hiervan is dat dit duidelik blyk dat die ITU se standpunt jeens Internetregulering geensins verander het in die sewe jaar wat verloop het sedert die WGIG-verslag ter tafel gelê is nie.

---

222 Radu *The Evolution of Global Internet Governance* 129.

223 Working Group on Internet Governance *Report of the Working Group on Internet Governance* (2005) 8–9. Sien ook afd 4.2.4.3 waar die WSIS-verslag in meer besonderhede bespreek word.

224 Working Group on Internet Governance *Report of the Working Group on Internet Governance* 8. Afd 4.2.4.3 vn 258 verskaf 'n lys van pligte wat die WGIG-vergadering aan regerings toegedig het.

225 Working Group on Internet Governance *Report of the Working Group on Internet Governance* 9. Afd 4.2.4.3 vn 259 verskaf 'n lys van pligte wat die WGIG-vergadering aan regerings toegedig het.

226 Working Group on Internet Governance *Report of the Working Group on Internet Governance* 9–10. Afd 4.2.4.3 vn 260 verskaf 'n lys van pligte wat die WGIG-vergadering aan regerings toegedig het.

227 Hierdie opinie kan besigtig word by Anoniem "World Telecommunication/ICT Policy Forum 2013: OPINION 5: Supporting Multi-stakeholderism in Internet Governance" http://www.itu.int/en/wtpf-13/Documents/WTPF-13-Opinion5.pdf. (besoek op 27 Mei 2014).

5.3.3.5 Die ITU in Perspektief

Mueller is baie versigtig vir enige regulerings-ingrepe waar state die hoofrolspelers is.[228] Hy noem tereg dat state die reg het om belastings te hef en onteienings te doen, 'n monopolie het op die gebruik van geweld, en die vermoë het om oorlog te maak en wapens te ontplooi.[229] As die ITU sou slaag om regeringsinvloed op die Internet te verstewig, kan dit die netwerk van netwerke onherroeplik verander.

Die ITU is ook glad nie gewild onder verskeie state van die wêreld nie. Soos hierbo aangetoon, het beide die VSA en die Europese Unie ernstig gemaan teen inmenging van die ITU op die Internet.[230] Die ITU het ontwikkel in 'n era waar telekommunikasie 'n monopolie was,[231] en dit wil voorkom asof die ITU nie hierdie stigma kan afskud nie. Marsden verduidelik dit treffend:

> This view has ... depicted the ITU as engaging in a pathetic and ultimately doomed effort to remain relevant in a post-monopoly world, launching a bureaucratic power grab for new turf, or having some secret strategy to force the Internet into the old model of centralized control.[232]

Die gevolg is dat die ITU nie allerweë as 'n gepaste organisasie beskou word om verreikende reguleringsmaatreëls op die Internet aan te bring nie. Dit wil voorkom asof die ITU se verlede sy grootste vyand is in die era van die Internet. Ook hierdie organisasie blyk nie die gepaste keuse te wees om 'n hoofrolspelers by Internetregulering te wees nie.

---

228 Mueller M L "WTF? WTPF! Internet Governance Project — The Continuing Battle Over Internet Governance Principles" http://www.internetgovernance.org/2013/04/23/wtf-wtpf-the-continuing-battle-over-internet-governance-principles/ (besoek op 27 Mei 2014).

229 Mueller M L "WTF? WTPF! Internet Governance Project — The Continuing Battle Over Internet Governance Principles" http://www.internetgovernance.org/2013/04/23/wtf-wtpf-the-continuing-battle-over-internet-governance-principles/ (besoek op 27 Mei 2014).

230 Afd 5.3.3.3.

231 Bertin E, Crespi N en Magedanz T *Evolution of Telecommunication Services: The Convergence of Telecom and Internet: Technologies and Ecosystems* (2013) 79 verduidelik dit soos volg: "The ITU developed during an era of government monopoly on provision of telecommunications services in most countries in Europe, and a period in the US when there was a monopoly in providing long-distance national and international telecommunications services".

232 Marsden C T (red) *Regulating the Global Information Society* (2005) 164.

5.3.4 Die Raad van Europa

Die Raad van Europa[233] is op 5 Mei 1949 deur die Verdrag van Londen gestig.[234] Die neiging na 'n Raad van Europa het begin met Winston Churchill wat van mening was dat daar 'n Verenigde State van Europa moet wees wat soortgelyk aan die VSA is.[235] Lidmaatskap kan toegeken word as die aansoeker-staat aan twee vereistes voldoen: dit moet geografies binne Europa val, en dit moet demokratiese waardes aanvaar.[236]

Die hoofdoel van die Raad van Europa is om demokrasie en menseregte te bevorder.[237] Dit word gedoen deurdat daar verdrae geskep word wat lidlande sowel as nie-lidlande kan onderteken.[238] Die gedagte is dat die verdrae sekere gemeenskaplike regsbeginsels van demokrasie en menseregte neerlê, en alle ondertekenaar-lande hulself dan verbind om hulle eie wetgewing in ooreenstemming met die algemene beginsels in die betrokke verdrag te bring.[239]

Die Raad van Europa is 'n erkende internasionale organisasie in die Internasionale reg, aangesien dit state verteenwoordig, en ook namens lidlande optree.[240] Dit geniet volle waarnemerstatus by die Verenigde Nasies.[241]

Die belangrikste bydrae wat Die Raad van Europa ten opsigte van Internetregulering gemaak het, was die skepping van die *Convention on*

233 "Council of Europe" in Engels.

234 Benoît-Rohmer F en Klebes H *Council of Europe Law: Towards a Pan-European Legal Area* (2005) 27.

235 Winston Churchill se visie was dat: "I trust that the European family can act unitedly as one under a council of Europe". Royer A *The Council of Europe* (2010) 4.

236 Wrońska I *Fundamental Rights Protection in the Council of Europe: The Role of the European Court of Human Rights* (2011) 75.

237 Wrońska *Fundamental Rights Protection in the Council of Europe* 76 verduidelik dit so: "The Council of Europe has become a community of values guided by the ideas of democracy, rule of law, and human rights. This was indeed the intention of its Founding Fathers".

238 Wrońska *Fundamental Rights Protection in the Council of Europe* 88.

239 Wrońska *Fundamental Rights Protection in the Council of Europe* 88.

240 Michals D B *International Privileges and Immunities: A Case for a Universal Statute* (2012) 101.

241 Council of Europe *Parliamentary Assembly of the Council of Europe* 17 Oktober 1994 Doc 7178 1 meld: "The Council of Europe has enjoyed observer status with the United Nations General Assembly since 1989 but has not so far made full use of the opportunities thus offered".

Cybercrime,[242] wat op 1 Julie 2004 in werking getree het.[243] Hierdie verdrag is enig in sy soort, en omdat dit 'n globale onderwerp behandel wat nie tot Europa beperk is nie, het die Raad van Europa die ondertekening daarvan oopgestel vir nie-Europese lande.[244] Suid Afrika, die VSA, Japan en Kanada het dadelik die verdrag onderteken,[245] alhoewel Suid-Afrika dit tot op datum nog nie geratifiseer het nie.[246] Suid-Afrika het wél verskeie van die hooftemas van die *Convention on Cybercrime*[247] in plaaslike wetgewing vervat. Byvoorbeeld, hoofstuk 2 van die verdrag op Kubermisdaad bevat bepalings van die substantiewe strafreg, en verklaar gedrag soos die onwettige verkryging van rekenaarsisteme, of onwettige onderskepping en inmenging met data, as misdrywe.[248] Artikels 86–88 van die Wet op Elektroniese Kommunikasies en Transaksies[249] bepaal dat soortgelyke gedrag as 'n misdaad beskou sal word. Net so bepaal artikel 9 van die verdrag op Kubermisdaad dat kinderpornografie 'n misdryf daarstel, en artikel 24 van die Wet op Films en Publikasies[250] bevat soortgelyke bepalings. Artikel 22 van die konvensie op Kubermisdaad reël aangeleenthede van jurisdiksie, en artikel 90 van die Wet op Elektroniese Kommunikasies en Transaksies[251] doen dieselfde. Artikel 29–30 van die konvensie op

---

242 Council of Europe *Convention on Cybercrime* CETS No.185. Die teks van die konvensie kan verkry word by Council of Europe "Convention on Cybercrime" http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (besoek op 22 Mei 2014).

243 August R "International Cyber-Jurisdiction: A Comparative Analysis" 2002 *American Business Law Journal* 531 545.

244 Blane J V *Cybercrime and Cyberterrorism: Current Issues* (2003) 2.

245 Watney M "The Evolution of Legal Regulation of the Internet to Address Terrorism and Other Crimes" 2007 *Tydskrif vir die Suid-Afrikaanse Reg* 494 499; Murray A D *The Regulation of Cyberspace: Control in the Online Environment* (2007) 224.

246 Die Raad van Europa se lys van lande wat die *Convention on Cybercrime* onderteken het, is verkrygbaar by Council of Europe "Chart of Signatures and Ratifications of Treaty 185" http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (besoek op 22 Mei 2014); Watney 2007 *Tydskrif vir die Suid-Afrikaanse Reg* 499; Murray *The Regulation of Cyberspace* 224.

247 "Konvensie op Kubermisdaad" in Afrikaans.

248 Art 2–8 van die verdrag op Kubermisdaad.

249 25 van 2002.

250 65 of 1996, soos gewysig deur die Wysigingswet op Films en publikasies 18 van 2004 en 3 van 2009.

251 25 van 2002.

Kubermisdaad reguleer die behoud van data vir latere ondersoek deur owerhede, en artikel 30 van die Wet op die Reëling van Onderskepping van Kommunikasies en Verstrekking van Kommunikasie-verwante Inligting[252] bevat soortgelyke bepalings. Dus word 'n wye verskeidenheid onderwerpe wat in die konvensie op Kubermisdaad vervat word, ook in Suid-Afrikaanse wetgewing aangespreek.

Deur die totstandkoming van die konvensie op Kubermisdaad is daar vir die eerste keer gepoog om Internetmisdaad vanuit 'n internasionaal-regtelike sfeer te reguleer.[253] Die konvensie skep 'n belangrike basislyn waaraan lande behoort te voldoen om internasionale samewerking in die bekamping van kubermisdaad te bewerkstellig.[254] Dit is dan ook die doel van die skrywers van die konvensie, wat van mening is dat hierdie konvensie tot gevolg het dat misdadigers nie meer 'n "feeling of impunity" het nie.[255]

Skeptici is egter nie so seker of hierdie maatreëls die nodige uitwerking sal hê nie: dit is juis die "probleem"-state wat nie ondertekenaars van die konvensie is nie.[256] Die konvensie op Kubermisdaad maak byvoorbeeld nie voorsiening vir polisie om oorgrens-monitering en -afdwinging te bewerkstellig nie, wat wetstoepassers grootliks verhinder om effektiewe

---

252 70 Van 2002.

253 August 2002 *American Business Law Journal* 545 meen egter dat die verdrag nie bevredigend is nie omdat dit nie internasionale jurisdiksie skep nie, maar bloot elke land se eie plaaslike jurisdiksie bevestig. Sien ook Murray *The Regulation of Cyberspace* 223 vir 'n verduideliking van die VSA se siening dat verdrae altyd ondergeskik is aan die Amerikaanse grondwet, en gevolglik sal die *Cybercrime Treaty* nie in die VSA die aandag kry wat dit verdien nie. Hierteenoor beskou die WSIS die *Convention on Cybercrime* as 'n belangrike item om kubermisdaad te beveg, en dring by lande van die wêreld daarop aan om die verdrag te onderteken. Sien art 40 van die *Tunis Agenda for the Information Society 2005*: "We underline the importance of the prosecution of cybercrime, including cybercrime committed in one jurisdiction, but having effects in another." World Summit on the Information Society "Tunis Agenda for the Information Society" http://www.itu.int/WSIS/docs2/tunis/off/6rev1.html (besoek op 7 September 2014) art 40.

254 Benedek W, Bauer V en Kettemann M C (red) *Internet Governance and the Information Society: Global Perspectives and European Dimensions* (2008) 109 meen dat die konvensie op Kubermisdaad 'n globale instrument is om kubermisdaad aan te spreek: "The ambition of the convention to become a global instrument is and was supported by the European Union. ... The impact of the Convention therefore goes far beyond its number of formal parties".

255 Blane *Cybercrime and Cyberterrorism* 3.

256 Blane *Cybercrime and Cyberterrorism* 4 noem byvoorbeeld dat kubermisdaad dikwels deur Yemen of Noord-Korea gestuur word, en beide hierdie state is nie ondertekenaars van die konvensie nie.

misdaadbekamping te bedryf.[257] In die teenoorgestelde kamp beweer groepe soos die *American Civil Liberties Union* dat die konvensie op Kubermisdaad se bepalings te ingrypend is, en dat dit onnodige magte aan die VSA-owerhede verleen.[258] Kommentaar soos hierdie bevestig net weer eens hoe geweldig ingewikkeld dit is om inhoud op die Internet vanuit 'n globale perspektief te reguleer, aangesien verskillende state se inwoners vanuit verskillende ideologieë na reguleringskwessies kyk. Ten spyte van die kritiek word daar aan die hand gedoen dat die bestaan van die konvensie op Kubermisdaad tóg 'n voordeel vir die wêreld se Internetgebruikers inhou.

***

Die raad van Europa het sedert sy bykans sewe-dekade bestaan 'n groot rol gespeel om veral menseregte 'n groter gestalte in Europa, en ook in die wêreld, te gee. Die fokus van hierdie organisasie bly egter die uitbreiding van menseregte, en dit is juis hier waar die Raad van Europa se sterk punt lê — dit kan 'n belangrike rolspeler wees om inhoud op die Internet te reguleer, maar nie ten aansien van basis-reguleringsfunksies nie.

5.4 Ander Internasionale Organisasies

Soos hierbo uiteengesit[259] is internasionale organisasies soos deur die Internasionale Regskommissie bepaal, nie ál rolspelers in die Internet-arena nie. Ander internasionale organisasies wat nie noodwendig deel van die Verenigde Nasies uitmaak nie, speel 'n kritieke rol in die suksesvolle funksionering van die Internet. Vervolgens sal die vernaamste van hierdie "ander" internasionale rolspelers bespreek word.

257 Blane *Cybercrime and Cyberterrorism* 4.

258 Blane *Cybercrime and Cyberterrorism* 4.

259 Afd 1.5 en afd 5.2.

5.4.1 Internet Corporation of Assigned Names and Numbers (ICANN)

5.4.1.1 Inleiding

Die Internet het sy ontstaan in die VSA gehad, en nadat dit duidelik geword het wat die Internet se belang is, het die Amerikaanse regering stappe geneem om die kern daarvan, te wete die IANA-funksie, te beskerm.[260] Hierdie stap is deur state van die wêreld as 'n monopolisering van basiese Internetdienste beskou.[261] Die argument was dat die Internet 'n globale netwerk was, en dat dit onaanvaarbaar is dat dit deur een regering beheer word.

Die VSA-regering het in 1997 besluit om openbare mening in te win om te bepaal hoe om die situasie te beredder.[262] Kommentaar wat ontvang is, is in 'n groenskrif vervat.[263]

Die groenskrif se oplossing tot die VSA se dilemma was om 'n privaatmaatskappy sonder winsbejag[264] in Kalifornië te stig.[265] Die doelwitte van die nuwe maatskappy sou wees om:

- Die IANA-funksie te behartig[266]
- vyf nuwe generiese topvlakdomeins te skep
- Internetregulering te bestudeer, en

260 Afd 3.4.

261 Afd 3.4; Mathiason *Internet Governance* 52–53.

262 Mathiason *Internet Governance* 54.

263 Die proses van openbare konsultasie is op 16 Junie 1997 deur die *National Telecommunications and Information Administration* begin. Teen Augustus 1997 is daar reeds 282 dokumente ontvang, en dit is deur Ira Magaziner, wat Bill Clinton se Internet-adviseur was, verwerk tot 'n groenskrif. Mathiason *Internet Governance* 53–54.

264 Non-profit organization in Engels.

265 Die voorgenome maatskappy sonder winsbejag sou volgens die wette van Kalifornië ingelyf word aangesien die sogenaamde IANA-funksie, wat die basisbeheer van die DNS is, deur Jon Postel in Kalifornië uitgeoefen is. Byers M en Nolte G *United States Hegemony and the Foundations of International Law* (2003) 50; Mathiason *Internet Governance* 58.

266 Afd 3.4.3.

- oorbruggingsfunksies tussen die ou- en nuwe bedeling te behartig.[267]

Die groenskrif is vir kommentaar oopgestel, en hierdie keer is meer as 500 skriftelike reaksies ontvang. Waar die vorige rondte kommentaar grootliks tot die VSA beperk was, het 20% van reaksies op die groenskrif van internasionale bronne gekom.[268] Een van die grootste bronne van kritiek was die feit dat die groenskrif Amerikaans-gesentreerd was, en daar was vele versoeke vir 'n meer globale hantering van die IANA-funksie.[269]

Kommentaar wat uit die groenskrif ontvang is, is tot 'n nuwe witskrif ontwikkel.[270] Hierdie dokument wat uit die aard van die saak meer omvattend as die groenskrif was, het vier beginsels vervat waarvolgens die nuwe organisasie bestuur sou moes word. Die vier beginsels was soos volg:

1. Stabiliteit — Die VSA moes hul rol in die hantering van die IANA-funksie op so 'n wyse beëindig dat dit op geen manier die werking van die Internet sou beïnvloed nie,

2. Kompetisie — Markkragte wat kompetisie bevoordeel moes toegelaat word om voort te werk,

3. Private, gedesentraliseerde koördinering — Regeringsinstansies neem gewoonlik lank om besluite te neem, en so 'n stelsel is nie sinvol in die vinnig-ontwikkelende Internet nie. Die Internet sélf het op 'n gedesentraliseerde wyse ontstaan, en die koördinering daarvan behoort op dieselfde beginsels te geskied.

4. Verteenwoordiging — Die nuwe organisasie behoort tot voordeel van die groter Internetgemeenskap te wees, en behoort dus nie 'n

267 Mathiason *Internet Governance* 54.

268 Mathiason *Internet Governance* 54.

269 Mathiason *Internet Governance* 55.

270 National Telecommunications and Information Administration United States Department of Commerce "Statement of Policy on the Management of Internet Names and Addresses" http://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses (besoek op 9 Mei 2014).

> regeringsorganisasie te wees nie. Daarom is daar juis besluit op die model van 'n privaatmaatskappy sonder winsbejag.[271]

Die Amerikaanse regering het besef dat die bestuur van die IANA-funksie[272] 'n globale aangeleentheid was, en het dit in die witskrif erken:

> The US Government believes that the Internet is a global medium and that its technical management should fully reflect the global diversity of Internet users. We recognize the need for and fully support mechanisms that would ensure international input into the management of the domain name system. In withdrawing the US Government from DNS management and promoting the establishment of a new, non-governmental entity to manage Internet names and addresses, a key US Government objective has been to ensure that the increasingly global Internet user community has a voice in decisions affecting the Internet's technical management.

Die gevolg was die totstandkoming van ICANN, die *Internet Corporation for Assigned Names and Numbers*, in September 1998.[273]

5.4.1.2 Struktuur van ICANN

Omdat een van die basisbeginsels van ICANN se bestaan 'n gedesentraliseerde, of meer korrek 'n "bottom up"-struktuur is, beteken dit dat ICANN grotendeels probeer om soveel insette van rolspelers in die Internetregulerings-arena te verkry.[274] Hierdie rolspelers is meestal vervat in ICANN se substrukture.

ICANN bestaan uit 'n verbysterende aantal substrukture. Daar sal egter in hierdie studie gepoog word om die uiteensetting ietwat te vereenvoudig om dit meer hanteerbaar te maak.

ICANN se hoofbestuur bestaan uit 'n raad van direkteure met 22 lede. Hiervan is 16 lede stemgeregtig.[275] Een-en-twintig raadslede verteenwoor-

271 Mathiason *Internet Governance* 56.

272 Segura-Serrano A "Internet Regulation and the Role of International Law" 2006 *Max Planck Yearbook of United Nations Law* 191 232.

273 Werbach K "The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart" 2008 *University of California Davis Law Review* 343 357.

274 Mathiason *Internet Governance* 58.

275 Mathiason *Internet Governance* 84.

dig ’n groepering wat hul tot die ICANN-raad genomineer het. Een raadslid is die ombudsman, wat nie ’n spesifieke groepering verteenwoordig nie.[276] Die res van die raad word soos volg verdeel:

- Een raadslid is die president van ICANN. Hierdie lid is ook die voorsitter van die raad.
- Twee raadslede verteenwoordig die globale topvlakdomeinstelsel, soos .com en .org.
- Twee raadslede verteenwoordig die streeksregistrateurs. Daar bestaan vyf streeksregistrateurs, te wete AfriNIC[277] (Afrika), APNIC[278] (Asië en Stille-Oseaan-gebied), ARIN[279] (Noord Amerika), LACNIC[280] (Suid-Amerika), en RIPE NCC[281] (Europa).
- Twee raadslede verteenwoordig die land-topvlakdomeinstelsel (soos .za, .uk, .it, .nl ensovoorts).
- Agt raadslede word verkies deur ICANN se “Nominating Committee” en moet aan ’n verskeidenheid vereistes voldoen, byvoorbeeld dat elke streeksgebied (soos direk hierbo by die streeksregistrateurs uiteengesit) in die wêreld verteenwoordig moet word en dat hul die tegniese standaarde van die Internet verstaan.[282]
- Een raadslid word vanuit die Internet-gemeenskap gekies. Hierdie raadslid verteenwoordig ’n magdom Internet-belangegroepe wat

276 Mathiason *Internet Governance* 84.

277 African Network Information Center (AfriNIC).

278 Asia Pacific Network Information Centre (APNIC).

279 American Registry for Internet Numbers (ARIN).

280 Latin American and Caribbean Internet Addresses Registry (LACNIC).

281 Réseaux IP Européens (RIPE NCC).

282 Sien ICANN se bywette rakende die verkiesing van die “Nominating Committee” en persone wat as verkose raadslede kan dien. Meer hieroor by Internet Corporation for Assigned Names and Numbers “ICANN Bylaws Provisions Relating to Nominating Committee” http://archive.ICANN.org/en/committees/nom-comm/bylaws.htm (besoek op 4 September 2014) veral artikel VI afd 2 rakende die verkiesing van direkteure, artikel VI afd 5 rakende internasionale verteenwoordiging, en artikel VII rakende die vereistes om op die “nominating committee” te kan dien.

onder ICANN ingelyf is.
Al 16 bogenoemde raadslede is stemgeregtig.

- Een raadslid verteenwoordig die "Security and Stability Advisory Committee".[283] Hierdie raadslid is nie stemgeregtig nie.

- Een raadslid verteenwoordig die "Root Server System Advisory Committee".[284] Hierdie raadslid is nie stemgeregtig nie.

- Een raadslid verteenwoordig die "Technical Liaison Group". Hierdie raadslid is nie stemgeregtig nie.

- Een raadslid verteenwoordig die "Internet Engineering Task Force".[285] Hierdie raadslid is nie stemgeregtig nie.

- Een raadslid verteenwoordig die "Governmental Advisory Committee".[286] Hierdie raadslid is nie stemgeregtig nie.

- Die laaste raadslid is ICANN se ombudsman, en is eweneens nie

283 "Security and Stability Advisory Committee" word gedefinieer as: "An advisory committee to the ICANN Board, composed of volunteer members who are recognized experts in the domain name, addressing, and/or security areas. All members provide independent advice and are expected to call attention to circumstances when the comments they offer are not their own". Internet Corporation for Assigned Names and Numbers "Beginner's Guide to Participating in ICANN" http://www.ICANN.org/en/system/files/files/participating-08nov13-en.pdf (besoek op 13 Mei 2014) 24.

284 "Root Server System Advisory Committee" word gedefinieer as: "An advisory committee to the ICANN Board about the operation of the root name servers of the Domain Name System." Internet Corporation for Assigned Names and Numbers "Beginner's Guide to Participating in ICANN" http://www.ICANN.org/en/system/files/files/participating-08nov13-en.pdf (besoek op 13 Mei 2014) 24..

285 "Technical Liaison Group" word gedefinieer as: "An open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet." Internet Corporation for Assigned Names and Numbers "Beginner's Guide to Participating in ICANN" http://www.ICANN.org/en/system/files/files/participating-08nov13-en.pdf (besoek op 13 Mei 2014) 20.

286 "Governmental Advisory Committee" word gedefinieer as: "An advisory committee to the ICANN Board, comprising appointed representatives of national governments, multi-national governmental organizations and treaty organizations, and distinct economies." Internet Corporation for Assigned Names and Numbers "Beginner's Guide to Participating in ICANN" http://www.ICANN.org/en/system/files/files/participating-08nov13-en.pdf (besoek op 13 Mei 2014) 19.

stemgeregtig nie.[287]

5.4.1.3 Werking van ICANN

ICANN hou voor dat hulle hele bestaan op 'n "multistakeholder governance model" gebaseer is.[288] Dit beteken dat ICANN poog om soveel as moontlik insette van hul "constituency", of belangegroepbasis, te ontvang. Dit is uiteraard deel van ICANN se oorspronklike mandaat van die VSA-regering.

Om hierdie doel te verwesenlik, het ICANN 'n magdom belangegroepe gestig en ander wat reeds bestaan het, onder sy vlerk geneem. Die "multistakeholder governance model" is aan die werk wanneer die struktuur van ICANN se raad van direkteure, soos hierbo uiteengesit, onder die vergrootglas geplaas word. Al die raadslede (behalwe die ombudsman), verteenwoordig een of meer belangegroepe, en so word daar probeer om die "bottom-up" bestuursmodel te laat funksioneer.[289] Dit is ongelukkig 'n geweldige lomp proses, want alle belangegroepe moet eers vergader en dan word die besluite van onder na bo geperkoleer totdat dit uiteindelik op die ICANN-raad bespreek en goedgekeur word.[290] Dit is ook 'n geweldige duur proses, en ICANN se begroting is besonder groot. In 2014 het ICANN se goedgekeurde begroting meer as 88 miljoen dollar beloop, waarvan meer as 36 miljoen dollar aan salarisse uitbetaal is.[291]

---

287 Ombudsman word gedefinieer as: "An independent, impartial and neutral officer of ICANN. It is an Alternative Dispute Resolution office for the ICANN community who may wish to lodge a complaint about a staff or Board decision, action or inaction." Internet Corporation for Assigned Names and Numbers "Beginner's Guide to Participating in ICANN" http://www.ICANN.org/en/system/files/files/participating-08nov13-en.pdf (besoek op 13 Mei 2014) 22.

288 Internet Corporation for Assigned Names and Numbers "Beginner's Guide to Participating in ICANN" http://www.ICANN.org/en/system/files/files/participating-08nov13-en.pdf (besoek op 13 Mei 2014) 2.

289 Mathiason *Internet Governance* 88.

290 Mathiason *Internet Governance* 88.

291 Internet Corporation for Assigned Names and Numbers "ICANN Board Meeting August 22 2013 FY14 Budget Approval" http://www.ICANN.org/en/about/financials/adopted-opplan-budget-fy14-22aug13-en.pdf (besoek op 13 Mei 2014) 3.

5.4.1.4 Kritiek op ICANN

In sy kort bestaan het ICANN onder geweldige kritiek deurgeloop.[292] In 'n mate is dit te verstane, want almal wat een of ander wyse beheer oor die Internet wil uitoefen, wil 'n sterk belang in ICANN hê. Andersyds is dit 'n bykans onbegonne taak om belangegroepe wat dikwels uiteenlopende sienings het, te akkommodeer.

ICANN se vormingsjare was baie stormagtig, en vergrype na magsposisies het algemeen voorgekom.[293] Dit het selfs tot litigasie aanleiding gegee toe een van die raadslede, Karl Auerbach, vir ICANN gedagvaar het om korporatiewe dokumente beskikbaar te stel.[294] Twee jaar nadat ICANN gestig is, was helfte van die oorspronklike raadslede vervang, en in 2003 (vyf jaar na stigting), was daar nie 'n enkele lid van die oorspronklike raad meer oor nie.[295] Koppell sê: "Substantive disagreement on its policies, ambiguities regarding its legitimacy and role, and a deeply divided constituency have all contributed to ICANN's tribulations."[296]

Hunter[297] meen dat ICANN op hierdie stadium so disfunksioneel was dat dit nie meer sy basisfunksie van demokratiese besluitneming kon uitoefen nie.

> ICANN is an institution besieged. Having moved beyond its initial technical mandate into policy setting, it is surrounded on all sides by outraged political actors and activists who routinely accuse it of lacking legitimacy, acting improperly, and behaving arbitrarily. The basis for much of the criticism is that ICANN fails to meet the most fundamental test of political institutions: that it is, in short, undemocratic.[298]

---

292 Bygrave L A en Bing J *Internet Governance: Infrastructure and Institutions* (2009) 111.

293 Mathiason *Internet Governance* 79.

294 Mathiason *Internet Governance* 80.

295 Mathiason *Internet Governance* 74.

296 Koppell J G S "Pathologies of Accountability: ICANN and the Challenge of 'Multiple Accountabilities Disorder'" 2005 *Public Administration Review* 94 104.

297 Hunter D "ICANN and the Concept of Democratic Deficit" 2002 *Loyola of Los Angeles Law Review* 1149 1149.

298 Hunter 2002 *Loyola of Los Angeles Law Review* 1154. Vir meer inligting oor ICANN se vroeë vormingsjare, sien Badgley R A "Improving ICANN in Ten Easy Steps: Ten Suggestions for ICANN to Improve its Anti-Cybersquatting Arbitration System." 2001 *Journal of Law, Technology and Policy at the University of Illinois* 109.

Een van die grootste punte van kritiek wat ICANN ontvang het, was in hulle goedkeuring van nuwe topvlakdomeins.[299] ICANN het na sy ontstaan bekend gemaak dat nuwe topvlakdomeins geregistreer kan word. 'n Nie-terugbetaalbare aansoekfooi van $50 000 per aansoek is vasgestel. Na ontvangs van verskeie aansoeke het ICANN sommige aansoeke goedgekeur, terwyl ander afgekeur is. Onsuksesvolle aansoekers was ontsteld, want ICANN het nooit enige kriteria vasgestel in die oorweging van nuwe topvlakdomeins nie. Dit was dan ook nie vreemd dat onsuksesvolle aansoekers ongelukkig was oor ICANN se "lukraak hantering" van die saak nie.[300] Koppel meen dat die wyse waarop ICANN hierdie situasie hanteer het, is bloot 'n aanwysing dat 'n diverse organisasie soos ICANN eenvoudig nie ál die eise van sy belangegroepe kan akkommodeer nie.[301]

5.4.1.5 ICANN in Perspektief

ICANN was spesifiek gestig met die doel om die IANA-funksie oor te neem.[302] Die VSA was van mening dat indien dit ICANN aan die wêreld voorhou as 'n internasionale organisasie wat deur rolspelers van regoor die wêreld verteenwoordig word, dit algemeen aanvaar sou word.[303] Dit was nie die geval nie.

Om die probleem met ICANN te beredder, is daar selfs in 2005 oorweging gegee aan die moontlikheid dat die Verenigde Nasies die organisasie onder sy vleuels neem.[304] Hierdie voorstel is egter ten sterkste deur die Amerikaanse regering teëgestaan.[305] Uiteindelik is daar by die WSIS-II in

299 Werbach 2008 *University of California Davis Law Review* 365.

300 Koppell 2005 *Public Administration Review* 104. Sien ook Sideri K "Questioning the Neutrality of Procedural Law: Internet Regulation in Europe Through the Lenses of Bourdieu's Notion of Symbolic Capital" 2004 *European Law Journal* 61 78–79, asook Werbach 2008 *University of California Davis Law Review* 365 vir 'n uiteensetting van die politieke stryery oor ICANN.

301 Koppell 2005 *Public Administration Review* 103.

302 Mathiason *Internet Governance* 70.

303 Mathiason *Internet Governance* 71.

304 Kleinman D L en Moore K *Routledge Handbook of Science, Technology, and Society* (2014) 215.

305 Kleinman *Routledge Handbook of Science, Technology, and Society* 215.

Tunisië in November 2005 besluit dat die Verenigde Nasies nie by die dag-tot-dag bedrywighede van ICANN betrokke sou wees nie.[306]

In Junie 2013 het die Snowden-onthullings plaasgevind wat die VSA se internasionale spioenasiebedrywighede op die Internet blootgelê het.[307] Dit het wêreldwye negatiewe kritiek ontlok, en ICANN het hier probeer om 'n sterk standpunt in te neem téén spioenasie op die Internet. In samewerking met ander groot Internet-rolspelers soos die IETF, IAB en die Internet Society het ICANN die *Montevideo Statement on the Future of Internet Cooperation* onderteken.[308] Daarvolgens is daar vier hoofpunte uiteengesit wat die Internet van die toekoms behoort te vorm, te wete:

- Internet-fragmentasie op nasionale vlak behoort ontmoedig te word. In hierdie verband word enige sogenaamde "surveillance" tussen state op die Internet ten sterkste veroordeel;
- Internetregulering behoort volgens 'n "multistakeholder governance model" bestuur te word;
- Die IANA-funksie, wat die kern van die beheer van die Internet vorm, behoort op 'n globale vlak hanteer te word, en
- die IPV6-protokol moet uitgerol word as 'n prioriteit. Dit sal die stabiliteit van die Internet help verseker.[309]

Hierdie verklaring toon aan dat verskeie belangrike rolspelers bereid is om 'n pad saam met ICANN te stap om behoorlike oorsig oor die IANA-funksie

306 Eriksson J en Giacomello G "Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State" 2009 *International Studies Review* 205 220 en 223.

307 Afd 6.4.1.5. Die Snowden spioenasieskandaal verwys na Edward Snowden wat aangetoon het hoe die Amerikaanse "National Security Agency" sedert 2007 'n reuse spioenasieveldtog geloods het wat oor 'n aantal kontinente gespan het. Dit is uiteindelik in Junie 2013 deur Edward Snowden oopgevlek. Gelman B en Poitras L "US, British Intelligence Mining Data From Nine US Internet Companies in Broad Secret Program" http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (besoek op 12 Mei 2014).

308 Internet Corporation of Assigned Names and Numbers "Montevideo Statement on the Future of Internet Cooperation" https://www.ICANN.org/news/announcement-2013-10-07-en (besoek op 20 Junie 2014).

309 Internet Corporation of Assigned Names and Numbers "Montevideo Statement on the Future of Internet Cooperation" https://www.ICANN.org/news/announcement-2013-10-07-en (besoek op 20 Junie 2014).

te bewerkstellig. Ten spyte van ICANN se tekortkominge bly dit steeds die organisasie wat die IANA-funksie in die internasionale sfeer kan plaas.

ICANN het op 10 Maart 2016 'n amptelike aansoek by die Amerikaanse "National Telecommunications and Information Administration" ingedien om finale oorsig van die IANA-funksie oor te neem.[310] Dit word ten tyde van hierdie skrywe nog oorweeg.[311]

5.4.2 Internet Society

Teen die einde van die tagtigerjare en vroeë negentigerjare het dit geblyk dat die Internet van kommersiële belang geword het.[312] As gevolg hiervan wou die Amerikaanse *National Science Foundation* (NSF) nie die *Internet Engineering Task Force* (IETF), wat verantwoordelik was vir die tegniese regulering van die Internet, verder befonds nie[313] Vinton Cerf, wat by die IETF betrokke was, het besef dat die IETF steeds 'n funksie het om die Internet in staat te stel om verder te ontwikkel, en daar moes 'n plan gemaak word om 'n nuwe tuiste vir die IETF te vind.[314] Cerf se voorstel was dat daar 'n professionele organisasie gestig moes word, en so het die *Internet Society* in 1992 sy ontstaan gehad[315] toe dit by die INET-konferensie in Kopenhagen

310 Internet Corporation for Assigned Names and Numbers *IANA Stewardship Transition Proposal and Enhancing ICANN Accountability Recommendations* (2016). Verkrygbaar op die Internet by Internet Corporation for Assigned Names and Numbers "IANA Stewardship Transition Proposal and Enhancing ICANN Accountability Recommendations" https://www.ICANN.org/en/system/files/files/IANA-stewardship-transition-package-10mar16-en.pdf (besoek op 19 Mei 2016).

311 National Telecommunications and Information Administration "Reviewing the IANA Transition Proposal" https://www.ntia.doc.gov/blog/2016/reviewing-IANA-transition-proposal (besoek op 19 Mei 2016).

312 Internet Society "An Oral History of the Internet Society's Founding" http://www.internetsociety.org/internet-society-founding (besoek op 20 Junie 2014).

313 Internet Society "An Oral History of the Internet Society's Founding" http://www.internetsociety.org/internet-society-founding (besoek op 20 Junie 2014). Afd 5.4.3.

314 Internet Society "An Oral History of the Internet Society's Founding" http://www.internetsociety.org/internet-society-founding (besoek op 20 Junie 2014).

315 Internet Society "An Oral History of the Internet Society's Founding" http://www.internetsociety.org/internet-society-founding (besoek op 20 Junie 2014).

bekend gestel is.[316] Dit is geregistreer as 'n nie-winsgewende organisasie.[317]

ISOC se verkorte missiestelling bepaal eenvoudig: "To promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world."[318] Tóg bepaal die missiestelling verder dat ISOC se taak is om oop standaarde vir die Internet te ontwikkel, opleiding in veral ontwikkelende lande te bevorder, internasionale samewerking ten opsigte van Internet-aangeleenthede te bewerkstellig en as 'n fokuspunt vir koöperatiewe Internetbelange te dien.[319]

In die twee-en-twintigjarige bestaan van die organisasie is vele van hierdie doelstellings al vermag. ISOC is inderdaad 'n fokuspunt vir

316 Internet Society "Formation of Internet Society Announced at INET '91 Copenhagen" http://www.internetsociety.org/history-timeline/formation-internet-society-announced-inet-%E2%80%9991-copenhagen (besoek op 20 Junie 2014). Die ISOC verklaringsdokument kan gelees word by Cerf V, Kahn B en Chapin L "Announcing the Internet Society" http://www.internetsociety.org/internet/what-internet/history-internet/announcing-internet-society (besoek op 20 Junie 2014).

317 Internet Society "Formation of Internet Society Announced at INET '91 Copenhagen" http://www.internetsociety.org/history-timeline/formation-internet-society-announced-inet-%E2%80%9991-copenhagen (besoek op 20 Junie 2014).

318 Internet Society "Internet Society Mission" http://www.internetsociety.org/who-we-are/mission (besoek op 20 Junie 2014).

319 To help achieve our mission, the Internet Society:

- Facilitates open development of standards, protocols, administration, and the technical infrastructure of the Internet.
- Supports education in developing countries specifically, and wherever the need exists.
- Promotes professional development and builds community to foster participation and leadership in areas important to the evolution of the Internet.
- Provides reliable information about the Internet.
- Provides forums for discussion of issues that affect Internet evolution, development and use in technical, commercial, societal, and other contexts.
- Fosters an environment for international cooperation, community, and a culture that enables self-governance to work.
- Serves as a focal point for cooperative efforts to promote the Internet as a positive tool to benefit all people throughout the world.
- Provides management and coordination for on-strategy initiatives and outreach efforts in humanitarian, educational, societal, and other contexts.

Internet Society "Internet Society Mission" http://www.internetsociety.org/who-we-are/mission (besoek op 20 Junie 2014); Gigante A "Blackhole in Cyberspace: The Legal Void in the Internet" 1997 *John Marshall Journal of Computer and Information Law* 413 418.

verskeie Internet-kritieke organisasies.[320] Die IETF, soos hieronder in meer besonderhede verduidelik sal word, is sekerlik die belangrikste, maar om te verhinder dat die IETF nie geskaak word deur persone of organisasies wat hulle eie belange wil bevorder nie, het ISOC ander werksgroepe tot stand gebring om as "checks and balances" vir die IETF te dien.[321] Daar is byvoorbeeld die *Internet Engineering Steering Group* (hierna IESG) wat as die bestuur van die IETF dien; die *Internet Architecture Board* (IAB), wat 'n oorsigfunksie ten opsigte van die IETF uitvoer en die *Internet Research Task Force* (IRTF) wat oorhoofs vir netwerkontwerp verantwoordelik is.[322] Dan het ISOC nog sogenaamde "chapters" in bykans elke land van die wêreld wat deel in ISOC se verskeidenheid bedrywighede.[323] Wanneer tegniese regulering van die Internet ter sprake is, het ISOC sonder twyfel die leisels in die hand.

5.4.3 Internet Engineering Task Force (IETF)

Die *Internet Engineering Task Force* kan as die tegniese hart van die Internet beskou word.[324] Omdat die Internet eintlik maar net 'n netwerk van netwerke is, en dus aaneengeskakel word deur soortgelyke standaarde en protokolle, is dit voor-die-hand-liggend dat ooreenkomste bereik moes word om algemeen geldende standaarde neer te lê. Dit is die IETF se taak om hierdie funksie te verrig.

Die IETF het sy ontstaan in 1986 gehad as 'n tegniese komitee van 'n handjievol persone om Internetbeleid vas te stel.[325] Dit het gegroei tot 'n organisasie van vrywilligers wat vandag nog die tegniese standaarde van die

320 Chatillon G *Internet International Law* (2005) 305.

321 Murray *The Regulation of Cyberspace* 92.

322 Sien die diagrammatiese uiteensetting van ISOC in Murray *The Regulation of Cyberspace* 93.

323 Murray *The Regulation of Cyberspace* 91.

324 Mathiason *Internet Governance* 33.

325 DiBona C en Ockman S *Open Sources: Voices from the Open Source Revolution* (1999) 48. Internet Engineering Task Force "Past Meetings" http://www.ietf.org/meeting/past.html (besoek op 22 Mei 2014). Die eerste vergadering van die IETF het op 16 Januarie 1986 in San Diego, Kalifornië plaasgevind. Daar was 21 persone by dié vergadering.

Internet bepaal. Die 2014-IETF vergadering het byvoorbeeld 1400 bywoners gehad.[326]

Daar word gepoog om formele strukture binne die IETF tot die minimum te beperk. Dit bestaan bloot uit 'n groepering wat soortgelyke belange bevorder, en daarom is die IETF byvoorbeeld nog nooit as 'n formele organisasie of -maatskappy ingelyf nie.[327] Alle onkoste wat aangegaan word, word deur die oorhoofse *Internet Society* gedra.[328]

DiBona meld dat die IETF "can be described as a membership organization without a defined membership".[329] Die enigste vereiste om mee te doen aan IETF-bedrywighede is dat die deelnemer 'n tegniese kennis van die onderwerp onder bespreking moet hê, en verteenwoordigers van organisasies word nie toegelaat nie.[330]

Alhoewel die IETF drie vergaderings per jaar hou, word korrespondensie tussen deelnemers op e-poslyste[331] gedoen.[332] Wanneer 'n nuwe tegniese aangeleentheid van die Internet opgelos moet word, sal enigeen wat in die aangeleentheid belang stel, 'n groep bymekaar bring en die tegniese redakteur van die IETF in kennis stel dat 'n nuwe groep gevorm is. Dit word dan bloot aangeteken en onder ander gebruikers versprei.[333] Wanneer die aangeleentheid deur die groep opgelos is, word dit aan die IESG voorgehou.[334] Laasgenoemde is 'n groep wat uit areabestuurders van "gewone" groepe bestaan. Die IESG besluit of die aangeleentheid in werking

---

326 Internet Engineering Task Force "Past Meetings" http://www.ietf.org/meeting/past.html (besoek op 22 Mei 2014).

327 DiBona *Open Sources* 48.

328 DiBona *Open Sources* 48.

329 DiBona *Open Sources* 48.

330 DiBona *Open Sources* 48; Hovey R "The Organizations Involved in the IETF Standards Process" http://tools.ietf.org/html/bcp11 (besoek op 22 Mei 2014) bepaal dat: "Participation in the IETF and its Working Groups is by individual technical contributors rather than by formal representatives of organizations." 2.

331 "Mailing Lists" in Engels.

332 Marsden C T *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (2011) 105.

333 DiBona *Open Sources* 49.

334 DiBona *Open Sources* 49.

gestel kan word, en indien wel, word dit uitgevoer en as 'n standaard in die IETF se "Standards-only" (STD) reeks gepubliseer.[335]

Sedert die vroegste vergaderings van die IETF word besluite geneem op die basis van "rough consensus and running code".[336] Dit beteken eenvoudig dat finale besluite ingevoer word indien die meerderheid tegnici daaroor saamstem. DiBona verduidelik:

> The IETF motto is "rough consensus and running code." Working group unanimity is not required for a proposal to be adopted, but a proposal that cannot demonstrate that most of the working group members think that it is the right thing to do will not be approved. There is no fixed percentage support that a proposal must achieve, but most proposals that have more than 90% support can be approved and those with less than 80% can often be rejected. lETF working groups do not actually vote, but can resort to a show of hands to see if the consensus is clear.[337]

Enige voorstelle vir nuwe standaarde wat nie met reeds-bestaande standaarde versoenbaar is nie, word met ernstige versigtigheid bejeën.[338]

Die IETF was in sy onstaansjare deur die VSA-regering befonds,[339] maar met verloop van tyd is daar besef dat hierdie stand van sake nie volhoubaar was nie. Vinton Cerf en andere het besluit om die *Internet Society* (ISOC) te stig met die doel "to keep the Internet going".[340] Een van die hoofdoelwitte was om die IETF 'n nuwe woning te gee, en daarmee saam die befondsing om die Internet werkbaar te hou. Sedert Junie 1995 was die IETF onder die vaandel van ISOC ingeskuif, waarvandaan dit vandag nog funksioneer.[341]

---

335 Marsden *Internet Co-Regulation* 105.

336 Domanski R J *Who Governs the Internet?: A Political Architecture* (2015) 67 verduidelik dit soos volg: "Rough consensus has been the guiding governance principle throughout the lnternet's developmental history. It has been the *de facto* method of generating norms and usable standards in an environment where there has been a historical lack of central regulatory agencies".

337 DiBona *Open Sources* 50.

338 Wikipedia "Internet Engineering Task Force" http://en.wikipedia.org/wiki/Internet_Engineering_Task_Force (besoek op 28 Mei 2014).

339 Cerf V "IETF and the Internet Society" http://www.internetsociety.org/internet/what-internet/history-internet/ietf-and-internet-society (besoek op 28 Mei 2014).

340 Cerf V "IETF and the Internet Society" http://www.internetsociety.org/internet/what-internet/history-internet/ietf-and-internet-society (besoek op 28 Mei 2014).

341 Cerf V "IETF and the Internet Society" http://www.internetsociety.org/internet/what-internet/history-internet/ietf-and-internet-society (besoek op 28 Mei 2014).

5.4.4 World Wide Web Consortium

Die ontwerper van die wêreldwye web, Tim Berners-Lee, het vroeg reeds besef dat die sukses van die web direk afhang van die konsekwente gebruik van standaard-protokolle.[342] Voortgesette standaardisering was 'n vereiste, en Berners-Lee het die *World Wide Web Consortium* (hierna W3C) reeds in 1994 gestig om júís hierdie doel te bereik.[343] Die W3C het net soos die IETF nie 'n formele bestaan as ingelyfde maatskappy nie, en het sy bestaan te danke aan 'n ooreenkoms wat tussen vier gasheer-organisasies gesluit is.[344] Die W3C stel lidmaatskap oop aan enige maatskappy wat 'n belang by Internetstandaarde het. Ten tyde van hierdie skrywe het die W3C 418 lede.[345]

Die W3c se oorhoofse besluitnemingsorgaan is die Adviserende komitee.[346] Elke lid van die W3C moet 'n verteenwoordiger op die Adviserende komitee plaas. Die taak van die Adviserende komitee is om aanstellings te doen vir twee suborgane, te wete die Adviserende raad en die Tegniese Argitektuursgroep.[347] Verder bestaan daar — net soos by die IETF — 'n aantal werksgroepe wat ten doel het om spesifieke kwessies ten aansien van standaarde te beredder.[348] Die Adviserende raad se taak is om werksgroepe te bestuur en van regsadvies te voorsien.[349] Wanneer werksgroepe die standaard voltooi het, word dit na die Tegniese Argitektuursgroep verwys

342 Afd 2.3.5.

343 Teague J C *DHTML and CSS for the World Wide Web* (2001) 4; Anoniem "Facts About W3C" http://www.w3.org/Consortium/facts#history (besoek op 3 Junie 2014).

344 Die vier organisasies wat die ooreenkoms gesluit het, was die Massachusetts Institute of Technology in die VSA, die "European Research Consortium for Informatics and Mathematics", die Keio universiteit in Japan en die Beihang universiteit in Sjina. W3C "Facts about W3C" https://www.w3.org/Consortium/facts (besoek op 19 Mei 2016).

345 W3C "Current Members" https://www.w3.org/Consortium/Member/List (besoek op 19 Mei 2016).

346 W3C "W3C Process Document" https://www.w3.org/2005/10/Process-20051014/organization.html#AB (besoek op 19 Mei 2016).

347 W3C "W3C Process Document" https://www.w3.org/2005/10/Process-20051014/organization.html#AB (besoek op 19 Mei 2016).

348 W3C "W3C Process Document" https://www.w3.org/2005/10/Process-20051014/organization.html#AB (besoek op 19 Mei 2016).

349 W3c "W3C Process Document" https://www.w3.org/2005/10/Process-20051014/organization.html#AB (besoek op 19 Mei 2016).

vir goedkeuring. Hierna kan dit op die Internet in werking gestel word.[350]

Net soos die IETF word nuwe standaarde op 'n relatiewe eenvoudige wyse in werking gestel. Daar bestaan geen behoefte aan ingewikkeld strukture of kwessies van gelyke verteenwoordiging van rolspelers nie. Die W3C stel bloot algemene standaarde wat op 'n tegniese wyse regoor die Internet ingestel kan word.

5.5 Internet-diensverskaffers as Reguleerders

Internet-diensverskaffers (hierna ISP's) speel 'n groot rol by Internetregulering, alhoewel dit nie altyd so opsigtelik voorkom nie.[351] Die rede daarvoor is dat ISP's se hooftaak is om Internet toegang aan gebruikers te verleen. Die oorgrote meerderheid van hierdie maatskappye het 'n winsoogmerk ten doel, en regulering *per se* is nie 'n prioriteit nie. ISP's is gewoonlik die eerste — en dikwels primêre — toegangskanale wat gebruikers en die Internet met mekaar skakel, en daarom is dit nie vreemd nie dat regerings al lank gelede besef het dat ISP's 'n belangrike reguleringsfunksie kan vervul.[352] Die rol van ISP's as tussengangers vir regeringsrolspelers word hieronder by afdeling 6.3.1 in meer besonderhede bespreek.

In hierdie afdeling val die klem egter op die rol wat ISP's *vrywiliglik* speel om die netwerk te manipuleer — gewoonlik tot hulle eie voordeel. In dié konteks is hulle Internetreguleringsrolspelers in eie reg, en nie bloot pionne vir regerings nie.[353]

Die regsgedinge tussen verskeie rolspelers hieronder illustreer die praktiese gevolge van Netwerk Neutraliteit, wat as 'n teoretiese model hierbo by afdeling 4.2.3.1 bespreek is. Dit is daarom belangrik om te begryp dat afdeling 4.2.3.1 en afdeling 5.5.1 in wese saam hoort, want eersgenoemde

350 W3C "W3C Process Document" https://www.w3.org/2005/10/Process-20051014/organization.html#AB (besoek op 19 Mei 2016).

351 Goldsmith J en Wu T *Who Controls the Internet? lllusions of a Borderless World* (2006) 68-72.

352 Goldsmith *Who Controls the Internet?* 68-72.

353 Afd 6.3.1.

is die teoretiese fundering van Netwerk Neutraliteit terwyl laasgenoemde die praktiese toepassing daarvan is. Dit is egter in twee verskillende hoofstukke bespreek aangesien eersgenoemde by die teoretiese fundering tuis hoort, terwyl laasgenoemde aantoon hoe Internetdiensverskaffers reguleringsrolspelers in eie reg is.

Die bespreking van ISP's as reguleerders word voorafgegaan deur 'n baie kriptiese bespreking van die tegnologie van "Deep Packet Inspection", aangesien dit die wyse waarop ISP's kan reguleer, onderlê.

5.5.1 Netwerkmanipulering deur "Deep Packet Inspection"

Reeds in hoofstuk 2 is daar aangedui hoe datapakkette op die Internet tussen bedieners vervoer word.[354] Eenvoudig gestel word inligting in 'n "pakkie" geplaas en sogenaamde "headers" word saam met die pakkie na sy bestemming versend. Tradisioneel het bedieners slegs die "headers" van die datagram gelees en dan die inligting na 'n ander bediener aangestuur. Die inligting wat vir die gebruiker bedoel was, is dus nooit gelees nie.

Die ontwikkeling van 'n nuwe tegnologie, genaamd "deep packet inspection" oftewel dieppakketinspeksie (hierna DPI), het dit alles verander. DPI is 'n tegnologie wat gebruik word om Internet-datagramme deeglik te ondersoek en dan besluite te neem hoe dit verder hanteer moet word.[355] Werbach beskryf dit soos volg:

> Deep packet inspection uses specialized high-speed hardware and software that can identify packets in real-time. A service provider could use deep packet inspection to distinguish peer-to-peer traffic or even just traffic from a single peer-to-peer file-sharing application and either block it or reduce its available bandwidth. Without deep packet inspection, service providers and others could only resort to crude application-level techniques, such as

354 Afd 2.3.3.

355 Mueller M L en Hadi A "Deep Packet Inspection and Bandwidth Management: Battles over BitTorrent in Canada and the United States" 2012 *Telecommunications Policy* 462 462; Frieden R "Internet Packet Sniffing and Its Impact on the Network Neutrality Debate and the Balance of Power Between Intellectual Property Creators and Consumers" 2008 *Fordham Intellectual Property, Media and Entertainment Law Journal* 633 652.

> cutting off all streaming video clips using standard formats after a certain time.[356]

Hierdie hele proses vind binne ’n breukdeel van ’n sekonde plaas.[357] Een van die kenmerke van DPI is dat die datagram se inhoud wat vir die gebruiker bestem was, gelees kan word.[358] Trouens, die datagram kan so deeglik ondersoek word dat daar dikwels vasgestel kan word watter rekenaarprogram (“application”) die datagram gebruik. Proch verduidelik dit so: “DPI also enables network administrators to examine traffic at all network layers across a series of datagrams, giving insight into the source, destination, application, and intent of the traffic in question.”[359] Die tegnologie is al so gevorderd dat ’n datagram aan 2000 operasies en algoritme-vergelykings onderwerp kan word sonder dat die lynspoed van die datagram beïnvloed word.[360]

Die gevolg van hierdie ontwikkeling is dat dit moontlik geword het om Internet-verkeer op ’n bloot tegniese vlak te manipuleer en te reguleer.[361] Mueller wys daarop dat: “(T)his new technological capability seems to carry the potential to fundamentally alter the governance of the Internet.”[362]

Skielik het ISP’s ’n kragtige instrument verkry waarop die netwerk gemanipuleer kon word. Die gebruik van DPI deur Amerika se grootse ISP’s soos Comcast en *Verizon*, asook die gebruik van DPI deur *Bell Canada,* in

---

356 Werbach K “Breaking the Ice: Rethinking Telecommunications Law for the Digital Age” 2005 *Journal on Telecommunications and High Technology Law* 59 92.

357 Radu *The Evolution of Global Internet Governance* 160.

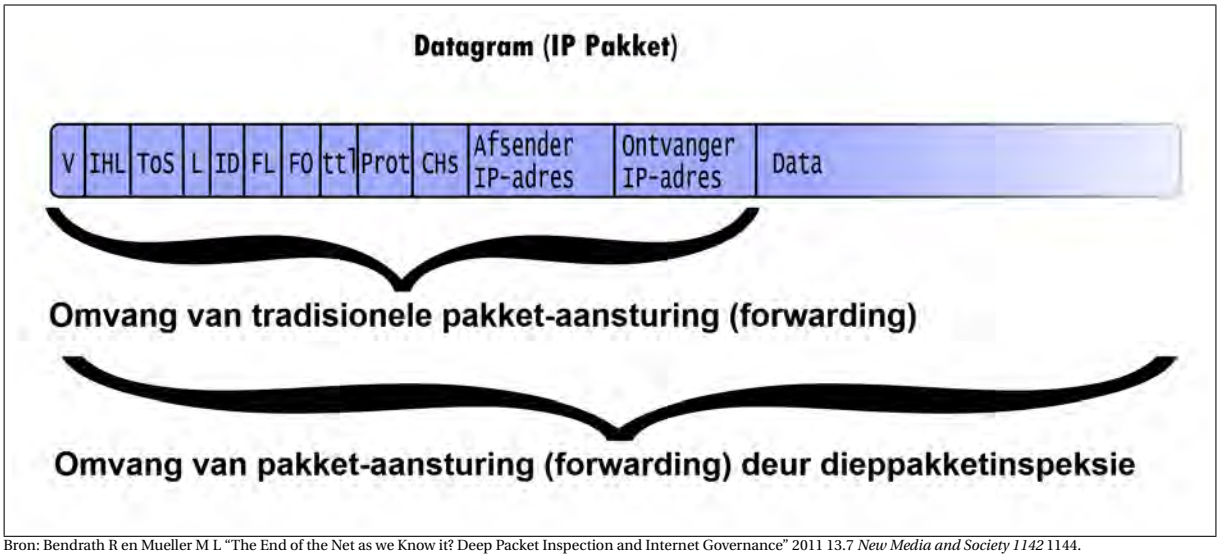
358 Mueller 2012 *Telecommunications Policy* 463.

359 Proch D “Plumb the Depths of Deep Packet Inspection” http://electronicdesign.com/communications/plumb-depths-deep-packet-inspection (besoek op 5 Junie 2014).

360 Proch D “Plumb the Depths of Deep Packet Inspection” http://electronicdesign.com/communications/plumb-depths-deep-packet-inspection (besoek op 5 Junie 2014).

361 Dit wil voorkom asof DPI algemeen gebruik word om P2P-verkeer te blokkeer. Sandoval C “Disclosure, Deception, and Deep-Packet Inspection: The Role of the Federal Trade Commission Act’s Deceptive Conduct Prohibitions in the Net Neutrality Debate” 2009 *Fordham Law Rev*iew 641 666–684; Dischinger M *et al* “Detecting BitTorrent Blocking” *8th ACM SIGCOMM Conference on Internet Measurement ACM 2008*; Kreibich C *et al* “Netalyzr: Illuminating the Edge Network” *10th ACM SIGCOMM Conference on Internet Measurement ACM 2010*.

362 Mueller 2012 *Telecommunications Policy* 463.



Bron: Bendrath R en Mueller M L "The End of the Net as we Know it? Deep Packet Inspection and Internet Governance" 2011 13.7 *New Media and Society 1142* 1144.

Figuur 5.1: *Deep Packet Inspection*-diagram

Kanada, illustreer hierdie fenomeen.

5.5.1.1 Netwerk Neutraliteit in Praktyk

Timothy Wu het die term Netwerk Neutraliteit geskep,[363] maar die probleme wat daarmee saamhang het teen ongeveer dieselfde tyd as wat Wu sy artikel geskryf het, kop uitgesteek. In 2002 reeds het verskeie groot rolspelers, soos *Amazon.com, Microsoft, Yahoo* en *Disney* die High Tech Broadband Coalition (hierna HTBC) geskep met die doel om 'n vrye Internet te bevorder.[364] Dit het in 2003 die "Broadband Principles for Consumer Connectivity" bekend gestel, en hierdie beginsels is in 2004 deur die *Federal Communications Committee* (hierna FCC) aanvaar.[365] Die gevolg was dat die FCC, wat die waghondreguleerder vir die Amerikaanse Telekommunikasiewese is, die beleid van Internetvryheid aanvaar het. Dit is verwoord in die sogenaamde Vier Internet-vryhede, wat behels het dat gebruikers (a) die reg het om wettige inhoud van hulle keuse te gebruik; (b) die reg het om programmatuur van hulle keuse op die Internet te

363 Afd 4.2.3.1.

364 Martinez J P *Net Neutrality: Contributions to the Debate* (2011) 49.

365 Martinez *Net Neutrality* 49.

gebruik; (c) die reg het om enige toestel van hulle keuse aan die Internet in hulle huise te koppel, en (d) die reg het om betekenisvolle inligting oor hulle Internetdiensplan van hulle ISP te verkry.[366] Hierdie Internetvryhede is vinnig getoets toe daar in Maart 2005 'n klagte by die FCC gelê is dat die groot breëbanddiensverskaffer *Madison River* sekere webdienste afsny. Die ondersoek het aangetoon dat dit inderdaad die geval was, en *Madison River* het dadelik onderneem om hierdie gedrag stop te sit.[367] Dit was 'n goeie eerste oorwinning vir Netwerk Neutraliteit-ondersteuners.

5.5.1.2 Die *Comcast*-geval in die VSA

In die VSA word kabel-Internet as 'n inligtingsdiens geklassifiseer, en gevolglik is dit grotendeels ongereguleerd en nie onderworpe aan die strenger regulasiereëls wat die *Communications Act*[368] op Internet-diensverskaffers plaas nie.[369] Om potensiële probleme met hierdie bedeling te voorkom, het die Amerikaanse telekommunikasiereguleerder, naamlik die *Federal Communications Commission* (FCC), in 2005 die *Internet Policy Statement* uitgevaardig waar daar "Four Principles of Internet Freedom" aanvaar is.[370] Daar is egter uitdruklik genoem dat hierdie vier beginsels aan "redelike netwerkbestuur" onderhewig is.[371]

Comcast se gebruikersbasis het in 2005 geweldig gegroei, en dit was duidelik dat netwerkbestuur nodig was om die saak te beredder.[372] Comcast het ondersoek ingestel, en het bevind dat "Peer-to-peer file sharing" (hierna P2P)[373] — wat dikwels verantwoordelik is vir onwettige verspreiding van

366 Martinez *Net Neutrality* 49; Dickerson N P "What Makes the Internet so Special? And Why, Where, How, and by Whom Should its Content be Regulated? 2009 *Houston Law Review* 61 96; Marsden C T *Net Neutrality: Towards a Co-regulatory Solution* (2010) 34; Mueller 2012 *Telecommunications Policy* 464.

367 Martinez *Net Neutrality* 50.

368 *Title II of the Communications Act of 1934 48 Stat 1064.*

369 Mueller 2012 *Telecommunications Policy* 464.

370 Mueller 2012 *Telecommunications Policy* 464. ; Martinez *Net Neutrality* 50.

371 Mueller 2012 *Telecommunications Policy* 464.

372 Bendrath R en Mueller M L "The End of the Net as We Know it? Deep Packet Inspection and Internet Governance" 2011 *New Media and Society* 1142 1152.

373 Federal Trade Commission *Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition*

digitale inligting soos films en musiek — vir die netwerkopeenhoping verantwoordelik was.[374] Om dit reg te stel het Comcast 'n nuwe toestel wat op die mark beskikbaar geword het, op hul netwerk geïnstalleer. Die toestel het dit vir Comcast moontlik gemaak om die protokol wat P2P-klante gebruik om hulle data te versprei, te manipuleer deur die hoeveelheid datagramme te tel, en indien dit 'n sekere telling bereik, dit eenvoudig af te sny. Sodoende het Comcast dit reggekry om persone wat buitensporige hoeveelhede data op hul netwerk gebruik, te beperk. Dit alles het Comcast gedoen sonder om 'n woord aan sy gebruikersbasis daaroor te rep.[375]

Dit het Comcast-gebruikers nie lank geneem om hierdie nuwe beleid te bespeur en die algemene publiek daaroor in te lig nie.[376] Comcast het die fout gemaak om eers te ontken dat die nuwe beleid in werking gestel is om spesifiek P2P-verkeer te filtreer, en later het Comcast aan die FCC verklaar dat hulle slegs P2P-verkeer tydens spitstye gemanipuleer het — terwyl dit later geblyk het dat beide stellings onwaar was.[377]

Op versoek van 'n vloedgolf van ontstelde Comcast-gebruikers het die FCC die saak ondersoek, en bevind dat: "Comcast's practices were discriminatory and did not constitute reasonable network management."[378] Comcast was ook skuldig bevind aan 'n gebrek om sy gebruikers van sy nuwe netwerkbeheerbeleid in kennis te stel.[379]

Issues: A Federal Trade Commission Staff Workshop Report (2005) 3 definieer lêerverspreiding so: "Broadly defined, P2P technology is a distributed computing software architecture that enables individual computers to connect to and communicate directly with other computers. Through this connection, computer users (known as 'peers') can share communications, processing power, and data files."

374 Bendrath 2011 *New Media and Society* 1152.

375 Bendrath 2011 *New Media and Society* 1152. Sien ook Sylvain O "Internet Governance and Democratic Legitimacy" 2010 *Federal Communications Law Journal* 205 218.

376 Bendrath 2011 *New Media and Society* 1152.

377 Bendrath 2011 *New Media and Society* 1152.

378 Comcast Network Management Practices Order FCC-08-183 WC Docket no 07-52. Beskikbaar op die Internet by Federal Communications Commission "Memorandum Opinion and Order" https://apps.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf (besoek op 4 September 2014).

379 Comcast Network Management Practices Order FCC-08-183 WC Docket no 07-52. Beskikbaar op die Internet by Federal Communications Commission "Memorandum Opinion and Order" https://apps.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf (besoek op 4 September 2014).

Die FCC-bevel het Comcast verder verbied om slegs die P2P-protokol te filtreer, en het Comcast beveel om nuwe metodes te vind om hulle netwerk te bestuur op 'n wyse wat nie teen enige spesifieke protokol gerig is nie.[380]

Die kombinasie van negatiewe publisiteit by Internetgebruikers en die FCC-beslissing het Comcast laat besluit om hulle bestaande gebruik van DPI te staak.[381] In September 2008 het Comcast egter 'n veranderde netwerkbestuursbeleid by die FCC ingehandig waarvolgens Comcast hulle netwerk in 15-minuut-intervalle sou toets om te sien waar die opeenhoping voorkom. Individuele gebruikers se datagramme wat die opeenhoping veroorsaak, word dan beperk. Op so 'n wyse word geen protokol afgesny nie, maar wel 'n spesifieke gebruiker wat die netwerk misbruik.[382]

Alhoewel Comcast aan die *FCC* se beslissings gehoor gegee het, het dié maatskappy 'n hofgeding teen die FCC aanhangig gemaak om laasgenoemde se gesag ten opsigte van Comcast se netwerkbestuursbeginsels te toets.[383] Comcast het beweer dat netwerkbestuursbeleid buite die sfeer van die FCC se gesag val, en die hof het Comcast gelyk gegee.[384]

Dit mag dalk vreemd voorkom dat 'n hof kan bevind dat 'n onafhanklike reguleerder soos die FCC nie by magte is om 'n ISP soos Comcast te reguleer nie. Die rede vir hierdie anomalie is te vinde in die feit dat die VSA 'n eienaardige sisteem het waarvolgens telekommunikasiesektore as óf 'n telekommunikasiediens óf 'n sogenaamde "common carrier" geklassifiseer moet word.[385] Die FCC het vroeg in die bestaan van die Internet alle kabel-Internet-diensverskaffers as 'n telekommunikasiediens geklassifiseer, wat beteken het dat die strenger reëls wat op "common carriers" van toepassing was, nie sou geld nie. Dus het die FCC, ten spyte daarvan dat dit die

380 Comcast Network Management Practices Order FCC-08-183 WC Docket no 07-52. Beskikbaar op die Internet by Federal Communications Commission "Memorandum Opinion and Order" https://apps.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf (besoek op 4 September 2014).

381 Mueller 2012 *Telecommunications Policy* 466.

382 Mueller 2012 *Telecommunications Policy* 466.

383 *Comcast v FCC* US Court of Appeals for the DC circuit April 6 2010 440 US.

384 Op 661 van die beslissing.

385 Volgens die *Communications Act of 1934* moet sodanige klassifikasie geskied.

VSA se nasionale reguleerder is, nie die bevoegdheid om sekere reëls vir telekommunikasiediensverskaffers neer te lê nie.

Die gevolg van die beslissing was dat die FCC nuwe, afgewaterde regulasies neergelê het in die vorm van die *Open Internet Order*.[386] Daarin word aanvaar dat ISP's hulle netwerke moet bestuur, maar word gemeld dat dit redelik moet wees,[387] en nie poog om ander oogmerke, soos verspreiding van onwettige materiaal, te reguleer nie.[388]

5.5.1.3 Die *Verizon*-geval in die VSA

Die Open Internet Order is egter in 2014 aangeveg in die saak van *Verizon Communications Inc v Federal Communications Commission*.[389] Die hof verduidelik dat die Open Internet Order onderskeid maak tussen landlyn-Internet-diensverskaffers en mobiele Internet-diensverskaffers.[390] Beide tipes ISP's word vereis om nie enige vorm van blokkering toe te pas nie, maar landlyn-Internet-diensverskaffers word verbied om enige vorm van smoring van 'n Internetdiens toe te pas.[391] Dan verduidelik die hof dat die kwessie voor hom nie een van Netwerk Neutraliteit *per se* is nie, maar eerder die kwessie of die FCC by magte is om Internetdiensverskaffers te reguleer.[392] Die hof lewer dus geen uitspraak oor die beginsel van Netwerk Neutraliteit

386 Sien Federal Communications Commission "In the Matter of Preserving the Open Internet" FCC 10-201. Die FCC-beslissing is vryelik beskikbaar by Anoniem "In the Matter of Preserving the Open Internet" https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf (besoek op 20 Junie 2014).

387 Par 82 van die *Open Internet Order* omskryf redelike netwerkbestuur as: "A network management practice is reasonable if it is appropriate and tailored to achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband Internet access service." Federal Communications Commission "In the Matter of Preserving the Open Internet" FCC 10-201. Die FCC-beslissing is vryelik beskikbaar by Anoniem "In the Matter of Preserving the Open Internet" https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf (besoek op 20 Junie 2014) par 82 17952.

388 Sien Federal Communications Commission "In the Matter of Preserving the Open Internet" FCC 10-201. Die FCC-beslissing is vryelik beskikbaar by Anoniem "In the Matter of Preserving the Open Internet" https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf (besoek op 20 Junie 2014).

389 *Verizon v FCC* 740 F 3d 623 — Court of Appeals Dist of Columbia Circuit 2014.

390 Op 633 van die beslissing.

391 Op 633 van die beslissing.

392 634.

nie.

Net soos in die geval van *Comcast v FCC* beslis die hof dat die FCC nie *Verizon* kan reguleer nie, aangesien dit nie 'n "common carrier" is nie.[393] Die smorings- en blokkeringsreëls word ongeldig verklaar.[394]

Die gevolg van die uitspraak was dat 'n ISP dus gebruikersverkeer kan smoor ("throttle") soos hulle goedvind, of selfs uit-en-uit blokkeer. Dit was 'n groot oorwinning vir ISP's.

Dit is egter belangrik om weer die punt te maak dat die hof in beide die *Comcast*- en *Verizon*-sake genoem het dat hulle taak nie is om oor die beginsel van Netwerk Neutraliteit te beslis nie, maar bloot om te bepaal of die FCC binne hulle bevoegdheidsfeer opgetree het om die reëls neer te lê.[395] In beide gevalle het dit geblyk dat die FCC buite hulle bevoegdheidsfeer opgetree het.

Alhoewel beide *Comcast* en *Verizon* hulle sake teen die FCC gewen het, was die uitkoms baie gunstig vir die gebruikers van hierdie ISP's. *Comcast* het byvoorbeeld sy gebruik van DPI so aangepas dat dit nie teen spesifieke protokolle diskrimineer nie, maar eerder teen gebruikers wat eensydig die netwerk misbruik.[396] *Verizon* het na die oorwinning oor die FCC in 2014 genoem dat hulle diens soos gewoon sal voortgaan, en dat die oorwinning nie Internetgebruikers negatief sal raak nie.[397]

In November 2014 het president Obama aanbeveel dat die FCC

---

393 659.

394 659.

395 In die *Verizon*-saak het die hof gemeld:

> Before beginning our analysis, we think it important to emphasize that although the question of net neutrality implicates serious policy questions, which have engaged lawmakers, regulators, businesses, and other members of the public for years, our inquiry here is relatively limited... Accordingly, our task as a reviewing court is not to assess the wisdom of the Open Internet Order regulations, but rather to determine whether the Commission has demonstrated that the regulations fall within the scope of its statutory grant of authority.

Op 634 van die beslissing.

396 Mueller M L en Asghari H "Deep Packet Inspection and Bandwidth Management: Battles Over BitTorrent in Canada and the United States" 2012 *Telecommunications Policy* 462 465–466.

397 Cicconi J "AT&T Statement on the US Court of Appeals D.C. Circuit Open Internet Decision" http://www.attpublicpolicy.com/fcc/att-statement-on-the-u-s-court-of-appeals-d-c-circuit-open-internet-decision/ (besoek op 6 Junie 2014).

breëband-Internetdienste as "common carriers" moet klassifiseer.[398] Deur dit te doen sal Internet-diensverskaffers onder die regulering-sambreel van die FCC val. Teen Februarie 2015 het die FCC hierdie aanbeveling ingevoer,[399] en in April 2015 het die FCC 'n nuwe lywige beleid getiteld "Protecting and Promoting the Open Internet" vrygestel.[400] Binne minute na die vrystelling van die dokument het US Telecom, 'n ISP-konsortium, 'n hofsaak teen die FCC aanhangig gemaak.[401] Dit is as't ware die oorlogsverklaring, aangesien die FCC se herklassifisering van breëband-Internetdienste die ISP's onder 'n nuwe bedeling plaas wat heelwat meer administratiewe gevolge inhou.[402] Die konsortium van ISP's het reeds aangetoon dat hulle die Netwerk Neutraliteitsbeginsels van die FCC sal aanvaar, maar nie die herklassifisering wat die FCC deurgevoer het nie.[403] Die gevolg is dat die aangeleentheid reeds deur verskeie regsprosesse geneem is,[404] maar die saak van *United States Telecom Association v FCC* is ten tyde van hierdie skrywe nog nie beslis nie.[405]

---

398 New York Times "Obama Asks F.C.C. to Adopt Tough Net Neutrality Rules" http://www.nytimes.com/2014/11/11/technology/obama-net-neutrality-fcc.html (besoek op 13 April 2016).

399 Federal Communications Commission *FCC Adopts Strong, Sustainable Rules to Protect the Open Internet* (2015) 1. In die persverklaring word die rede vir die herklassifisering uiteengesit:

> Today, the Commission — once and for all — enacts strong, sustainable rules, grounded in multiple sources of legal authority, to ensure that Americans reap the economic, social, and civic benefits of an Open Internet today and into the future. These new rules are guided by three principles: America's broadband networks must be fast, fair and open.

400 Federal Communications Commission *Protecting and Promoting the Open Internet* Federal Register Vol 80 No 70 April 13 2015.

401 Cnet "Net Neutrality Rules get Published — Let the Lawsuits Begin" http://www.cnet.com/news/fccs-net-neutrality-rules-hit-federal-register-lawsuit-underway/ (besoek op 13 April 2016).

402 Cnet "Net Neutrality Rules get Published — Let the Lawsuits Begin" http://www.cnet.com/news/fccs-net-neutrality-rules-hit-federal-register-lawsuit-underway/ (besoek op 13 April 2016).

403 Reuters "AT&T, US Telecom Groups Seek to Block New Internet Rules" http://in.reuters.com/article/usa-internet-neutrality-idINKBN0NM4AH20150501 (besoek op 13 April 2016).

404 Law 360 "Telecom Cases To Watch In 2016" http://www.law360.com/articles/737221/telecom-cases-to-watch-in-2016 (besoek op 13 April 2016).

405 'n Oorsig van *United States Telecom Association v FCC* asook al die ondersteunende dokumente daarvan is te vinde by US Chamber Litigation Center "United States Telecom Association v FCC" http://www.chamberlitigation.com/united-states-telecom-association-v-fcc-et-al (besoek op 13 April 2016).

5.5.1.4 Diensverskaffer-regulering in Kanada

Gedurende dieselfde tyd wat Comcast sy DPI in die VSA begin het (2005), het 'n bykans soortgelyke situasie hom in Kanada met Bell Canada afgespeel. Voordat die saak egter bespreek kan word, moet die verskille in die regulatoriese sisteem tussen die VSA en Kanada kortliks uitgestip word.

Soos hierbo bespreek is die VSA se telekommunikasiereguleerder die FCC, wat by magte is om grotendeels "common carriers" te reguleer, maar nie telekommunikasiedienste nie. Hierteenoor word Kanadese telekommunikasie deur die Canadian Radio–Television and Telecommunications Commission (CRTC) gereguleer.[406] Laasgenoemde het egter die voordeel bo die Amerikaanse FCC dat *alle* kommunikasie gereguleer kan word.[407] 'n Verdere verskil tussen die Amerikaanse en Kanadese reguleringsisteme is dat Kanada 'n telekommunikasiemonopolie het waar een rolspeler, te wete Bell Canada, bykans die hele mark oorheers.[408] Gevolglik is Bell Canada deur die regering verplig om bandwydte aan kleiner ISP's teen 'n groothandelprys te verkoop en so 'n meer kompeterende mark te skep.[409] Bell Canada het ook sy eie kleinhandelsfiliaal genaamd Sympatico wat op kleinhandelvlak met die kleiner ISP's kompeteer.[410]

In 2007 en 2008 het ISP's in Kanada begin om DPI op hulle netwerke toe te pas. Sommige het gefokus om P2P protokolle se verkeer die heel dag te beperk (soortgelyk aan Comcast se aanvanklike gebruik van DPI); ander het weer slegs P2P op nie-spitstye beperk.[411] Sommige ISP's het besluit om eerder gebruikers se Internet-toegang te beperk tot 'n sekere volume per maand (algemeen bekend as "capping"), terwyl ander ISP's glad nie DPI gebruik het nie, maar eerder hulle kapasiteit probeer verhoog het.[412] Bell

406 Mueller 2012 *Telecommunications Policy* 466.
407 Mueller 2012 *Telecommunications Policy* 466.
408 Bendrath 2011 *New Media and Society* 1153.
409 Mueller 2012 *Telecommunications Policy* 466.
410 Mueller 2012 *Telecommunications Policy* 466.
411 Mueller 2012 *Telecommunications Policy* 466.
412 Mueller 2012 *Telecommunications Policy* 467.

Canada se kleinhandelfiliaal, Sympatico, het ook DPI begin gebruik. Soos te verstane het gebruikers begin om te kla, en Bell Canada se bestuur het besef dat hulle eintlik hulle groothandelverkope bevorder het omdat DPI nie dáár plaasvind nie, en alle besparings van bandwydte wat Sympatico meebring, aan die groothandel gelewer word sonder enige voordele vir Bell Canada.[413]

Die bestuur van Bell Canada het eensydig besluit om DPI ook na hulle groothandelkanaal uit te brei.[414] Al die kleiner ISP's wat by Bell Canada hulle bandwydte gekoop het, was nou beïnvloed deur die gebruik van DPI, en kon dus nie self besluit of hulle DPI aan hulle eie gebruikers wou bekend stel nie. Mueller verduidelik dit so: "If DPI-based throttling was applied to the wholesale G(ateway) A(ccess) S(ervice), the smaller retail ISPs dependent on Bell Canada facilities could not offer customers a service without such throttling."[415]

Die Canadian Association of Internet Providers (CAIP), wat die vereniging is waar kleiner ISP's met mekaar kan skakel om gemeenskaplike belange te bevorder, het dadelik 'n aansoek by die Kanadese reguleerder (die CRTC) ingedien om Bell Canada te verplig om nie DPI teenoor hulle toe te pas nie.

Die CRTC het bevind dat Bell Canada korrek opgetree het in die hantering van sy netwerkopeenhopingsprobleme, en dat die gebruik van DPI nie 'n oortreding van die groothandeltariefbepalings was nie.[416]

Hierdie beslissing het die CRTC egter laat besef dat die groter aangeleentheid van sinvolle netwerkbestuur van ISP's aangespreek sal moet word. 'n "Telecom Public Notice CRTC 2008–19" is uitgevaardig waar ISP's se netwerkbestuur onder die soeklig geplaas sou word.[417] Dit beteken dat 'n

413 Mueller 2012 *Telecommunications Policy* 467.

414 Mueller 2012 *Telecommunications Policy* 467.

415 Mueller 2012 *Telecommunications Policy* 467.

416 Sien die CRTC Beslissing: The Canadian Association of Internet Providers' Application Regarding Bell Canada's Traffic Shaping of its Wholesale Gateway Access Service Telecom Decision CRTC 2008–108 20 Nov 2008 by Anoniem "Telecom Decision CRTC 2008–108" http://www.crtc.gc.ca/eng/archive/2008/dt2008-108.htm#archived (besoek op 15 September 2014).

417 Mueller 2012 *Telecommunications Policy* 468.

publieke forum geskep word waar alle rolspelers hulle saak kan stel, en die CRTC dan ’n beleidsdokument saamstel.

Die finale beleidsdokument is op vier beginsels gebou, te wete deursigtigheid, innovering, duidelikheid en neutraliteit.[418] Deursigtigheid het behels dat ISP’s hulle netwerkbestuursbeginsels aan gebruikers moet verduidelik; innovering het behels dat ISP’s primêr van netwerkuitbreiding gebruik moet maak om opeenhopings te beperk; duidelikheid het behels dat ISP’s nie sekere protokolle mag blokkeer nie, en neutraliteit het te doen gehad met die handhawing van kompetisie tussen ISP’s.[419]

Die gevolg van die gebruik van DPI deur Bell Canada was dat die nasionale kommunikasiereguleerder nuwe regulasies vir die land geskep het. Tog is die interessante gevolg dat ten spyte van die nuwe regulasies, die gebruik van DPI deur ál die ISP’s in Kanada verhoog het.[420] Die gebruik van DPI was dus hoër ná die nuwe regulasies as daarvoor.

5.5.1.5 *Deep Packet Inspection* as Reguleringshulpmiddel

Dit is baie insiggewend dat wanneer mens die VSA-scenario met dié van Kanada vergelyk, ’n eienaardige prentjie ontvou. Waar die VSA se regulering van DPI in duie gestort het, het dit tot gevolg gehad dat DPI *minder* gebruik is (en gebruikers dus bevoordeel is), terwyl die strenger regulering van DPI in Kanada die teenoorgestelde effek gehad het. Daar het die regulering van DPI tot nadeel van die algemene gebruiker gestrek deurdat die gebruik van DPI *toegeneem* het.[421]

Mueller toon met statistiese data aan dat die gebruik van DPI in die VSA én Kanada ’n effek op Internetregulering gehad het: “DPI does have

418 Mueller 2012 *Telecommunications Policy* 468.

419 Mueller 2012 *Telecommunications Policy* 468–469.

420 Mueller 2012 *Telecommunications Policy* 470–473 waar hy statistiese data gebruik wat die verhoogde gebruik van DPI illustreer.

421 Die VSA en Kanada is nie die enigste lande wat DPI gebruik nie. Vir ’n oorsig van DPI-gebruik in Brittanje, sien Bitso C, Fourie I en Bothma T “Trends in Transition From Classical Censorship to Internet Censorship: Selected Country Overviews” 2012 *FAIFE Spotlight* 182.

disruptive effects on Internet governance. It thrusts into the hands of network operators powerful new capabilities to manipulate traffic."[422] Wat egter vreemd is, is dat die land met méér regulering van DPI (Kanada) swakker gevaar het om ISP's te ontmoedig om DPI te gebruik as die land waar DPI-regulering gefaal het (die VSA). Mueller erken dat hy nie dié statistiek kan verklaar nie.[423]

Alhoewel die doel van die bespreking van DPI-gebruik deur ISP's in hierdie afdeling was om te illustreer hoe ISP's in eie reg reguleringsrolspelers kan wees, word daar aan die hand gedoen dat die verklaring van die anomalie soos hierbo te vinde, is in die feit dat Bell Canada steeds 'n monopolie bly. Die CRTC se goedkeuring van die gebruik van DPI was as't ware 'n bevestiging vir Bell Canada dat hulle kan voortgaan met hierdie praktyk. Die kleiner ISP's het nie 'n keuse gehad nie, en moes eenvoudig hulle eie besigheidsmodelle aanpas met die DPI-data-pakkette wat hulle van Bell Canada ontvang het. Daarteenoor is daar werklike kompetisie in die Amerikaanse mark, en Comcast sou ongetwyfeld 'n deel van sy markaandeel moes inboet as dit aangehou het om DPI so toe te pas dat gebruikers na 'n ander ISP sou oorskakel.

Hoe dit ook al sy, die gebruik van 'n nuwe tegnologie soos deep packet inspection wys in welke mate dit die vermoë het om regulatoriese veranderinge in die Internet te bewerkstellig.

Die laaste woord oor die gebruik van deep packet inspection is geensins geskryf nie, want dit wil voorkom asof ISP's hierdie tegnologie wil gebruik om verskillende produkte te skep.[424] Dit is moontlik om byvoorbeeld alle P2P protokolle met DPI te blokkeer (soos hierbo aangetoon), en dan 'n afsonderlike produk saam te stel waarby gebruikers kan inskakel om P2P-protokolle te gebruik.[425] Die ISP kry dit dan reg dat die gebruiker

422 Mueller 2012 *Telecommunications Policy* 473.

423 Mueller 2012 *Telecommunications Policy* 474.

424 Bendrath 2011 *New Media and Society* 1145.

425 Bendrath 2011 *New Media and Society* 1145.

twee subskripsies moet uitneem — een vir die gebruik van die "gewone" protokolle van die Internet, soos die web (http)[426] en e-pos (smtp),[427] en 'n tweede subskripsie vir P2P soos Bittorrent.[428] Dit sal selfs moontlik wees om 'n afsonderlike subskripsie vir "video-on-demand" te skep.[429] Die gevolg is dat die ISP hoër winste kan genereer deur afsonderlike produkte daar te stel.

5.6 Gevolgtrekking

Verskeie rolspelers het saamgewerk om die Internet tot stand te bring en dit te ontwikkel tot die internasionale verskynsel wat dit vandag is.[430] Hierdie rolspelers het gewissel van klein organisasies tot multinasionale maatskappye. Regulering was vroeg reeds noodsaaklik, en aangesien state nog geensins in die regulering van die ontwikkelende Internet betrokke was nie, is regulering deur verskeie internasionale organisasies bedryf.[431] Hulle het gewissel van "informele" internasionale organisasies tot entiteite wat deur die Verenigde Nasies in die lewe geroep is.

Om enigsins in die sfeer van die tradisionele Internasionale reg te wil funksioneer, moet internasionale organisasies aan sekere vereistes

426 Toexcell Inc *Hypertext Transfer Protocol HTTP 1.0 Specifications* (1999) vii beskou http eenvoudig as: "The Hypertext Transfer Protocol (HTTP) is an application-level protocol that makes the World Wide Web 'tick'".

427 Die "Simple Mail Transfer Protocol" (smtp) word gebruik om e-poskommunikasie moontlik te maak. Miller P *TCP/IP: The Ultimate Protocol Guide* (2009) 655 beskryf smtp so: "It is the Simple Mail Transfer Protocol (SMTP) that is used to deliver mail from the client to a server, and indeed that servers then use to transfer mail between themselves when they are acting as relay agents".

428 Bittorrent is 'n rekenaarsagtewareprogram wat gebruik word om groot hoeveelhede data van ander gebruikers af te laai. Rutenbeck J *Tech Terms: What Every Telecommunications and Digital Media Professional Should Know* (2012) 27 beskryf dit so: "A peer-to-peer file-sharing platform particularly well suited to distributing very large digital files (e.g., concerts, movies, television shows) because it takes advantage of the unused bandwidth of broadband network connections. Instead of connecting to a single computer to download a file, BitTorrent works by connecting that user with potentially hundreds of other computers to download individual parts of the file that are put together once all of the pieces have reached their destination".

429 Werbach 2008 *University of California Davis Law Review* 376.

430 Afd 5.1.

431 Afd 5.1.

voldoen.[432] Daar is verduidelik hoe internasionale organisasies so onlangs as een-en-'n-half eeue gelede onbekend in die Internasionale Reg was, en die werking van internasionale organisasies 'n relatief nuwe verskynsel in die Volkereg is.[433] Om konteks aan die onderwerp onder bespreking te gee, is die voorbeeld van die Verenigde Nasies as internasionale organisasie uitgewys, en hoe daar in die *Reparation for Injuries Suffered in the Service of the United Nations*-beslissing[434] verklaar is dat die Verenigde Nasies wél regspersoonlikheid geniet, en dus in die internasionale sfeer kan funksioneer.[435]

Sedert daardie beslissing in 1949 gegee is, het internasionale organisasies 'n groterwordende rol in die Internasionale reg begin speel.[436] Trouens, daar bestaan tans verskeie kategorieë internasionale organisasies, en dit wil voorkom asof hierdie tendens nie spoedig sal verander nie.[437]

Die vinnige ontwikkeling van die Internet het tot gevolg gehad dat internasionale organisasies wat met die Internet te doen het, dikwels nie aan die strenger vereistes van internasionale organisasies ingevolge die Internasionale Reg voldoen het nie, en dit is tot op hede nog die geval.[438] Daarom is die hoofstuk verdeel in internasionale organisasies wat deur verdrae geskep is (die "tradisionele" beskouing volgens die Internasionale reg), asook "ander" internasionale organisasies wat nie deur verdrae in die lewe geroep is nie.

Die eerste internasionale organisasie wat bespreek is, is die "Internet Governance Forum".[439] Dit is gestig deur die "World Summit on the Information Society I", wat in 2003 plaasgevind het. Die doel van die

---

432 Afd 5.2.

433 Afd 5.2.

434 *Reparation for Injuries Suffered in the Service of the United Nations* International Court of Justice Reports 1949 174.

435 Afd 5.2.

436 Afd 5.2.

437 Afd 5.2.

438 Afd 5.2.

439 Afd 5.3.2.

IGF is om ’n globale gespreksforum te vorm om Internetregulerings-aangeleenthede te bespreek. Dit het sedert 2006 op ’n jaarlikse basis vergader.[440] Die IGF funksioneer inderdaad baie goed as gespreksforum, maar sedert sy ontstaan het die IGF nog geen formele besluite geneem nie, en selfs indien dit kon, sou daar geen meganisme wees om dit in werking te stel nie. Daarom word die IGF wyd gekritiseer as ’n “talk-shop” wat geen uitvoerbare besluite kan neem nie.[441] Tog hou die IGF die voordeel in dat dit verskeie Internetreguleringsrolspelers op ’n jaarlikse basis bymekaar bring om met mekaar te netwerk en gedagtes uit te ruil.[442]

Hierteenoor is die Internasionale Telekommunikasie Unie, wat tweede bespreek is, ’n magtige organisasie wat in sy bestaan van meer as ’n eeu al geweldig baie vermag het.[443] Lidmaatskap van die ITU word beperk tot state, en formele besluite word geneem wat in sogenaamde “internasionale telekommunikasieregulasies” uitgevaardig word.[444] Dit word dan onder lidlande versprei, wat dit in nasionale wetgewing in werking stel.[445]

Sedert die laat 1990’s probeer die ITU om ’n groter rol by Internetregulering te vervul.[446] Die VSA, wat effektiewe beheer oor die basisfunksies van die Internet uitoefen, was van mening dat ITU-betrokkenheid ten aansien van Internetregulering ’n poging is om die beheer van die Internet uit sy mag te neem.[447] Dit het in ’n magstryd ontwikkel wat tot op hede nog bestaan.[448] Dit wil voorkom asof die ITU huidig deur veral Sjina en Rusland gebruik word as ’n instrument om Internetregulering binne die uitsluitlike sfeer van state te probeer plaas.[449] Die gevolg hiervan is dat

440 Afd 5.3.2.
441 Afd 5.3.2.5.
442 Afd 5.3.2.4.
443 Afd 5.3.3.
444 Afd 5.3.3.3.
445 Afd 5.3.3.3.
446 Afd 5.3.3.2.
447 Afd 5.3.3.2.
448 Afd 5.3.3.2.
449 Afd 5.3.3.3.

state wat nie hierdie ideologie voorstaan nie, soos Europa en die VSA, baie sterk standpunt inneem om *nie* die ITU in staat te stel om enigsins by Internetregulering betrokke te raak nie.[450] Die uiteinde van die saak is dat dit wil voorkom asof die ITU so verpolitiseer het dat dit nie die aangewese internasionale organisasie is om fundamentele regulering van die Internet in die internasionale sfeer te verrig nie.

Die Raad van Europa is volgende bespreek.[451] Dit is deur die verdrag van Londen in 1949 geskep met die doel om menseregte binne die groter Europa en die wêreld te bevorder.[452] Hierdie internasionale organisasie se bydrae tot regsbeheer van die Internet is geleë in die Konvensie op Kubermisdaad.[453] Omdat kubermisdaad 'n wêreldwye verskynsel is, is die konvensie vir alle state van die wêreld oopgestel, en het verskeie state buite Europa, onder meer die VSA en Suid-Afrika, reeds hierdie konvensie onderteken.[454] Die Raad van Europa se bydrae tot Internetregulering is om *gedrag op* die Internet te reguleer, eerder as regulering van die werking van die Internet self.[455] Die bespreking van die Raad van Europa het die afdeling van internasionale organisasies geskep deur verdrae, afgesluit.

Die "Internet Corporation for Assigned Names and Numbers" (ICANN) is 'n vreemdheid binne die Internasionale Reg. Dit is 'n nie-winsgewende organisasie wat ingelyf is volgens die wette van Kalifornië in die VSA.[456] Daarom is dit onderworpe aan die jurisdiksie van die VSA, en val dit nie binne die internasionale sfeer soos tradisionele internasionale maatskappye nie.[457] Dit is daarom nie vreemd dat ICANN in sy bestaan reeds baie kritiek ontvang het nie.[458]

450 Afd 5.3.3.5.
451 Afd 5.3.4.
452 Afd 5.3.4.
453 Afd 5.3.4.
454 Afd 5.3.4.
455 Afd 5.3.4.
456 Afd 5.4.1.
457 Afd 5.4.1.
458 Afd 5.4.1.4.

ICANN is in 1998 gestig met die spesifieke doel om die IANA-funksie te verrig.[459] Dit funksioneer as 'n multi-belangegroep-organisasie, wat beteken dat ICANN uit 'n verskeidenheid kleiner groepe bestaan wat elkeen spesifieke belange op die Internet verteenwoordig.[460] Hierdie verskillende belangegroepe lewer almal insette oor sake van gemeenskaplike belang, en terugvoer word na die ICANN-raad geneem vir uiteindelike besluitneming.[461] Dit is uiteraard 'n baie omslagtige proses.

ICANN vervul tans tegniese regulering van die IANA-funksie, maar dit staan steeds onder die beheer van die VSA, wat steeds 'n oorsigfunksie oor ICANN uitoefen.[462] In Maart 2016 het ICANN 'n formele aansoek gebring om die IANA-funksie in sy geheel oor te neem, en dit word tydens hierdie skrywe deur die Amerikaanse regering oorweeg.[463]

Die "Internet Society" (ISOC) is tegnies 'n internasionale nie-regeringsorganisasie aangesien dit nie deur enige regering gestig is nie, maar eerder deur 'n groep ontwikkelaars van die vroeë Internet tot stand gebring is.[464] Die doel daarvan is om sekere tegniese komitees wat die effektiewe werking van die Internet verseker, te huisves.[465] ISOC poog om so inklusief moontlik te wees, en daarom is daar takkantore regoor die wêreld te vinde.[466]

Die "Internet Engineering Task Force" (IETF) is 'n informele groepering wat ten doel het om tegniese kwessies ten opsigte van die Internet op te los.[467] Dit voer geen fisiese bestaan nie, en is dus nie ingelyf of geregistreer as 'n amptelike entiteit nie. Die IETF funksioneer geheel en al deur gebruikmaking van vrywilligers, en val struktureel onder die sambreel van

459 Afd 5.4.1.
460 Afd 5.4.1.3.
461 Afd 5.4.1.2.
462 Afd 5.4.1.5.
463 Afd 5.4.1.5.
464 Afd 5.4.2.
465 Afd 5.4.2.
466 Afd 5.4.2.
467 Afd 5.4.3.

ISOC.[468]

Die laaste organisasie wat onder bespreking geneem is en wat tegniese regulering vir die Internet verrig, is die "World Wide Web Consortium" (W3C).[469] Dit is reeds in 1994 gestig met die uitsluitlike doel om protokolle vir die Web te standaardiseer.[470] Die W3C se lidmaatskap bestaan uit privaatmaatskappye wat 'n belang by web-protokolstandaardisering het.[471] 'n Adviserende raad doen aanstellings op 'n Tegniese Argitektuursgroep, en laasgenoemde is verantwoordelik om werkgroepe wat protokolstandaarde geskep het, te evalueer en goed te keur waarna dit op die groter Internet in werking gestel kan word.[472]

Omdat hierdie hoofstuk oor nie-regeringreguleringrolspelers gehandel het, is die werking van Internetdiensverskaffers (ISP's) as besprekingspunt ingesluit.[473] Die rede daarvoor is dat ISP's nie slegs deur state gebruik word om regulering van hul staat-intranette te bewerkstellig nie, maar dat ISP's in eie reg ook kragtige reguleerders is.[474] 'n Kragtige instrument wat ISP's gebruik om regulering op hul netwerke te bewerkstellig, is "deep packet inspection" oftewel dieppakketinspeksie (DPI).[475]

Die gebruik van DPI stel ISP's in staat om alle data wat oor hulle netwerke vloei, diepliggend te ondersoek.[476] Deur dit te doen kan sekere data óf afgesny en gesmoor word, óf dit kan versnel en dus bevoordeel word.[477] Die gevolg is dat data op die netwerk so gemanipuleer kan word tot finansiële voordeel vir die netwerk-eienaar, en dikwels tot nadeel van die gebruiker.

Twee gevallestudies van DPI is ondersoek: een in die VSA en 'n ander in

468 Afd 5.4.3.
469 Afd 5.4.4.
470 Afd 5.4.4.
471 Afd 5.4.4.
472 Afd 5.4.4.
473 Afd 5.5.
474 Afd 5.5.
475 Afd 5.5.1.
476 Afd 5.5.1.
477 Afd 5.5.1.

Kanada.[478] In beide gevalle het die gebruik van DPI tot nadeel van gebruikers gelei. Die VSA het verskeie reguleringsmaatreëls ingestel om DPI te beperk, maar dit is deur die ISP-bedryf aangeveg — in so 'n mate dat die regulasies ongrondwetlik verklaar is.[479] Kanada het eweneens regulatoriese ingrepe gedoen om DPI te beperk.[480] Die gevolg was verrassend: die gebruik van DPI in die VSA is getemper deur markkragte, terwyl Kanada, wat suksesvol was met die inwerkingstelling van regulasiemaatreëls, nie enige voordeel daaruit kon put nie aangesien DPI ná die regulasies toegeneem het.[481]

***

Die belangrike rol wat nie-regeringsrolspelers by regulering van die Internet speel, is in hierdie hoofstuk toegelig. Deur slegs sulke rolspelers te oorweeg, sou egter kortsigtig wees, want state speel al hoe meer 'n leidende rol by Internetregulering. Dít word vervolgens bespreek.

478 Afd 5.5.1.2, afd 5.5.1.3 en afd 5.5.1.4.

479 Afd 5.5.1.2 en afd 5.5.1.3.

480 Afd 5.5.1.4.

481 Afd 5.5.1.4.

Hoofstuk 6

Regulering deur Soewereine State

The open, global Internet is unlikely to continue to flourish without deliberate action to promote and defend it. Political, economic, and technological forces are seeking to splinter the Internet into something that looks more like national networks, with each government controlling its domestic sphere as well as the flow of data and information between countries.[1]

John Negroponte

6.1 Inleiding

IN DIE VROEË ontwikkelingsjare van die Internet het regerings van die wêreld hul weinig gesteur aan die regulering daarvan.[2] Alhoewel die vroeë Internet tot stand gekom het met fondse van die Amerikaanse regering, het hierdie regering sélf nie enige reguleringspogings aangewend

[1] Negroponte, J D Palmisano S J en Segal A "Defending an Open, Global, Secure, and Resilient Internet" 2013 *Independent Task Force Report No 70* 13.

[2] Pohlmann N, Reimer H en Schneidemeld W *ISSE/SECURE 2007 Securing Electronic Business Processes: Highlights of the Information Security* (2007) meld op 28: "Governments were initially not concerned with Internet legal regulation and the Internet was left to self-regulation. This can be seen as the first phase of the Internet evolution".

nie.[3] Eers nadat dit geblyk het dat die Internet 'n strategiese ekonomiese hulpbron geword het, is daar pogings aangewend om beheer oor die Internet te verkry.[4] Op hierdie stadium was dit nie net die regering van die VSA wat gepoog het om regulering te bewerkstellig nie, maar meeste soewereine state het ook begin insien dat dit nodig geword het om een of ander vorm van regulering daar te stel.[5]

Om regulering op nasionale vlak te bewerkstellig was egter aanvanklik nie maklik nie. Toe die eerste pogings tot Internetregulering op nasionale vlak aangewend is, was die Internet steeds 'n internasionale netwerk wat oor landsgrense heen versprei was.[6] Een van die basiese reëls van die Internasionale reg bepaal egter dat lande nie hul territoriale jurisdiksie buite hulle landsgrense heen behoort uit te oefen nie.[7] Die vraag wat ontstaan is hoe hierdie internasionale netwerk op 'n nasionale vlak gereguleer kan word wanneer die Internasionale reg vereis dat jurisdiksie nie in die buiteland uitgeoefen moet word nie? Hierdie hoofstuk het ten doel om vas te stel hoe 'n verskeidenheid state dit hanteer het.

---

3 Sien afd 3.4.1 vir 'n uiteensetting waar die VSA vir die eerste keer 'n daadwerklike poging aangewend het om beheer oor die Internet te kry.

4 Afd 3.4.1.

5 Watney M "The Use of Electronic Surveillance in Conducting Criminal Investigations on the Internet" in Jahankhani H (red) *Handbook of Electronic Security and Digital Forensics* (2010) 536.

6 Sien Johnson D R en Post D G "Law and Borders — The Rise of Law in Cyberspace" 1996 *Stanford Law Review* 1367 1370 waar hulle sê dat: "Cyberspace has no territorially based boundaries" en 1372: "Individual electrons can easily, and without any realistic prospect of detection, 'enter' any sovereign's territory. The volume of electronic communications crossing territorial boundaries is just too great in relation to the resources available to government authorities. United States Customs officials have generally given up. They assert jurisdiction only over the physical goods that cross the geographic borders they guard".

7 Die klassieke saak rakende hierdie beginsel in die Internasionale reg is sekerlik die *Lotus-saak* (*Fr v Turk* 1927 PCIJ (ser A) 10 (1927)), waar die volgende beginsels duidelik neergelê is:

1. 'n Staat "may not exercise its power in any form in the territory of *another* state". Sien 18–19 van die uitspraak.
2. Tog verhinder die beginsels van Internasionale reg nie 'n staat om *in sy eie grondgebied* sekere reëls neer te lê aangaande optrede wat buite sy grondgebied plaasvind nie. Sien 19 van die uitspraak.

Dus het 'n staat 'n aansienlike mate van diskresie oor die maak van wette ten opsigte van optrede *buite sy grondgebied*, alhoewel dit slegs *binne die staat se grondgebied* toegepas kan word. Dugard J *International Law — A South African Perspective* (2011) 117.

Let daarop dat hierdie hoofstuk as't ware na 'n bewegende teiken skiet. Soos reeds vroeër aangedui, het die Internet sedert die vroeë 2000's ontwikkel van 'n internasionale eenheidsnetwerk na 'n hoogs gefragmenteerde netwerk wat rofweg die nasionaliteite van die wêreld verteenwoordig.[8] Soos tegnologiese maatreëls verbeter, word die Internet al hoe meer verdeel in nasionale intranette[9] wat aan die groter Internet gekoppel word. Die gevolg is dat die argitektuur van die Internet verander, en dit beïnvloed die inhoud wat daarop te vinde is. Dit veroorsaak ook dat vroeëre regulatoriese ingrepe uitgedien word.

Hierdie hoofstuk bestaan uit twee afdelings: die eerste bespreek die teoretiese onderbou van hoe dit moontlik kan wees vir 'n staat om sy nasionale intranet te reguleer, en verwys ook na maniere waarop indirekte internasionale regulering moontlik is. Die tweede afdeling van die hoofstuk hanteer verskillende state se reguleringspogings. Die eerste staat wat aan die beurt kom, is die VSA. Dit is gekies omdat die Internet daar ontwikkel het, en dit die eerste was wat met Internetregulering moes worstel. Die tweede staat wat bespreek word, is Sjina. Dit is algemeen bekend dat Sjina se regulering van sy intranet die gesofistikeerdste ter wêreld is. Sjina se uitgangspunt is geheel en al anders as die westerse wêreld, en dit is insiggewend hoe hierdie wêreld-ekonomiese reus te werk gaan om sy intranet te omvorm tot dit wat dit vandag is. Die derde staat wat bespreek word, is die groter Europese Unie: dit is *per se* nie 'n staat nie, maar dit is nogtans gekies omdat dit reeds vroeg in die ontstaan van die Internet wetgewende ingrepe gemaak het om regulering te bewerkstellig. Die vierde staat wat onder die loep geneem word, is Suid-Afrika. Hierdie studie word onderneem met inagneming van Suid-Afrikaanse regsbeginsels, en daarom is dit te verstane dat hierdie staat se reguleringspogings oorweeg word. Met die agtergrond

8 Afd 2.3.6.

9 In hierdie hoofstuk sal daar dikwels tussen die Internet en intranet of intranette onderskei word. Met "Internet" word bedoel die globale netwerk waartoe al die state van die wêreld toegang het. Met "intranet" word bedoel die nasionale netwerk van 'n staat wat afgeskei is van die groter Internet deur gebruikmaking van tegnologiese middels soos die "border gateway protocol" of 'n vuur muur ("firewall") soos in Sjina.

wat reeds in ander state plaasvind, is dit dan makliker om te bepaal waar Suid-Afrika se reguleringspogings voldoende is, en daar waar dit te kort skiet.

Daar sal nou ondersoek ingestel word na die wyse waarop regerings buite hulle grense reguleer.

6.2 Hoe Regerings Buite hul Grense Reguleer

6.2.1 Verskeie Rolspelers

Die effektiefste wyse waarop regerings ongewenste optrede van buite hul jurisdiksie kan reguleer, is om *tussengangers* wat *binne die gebied* van die land is, te reguleer.[10] Hierdie belangrike beginsel kan aan die hand van 'n paar voorbeelde bespreek word.

Wanneer 'n staat optrede wil reguleer, is daar altyd ten minste drie partye betrokke, te wete die bron, die tussenganger, en die eindgebruiker.[11] Die eerste is die vervaardiger van die produk of leweraar van die diens; die tweede is die tussenganger wat die produk of diens aan die eindgebruiker lewer, en die derde is die gebruiker van die goedere of die diens.[12] Gewoonlik is ál die partye binne die jurisdiksie van die staat, en dit kan skematies soos volg voorgestel word:

'n Eenvoudige voorbeeld hiervan is waar films onwettig op DVD geplaas word, en deur straatverkopers verkoop word.[13] In so 'n geval sal die plaaslike vervaardiger die bron wees, die straatverkoper die tussenganger, en die koper die eindgebruiker.

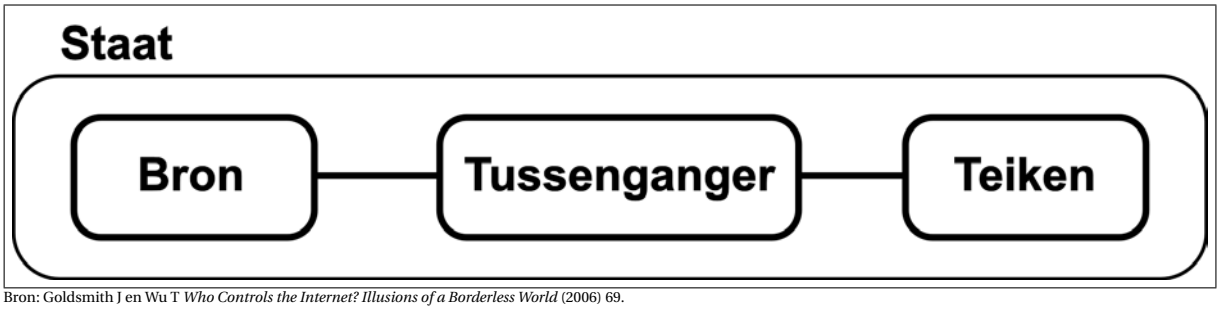
---

10 Goldsmith J en Wu T *Who Controls the Internet? lllusions of a Borderless World* (2006) 68 en Levinson D J "Collective Sanctions" 2003 *Stanford Law Review* 345 362 waar hy die konsep van "gatekeeper liability" verduidelik.

11 Goldsmith en Wu *Who Controls the Internet?* 69.

12 Goldsmith en Wu *Who Controls the Internet?* 69.

13 Mybroadband "South African Movie, Music Piracy Labs Busted — Here They Are" http://mybroadband.co.za/news/general/119234-south-african-movie-music-piracy-labs-busted-here-they-are.html (besoek op 30 Maart 2016).

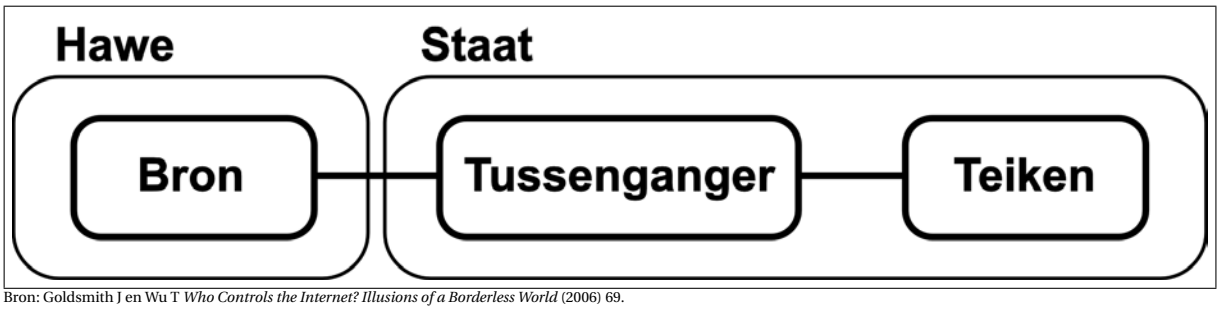


Bron: Goldsmith J en Wu T *Who Controls the Internet? Illusions of a Borderless World* (2006) 69.

Figuur 6.1: Rolspelers Almal Binne Dieselfde Regsgebied

Om die gewraakte gedrag te beëindig, is relatief eenvoudig. Die onwettige vervaardiger se besigheid kan gesluit word, die straatverkopers se onwettige DVD-produkte kan gekonfiskeer word, of die eindgebruiker kan beboet word. Al drie hierdie partye is binne die jurisdiksie van die staat, en deur bloot een van hierdie rolspelers te teiken, sal die gewenste uitwerking hê.[14]

Die logiese gevolg van hierdie argument is dat indien 'n party die reg wil ontduik, hy bloot buite die jurisdiksionele gebied van die staat moet beweeg. Dit kan skematies so voorgestel word:



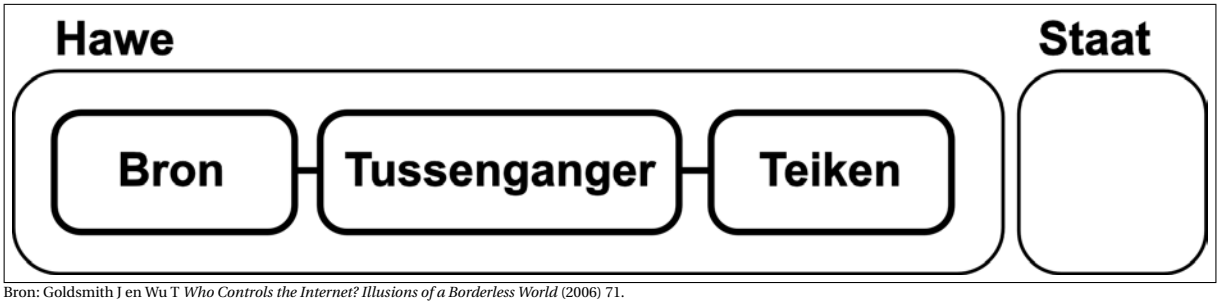
Bron: Goldsmith J en Wu T *Who Controls the Internet? Illusions of a Borderless World* (2006) 69.

Figuur 6.2: Die Bron Buite die Regsgebied van die Staat

In hierdie geval is die bron buite die jurisdiksie van die betrokke staat, en kan die staat nie enige stappe neem om die bron aan die pen te laat ry nie. Soos egter reeds hierbo genoem, is die tussenganger en die gebruiker steeds binne die jurisdiksie van die staat, en kan die gewraakte gedrag verhinder word deur enige van hierdie twee rolspelers te teiken. Die enigste wyse

14 Goldsmith *Who Controls the Internet?* 69.

waarop al drie hierdie rolspelers regsoptrede van die staat kan vryspring, is om *almal* buite die jurisdiksie van die staat te beweeg, soos in figuur 6.3 aangetoon, en indien dit gebeur, is dit in elk geval nie meer die staat se probleem om die gedrag te reguleer nie, aangesien die optrede geheel en al buite sy invloedsfeer val.



Bron: Goldsmith J en Wu T *Who Controls the Internet? Illusions of a Borderless World* (2006) 71.

Figuur 6.3: Alle Rolspelers Buite die Regsgebied van die Staat

Met hierdie eenvoudige verduideliking is dit voor-die-hand-liggend wat die oplossing tot regulering van die plaaslike intranet is: reguleer *enige* van die tussengangers, en deur dit te doen kan volle beheer oor die staat se intranet verkry word.[15]

Die belangrike vraag wat dus gevra moet word, is wie die Internet se tussengangers is, en of hulle onder die beheer van die staat geplaas kan word. Dit blyk soms dat dit nie eenvoudig vasgestel kan word nie, soos wat die volgende voorbeeld sal aantoon.

6.2.2 *HavenCo*

Tydens die tweede wêreldoorlog het die Engelse regering op verskeie plekke in die see tussen hulle en die vasteland van Europa 'n reeks forte opgerig wat as 'n skans kon dien vir moontlike invalle van buite.[16] 'n Britse majoor met die naam Paddy Bates het in 1966 een van hierdie verlate forte geannekseer en dit tot 'n onafhanklike staat verklaar en dit die "Principality of Sealand" genoem waar hy paspoorte uitgereik het vir enigiemand wat in

15 Dit is presies wat in Sjina gebeur, soos wat breedvoerig in afd 6.4.2 aangetoon sal word.

16 Grimmelmann J "Sealand, *HavenCo*, and the Rule of Law" 2012 *University of Illinois Law Review* 405 406.

hierdie eienaardigheid wou deel. Eienaardig genoeg is Bates se gekkigheid 'n sweempie legitimiteit gegee deur die optrede van 'n Britse hof. In 1968 het Bates op werkers geskiet wat 'n drywende boei naby die platform probeer diens het. Hy is in 'n Britse hof aangekla, maar die hof het beslis dat dit nie jurisdiksie oor die aangeleentheid het nie aangesien die platform buite die drie seemyl-gebiedswaters van Brittanje val.[17]

In 2000 is 'n maatskappy met die naam *HavenCo* op Sealand gevestig.[18] Die doel daarvan was om 'n veilige hawe aan maatskappye wat in ander lande verbied of gereguleer word, te verskaf.[19] In 2003 het *HavenCo* egter opgehou om besigheid te doen.[20] 'n Adviseur het aan Bates verduidelik dat *HavenCo* se besigheid slegte publisiteit inhou, en dat dit verhoudings met Brittanje kan versuur.[21] Die vrees was veral dat Brittanje teen Sealand kan ingryp,[22] veral aangesien Sealand se soewereiniteit gekoppel was aan Brittanje se onwilligheid om teen Sealand op te tree.[23]

Die lank en kort van hierdie verhaal is dat optrede teen tussengangers absolute beheer bewerkstellig. In hierdie geval was dit nie eers nodig vir 'n erkende staat om teen Sealand op te tree nie. Bates het besef dat sy optrede nie in die internasionale gemeenskap sal opgaan nie, en het dadelik die besigheid binne sy beheer — *HavenCo* — aangespreek. Indien dit byvoorbeeld sou blyk dat *HavenCo* wél suksesvol besigheid kon doen, sou ander tussengangers wat in die sfeer van die betrokke staat hom bevind, geteiken kan word vir regulering.

Dit is daarom nodig om vas te stel watter tussengangers in die konteks van die Internet funksioneer, aangesien die identifisering van hulle die

17 *Regina v Paddy Roy Bates and Michael Roy Bates* [1968] (UK-NA LO 2/1088) asook Grimmelmann 2012 *University of Illinois Law Review* 414 vn 28 en 422 vn 121.

18 Grimmelmann 2012 *University of Illinois Law Review* 407.

19 Besighede soos Internet-casino's of pornografie-verskaffers was beskou as moontlike kliënte van *HavenCo*. Grimmelmann 2012 *University of Illinois Law Review* 405 407.

20 Grimmelmann 2012 *University of Illinois Law Review* 453.

21 Grimmelmann 2012 *University of Illinois Law Review* 455.

22 Grimmelmann 2012 *University of Illinois Law Review* 455.

23 Grimmelmann 2012 *University of Illinois Law Review* 465.

sleutel tot Internetregulering inhou.

6.2.3 Samevatting

Hierdie afdeling het aangetoon dat die gebruikmaking van tussengangers die effektiefste wyse is waarop die Internet gereguleer kan word.[24] Daar is ten minste drie rolspelers in enige transaksie, hetsy dit fisies of op die Internet is, te wete die bron, die tussenganger, en die teiken. Daardie rolspelers wat hulle binne die staat se regsgebied bevind, kan direk geteiken word vir doeleindes van regulering. Somtyds bevind sekere rolspelers hulle buite die gebied van die staat, maar indirekte regulering kan steeds toegepas word deur ander rolspelers wat *wel binne* die staat se regsgebied is, te teiken. In so 'n geval word die ketting van die transaksie (hetsy fisies of inligting) gewysig, en kan effektiewe regulering plaasvind.[25] Die voorbeeld van *HavenCo* is gebruik om aan te toon hoe regulering op 'n *indirekte wyse* kan geskied.[26]

6.3 Die Internet se Tussengangers

6.3.1 Internet-diensverskaffers

Internet-diensverskaffers (ISP's) is seker die mees opvallende tussenganger in die konteks van die Internet. Dit is ISP's wat gebruikers aan die Internet koppel, en wanneer ISP's beheer word, kan die gedrag van meeste gebruikers effektief beheer word.

Hierdie beginsel is reeds vroeg in die bestaan van die Internet getoets. In Desember 1995 het Duitse wetstoepassers opgemerk dat *Compuserve*, wat 'n Amerikaanse maatskappy is en 'n Duitse filiaal met dieselfde naam het, op

[24] Afd 6.2.1.

[25] Afd 6.2.1.

[26] Afd 6.2.2.

282 verskillende nuusgroepe erge pornografiese materiaal versprei het.[27] Dit het onder andere kinderpornografie ingesluit.[28] Die Prokureur-generaal in Munich het *Compuserve GmbH* (die Duitse filiaal) ingelig van hierdie stand van sake en hul verwittig dat sulke gedrag onwettig is volgens die Duitse reg, en dat dit strafbaar was. Verder het die Prokureur-generaal versoek dat die verspreiding van hierdie materiaal dadelik gestop moet word.

Die direkteur van *Compuserve GmbH* het dadelik die moedermaatskappy in die VSA van hierdie feite verwittig, en gevolglik het *Compuserve* in Amerika dadelik toegang tot die spesifieke nuusgroepe geblokkeer om strafsanksies teen *Compuserve GmbH* af te weer. Die probleem was egter dat die nuusgroepe op Amerikaanse rekenaarbedieners was, en dit het tot gevolg gehad dat al *Compuserve* se gebruikers wêreldwyd nou nie meer toegang tot hierdie nuusgroepe gehad het nie. Gebruikers in veral Amerika was woedend hieroor, en *Compuserve* se optrede het nie net slegte publisiteit meegebring nie, maar ook finansiële verliese.[29] Daarom het *Compuserve* in Februarie 1996 wêreldwye toegang tot die gewraakte nuusgroepe herstel — ook in Duitsland. Om egter die Duitse filiaal te beskerm, is gratis sagteware aan Duitse gebruikers aangebied om toegang tot die betrokke nuusgroepe te blokkeer. *Compuserve* in Duitsland het aangevoer dat verdere pogings tot blokkasie nie meer nodig is nie weens die sagteware wat beskikbaar gestel is. Die sagteware getiteld “Cyber patrol” was ’n program wat eintlik ontwikkel is om ouers in staat te stel om hulle minderjarige kinders se vrye toegang tot die Internet te beperk, en dit het uiteraard beteken dat die nuusgroepe vryelik beskikbaar was vir volwassenes en enigiemand wat nie die “Cyber patrol” sagteware gebruik het nie.[30]

Die Prokureur-generaal van Munich was geensins met hierdie toedrag

---

27 Determann L “Case Update: German *Compuserve* Director Acquitted on Appeal” 1999 *Hastings International and Comparative Law Review* 109 111.

28 Determann 1999 *Hastings International and Comparative Law Review* 111.

29 Determann 1999 *Hastings International and Comparative Law Review* 111.

30 Determann 1999 *Hastings International and Comparative Law Review* 111.

van sake tevrede nie, aangesien die verspreiding van gewelddadige- en kinderpornografie aan enigiemand in Duitsland as 'n misdryf beskou word.[31] Die betrokke sagteware het geensins die verspreiding van kinderpornografie aan volwassenes gekeer nie, en gevolglik is daar besluit om Felix Somm, die direkteur van *Compuserve* in Duitsland, strafregtelik aan te kla. Hy word in 1998 skuldig bevind[32] en vir 2 jaar onder korrektiewe toesig geplaas.[33]

Die saak word op appèl geneem, aangesien Duitsland kort voor die uitspraak spesifieke kuberwetgewing uitgevaardig het wat terugwerkend van krag is, en wat die uitspraak sou kon beïnvloed.[34] Die hof *a quo* het die nuwe wetgewing egter nie in ag geneem nie. In die hoër hof word Somm kwytgeskeld van alle aanklagte, aangesien die betrokke wetgewing bepaal dat blote "Internet access providers" nie aanspreeklik gehou kan word vir inhoud wat deur hulle versend word nie.[35]

Duitsland is egter nie die enigste land wat vroeg reeds ingesien het dat Internet-diensverskaffers 'n belangrike deel van Internetregulering is nie. ISP-aanspreeklikheid word volledig in afdeling 6.4 hieronder bespreek, en dit bereik sy klimaks met die bespreking van Internetregulering in Sjina.

---

31 Determann 1999 *Hastings International and Comparative Law Review* 111.

32 Die skuldigbevinding is op grond van artikel 184 III van die Duitse Strafkode, wat bepaal dat die opsetlike verspreiding van pornografie van kinders, diere, en gewelddadige pornografie verbode is. Verder word die beskuldigde ook skuldig bevind aan die oortreding van artikel 21 III van die Duitse Kode op die beskerming van Jeugdiges (Gesetz ueber die Verbreitung jugendgefahrdender Schriften [GjS]) v 28.10.1998 (BGBI I S.3186) wat die verspreiding van PG-18-videospeletjies aan minderjariges (onder 18) strafbaar maak.

33 Somm is onder korrektiewe toesig geplaas sodat die Duitse strafstelsel hom kon monitor om te bepaal of *Compuserve GmbH* hul weer aan onwettige gedrag skuldig maak deur toegang te verleen tot kinderpornografie, wat soos reeds genoem, 'n misdryf in Duitsland is. Determann 1999 *Hastings International and Comparative Law Review* 119.

34 Duitsland het in 1997 spesifieke kuberwetgewing uitgevaardig wat Internet-diensverskaffers reguleer. Die wetgewing onderskei tussen drie groepe Internet-diensverskaffers, te wete inhoudsleweraars ("content providers"), toegangsleweraars ("access providers") en diensverskaffers ("service providers"). Determann 1999 *Hastings International and Comparative Law Review* 114. Die onderskeid word gemaak aangesien verskillende soorte diensverskaffers se regsaanspreeklikheid wissel na gelang van die rol van wat hulle vervul. Dit word volledig in Determann 1999 *Hastings International and Comparative Law Review* 115-118 bespreek.

35 Determann 1999 *Hastings International and Comparative Law Review* 114.

6.3.2 Inligtingstussengangers

Inligtingstussengangers speel 'n geweldige rol in die funksionering van die Internet. Hierdie tussengangers — soekenjins soos *Google* en Yahoo — vervul 'n noodsaaklike funksie om inligting vir gebruikers op te spoor en aan te bied. Hulle is alreeds in so 'n mate deel van die daaglikse lewe dat daar reeds vrae is of die mens se afhanklikheid van hierdie tussengangers nie 'n probleem begin word nie.[36] Dit is daarom te verstane dat indien 'n inligtingstussenganger aangesê word om inligting uit te vee, dit amper so goed is asof dit nie bestaan nie. Gebruikers sal eenvoudig geen meganisme hê om die inligting op te spoor nie. Soos Goldsmith dit stel: "It is hard, in other words, to know what you don't know".[37]

Hierdie beginsel is tans besig om uitgeklaar te word in uitsprake van regoor die wêreld, en die uiteinde van die saak is nog nie bepaal nie. In *Google Inc v Agencia Española de Protección de Datos (AEPD)*[38] het die Europese Geregshof bepaal dat *Google* — as soekenjin, en dus inligtingstussenganger — 'n beheerder[39] is van persoonlike inligting, en dat dit as sodanig aan die vereistes van die EU Direktief[40] moet voldoen deur alle persoonlike inligting van gebruikers van sy soekenjin te skrap.[41] Dit is beslis ten spyte daarvan dat *Google* 'n Amerikaanse maatskappy is, en die saak volgens die EU-reg beslis is.

---

36 Carr N "Is *Google* Making Us Stupid?" 2008 *Yearbook of the National Society for the Study of Education* 89-94.

37 Goldsmith *Who Controls the Internet?* 76.

38 ECLI:EU:C:2014:317.

39 'n Beheerder, of "controller" het 'n regstegniese betekenis volgens die EU se Databeskermingsdirektief 95/46 en word gedefinieer as: "'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law".

40 In hierdie geval direktief 95/46.

41 Sien par 100 van die uitspraak, en veral punt 3 van die bevinding waar daar spesifiek beslis word dat: " the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person".

In *Equustek Solutions Inc v Google Inc*[42] het dieselfde beginsel ter sprake gekom waar 'n Kanadese hof beslis het dat *Google* sekere inligting uit sy *internasionale databasis* moet verwyder.[43] Dit beteken noodwendig dat die Kanadese hof sy jurisdiksie uitoefen in elke land waar *Google* aanwesig is. Die saak is ten tyde van hierdie skrywe geplaas om deur die Kanadese Hooggeregshof aangehoor te word, en daar is dus nog nie 'n finale bevel daaroor nie.[44]

Die wyse waarop inligtingstussengangers effektief beheer word, word ook in fyn besonderhede onder afdeling 2.3.6.3 bespreek.

6.3.3 Finansiële Tussengangers

Die regulering van finansiële tussengangers en die effektiwiteit daarvan is reeds in 2005 geïllustreer. Sigarette is sedert 2001 in die VSA onwettig verkoop, meestal vanuit Amerikaans-Indiaanse reservate.[45] In plaas daarvan om te probeer om hierdie verkopers, wat regoor die hele VSA te vinde was, op te spoor en aan die pen te laat ry, het die kantoor van die Prokureur-generaal bloot 'n ooreenkoms met kredietkaartmaatskappye aangegaan om nie meer enige onwettige sigaretverkope te prosesseer nie.[46] Binne etlike weke was meeste van hierdie besighede nie meer in bedryf nie.[47]

Dieselfde strategie is gevolg toe die *Unlawful Internet Gambling Enfor-*

---

42 2014 BCCA 295 en op appèl *Equustek Solutions Inc v Google Inc* 2015 BCCA 265.

43 Par 9 van die appèluitspraak.

44 The Globe and Mail "Supreme Court Grants *Google* Appeal in Case of Blocked Search Results" http://www.theglobeandmail.com/technology/tech-news/supreme-court-to-hear-*Google*s-appeal-in-bc-search-injunction-case/article28794728/ (besoek op 30 Maart 2016).

45 Forbes "Online Cigarette Sales? Shocking!" http://www.forbes.com/2001/12/11/1211tobacco.html (besoek op 30 Maart 2016).

46 Office of the Attorney General "Attorneys General and ATF Join with Credit Card Companies to Prevent Illegal Internet Cigarette Sales" http://www.ag.idaho.gov/media/newsReleases/2005/nr_03172005b.html (besoek op 30 Maart 2016).

47 New York Times "E-Commerce Report; Now that Credit Card Companies Won't Handle Online Tobacco Sales, Many Merchants are Calling it Quits" http://query.nytimes.com/gst/fullpage.html?res=9800E3DD1E3FF937A35757C0A9639C8B63 (besoek op 30 Maart 2016).

cement Act van 2006[48] in die VSA uitgevaardig is. Dit plaas 'n verpligting op betalingsmaatskappye om nie betalings van onwettige dobbelhuise te prosesseer nie.[49]

Effektiewe regulering van finansiële tussengangers *binne* die staat se regsgebied is dus 'n uitstekende wyse om betaling *buite* die regsgebied te reguleer.

6.3.4 Individue

Individue kan kragtige tussengangers op die Internet wees, en in hierdie gebied is Sjina by verre die voorloper. Regulering van Sjina se intranet word in afdeling 2.3.6.3 hieronder bespreek, en daar sal aangetoon word hoe Sjina se intranetregulering in verskillende fases verdeel kan word. Dit is genoegsaam om in hierdie konteks te noem dat 'n magdom regulasies geformuleer is om, onder andere, persone as tussengangers te teiken. Byvoorbeeld, die *Interim Provisions on the Administration of Internet Publication* wat in 2002 uitgevaardig is, bepaal dat die bestuurder of hoof van die Internet-publikasiemaatskappy verantwoordelik sal wees vir die wettigheid van plasings wat op sy bediener gedoen word. Die gebruiker moet die publiseerder as die tussenganger gebruik, en indien die publiseerder meen die stuk is nie geskik vir publikasie nie (omdat dit byvoorbeeld die regering kritiseer), sal dit eenvoudig nie gepubliseer word nie.[50]

Individue kan ook kragtige reguleerders wees. Hier is Sjina weer eens die voorloper, met 'n enorme Internet-polisiediens wat multidimensioneel is. Daarmee word bedoel dat daar 'n kerngroep bestaan wat tradisionele

48 31 USC hfst 53 subpar IV.

49 Hornle J en Zammit B *Cross-border Online Gambling Law and Policy* (2010) 114 verduidelik hoe die wet magtiging verleen dat regulasies uitgevaardig kan word, en dat die "Regulations require that financial intermediaries providing certain designated payment services must establish and implement policies and procedures to identify and block or otherwise prevent payments in respect of unlawful online gambling by 1 December 2009".

50 Afd 6.4.2.3.3 hieronder.

polisiefunksies verrig, soos om mense te teiken, te arresteer en te vervolg, maar daar is ook 'n enorme groep moniteerders van inligting. Die eersgenoemde groep word gereken op ongeveer 40 000 persone,[51] maar die tweede groep is baie groter, en kan volgens berigte so groot as 2 miljoen moniteerders wees.[52] Hierdie tweede groep word vir verskillende funksies gebruik — daar is die sogenaamde "50 Cent Party" wat spesifiek getaak word om goeie kommentaar van die regering op openbare nuusblaaie en ander plekke waar openbare kommentaar gelewer kan word, te plaas.[53] Die grootste groep moniteerders is te vinde op *Sina Weibo*,[54] wat Sjina se grootste mikroblog-webwerf is, en wat 'n kombinasie tussen *Facebook* en *Twitter* (wat beide in Sjina verbied word) is.[55] Hierdie moniteerders se taak is om in die agtergrond die aktiwiteit van gebruikers te moniteer, en verslae saam te stel wat deur senior-besluitnemers gelees kan word.[56] 'n Derde groep moniteerders is te vinde by *Baidu*, Sjina se grootste soekenjin, wat soortgelyk aan die weste se *Google* is. Hierdie moniteerders se taak is om massas inligting van die soekenjin te verwyder — soveel as een miljoen skakels per dag.[57] Dan is daar ook moniteerders by bykans elke groot maatskappy wat besigheid op Sjina se intranet doen, en wat toesien dat alle gebruik op die netwerk wettig is.[58]

---

51 Bigthink "The Long Arm Of China's Internet Police" http://bigthink.com/think-tank/how-to-censor-the-internet-in-china-2 (besoek op 31 Maart 2016). Dong F "Controlling the Internet in China: The Real Story" 2012 *Convergence* 403 noem op 405 dat "internet police are the upper-level supervisors of the internet".

52 Cable News Network "China Employs 2 Million to Police Internet" http://edition.cnn.com/2013/10/07/world/asia/china-internet-monitors/ (besoek op 31 Maart 2016); British Broadcasting Corporation "China Employs Two Million Microblog Monitors State Media Say" http://www.bbc.com/news/world-asia-china-24396957 (besoek op 31 Maart 2016).

53 Kelly S, Cook S en Truong M (red) *Freedom on the Net* 2015 (2015) 200; Reporters Without Borders *Internet Enemies Report 2012* (2012) 5.

54 *Sina* is 'n Sjinese mediamaatskappy, en *Weibo* beteken mikroblog in Sjinees. *Sina Weibo* is die grootste sosiale platform in Sjina, en is 'n kombinasie tussen *Facebook* en *Twitter*.

55 British Broadcasting Corporation "China Employs Two Million Microblog Monitors State Media Say" http://www.bbc.com/news/world-asia-china-24396957 (besoek op 31 Maart 2016).

56 British Broadcasting Corporation "China Employs Two Million Microblog Monitors State Media Say" http://www.bbc.com/news/world-asia-china-24396957 (besoek op 31 Maart 2016).

57 Kelly S en Cook S (red) *Freedom on the Net 2011* (2011) 94.

58 Afd 2.3.6.3.

6.3.5 Netwerk-tussengangers

6.3.5.1 Eienaars van die Netwerk

In afdeling 6.3.1 hierbo is daar aangetoon hoe Internet-diensverskaffers tussengangers kan wees. In daardie konteks is daar aangetoon hoe *regerings van die wêreld* ISP's gebruik om regulering deur te voer. In wese is die regering die manipuleerder, en die Internet-diensverskaffer die een wat gemanipuleer word.

Internet-diensverskaffers kan as *netwerk-eienaars* ook reguleer. In hierdie konteks is hulle die manipuleerder, en doen dit om hul eie agenda (wat gewoonlik kommersieel van aard is) te bevorder. Hierdie aangeleentheid is reeds in besonderhede in afdeling 5.5.1.5 bespreek waar "deep packet inspection" gebruik word om die netwerk vir eie gewin te manipuleer.

Dus is afdeling 6.3.1 en 5.5.1.5 in wese twee kante van dieselfde ISP-muntstuk — afdeling 6.3.1 toon aan hoe regerings ISP's manipuleer vir nasionale gewin, terwyl afdeling 5.5.1.5 aantoon hoe ISP's self hulle netwerke manipuleer.

Hierdie afdeling[59] dien bloot om die leser daarvan bewus te maak dat ISP's 'n dubbele funksie verrig — as gemanipuleerde staats-instrument sowel as manipulerende netwerk-eienaar.

6.3.5.2 Fisiese Argitektuur

Gedurende die laaste helfte van 2010 tot ongeveer 2012 het 'n gebeurtenis plaasgevind wat vandag as die Arabiese Lente ("Arab Spring") bekend staan.[60] Dit was 'n tyd van geweldige politieke onstabiliteit in verskeie

59 Afd 6.3.5.1.

60 Benmamoun M, Kalliny M en Cropf R A "The Arab Spring, MNEs, and Virtual Public Spheres" 2012 *Multinational Business Review* 26 26; Howard P N en Hussain M M "The Role of Digital Media" 2011 *Journal of Democracy* 35 38; Robertson A "Connecting in Crisis: 'Old' and 'New' Media and the Arab Spring" 2013 *The International Journal of Press/Politics* 1 2; Kurbalija J *An Introduction to Internet Governance* (2012) 12; Anderson L "Demystifying the Arab Spring" 2011 *Foreign Affairs* 2.

Arabiese lande, soos Tunisië, Egipte, Libië, Yemen, Morocco, en Sirië.[61] In Egipte was *Facebook* baie gewild, en gedurende Januarie 2011 het dit geblyk dat hierdie sosiale-medium gebruik word om groot groepe mense te mobiliseer vir opstande wat besig was om uit te breek.[62] Op die 27ste Januarie 2011 teen 10:30 in die oggend het die Egiptiese regering die hele land se kommunikasiestelsels tot 'n stilstand gebring.[63] Egipte se intranet is geheel en al van die groter Internet afgeskakel.[64] Die wyse waarop die regering dit kon regkry, was deur die "Border Gateway Protocol Rules" af te skakel.[65] Die hele proses het minder as 'n uur geduur.[66]

In Sjina is die nasionale intranet reeds so gesofistikeerd dat dele daarvan afgeskakel of gefiltreer kan word. In Xinjiang is toegang tot die Sjinese intranet (en dus ook die Internet) van Julie 2009 tot Mei 2010 afgeskakel om protesoptrede onder bedwang te bring.[67] Soortgelyke optrede het in Wukan in Desember 2011 voorgekom, en in Februarie 2012 is verskeie areas in Tibet afgesny.[68]

Hierdie gebeure illustreer hoe die fisiese argitektuur gebruik kan word om regulering daar te stel.

Sagteware het ook die vermoë om te kan reguleer. In 2008 vereis die Sjinese regering van rekenaarvervaardigers om sagteware met die naam "Green Dam Youth Escort" op alle nuwe rekenaars te installeer met die doel om morele waardes te bevorder.[69] Dit blyk dat hierdie sagteware ook

---

61 Benmamoun, Kalliny en Cropf 2012 *Multinational Business Review* 26.

62 Guadamuz A *Networks, Complexity and Internet Regulation* (2011) 214.

63 Guadamuz *Networks, Complexity and Internet Regulation* 214; Benmamoun, Kalliny en Cropf 2012 *Multinational Business Review* 38.

64 Howard en Hussain 2011 *Journal of Democracy* verduidelik op 44 dat: "Banning access to social-media websites, powering down cell towers, or disconnecting Internet switching points in major cities were among the desperate tactics to which authoritarian regimes resorted as they strove to maintain control".

65 Kelly, Cook en Truong (red) *Freedom on the Net 2015* 271; Guadamuz *Networks, Complexity and Internet Regulation* 214.

66 Kelly, Cook en Truong (red) *Freedom on the Net 2015* 271.

67 Kelly S, Cook S en Truong M (red) *Freedom on the Net 2012* (2012) 129.

68 Kelly, Cook en Truong (red) *Freedom on the Net 2012* 129.

69 Zheng H "Regulating the Internet: China's Law and Practice" 2013 *Beijing Law Review* 37 38.

politieke filtrering doen, en word wyd gekritiseer.[70] Weens die negatiewe houding van Sjinese burgers jeens die sagteware word die projek geskrap.[71]

Sjinese reguleerders maak op 'n interessante wyse van intimidasie gebruik om selfregulering op hulle intranet te bevorder.[72] Sedert 2006 is twee geanimeerde karakters, genaamd Jingjing en Chacha, op die Sjinese intranet te bespeur.[73] Hierdie karakters verskyn op die rekenaarskerm wanneer die Sjinese intranet en groter Internet besoek word, en dui aan dat die gebruiker dopgehou word. Elke dertig minute beweeg die karakters op die skerm rond om aan te dui dat monitering deurlopend geskied.[74] Figuur 6.4 toon aan hoe hierdie karakters op 'n tipiese skerm vertoon word.

Sagteware wat 'n verreikende effek op regulering van die Internet kan hê, is dié wat deur regerings gebruik word om op mekaar en hul inwoners te spioeneer. In 1997 het die wêreld kennis geneem van die "*Carnivore*"–sisteem wat deur die Amerikaanse regering gebruik word om op e-posse en Internetkommunikasie te spioeneer.[75] In 2013 is soortgelyke sisteme in die VSA en Brittanje blootgelê in die Snowden-spioenasieskandaal.[76] Afdeling 6.4.1.5 bespreek hierdie aangeleentheid volledig.

---

70 Kelly en Cook (red) *Freedom on the Net 2011* 96. Wolchok S, Yao R en Halderman J A "Analysis of the Green Dam Censorware System" https://jhalderm.com/pub/gd/ (besoek op 31 Maart 2016).

71 Lee J A en Liu C Y "Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China" 2012 *Minnesota Journal of Law, Science, and Technology* 125 141. Zheng 2013 *Beijing Law Review* 38.

72 Zheng 2013 *Beijing Law Review* 40.

73 Kissel T K "Licence to Blog: Internet Regulation in the People's Republic of China" 2007 *Indiana International and Comparative Law Review* 229 250.

74 SFGate "China Censors Internet Users With Site Bans, Cartoon Cop Spies" http://www.sfgate.com/opinion/article/China-censors-Internet-users-with-site-bans-2501596.php (besoek op 31 Maart 2016).

75 Marsden C T *Net Neutrality* (2010) 75; 191; Ibrahim Y *Global Governance and the Local Internet* (2007) 191; Lessig L *Code 2.0* (2006) 140.

76 Afd 5.3.2.4 en 6.4.1.5.2.

Bron: Committee to Protect Journalists "Olympics: Jing Jing, Cha Cha, and Other Online Cops" https://www.cpj.org/blog/2008/08/olympics-jing-jing-cha-cha-and-other-online-cops.php (besoek op 31 Maart 2016).

Figuur 6.4: Jingjing en Chacha

6.3.6 Samevatting

Dit is krities belangrik om vas te stel wie die Internet se tussengangers is, want daarsonder kan effektiewe regulering nie plaasvind nie.[77]

Hierdie afdeling het getoon wie die Internet se tussengangers is. In die eerste plek is daar Internet-diensverskaffers, wat die voor-die-hand-liggendste tussengangers op die Internet is.[78] Elke persoon wat die Internet wil gebruik, kry toegang daartoe deur 'n Internet-diensverskaffer, en daarom is dit nie vreemd nie dat state so graag hierdie tussengangers teiken vir doeleindes van regulering. Daar is egter aangetoon dat Internet-diensverskaffers *twee* oorkoepelende rolle vervul, naamlik om die gemanipuleerdes te wees wat deur die staat gebruik word om regulering daar te

77 Afd 6.3.

78 Afd 6.3.1.

stel,[79] maar ook die manipuleerders van die netwerk vir eie gewin.[80] In beide gevalle word die eindgebruiker se gedrag gesmee na die wil van óf die staat, óf die betrokke ISP.

Deur Inligtingstussengangers te reguleer, word die beskikbaarheid van inligting op die Internet beperk,[81] en Finansiële tussengangers kan baie effektief gebruik word om industrieë wat 'n winsoogmerk het, maar nie binne die betrokke staat se regsgebied is nie, te reguleer. Die onwettige verkoop van sigarette is aangetoon as illustrasie van hoe effektief hierdie tipe regulering kan wees.[82]

Individue kan as tussengangers op die Internet 'n wyse verskeidenheid funksies verrig, soos om te polisiëer,[83] of om selfs die regerende party in 'n positiewe lig te plaas — soos wat in Sjina die geval is.[84] Selfs sosiale media kan onder die vergrootglas geplaas word.[85]

Laastens is daar aangetoon dat die fisiese argitektuur van die Internet 'n kragtige reguleerder kan wees.[86] Die plaaslike intranet kan afgeskakel word, soos in Egipte, of beperk word soos in Sjina, en selfs sagteware kan deur state ingespan word om op mense te spioeneer.

Die Internet se tussengangers is dus *legio*, en daar kan verskeie meganismes gebruik word om regulering daar te stel. Die volgende afdeling sal juis aantoon hoe verskillende state van die wêreld hierdie teoretiese konsepte in die praktyk aanwend, en dit sal vervolgens bespreek word.

79 Afd 6.3.1.

80 Afd 6.3.5.1.

81 Afd 6.3.2.

82 Afd 6.3.3.

83 Afd 6.3.4.

84 Afd 6.3.4.

85 Afd 6.3.4, veral die gedeelte oor die monitering van *Sina Weibo*.

86 Afd 6.3.5.2.

6.4 Spesifieke State se Reguleringspogings

'n Keur van vier state se Internetreguleringspogings sal vervolgens bespreek word. Die eerste staat wat uitgesonder word, is die VSA.[87] Die Internet het in die VSA ontwikkel, en daarom is dit nie vreemd dat die howe van die VSA die eerste met regulatoriese vrae moes worstel nie. Vele uitsprake het gevolg, en daarom is dit sinvol om daarop te let wanneer Internetregulering beoordeel word.

Die tweede staat wat beoordeel word, is die Volksrepubliek van Sjina.[88] Hierdie staat het sedert sy koppeling aan die groter Internet sekerlik die mees omvangryke meganismes in plek gestel om sy plaaslike intranet te reguleer. Die *Golden Shield*-sisteem[89] stel wye argitektuur-reguleringsmeganismes in werking om die gewenste uitwerking voort te bring, asook wetgewende maatreëls om gehoorsaamheid daaraan af te dwing. Dit is die enigste staat in die keur van state wat nie 'n demokrasie is nie, en die gevolge daarvan skemer duidelik in Sjina se reguleringsisteem deur. Omdat die *Golden Shield*-sisteem so omvangryk is, skep dit 'n goeie bron om reguleringskwessies aan te spreek.

Die Europese Unie word in die keur van state wat onder bespreking geneem sal word, ingesluit.[90] Dit is nie 'n staat *per se* nie, maar verskaf vrugbare materiaal wat oorweeg kan word. Die rede hiervoor is dat die Europese Unie vroeg in die bestaan van die Internet reeds bewus was van die belang van die Internet, en verskeie reguleringsmaatreëls deurgevoer het.[91]

---

87 Afd 6.4.1.

88 Afd 6.4.2.

89 Dit is die amptelike naam van die Sjinese sisteem wat Internet-data filtreer. Dit word spottenderwys die "Great Firewall of China" genoem. Hagestad W *21st Century Chinese Cyberwarfare* (2013) 253 verduidelik: "This project was called the 'Golden Shield Project' and is also known as the 'Great Firewall of China'. Under the direct policy enforcement of the Ministry of Public Security of the People's Republic of China (MPS) 'Golden Shield' provides the People's Republic of China with Internet censorship at the Internet backbone and ISP level". Ook International Business Publications USA *China E-commerce Business and Investment Opportunities Handbook* (2007) 106; Firmino R J *ICTs for Mobile and Ubiquitous Urban Infrastructures: Surveillance, Locative Media and Global Networks* (2010) 240.

90 Afd 6.4.3.

91 Afd 6.4.3.2.

Suid-Afrika is die laaste staat wat in hierdie studie ingesluit word.[92] Verskeie wetgewende maatreëls is reeds in werking gestel om Internetregulering te bewerkstellig, en dit word onder die loep geneem en beoordeel aan die hand van ander state se reguleringsmaatreëls.[93]

Dit is voor-die-hand-liggend dat state wat in hierdie studie ondersoek word, elkeen 'n wye reeks regulatoriese ingrepe gemaak het om Internetregulering in hul staat moontlik te maak. Dit sou onsinnig wees om in hierdie studie te poog om ál hierdie maatreëls te bespreek, aangesien dit eenvoudig te wydverspreid en uitgebreid is. Daarom word daar in hierdie studie slegs die beginsels wat Internetregulering op 'n makro vlak beheer, onder die loep geneem. Daarmee word bedoel dat die studie Internetregulering vanuit 'n Internasionaalregtelike oogpunt sal beskou. Die fokus bly dus op die wyse waarop die regering van die land poog om Internetregulering *in die geheel* daar te stel. Om die studie binne perke te hou, sal die wyse beoordeel word waarop Internet-diensverskaffers gereguleer word. Dit skep 'n goeie voorbeeld van hoe die ideologie van die regerende party na Internetregulering deurgetrek word. Internet-diensverskaffers is die sentrale rolspelers wat 'n land in staat stel om spesifieke regulatoriese ingrepe op die Internet te maak.[94] Dit skep dus 'n goeie barometer vir die beoordeling van 'n staat se Internetregulerings-ingrepe. Dit beteken egter ook dat spesifieke misdrywe, soos Internetpornografie, krakery en verwante misdade nié bespreek sal word nie, aangesien dit grootliks 'n nasionale aangeleentheid is en nie noodwendig Internetregulering op Internasionale vlak aanspreek nie.

92 Afd 6.4.4.

93 Afd 6.4.4.

94 Afd 6.3.1.

6.4.1 Die Verenigde State van Amerika

6.4.1.1 Inleiding

Aangesien die Internet 'n skepping van die VSA is, is dit nie vreemd dat die aanspreeklikheid van Internet-diensverskaffers die eerste keer hier bereg moes word nie.[95] Nog voordat daar enige wetgewing daaroor geformuleer is, moes die howe al uitspraak lewer. Soos wat die norm in die regswese is, is algemene beginsels aangaande 'n onderwerp gebruik om tot 'n sinvolle uitspraak te kom. Die algemene beginsels in die reg aangaande geleiers (met ander woorde mense of organisasies wat 'n diens lewer deur 'n produk of boodskap van een entiteit na 'n ander te gelei) is dat die geleier nie aanspreeklik vir die inhoud van die kommunikasie of produk is nie. In *O'Brien v Western Union Telegraph Co*[96] is daar reeds in 1940 bevind dat die betrokke telegraafmaatskappy nie aanspreeklik gehou kan word vir die inhoud van telegraafboodskappe nie,[97] aangesien dit meer as 70 000 boodskappe per dag versend, en indien dit die hekwagter vir potensiële laster sou wees, sou dit nie in staat wees om sy funksie te kan verrig nie:

> If the telegraph companies are to handle such a volume of business expeditiously, it is obvious that their agents cannot spend much time pondering the contents of the messages with a view to determining whether they bear a defamatory meaning, and if so, whether the sender might nevertheless be privileged. The effect of putting such a burden upon the telegraph companies could only result in delayed transmission of, and in some cases refusal to transmit, messages which the courts after protracted litigation might ultimately determine to have been properly offered for transmission and which the sender was entitled to have dispatched promptly even though defamatory matter was contained therein.[98]

---

95 'n Volledige verduideliking van die ontstaan van die Internet word in hfst 2 hierbo gegee. Die *Scientific and Advanced-Technology Act* van 1992 het in artikel 4 magtiging aan die *National Science Foundation* verleen om die ARPANET aan die groter Internet te koppel. Anoniem "Text of the Scientific and Advanced-Technology Act of 1992" https://www.govtrack.us/congress/bills/102/s1146/text (besoek op 25 Februarie 2016).

96 113 F 2d 539 (lst Cir 1940).

97 Op 541 meld die hof: "The immunity of the telegraph company from liability to a defamed person when it transmits a libellous message must be broad enough to enable the company to render its public service efficiently and with dispatch. Speed is the essence of the service".

98 *O'Brien v Western Union Telegraph Co* 113 F 2d 539 (lst Cir 1940) 542.

Aangesien die Internet soveel fasette het, was dit reeds aan die begin van die Internet-era moeilik om te bepaal hoe hierdie algemene beginsel toegepas behoort te word. In *Cubby v Compuserve*[99] is daar byvoorbeeld bevind dat die Internet-diensverskaffer 'n *verspreider* (distributor) was, en dit het beteken dat hy nie aanspreeklik gehou kon word vir inhoud nie. Hierteenoor het die hof in *Stratton Oakmont, Inc v Prodigy Services Co* [100] beslis dat die Internet-diensverskaffer 'n *uitgewer* was, aangesien hy meer beheer oor die inhoud van die inligting gehad het, en gevolglik wél aanspreeklik daarvoor gehou kon word.[101] Wetgewing was duidelik nodig om duidelikheid te bring. Dit is gedoen deur drie stukke wetgewing, te wete die *Communications Decency Act,*[102] die *Digital Millennium Copyright Act,*[103] en die *Lanham Act.*[104]

Vervolgens word hierdie stukke wetgewing bespreek.

6.4.1.2 *Communications Decency Act*

Die *Communications Decency Act* (hierna die CDA) is in 1996 uitgevaardig. Daar is reeds met hierdie wet kennis gemaak in afdeling 3.3.2 waar dit aangeveg is weens die poging om onsedelike kommunikasie op die Internet te reguleer. Die paragraaf wat egter in hierdie konteks bespreek word, is eers later bygevoeg.[105] Dit is algemeen verwelkom aangesien dit 'n wye nie-aanspreeklikheidsklousule vir Internet-diensverskaffers invoer.[106]

Paragraaf 230 van die CDA maak dit duidelik waarom die voorgenome reël van nie-aanspreeklikheid van diensverskaffers uitgevaardig word: "The Internet and other interactive computer services have flourished, to the

99 776 F Supp 135 (S D N Y 1991).

100 1995 WL 323710 (N.Y. Sup Ct May 24 1995).

101 Zeran v *America Online* Inc 129 F 3d 327 330 (4th Cir 1997) verskaf 'n bevestiging hiervan.

102 47 USC § 230 (2006).

103 17 USC § 512 (2012).

104 15 USC § 1114(2)(B) en (C) (2006).

105 Myer K S "Wikimmunity: Fitting the Communications Decency Act to Wikipedia" 2006 *Harvard Journal of Law and Technology* 163.

106 Myer 2006 *Harvard Journal of Law and Technology* 163.

benefit of all Americans, with a minimum of government regulation"[107] en daarom is dit die beleid van die VSA om te: "promote the continued development of the Internet and other interactive computer services and other interactive media".[108] Dit was duidelik in 1996 dat die Internet sonder enige staatsinmenging ontplof het, en daardie uitgebreide ontwikkeling was as 'n prioriteit beskou, wat dan aanleiding gegee het tot die beginsel van nie-aanspreeklikheid van Internet-diensverskaffers.[109]

Die beginsel word dan in paragraaf 230(c)(1) verwoord as: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". Die probleem van *Cubby v Compuserve*[110] en *Stratton Oakmont, Inc v Prodigy Services Co*[111] is dus ondervang: 'n Internet-diensverskaffer is nie 'n uitgewer nie.

Paragraaf 230 van die CDA is spoedig getoets in *Zeran v America Online Inc*[112] Die hof was ferm daaroor dat 'n ISP nie aanspreeklik is vir enige inligting op sy bedieners nie, aangesien dit: "creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service".[113] Dit is die geval selfs al het die ISP vooraf kennis gekry van die gewraakte gedrag en dit nie verwyder het nie.[114] Die gevolg was dus verreikend, en Rustad verduidelik dat ISP's "no obligation to remove tortious materials, to prevent the reposting of objectionable materials, or to help victims track down the primary wrongdoers" het nie.[115] Ehrlich stel dit net so sterk wanneer hy

---

107 Par 230(a)(4).

108 Par 230(b)(1).

109 Noeth K "The Never-Ending Limits of § 230: Extending ISP Immunity to the Sexual Exploitation of Children" 2009 *Federal Communications Law Journal* 765 768.

110 776 F Supp 135 (S D N Y 1991).

111 995 WL 323710 (N.Y. Sup Ct May 24 1995).

112 129 F 3d 327 (4th Cir 1997).

113 *Zeran v America Online Inc* 330.

114 Op 332–333 van die uitspraak.

115 Rustad M L en Koenig TH "Rebooting Cybertort Law" 2005 *Washington Law Review* 335 341.

verduidelik dat die effek van hierdie uitgebreide regsinterpretasies is dat paragraaf 230 'n volledige en oorkoepelende immuniteit aan ISP's verleen solank hulle nie die outeurs van inligting op hulle bedieners is nie.[116] Rustad som dit op deur te noem dat "judiciary's inflated interpretation of § 230 has created a legal environment that is ideal for injury and difficult for redress".[117] Dus, die kort en lank van hierdie bespreking is dat Par 230 van die CDA aan die Amerikaanse ISP as't ware 'n blanko tjek gegee het om aanspreeklikheid op hulle bedieners te vermy, solank dit vasstaan dat die inligting nie deur die ISP self nie, maar sy gebruikers geskep is.

Die trefwydte van Internet-diensverskaffers het so ver gegaan dat dit selfs toegepas is in gevalle van kinderpornografie.[118] Dit is daarom nie vreemd dat regshervormings versoek word nie.[119]

Mehra en Trimble wys op 'n ander interessante gevolg van die wye trefwydte van Paragraaf 230, naamlik dat dit juis die oorspronklike doel van ontwikkeling van die Internet, fnuik.[120] Die doel van die skepping van die algemene en blanko nie-aanspreeklikheid van ISP's was júis om die ontwikkeling van die Internet te bevorder.[121] Die regsbepaling is egter in 1996 geformuleer toe die Internet nog in sy kinderskoene was, en twintig jaar het alreeds verbygegaan sedert die CDA tot stand gebring is. Intussen het daar verskeie sterk rolspelers, soos *Google* en *Yahoo* na vore getree, en die wye beskerming wat hulle van die CDA geniet kan veroorsaak dat dit 'n

116 Ehrlich P "Communications Decency Act § 230" 2002 *Berkeley Technology Law Journal* 401 406–11.

117 Rustad en Koenig 2005 *Washington Law Review* 335 341.

118 *Doe v Bates* 2006 W.L. 3813758 (2006), *Doe v MySpace Inc* 474 F Supp 2d 843 (W.D. Tex 2007) asook *Doe v Sexsearch.com* 502 F Supp 2d 719 (N D Ohio 2007). In ál hierdie sake het ISP's finansiële voordeel uit kinderpornografie verkry, *wetend* dat dit op hulle bedieners is. Dit is daarom nie vreemd nie dat Noeth 'n ernstige beroep doen om die huidige ongunstige posisie te beredder. In haar artikel noem sy verskeie maniere waarop dit gedoen kan word. Noeth 2009 *Federal Communications Law Journal* 770–784.

119 Noeth 2009 *Federal Communications Law Journal* 770–784.

120 Mehra S K en Trimble M "Secondary Liability, ISP Immunity, and Incumbent Entrenchment" 2014 *American Journal of Comparative Law* 685. Op 694 meld hulle: "Although case law developed so that the law does not penalize ISPs for deploying the technologies, the statute and case law *do nothing to prompt ISPs to innovate*". My kursivering.

121 Vn 107 hierbo.

hindernis vir nuwe besighede is om tot dieselfde mark toe te tree.[122]

Mehra en Trimble wys ook daarop dat paragraaf 230 van die CDA nie slegs op Internet-diensverskaffers van toepassing is nie, maar selfs ook op "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions".[123] Enige persoon of instansie wat dus blote toegang tot die Internet verskaf — en dus ook plekke soos openbare biblioteke en opvoedkundige instansies — sal onder die beskerming van paragraaf 230 van die CDA val.

Uit die bespreking hierbo is dit baie duidelik dat paragraaf 230 van die CDA uitermate beskerming aan diensverskaffers bied. Die vraag is egter of hierdie tipe beskerming nie dalk heeltemal skeefgetrek is in die guns van die diensverskaffer nie. Ardia bied 'n antwoord op hierdie vraag.[124] Hy het empiriese navorsing onderneem deur ál die opgetekende regspraak sedert die CDA se uitvaardiging na te speur.[125] Een-honderd-vier-en-tagtig hofsake is tussen 1996 en 2010 statisties ondersoek. Die gevolgtrekking is interessant, deurdat een-derde van die eise geslaag het, en dus die streng vereistes van paragraaf 230 kon weerstaan.[126] In meer as 'n helfte van die sake wat ondersoek is, was die eisers in staat om die Internet-diensverskaffers te verplig om die gewraakte inligting op hul bedieners te verwyder.[127]

---

122 Mehra en Trimble 2014 *American Journal of Comparative Law* 703. Daar is al verskeie aanbevelings gemaak dat die CDA meer omvattend met ISP's moet handel (soos wat die geval met die DMCA is wat vervolgens bespreek word). Vir meer hieroor sien Scott M D "Would a 'Right of Reply' Fix Section 230 of the Communications Decency Act?" 2012 *International Journal of Law and Information Technology* 73 79.

123 Par 230(f)(2) van die CDA. Sien ook Mehra 2014 *American Journal of Comparative Law* 701.

124 Ardia D S "Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity under Section 230 of the Communications Decency Act" 2010 *Loyola of Los Angeles Law Review* 373 373.

125 Ardia noem dat hy 184 beslissings oor paragraaf 230 van die CDA in sy studie ingesluit het. Ardia 2010 *Loyola of Los Angeles Law Review* 373.

126 Ardia 2010 *Loyola of Los Angeles Law Review* 493.

127 Ardia 2010 *Loyola of Los Angeles Law Review* 493.

6.4.1.3 *Digital Millennium Copyright Act*

Die tweede stuk wetgewing wat ISP-aanspreeklikheid in die VSA reguleer, is die *Digital Millennium Copyright Act* (hierna DMCA).[128] Dit is in 1998 uitgevaardig in reaksie op twee *World Intellectual Property Organization* (WIPO) verdrae, te wete die *WIPO Copyright*-verdrag[129] en die *WIPO Performances and Phonograms*-verdrag.[130] Soos die naam aandui is die primêre taak van die DMCA om kopieregskending hok te slaan. Dit reguleer dan ook kopiereg in heelwat fyn besonderhede. In hierdie studie is paragraaf 512 van belang, aangesien dit spesifiek Internet-diensverskaffers raak.[131]

Paragraaf 512 skep vier kategorieë waar Internet-diensverskaffers aanspreeklikheid kan ontduik vir werke op hulle bedieners waarop daar kopiereg is.[132] Die eerste is inligting wat van deurgaande aard is, met ander woorde die Internetdiensverskaffer roeteer bloot die inligting van een plek na 'n ander, en die netwerke van die Internetdiensverskaffer is bloot die meganisme om die oordrag van die inligting te fasiliteer.[133] Die tweede is wanneer die ISP data in sy netwerk se kasgeheue berg,[134] en die derde is die berging van data op versoek van netwerk gebruikers.[135] Die vierde kategorie waar Internet-diensverskaffers aanspreeklikheid vir kopieregskending kan ontduik, het te doen met inligtingsopsporingsgereedskap.[136] Indien die ISP aan die vereistes van enige van hierdie kategorieë voldoen, bestaan daar

128 112 Stat 2860 (1998).

129 Geneve 1996.

130 Geneve 1996. Vir meer oor WIPO Internet-verdrae, sien Kumar A "Internet Intermediary (ISP) Liability for Contributory Copyright Infringement in USA and India: Lack of Uniformity as a Trade Barrier" 2014 *Journal of Intellectual Property Rights* 272 273.

131 Die DMCA word statutêr gekodifiseer in 17 USC § 512.

132 Band J en Schruers M "Safe Harbors Against the Liability Hurricane: The Communications Decency Act and the Digital Millennium Copyright Act" 2002 *Cardozo Arts and Entertainment Law Journal* 295 304; Karjala D S, Brown J E en O'Connor S D "International Convergence on the Need for Third Parties to Become Internet Copyright Police (But Why?)" 2013 *Richmond Journal of Global Law and Business* 189 193; Bretan J "Harboring Doubts About the Efficacy of § 512 Immunity Under the DMCA" 2003 *Berkeley Technology Law Journal* 43 48–50.

133 Par 512(a).

134 Par 512(b).

135 Par 512(c).

136 Par 512(d).

'n absolute verbod op regsaanspreeklikheid vir enige eise, asook interdikte van kopiereghouers teen die ISP. Die vier kategorieë word kortliks hieronder bespreek.

6.4.1.3.1 Inligting van Deurgaande Aard

Paragraaf 512(a) van die DMCA bepaal dat 'n ISP nie aanspreeklik sal wees vir enige kopieregskending op sy bediener vir die deurstuur, roetering of die beskikbaarstelling van konneksies om inligting deur te stuur nie, mits dit aan vier vereistes voldoen, te wete:

(a) die deurstuur van die materiaal was deur iemand anders begin of geïnisieer;[137]

(b) dit word gedoen deur 'n geoutomatiseerde proses;[138]

(c) die Internetdiensverskaffer kies nie die ontvangers van die boodskap nie, en[139]

(d) die inligting word nie op die bediener geberg vir 'n langer tydperk as wat dit redelikerwys nodig is nie, en dit moet ook nie beskikbaar wees vir enigiemand anders as die voorgenome ontvanger nie.[140]

Uit die parafrase van paragraaf 512(a) hierbo is dit duidelik dat hierdie artikel ten doel het om aspekte te hanteer waar die ISP spesifiek 'n geleidingsbuis van die data is. Die vier vereistes wat gestel word toon ook aan dat die ISP 'n passiewe rol speel, en dus nie sy netwerk spesifiek moniteer om die data op enige wyse te manipuleer of te stoor nie.

In *Perfect 10 Inc v Ccbill LLC*[141] het die hof van appèl beslis dat iemand wat bloot 'n konneksie of skakeling bewerkstellig om data te

137 Par 512(a)(1).

138 Par 512(a)(2).

139 Par 512(a)(3).

140 Par 512(a)(4).

141 488 F 3d 1102 — Court of Appeals 9th Circuit 2007.

roeteer, as 'n diensverskaffer gereken kan word, en dus op paragraaf 512 se nie-aanspreeklikheidsklousules kan steun.[142] Dit is dus nie slegs diensverskaffers wat inderwaarheid data roeteer, wat op die bepalings van paragraaf 512 kan steun nie, maar selfs ook diensverskaffers wat bloot 'n skakeling na die data bewerkstellig.

In *Lightspeed Media Corp v Smith*[143] het die hof van appèl genoem dat indien 'n Internet-diensverskaffer finansiële voordeel uit 'n gebruiker se kopieregskending verkry, dit nog steeds op die beskerming van paragraaf 512(a) geregtig is.[144]

6.4.1.3.2 Berging in Kasgeheue

Die tweede beskerming wat paragraaf 512 aan Internet-diensverskaffers bied, is om beskerming te verleen in gevalle waar die data tydelik op die ISP se bedieners gestoor word.[145] Die artikel praat spesifiek van "intermediary and temporary storage", so dit is baie duidelik dat langdurige berging van hierdie bepaling uitgesluit word.

Met hierdie bepaling het die wetgewer 'n baie spesifieke soort databerging in gedagte gehad, naamlik *kasgeheue*. Die Engelse term "caching" is dalk meer bekend. Dit het te make met die gebruik waar ISP's webwerwe en ander data wat gereeld deur gebruikers aangevra word — soos byvoorbeeld nuusberigte en ander aktuele sake — op hulle eie bedieners te plaas. Deur dit te doen kan die inligting baie vinniger aan gebruikers deurgegee word, en verlig dit ook die las op die betrokke ISP se data-lyn. Kasgeheue word gereeld verfris — dit kan elke paar minute gedoen word, en in sommige gevalle kan dit so lank as 'n paar uur wees voordat die kasgeheue verfris word.

Hierdie hele proses vind plaas sonder die inmenging van mense. Rekenaars word geprogrammeer om sekere inligting in die kasgeheue te

142 Die hof meld: "We reject Perfect 10's argument that CCBill is not eligible for immunity under § 512(a) because it does not itself transmit the infringing material" 1116 van die uitspraak.

143 761 F 3d 699 — Court of Appeals, 7th Circuit 2014

144 Op 709.

145 Par 512(b).

plaas, en die sagteware bepaal hoe dikwels die kasgeheue verfris word.

Met paragraaf 512 het die wetgewer gepoog om spesifiek uiteen te sit wanneer die nie-aanspreeklikheidsbepaling in werking sal tree. Daar is spesifiek drie aspekte neergelê wat kasgeheue onderlê, te wete:

(a) dat die kopieregskendende materiaal deur iemand anders as die ISP op die bediener geplaas moes word;[146]

(b) dat die kopieregskender die data deur die betrokke ISP se netwerk na 'n ander bestemming moes stuur (met ander woorde die ISP se netwerk is vir die kopieregskendende gedrag gebruik),[147] en

(c) dat die diens wat aan die kopieregskender verleen is, op 'n geoutomatiseerde wyse plaasgevind het.[148]

Die drie bovermelde aspekte kan baie maklik misverstaan word. Wat die bepaling eintlik sê is dat iemand anders as die ISP die kopieregskendende materiaal beskikbaar gestel het. Dit gebeur byvoorbeeld wanneer iemand 'n boek waarop daar kopiereg is, skandeer en dit op die Internet plaas. Dit kan dan maklik gebeur dat die betrokke boek aangestuur word, en die spesifieke ISP se netwerk gebruik word om dit te doen. As die ISP se rekenaars dus die boek in die kasgeheue plaas, sal die ISP nie aanspreeklik gehou kan word dat dit kopieregskendende materiaal op sy netwerk het nie. Die tweede aspek ((b)-hierbo) verduidelik eenvoudig dat die ISP geen aktiewe aandeel gehad het om die kopieregskendende materiaal op sy netwerk te plaas nie. Die gebruiker het die inisiatief geneem om die kopieregskendende materiaal deur die netwerk van die ISP te stuur. Die derde aspek behels eenvoudig dat

146 Par 512(b)(1)(a).

147 Par 512(b)(1)(b).

148 Par 512(b)(1)(c). My parafrase van hierdie bepaling is baie vereenvoudig. Die volledige bepaling lees soos volg: "the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A)". Dit het dus te doen met die geval waar die kopieregskender van 'n geoutomatiseerde proses gebruik maak om die kopieregskendende materiaal "op te laai" na die bedieners van die ISP.

die ISP se netwerk so saamgestel is dat dit outomaties die materiaal van die gebruiker verkry en dit na die ontvanger aanstuur.

Weer eens is dit duidelik dat die bedoeling van die wetgewer is dat die ISP nie 'n *aktiewe* aandeel in die aanstuur van die materiaal gehad het nie.

In *Ellison v Robertson* [149] het kopieregskendende materiaal op die bedieners van 'n ISP geland. Ellison was die skrywer van 'n aantal kortverhale, en 'n ene Stephen Robertson het die werke geskandeer en verder versprei. Dit het op die netwerk van *America Online* geland, en laasgenoemde is gedagvaar omdat daar kopieregskendende werke van Ellison op *AOL* se bedieners was. In hierdie geval het die hof op die feite beslis dat *AOL* nie op paragraaf 512(a-d) van die DMCA kan staat maak nie, omdat dit nie die vereistes ten aansien van interdikte in paragraaf 512(i) nagekom het nie.[150]

6.4.1.3.3 Inligting van Gebruikers

Paragraaf 512(c) het te doen met gevalle waar gebruikers kopieregskendende data direk op die netwerk van die ISP plaas. Subparagraaf (1) bepaal dat die ISP nie vir kopieregskending aanspreeklik sal wees nie, mits dit:

(a) nie werklike kennis het dat die materiaal kopieregskendend is nie;[151]

(b) nie van enige inligting bewus is wat die ISP daarop moes gewys het dat daar kopieregskendende materiaal op sy netwerk is nie;[152]

(c) wanneer die ISP daarvan bewus word dat daar kopieregskendende materiaal op sy netwerk is, spoedig optree om dit te verwyder, of toegang daartoe te beperk;[153]

149 357 F 3d 1072 — Court of Appeals 9th Circuit 2004.

150 Vir meer inligting oor art 512(i), sien Chang L "The Red Flag Test for Apparent Knowledge Under the DMCA § 512(c) Safe Harbor" 2010 *Cardozo Arts and Entertainment Law Journal* 195 199.

151 Par 512(c)(A)(i).

152 Par 512(c)(A)(ii).

153 Par 512(c)(A)(iii).

(d) die ISP nie enige finansiële voordeel uit die kopieregskendende aktiwiteit verkry nie terwyl hy die vermoë het om sodanige aktiwiteit te beheer, en[154]

(e) wanneer die ISP 'n kennisgewing ontvang dat daar kopieregskendende materiaal op sy netwerk is, vinnig optree om dit te verwyder of om toegang daartoe te verbied.[155]

Alhoewel die vereistes redelik duidelik is, het hierdie mondvol-bepaling al tot menigte regspraak aanleiding gegee. Slegs in 2015 was daar reeds 15 hofsake in die VSA oor subparagraaf 512(c).[156] Die probleem wat gewoonlik opduik is dat die kopiereghouer verwag dat die ISP sy netwerk so bestuur dat kopieregskendende materiaal outomaties verwyder word, terwyl die ISP weer van mening is dat die kopiereghouer hom van die skending in kennis moet stel. In *Perfect 10 Inc v Ccbill Llc* [157] het die hof die saak opgeklaar deur te bepaal dat die *onus* op die kopiereghouer rus om die skending aan die ISP bekend te maak.[158] Dit is bevestig in *UMG Recordings Inc v Shelter Capital Partners.*[159] In laasgenoemde saak het die hof dit baie duidelik gemaak dat: "the DMCA recognizes that service providers who do not locate and remove

154 Par 512(c)(B).

155 Par 512(c)(C). Vir verdere inligting oor par 512(c) sien Karjala D S "Liability of Internet Service Providers Under United States Law" 2006 *Jurisprudencia* 9 12.

156 *Lenz v Universal Music Corp* 801 F 3d 1126 (9th Cir 2015); *Totallyher Media v BWP Media USA* No 2 13-cv-08379-AB-PLAX (C.D. Cal Apr 7 2015); *Square Ring Inc v John Doe-1* Civil Action No 09-563 (GMS) (D. Del. Jan 23 2015); *Milo and Gabby v Amazon.com* No C13-1932RSM (W.D. Wash. July 16 2015); *Avdeef v Google* No 4: 14-CV-788-A (N. D. Tex. Aug 26 2015); *BWP Media USA v Clarity Digital Group* Civil Action No 14-cv-00467-PAB-KMT (D. Colo. Mar 31 2015); *Sarvis v Polyvore* Civil Action No 12-12233-LTS (D. Mass. Mar 2 2015); *Google v Hood* 96 F Supp 3d 584 (S.D. Miss. 2015); *China Central Television v Create New Technology (HK)* No CV 15-01869 MMM (MRWx) (C.D. Cal. June 11 2015); *William Business Services v Waterside Chiropractic* No 3: 14-cv-05873-BHS (W.D. Wash. Mar 18 2015); *Automattic Inc v Steiner* 82 F Supp 3d 1011 (N D Cal. 2015); *TD Bank v Hill* Civil No 12-7188 (RBK/JS) (D.N.Y. July 27 2015); *BMG Rights Management v Cox Communications* Civil No 1: 14-cv-1611 (E.D. Va. Dec 1 2015); *UMG Recordings v Escape Media Group* No 11 Civ. 8407 (TPG) (S D N Y Apr 23 2015) en *FC Online Marketing v Burke's Martial Arts* No 14-CV-3685 (SJF)(SIL) (E D N Y July 8 2015).

157 488 F 3d 1102 — Court of Appeals 9th Circuit 2007. Vir 'n bespreking van hierdie saak sien Garon J M "Tidying Up the Internet: Takedown of Unauthorized Content Under Copyright, Trademark, and Defamation Law" 2013 *Capital University Law Review* 513 520.

158 Op 1114 van die uitspraak.

159 718 F 3d 1006 — Court of Appeals 9th Circuit 2013 1023.

infringing materials *they do not specifically know of* should not suffer the loss of safe harbor protection".[160] In hierdie geval het Veoh (die netwerk-eienaar en ISP) spoedig gereageer om kopieregskendende materiaal te verwyder waarvan dit in kennis gestel is, en dit het veroorsaak dat die ISP steeds op paragraaf 512(c) van die DMCA kon steun.[161]

Paragraaf 512(c)(3) bevat 'n uitgebreide bepaling oor hoe daar aan die ISP kennis gegee moet word van kopieregskendende materiaal, soos die ligging van die materiaal (die web-adres), besonderhede van die kopie-reghouer, en kontakbesonderhede.[162] Om seker te maak dat moedswillige kennisgewings beperk word, bevat paragraaf 512(g)(3) 'n klousule waar die ISP 'n teen-kennisgewing kan aanteken waarom die materiaal nie onttrek behoort te word nie.[163]

6.4.1.3.4 Inligtingsopsporingsgereedskap

Paragraaf 512(d) handel oor inligtingsopsporingsgereedskap, en hanteer maar eintlik net twee spesifieke aspekte. Die eerste is dat 'n ISP nie aanspreeklik gehou sal word indien dit 'n skakel na 'n kopieregskendende werk verskaf nie. Die tweede is dat 'n ISP eweneens aanspreeklikheid sal vryspring indien dit 'n soekenjin of gids (directory) verskaf wat 'n gebruiker

---

160 Op 1023. My kursivering. Sien Reese R A "The Relationship Between the ISP Safe Harbors and the Ordinary Rules of Copyright Liability" 2009 *Columbia Journal of Law and the Arts* 427 433 vir meer inligting oor die kennisvereiste in die VSA-reg.

161 Op 1023 van die uitspraak.

162 Vir volledigheidshalwe word die inhoud van par 512(c)(3) hier weergegee:
Die kennisgewing moet in geskrewe vorm wees en aan die toegewysde agent (designated agent) gestuur word. Dit moet die volgende inligting bevat:
(i) 'n Fisiese of elektroniese handtekening van 'n persoon wat namens die kopiereghouer kan optree;
(ii) identifisering van die werk waarop daar kopiereg is, of 'n lys as daar meerdere werke is;
(iii) identifisering van die kopieregskendende materiaal op die netwerk van die ISP sodat laasgenoemde die werke op sy netwerk kan opspoor;
(iv) kontakbesonderhede van die klaer, soos adres, telefoonnommer en e-posadres;
(v) 'n verklaring wat aantoon dat die kopieregskendende werk nie op 'n gemagtigde wyse gebruik word nie, en
(vi) 'n verklaring van die klaer dat die inligting in die verklaring na sy beste wete akkuraat is, en dat hy (die aflegger van die verklaring) magtiging het om namens die kopiereghouer op te tree.

163 'n Voorbeeld van 'n teen-kennisgewing is te vinde in *Lenz v Universal Music Corp* 801 F 3d 1126 — Court of Appeals 9th Circuit 2015 1130; *Tuteur v Crosley-Corcoran* 961 F Supp 2d 333 — Dist Court D. Massachusetts 2013 335–336.

in staat stel om toegang tot 'n betrokke (kopieregskendende) werk te verkry.[164] Die vereistes waaraan die ISP moet voldoen, is identies aan dié wat hierbo in paragraaf 512(c) gestel is, en daarom sal dit nie weer spesifiek herhaal word nie.

Dit is duidelik dat hierdie paragraaf op soekenjins soos *Google*, *Yahoo*, *Bing* en andere van toepassing is. Solank die soekenjin nie bewus is van die kopieregskendende werk nie, sal dit beskerming onder paragraaf 512(d) geniet. Sodra kennis gegee word van 'n kopieregskendende werk, moet die soekenjin spoedig optree om dit te verwyder.[165]

6.4.1.3.5 Diverse bepalings

Paragraaf 512 van die DMCA bevat ook nog 'n verskeidenheid ander bepalings wat nie-aanspreeklikheid verleen, soos in die geval van nie-winsgewende opvoedkundige instellings.[166] Daar word spesifiek gepraat van "nonprofit institution of higher education", en dit is duidelik dat universiteite en kolleges hier ter sprake is.[167] Die universiteit word beskerm deurdat 'n fakulteitslid of studente-assistent (wat as 'n "graduate student" beskryf word) beskou sal word as "a person other than the institution", en dus nie iemand wat namens die universiteit optree nie.[168] So word die universiteit beskerm teen persone wat moontlik kopiereg kan skend.

Indien 'n Internetdiensverskaffer op sy eie uit goeder trou materiaal verwyder, kan hy nie daarvoor aanspreeklik gehou word nie.[169]

Paragraaf 512(k)(1) verduidelik wat 'n Internet-diensverskaffer ingevolge hierdie wetgewing is. Daar word twee definisies gegee: die eerste is van toepassing op paragraaf 512(a) (wat handel oor inligting van deurgaande

164 Par 512(d).

165 Par 512(d)(1)(C).

166 Par 512(e).

167 Par 512(e).

168 Par 512(e).

169 Par 512(g)(1).

aard)[170] terwyl die tweede op die res van paragraaf 512 van toepassing is. Die eerste definisie lui:

> As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.[171]

Uit die definisie is dit duidelik dat woorde soos "transmission", "routing", "providing connections" en "between or among points" die klem laat val op die diensverskaffer wat sy netwerk gebruik as 'n *verspreidingsmeganisme* — amper soos die posdiens. Hierteenoor is die tweede definisie meer generies waar die klem op *toegang* val, soos blyk uit woorde soos "network access" en "facilities". Die tweede definisie lui soos volg:

> As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).[172]

In *Viacom International v YouTube* [173] het die hof die twee definisies van paragraaf 512(k) bespreek. Benewens die feit dat die eerste definisie slegs op paragraaf 512(a) van toepassing is en die tweede definisie op die res van paragraaf 512, het die hof spesifiek genoem dat die eerste definisie spesifiseer dat die inligting wat deur die ISP se netwerk beweeg, sonder enige verandering deurgestuur moet word.[174] Die belang daarvan is dat daardie vereiste nie in die tweede definisie voorkom nie, en gevolglik meen die hof dat in gevalle anders as in paragraaf 512(a), die data wél verander mag word.[175] Dié siening is bevestig in *Columbia Pictures Industries v*

170 Afd 6.4.1.3.1.

171 Par 512(k)(1)(A).

172 Par 512(k)(1)(B).

173 676 F 3d 19 — Court of Appeals 2nd Circuit 2012; Kumar 2014 *Journal of Intellectual Property Rights* 275.

174 Op 39.

175 Die hof meld op 39: "No such limitation appears in the broader definition, which applies to service providers ... we conclude that § 512(c) is clearly meant to cover more than mere electronic storage lockers".

Fung[176]

Uit die bespreking hierbo is dit duidelik dat die DMCA uitvoerige riglyne neerlê vir die beskerming van ISP's — mits hulle aan die nodige vereistes voldoen. Tóg is dit steeds nie die einde van ISP-beskerming in die VSA nie, aangesien daar nog 'n derde stuk wetgewing is wat aan ISP's beskerming verleen. Dit is te vinde in die *Lanham*-wet, wat vervolgens kortliks bespreek word.

6.4.1.4 *Lanham*-Wet

Die derde — en laaste — stuk wetgewing wat Internet-diensverskaffer aanspreeklikheid reguleer, is die sogenaamde *Lanham*-wet, wat reeds in 1946 uitgevaardig is.[177] Verskeie wetswysigings[178] het dié wet in die digitale era ingebring, en dit maak in paragraaf 1114(2)(B) en (C) voorsiening vir die nie-aanspreeklikheid vir (onder andere) diensverskaffers wat onwetend hulle aan handelsmerkskending[179] skuldig maak.

Paragraaf 1114(2) is duidelik in 'n era geskryf waar die Internet nog nie bestaan het nie, en die wysigings om "electronic communication" daarby in te sluit, het nie die bedoelde effek gehad nie. Die bondige bespreking wat volg sal die probleem uitlig.

Die argaïese formulering van die bepaling is duidelik sigbaar:

> Where the infringement or violation complained of is contained in or is part of paid advertising matter in a newspaper, magazine, or other similar periodical or in an electronic communication as defined in section 2510(12) of title 18, the remedies of the owner of the right infringed or person bringing the action under section 1125(a) of this title as against the publisher or

176 710 F 3d 1020 — Court of Appeals 9th Circuit 2013 1040; *UMG Recordings v Shelter Capital Partners* 718 F 3d 1006 — Court of Appeals 9th Circuit 2013 1019 vn 9.

177 Die Lanham-wet is gekodifiseer in 15 USC § 1051.

178 Sien die notas by Legal Information Institute "15 USC § 1114 — Remedies; Infringement; Innocent Infringement by Printers and Publishers" https://www.law.cornell.edu/uscode/text/15/1114#2_D (besoek op 2 Maart 2016).

179 'n Algemene bespreking van Handelsmerke onder die Lanham-wet maak nie deel uit van hierdie studie nie. Vir meer inligting daaroor sien Goldsmith T J "What's Wrong with this Picture? When the Lanham Act Clashes with Artistic Expression" 1997 *Fordham Intellectual Property, Media and Entertainment Law Journal* 821 829.

> distributor of such newspaper, magazine, or other similar periodical or electronic communication shall be limited to an injunction against the presentation of such advertising matter in future issues of such newspapers, magazines, or other similar periodicals or in future transmissions of such electronic communications. The limitations of this subparagraph shall apply only to innocent infringers and innocent violators.[180]

Let daarop dat daar nêrens in die bepaling by name van Internet-diensverskaffers melding gemaak word nie. Net so wil dit voorkom asof die klem eintlik op "newspaper, magazine, or other similar periodical" is, en dat "electronic communication" maar 'n nagedagte was. Die doel van die wetsbepaling kom darem deur, en dit behels dat 'n ISP (in die huidige konteks) nie aanspreeklik sal wees vir 'n onwetende of onskuldige handelsmerkskending nie, en dat 'n klaer of eiser se aansoek beperk sal word tot 'n interdik wat 'n volgende skending sal probeer beperk.

Om te bepaal hoe hierdie verouderde stuk wetgewing in die konteks van die Internet gebruik kan word, moet *Hendrickson v eBay*[181] beskou word. Die eiser het die verweerder gedagvaar omdat laasgenoemde vervalste kopieë van die eiser se handelsmerk beskikbaar gestel het. Die verweerder, *eBay*, het nie sélf die vervalsings verkoop nie, maar bloot die platvorm geskep waar gebruikers van *eBay* die handelsmerk geskend het (*eBay* is 'n elektroniese veilingswebwerf).

Die hof het eerstens bevestig dat volgens die Lanham-wet is die eiser se remedies beperk tot 'n interdik teen verdere handelsmerkskending.[182] Dan bespreek die hof die partye se versoeke: *eBay* voer aan dat die interdik nie meer nodig is nie, aangesien dit reeds alle handelsmerkskendings verwyder het, en ook 'n advertensie wat die handelsmerk geadverteer het, verwyder het. *eBay* voer verder aan dat dit nie enige bedoeling het om enigsins meer iets met die handelsmerk te doen wat op enige vorm van skending neerkom

---

180 Par 1114(2)(B).

181 165 F Supp 2d 1082 — Dist Court CD California 2001.

182 Op 1095 noem die hof dat: "Plaintiff's remedy is limited to an injunction against the future publication or transmission of the infringing advertisements on eBay's website".

nie.[183] Hierteenoor voer die eiser aan dat hy aansoek doen vir 'n interdik wat *eBay* verhoed om *enige* verdere advertensies of vervalsing te eniger tyd in die toekoms te adverteer of aan te bied. Die hof beskou die aansoek as: "Plaintiff seeks an injunction enjoining any and all false and/or misleading advertisements that may be posted on eBay's website by users in the future, regardless of whether they are the basis of this lawsuit and whether they have been identified by Plaintiff"[184] en meld dan ewe bot dat: "No authority supports Plaintiff's position".[185] Die hof verklaar dan dat dit sou beteken dat *eBay* elkeen van die miljoene advertensies wat dit op 'n daaglikse basis vertoon, moet moniteer, en kom tot die gevolgtrekking dat "no law currently imposes an affirmative duty on companies such as *eBay* to engage in such monitoring".[186] Die beskerming van die Lanham-wet word bevestig.

Aangesien die Lanham-wet so argaïes en onduidelik geformuleer is, is dit nie vreemd nie dat die oorgrote meerderheid hofsake wat met ISP-aanspreeklikheid te doen het, onder die CDA en DMCA bereg word. Powell meen dat die Lanham-wet uitvoerig aangepas moet word om dit in lyn met moderne wetgewing te bring.[187] In haar artikel "The *eBay* Trademark Exception: Restructuring the Trademark Safe Harbor for Online Marketplaces"[188] formuleer sy 'n twee-bladsy wysiging tot die Lanham-wet wat dit in lyn met die breedvoerige bepalings van die DMCA bring.[189] Of dit aanvaarbaar vir 'n VSA-wetgewer sal wees, is nog onduidelik, maar 'n modernisering van hierdie wetgewing sal tog 'n welkome byvoeging tot die elektroniese handelsmerkereg wees.

Tot op hede is die drie stukke wetgewing bespreek wat in die VSA geformuleer is om Internet-diensverskaffers se aanspreeklikheid te reguleer.

183 *Hendrickson v eBay* 1095.

184 *Hendrickson v eBay* 1095.

185 *Hendrickson v eBay* 1095.

186 *Hendrickson v eBay* 1095.

187 Powell C D "The *eBay* Trademark Exception: Restructuring the Trademark Safe Harbor for Online Marketplaces" 2011 *Santa Clara High Technology Law Journal* 1 1.

188 Powell 2011 *Santa Clara High Technology Law Journal* 1.

189 Powell 2011 *Santa Clara High Technology Law Journal* 18–20.

ISP's is 'n integrale deel van die regulatoriese sisteem, en dit wil voorkom asof hulle aansienlike vryheid geniet. Eienaardig genoeg is dit slegs een kant van die muntstuk wanneer die groter regulatoriese vraagstuk beskou word, want daar is 'n ander, meer duistere aangeleentheid wat aangespreek moet word om die hele prentjie te voltooi. Dit het reeds begin met gebeure wat 'n president tot 'n val gebring het, en word vervolgens bespreek.

6.4.1.5 VSA Intelligensiediens

6.4.1.5.1 *Foreign Intelligence Surveillance Act*[190]

Die 1970's is ingelui met die *Watergate*-skandaal waar dit geblyk het dat President Nixon se administrasie onwettige metodes gebruik het om op verskeie persone en organisasies te spioeneer.[191] Die klem het veral op elektroniese monitering (electronic surveillance) geval asook die wyse waarop die verskeie afdelings van die VSA se intelligensiediens opgetree het. President Nixon het as gevolg hiervan bedank.[192]

Die publiek het nie meer vertroue in die regering se *bona fides* gehad nie en die Amerikaanse kongres moes 'n wyse kry om die publiek se kommer aan te spreek terwyl dit ook die intelligensiediens in staat moes stel om sy werk te kan doen. Om die groot probleem aan te spreek, is die *Church*-kommissie daargestel.[193] Dit het die enkele grootste ondersoek in die geskiedenis van die Amerikaanse intelligensiediensbedrywighede ingelui. Donohue verduidelik:

> The Church Committee subsequently took testimony from hundreds of people, inside and outside of government, in public and private hearings.

190 *50 USC Chapter 36 — Foreign Intelligence Surveillance.*

191 Donohue L K "Bulk Metadata Collection: Statutory and Constitutional Considerations" 2014 *Harvard Journal of Law and Public Policy* 757 778–779.

192 Donohue 2014 *Harvard Journal of Law and Public Policy* 778–779.

193 Die kommissie het sy naam te danke aan senator Frank F Church wat die voorsitter van die kommissie was. Rascoff S J "Presidential Intelligence" 2016 *Harvard Law Review* 633 647 verduidelik die onstaansgeskiedenis van die Church-kommissie.

> The NSA, FBI, CIA, Internal Revenue Service, Post Office, and other federal agencies submitted documents.[194]

Die bevindings was skokkend. Die komitee het bevind dat die intelligensiediens 'n breë binnelandse moniteringsprogram onder die skyn van internasionale spioenasie bedryf het, en dat dit die privaatheid van VSA-burgers geskend het.[195] Die *National Security Agency* (hierna NSA) was blykbaar die grootste oortreder.[196]

Volgens die *Church*-kommissie was die oplossing 'n sisteem wat oorsig oor die intelligensiedienste moet kan handhaaf. Die *National Security Act* van 1947 is herskryf,[197] en 'n splinternuwe *Foreign Intelligence Surveillance Act* van 1978[198] (hierna FISA) is geskep.[199] Laasgenoemde sou "at long last place foreign intelligence electronic surveillance under the rule of law".[200] FISA het die kernvoorstelle van die *Church*-kommissie bevat, want dit het vier ingrypende veranderinge aan die sekuriteitswetgewing gemaak: eerstens is die vereiste geskep dat 'n *spesifieke* persoon of entiteit ondersoek moes word, en dat daardie persoon of entiteit aan 'n spesifieke buitelandse staat gekoppel moes word; tweedens is die "probable cause"-vereiste[201] daargestel wat beteken dat 'n persoon slegs ondersoek mag word indien daar 'n waarskynlike oorsaak is dat die persoon met onwettige bedrywighede besig is; derdens is daar sogenaamde "minimization procedures" daargestel om die tipe inligting wat verkry kan word, te beperk, en vierdens — en waarskynlik die belangrikste — is daar 'n *Foreign Intelligence Surveillance Court* (hierna FISC) en *Foreign Intelligence Surveillance Court of Appeal* daargestel om oorsig en monitering

194 Donohue 2014 *Harvard Journal of Law and Public Policy* 769.

195 Donohue 2014 *Harvard Journal of Law and Public Policy* 770.

196 Donohue 2014 *Harvard Journal of Law and Public Policy* 770.

197 Donohue 2014 *Harvard Journal of Law and Public Policy* 781.

198 Daar was eintlik twee *Foreign Intelligence Surveillance*-wette (en beide het dieselfde name gehad): die eerste van 1976 en die tweede van 1978. Donohue 2014 *Harvard Journal of Law and Public Policy* 782.

199 Donohue 2014 *Harvard Journal of Law and Public Policy* 782.

200 Aldus die woorde van senator Ted Kennedy. 124 Congress Records 34,845 (1978).

201 Vir meer inligting oor die "probable cause" vereiste, sien Landau S "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations" 2013 *IEEE Security and Privacy* 54 55.

vir die intelligensiedienste daar te stel.[202] Laasgenoemde was howe wat nie toeganklik was vir die publiek nie, en wat dus in die geheim gesit het — en dit is steeds die geval — maar wat ten minste 'n waghond was om die optrede van die intelligensiedienste te moniteer.

Die FISA was wyd verwelkom, aangesien dit "checks and balances" daargestel het om vrye teuels van die intelligensiedienste te beperk.[203]

6.4.1.5.2 FISA-wysigings

Dit het alles ongelukkig verander met 'n handjievol wette wat ná die gebeure van 9/11 se terreuraanvalle op die New York handelsentrum, uitgevaardig is.[204] Die gevolg is dat die wet wat wyd besing is om die intelligensiediens in toom te hou, in 'n drakoniese stuk wetgewing verander is. Die omvang van die wysigings het begin deurskemer nadat die *Electronic Frontier Foundation* die regering in 2006 gedagvaar het met 'n versoek van inligting onder die *Freedom of Information Act*.[205] Daarvolgens het dit geblyk dat die FISC 'n aansoek van die *Federal Bureau of Investigations* (hierna FBI) goedgekeur het om die VSA se grootste telefoonmaatskappy, *Verizon*, te dwing om *alle* metadata aan hulle oor dra.[206] Om die geweldige omvang van hierdie hofbevel te begryp, moet daar kortliks aangedui word wat metadata is.

Metadata word deur elke telefoon- en selfoonmaatskappy gegenereer

202 Donohue 2014 *Harvard Journal of Law and Public Policy* 784.

203 Donohue 2014 *Harvard Journal of Law and Public Policy* 779.

204 Die USA PATRIOT-wet van 2001 Pub L No 107-56 het die ingrypendste veranderinge aangebring. Sien Donohue 2014 *Harvard Journal of Law and Public Policy* op 793 vn 166 vir meer hieroor, asook 794–800 vir 'n breedvoerige bespreking daarvan. Ander wette wat die FISA-wet gewysig het, is die *Intelligence Authorization Act for Fiscal Year 1995* Pub L No 103–359 § 302(c) 108 Stat 3423 3445 (1994) (gekodifiseer deur 50 USC §§ 1821–1829) en *Intelligence Authorization Act for Fiscal Year 1999* Pub L No 105–272, § 601 112 Stat 2396 2404–2410 (1998) (gekodifiseer deur 50 USC §§ 1841–1846). Vir 'n bespreking van die 9/11 gebeure en die resulterende PATRIOT-wetgewing, sien Welch K "The PATRIOT-act and Crisis Legislation: The Unintended Consequences of Disaster Lawmaking" 2015 *Capital University Law Review* 481 485–488.

205 5 USC § 552.

206 Donohue 2014 *Harvard Journal of Law and Public Policy* 759; Forsyth B "Banning Bulk: Passage of the *USA FREEDOM* Act and Ending Bulk Collection" 2015 *Washington and Lee Law Review* 1307 1309.

om hulle in staat te stel om hulle diens te kan verrig. Wanneer 'n gebruiker byvoorbeeld sy selfoon aanskakel, genereer dit 'n inskrywing in die selfoonmaatskappy se databasis wat die tyd aandui, asook onder watter selfoontoring die gebruiker val. Wanneer die gebruiker 'n telefoonoproep maak, word die inligting soos die tydsduur daarvan, asook die roete wat dit geneem het om die skakeling te kan bewerkstellig, aangeteken. So kan die persoon wat geskakel word, ook maklik geïdentifiseer word. Wanneer die gebruiker rondbeweeg van een plek na 'n ander, word sy/haar selfoonnommer van een selfoontoring na 'n volgende oorhandig. So kan die algemene ligging van die gebruiker bepaal word sonder dat GPS-inligting[207] gebruik hoef te word.[208] Let daarop dat metadata dus nie persoonlike inligting is wat die gebruiker self genereer nie, en dit bevat ook nie die *inhoud* van die kommunikasie nie.[209] Tóg verklap hierdie tipe inligting geweldig baie van die algemene gebruiker. Donohue wys dat deur die data te ontgin, kan "Alliances, friendships, and predilections ... be uncovered by studying patterns in behavior".[210] En Felten wys daarop dat:

> [C]ertain telephone numbers are used for a single purpose, such that any contact reveals basic and often sensitive information about the caller. Examples include support hotlines for victims of domestic violence and rape. ... The phone records indicating that someone called a sexual assault hotline or a tax fraud hotline will of course not reveal the exact words that were spoken during those calls, but phone records indicating a 30-minute call to one of these numbers will still reveal information that virtually everyone would consider extremely private.[211]

---

207 Liggingsinligting word gewoonlik verkry deur van die *Global Positioning System* (GPS) gebruik te maak. Hiervolgens gebruik 'n GPS-toestel 'n reeks seine vanaf satelliete om deur driehoeksmeting die ligging van die toestel op die aarde vas te stel. Dit is akkuraat tot ongeveer 'n meter vanaf die toestel.

208 Interessant genoeg kan selfoontorings deesdae ook 'n persoon se ligging volgens "selfoondriehoeksmeting" (Cell Phone Triangulation) bepaal, alhoewel dit nie naastenby so akkuraat soos GPS-sisteme is nie. Die selfoontorings wat in die omgewing van die selfoon is, kan bepaal hoe sterk die sein van die selfoon is, en daarvolgens bepaal ongeveer hoe ver die selfoon van die toring af is. Deur daardie inligting met ander selfoontorings in die omgewing te vergelyk, kan 'n kleiner matriks van die ligging van die gebruiker getrek word. Smith CS "Cell Phone Triangulation Accuracy Is All Over The Map" http://searchengineland.com/cell-phone-triangulation-accuracy-is-all-over-the-map-14790 (besoek op 4 Maart 2016).

209 Donohue 2014 *Harvard Journal of Law and Public Policy* 760

210 Donohue 2014 *Harvard Journal of Law and Public Policy* 871.

211 Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act Before the Senate

Trouens, in sekere opsigte is metadata meer waardevol as inhoudelike inligting, aangesien dit *gestruktureerd* is, wat beteken dat waardevolle inligting baie maklik daarvan onttrek kan word.[212]

Die FISC se magtiging aan die FBI om *Verizon* te verplig om *al* hulle metadata van *al* hulle gebruikers aan die FBI te oorhandig kan nou in konteks beskou word.[213] Trouens, hierdie drakoniese bevel is sedert 2006 uitgebrei na *alle* groot VSA telekommunikasiediensverskaffers.[214] Donohue plaas dit in perspektief:

> ... *Verizon* has 98.9 million wireless customers and 22.2 million landline customers; AT&T has 107.3 million wireless customers and 31.2 million landline customers; and Sprint has 55 million customers in total. In short, the program monitors hundreds of millions of people.[215]

Die omvang van hierdie moniteringsisteem was so omvangryk dat dit amper onwerklik voorkom. Die vraag wat onwillekeurig ontstaan is hoe hierdie situasie kon ontstaan te midde van die wye veranderinge wat deur die *Church*-kommissie ingebring is? Wat is die regsbasis van so 'n wye moniteringsisteem? Die antwoord is te vinde in die *Administration White Paper: Bulk Collection of Telephony Metadata under Section 215 of the USA PATRIOT Act.*[216] Hierdie witskrif is noodgedwonge vrygestel na aanleiding van die Electronic Freedom Foundation se regsgeding om die inligting te bekom.[217]

Committee on the Judiciary 113th Congress 3 (2013) 8–9 (geskrewe getuienis van Edward W Felten, Professor by Princeton Universiteit).

212 Felten sê bv: "Telephony metadata is easy to aggregate and analyze because it is, by its nature, *structured* data." Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act Before the Senate Committee on the Judiciary 113th Congress 3 (2013) 4 (geskrewe getuienis van Edward W Felten, Professor by Princeton Universiteit).

213 *Verizon* is in die internasionale sfeer as 'n sekuriteitsrisiko beskou. bv, die Duitse regering het 'n kontrak met *Verizon* gekanselleer nadat dit bekend geword het dat die NSA se metadata-program Verizon-kliënte teiken. Czas J "Note: Business, Law and Project *PRISM*" 2014 *The Georgetown Journal of Law and Public Policy* 897 897.

214 Donohue 2014 *Harvard Journal of Law and Public Policy* 759. Forsyth 2015 *Washington and Lee Law Review* 1309.

215 Donohue 2014 *Harvard Journal of Law and Public Policy* 872.

216 Anoniem "Administration White Paper: Bulk Collection of Telephony Metadata under Section 215 of the *USA PATRIOT* Act" http://perma.cc/V7VM-5MAU (besoek op 8 Maart 2016).

217 Afd 6.4.1.5.2. Hierdie dokument is blootgelê na aanleiding van 'n 2011 opvolgregsgeding om

Die witskrif begin deur te verklaar dat "This white paper explains the Government's legal basis for an intelligence collection program directing certain telecommunications service providers to *produce telephony metadata in bulk*".[218] Die witskrif verklaar dan dat die regsbasis van so 'n omvangryke spioenasieprogram te vinde is in artikel 215 van die *USA PATRIOT* wet, wat die FISA gewysig het, en wat statutêr in 50 USC § 1861 vervat is.

Weens die belangrikheid van hierdie artikel word dit hier weergegee, en dan in besonderhede bespreek aan die hand van die VSA-regering se witskrif:

> Subject to paragraph (3), the Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.[219]

Met die eerste lees van die artikel blyk dit dat die doel daarvan duidelik te make het met "foreign intelligence information". Die gedagte is dus om intelligensie te kry van bedrywighede in die buiteland, en daar word selfs genoem dat die doel is om teen internasionale terrorisme te veg. Die witskrif beaam dit kategories en sê dat die verkryging van metadata in groot maat (die sogenaamde "bulk metadata program") juis ten doel het om telefoon-inligting te kry tussen die VSA en ander lande.[220] Metadata is juis belangrik omdat: "by analyzing it, the Government can determine whether known or suspected terrorist operatives have been in contact with other persons who may be engaged in terrorist activities, including persons and

inligting te bekom. Electronic Freedom Foundation "Section 215 of the *USA PATRIOT* Act" https://www.eff.org/foia/section-215-usa-patriot-act (besoek op 8 Maart 2016).

218 My kursivering. Vn 216 2.

219 50 USC § 1861(a)(1).

220 Vn 216. Bl 2 van die witskrif.

activities within the United States".[221] Hier skemer die eerste regverdiging van die *binnelandse* metadata-program deur. Terroriste in die buiteland skakel met persone *in* die VSA, en die metadata-program stel die NSA in staat om te bepaal wie hulle is. Volgens die witskrif gee hierdie artikel dus aan die NSA die bevoegdheid om ook *binnelands* op grootskaalse vlak te moniteer. Die regverdiging word elders so verwoord: "Specifically, in the circumstance where the Government has reason to believe that conducting a search of a broad collection of telephony metadata records will produce counterterrorism information—and that it is necessary to collect a large volume of data in order to employ the analytic tools needed to identify that information—the standard of relevance under Section 215 is satisfied."[222]

Volgens die witskrif is relevansie 'n "broad standard that permits discovery of large volumes of data in circumstances where doing so is necessary to identify much smaller amounts of information within that data that directly bears on the matter being investigated".[223]

Dit is dus duidelik dat die interpretasie van relevantheid volgens die FBI baie wyd is. Forsyth kritiseer die regering se wye interpretasie van relevantheid en noem dat dit "creates a perverse incentive to over-collect records because a larger volume of data is more likely to include relevant material".[224] Donohue is eweneens van mening dat die witskrif se interpretasie van "relevantheid" agterstevoor is. Sy sê dat so 'n siening van relevantheid "collapses the statutory distinction between relevant and irrelevant records, thus obviating the government's obligation to discriminate between the two".[225] Dus is beide skrywers van mening dat so 'n interpretasie van relevantheid onsinnig is, omdat relevantheid per definisie juis 'n nouer konsep is wat die net kleiner trek om privaatheid te beskerm en slegs dié inligting wat op die ondersoek betrekking het, uit

221 Bl 2 van die witskrif.

222 Bl 8–9 van die witskrif.

223 Bl 3 van die witskrif.

224 Forsyth 2015 *Washington and Lee Law Review* 1313.

225 Donohue 2014 *Harvard Journal of Law and Public Policy* 838.

te lig. Donohue sê verder dat dit nooit die wetgewer se bedoeling was om *interne* monitering te magtig nie.[226] Daar word aan die hand gedoen dat hierdie siening korrek is — die *Foreign Intelligence Surveillance Act* handel immers oor buitelandse intelligensie — en met selfs 'n oorsigtelike lees van paragraaf 1861(a)(1) is dit duidelik dat die fokus op buitelandse inligting is en "not concerning a United States person".

Die witskrif verduidelik dat die metadata-program aan ondersoek onderhewig is, en dat meerdere FISC-regters toestemming gegee het dat metadata op groot skaal ingewin mag word (en dat dit om daardie rede wettig is).[227] Aangesien die FISC in die geheim sit, is dit nie moontlik om hierdie feit objektief te verifieer nie, maar uit die media is dit duidelik dat FISC-regters wél hierdie program gemagtig het: *Verizon* was die eerste wat aangesê is om metadata aan die NSA beskikbaar te stel,[228] en dit is gevolg deur verskeie ander groot rolspelers.[229]

Hierdie toedrag van sake het vir ten minste van 2006 tot 2015 voortgeduur. In 2013 is die wêreld se intelligensiedienste tot in hul fondament geskud toe Edward Snowden, wat 'n agent vir die Amerikaanse regering was, 'n reeks onthullings gemaak het. Dit het gewissel van dokumente wat blootlê hoe die Duitse kansellier, Angela Merkel, se foon deur die VSA gemoniteer is,[230] tot gruweldade in die oorlog teen Afganistan.[231] In terme van hierdie studie is daar aangetoon hoe die NSA artikel 215 van FISA so wyd interpreteer dat die bevolking van die VSA met die metadata-

226 Donohue 2014 *Harvard Journal of Law and Public Policy* 838.

227 Die witskrif meld: "The program includes internal oversight mechanisms to prevent misuse, as well as external reporting requirements to the FISC and Congress" 2.

228 The Guardian "NSA collecting phone records of millions of *Verizon* customers daily" http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (besoek op 8 Maart 2016).

229 Forsyth 2015 *Washington and Lee Law Review* 1309.

230 Deeks A "An International Legal Framework for Surveillance" 2015 *Virginia Journal of International Law* 291 329.

231 Yuen S "Becoming a Cyber Power: China's cybersecurity upgrade and its consequences" 2015 *China Perspectives* 53 56; The Hill "Spy Chief: Snowden Killed 'Important' Spy Program in Afghanistan" http://thehill.com/policy/national-security/253040-snowden-killed-important-spy-program-in-afghanistan-spy-chief-says (besoek op 9 Maart 2016).

program gemoniteer kon word.[232] Dit het 'n openbare uitroep ontlok, en Amerikaanse burgers het antwoorde gesoek. Forsyth verduidelik hoe daar dadelik ná die Snowden-skandaal begin is om wetgewing te formuleer wat die NSA se metadata-program kon kelder.[233] Dit het gekom in die vorm van die *USA FREEDOM* Act.

6.4.1.5.3 *USA FREEDOM Act*

Dit is verbasend om te dink dat die monitering van miljoene burgers sedert ten minste 2006 in "the land of the free"[234] kon voortduur. Gelukkig het daar as gevolg van geweldige druk op die regering 'n verandering plaasgevind. Omdat die USA-PATRIOT-wet verreikende bepalings bevat wat 'n verskeidenheid beperkings op burgers se vryheid meebring, is dit so geformuleer dat dit outomaties verval (die wet is egter 'n *legio* kere herbevestig, en sekere dele van die USA-PATRIOT-wet is steeds van krag), en die bepalings wat die FISA gewysig het, het verval op 31 Mei 2015. Twee dae later[235] is 'n gewysigde artikel 215 deur die *USA FREEDOM*-wet[236] ingestel, wat bepaal het dat die metadata moniteringsprogram binne 180 dae na inwerkingtreding uitgefaseer moes word, en dat metadata slegs deur die FBI of NSA verkry mag word deur gebruikmaking van 'n hofbevel.[237]

---

232 Die oorspronklike artikel wat die VSA metadata-program ontbloot, is hier te vind: The Guardian "NSA Collecting Phone Records of Millions of *Verizon* Customers Daily" http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (besoek op 9 Maart 2016).

233 Forsyth 2015 *Washington and Lee Law Review* 1308.

234 Hierdie term kom in die laaste frase van elkeen van die vier verse van die *Star Spangled Banner,* wat die Amerikaanse volkslied is, voor. Wikipedia "The Star-Spangled Banner" https://en.wikipedia.org/wiki/The_Star-Spangled_Banner (besoek op 9 Maart 2016).

235 Die *USA FREEDOM Act* het op 2 Junie 2015 in werking getree.

236 H.R.2048 — *USA FREEDOM Act* van 2015.

237 Hierdie is 'n hoogs vereenvoudigde stelling om die inhoud van die *USA FREEDOM Act* te verduidelik. Dit is 'n ingewikkelde stuk wetgewing wat tot intense debat aanleiding gegee het voordat dit aanvaar is (Forsyth 2015 *Washington and Lee Law Review* 1336). Die doel was altyd om die metadata-program te kelder, maar in dieselfde asem moes dit nie die owerhede lam lê om hulle werk te kan doen nie. Die kompromis was die skepping van 'n sogenaamde *specific selection term*, wat meebring dat slegs metadata wat aan die *specific selection term* voldoen, ingewin mag word. Forsyth stel dit so op 1339: "The SST is, therefore, not intended to put a cap on the total amount of records, but instead, to limit the number of records to the greatest extent possible". Forsyth 2015 *Washington and Lee Law Review*

Dus, die reg aangaande die versameling van metadata op groot skaal van Amerikaanse burgers het in 2015 verander. Tussen ten minste 2006 en 2015 was sulke data vryelik deur die NSA vergader, maar sedert die inwerkingtreding van die *USA FREEDOM Act* is die program getemper.[238]

6.4.1.5.4 Artikel 702 van FISA

Artikel 702 van FISA[239] is op die wetboek geplaas om die VSA intelligensie-dienste in staat te stel om buitelandse intelligensie te verkry.[240] Die artikel bepaal:

> Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.[241]

Die artikel is redelik duidelik: die Prokureur-generaal en die direkteur van Nasionale Intelligensie is by magte om te beveel dat 'n persoon wat hom buite die VSA bevind, vir 'n periode van tot een jaar ondersoek mag word.[242]

Subartikel (b) maak dit duidelik dat die teiken 'n nie-VSA burger moet wees. Dit bepaal vyf beperkings wat op subartikel (a) (hierbo) geplaas word:[243]

1338. 'n *Specific selection term* word dan ook beskryf as "it is a term that specifically identifies a person, account, address, or personal device, or any other specific identifier, that is used to limit, to the greatest extent reasonably practicable, the scope of information sought, consistent with the purpose for the use of a pen register or trap and trace device".

238 Forsyth 2015 *Washington and Lee Law Review* 1321–1334 verduidelik die hele proses wat gevolg is om uiteindelik die *USA FREEDOM*-wet te kon uitvaardig. Interessant genoeg wil dit voorkom dat dit júís Snowden se bekendstellings is wat tot die formulering van hierdie wet aanleiding gegee het. 1322.

239 50 USC § 1881a — Procedures for Targeting Certain Persons Outside the United States other than United States Persons.

240 Margulies P "Defining Foreign Affairs in Section 702 of the FISA Amendments Act: The Virtues and Deficits of Post-Snowden Dialogue on US Surveillance Policy" 2015 *Washington and Lee Law Review* 1283 1287.

241 50 USC § 1881a(a).

242 50 USC § 1881a(a).

243 Colonna L "*PRISM* and the European Union's Data Protection Directive" 2013 *Journal of Information Technology and Privacy Law* 227 236.

(1) die persoon wat geteiken word, moenie homself binne die VSA bevind nie;[244]

(2) 'n persoon wat homself buite die VSA bevind, mag nie geteiken word met die doel om 'n persoon binne die VSA te ondersoek nie;[245]

(3) 'n VSA-persoon[246] wat homself buite die VSA bevind, mag nie onder hierdie bepaling geteiken word nie;[247]

(4) kommunikasie mag nie onderskep word indien dit bekend is dat die sender en *ál* die ontvangers daarvan hulself binne die VSA bevind nie;[248] en

(5) die ondersoek sal gedoen word in ooreenstemming met die vierde amendement[249] van die Amerikaanse grondwet.[250]

Weer eens is dit duidelik vanuit die wetsbepaling dat die doel daarvan is om "nie-VSA persone" te teiken.

---

244 50 USC § 1881a(b)(1).

245 50 USC § 1881a(b)(2).

246 'n "United States person" word beskou as "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section." 50 USC § 1801(i).

247 50 USC § 1881a(b)(3).

248 50 USC § 1881a(b)(4).

249 US Constitution Amendment IV. Die geskiedenis van die vierde amendement van die VSA Grondwet is baie interessant. Meer kan hieroor gelees word in Doney L "NSA Surveillance, Smith and Section 215: Practical Limitations to the Third-Party Doctrine in the Digital Age" 2015 *National Security Law Journal* 462 469.

250 50 USC § 1881a(b)(5). Hierdie is, interessant genoeg, nie so 'n voor-die-hand-liggende bepaling as wat met die eerste oogopslag blyk nie. Artikel 702 maak melding van "VSA persone" én "nie-VSA persone". Dit is duidelik dat VSA persone die beskerming van die vierde amendement geniet, maar dit is nie duidelik of hierdie bepaling geld in die geval van nie-persone nie. Milanovic M "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" 2015 *Harvard International Law Journal* 81 95 beweer dat nie-VSA persone wél geregtig is op die beskerming van die vierde amendement, terwyl Colonna 2013 *Journal of Information Technology and Privacy Law* 240 en Landau 2013 *IEEE Security and Privacy* 58 van mening is dat nie-VSA persone níe geregtig is op die beskerming daarvan nie.

Op die 6de Junie 2013 is daar in die pers aangetoon hoe die Amerikaanse intelligensiedienste 'n program met die naam *PRISM* bedryf.[251] Dit versamel 'n magdom inligting met die samewerking van reuse Internet-diensverskaffers, soos *Microsoft*, *Google*, *Yahoo*, *Facebook*, *PalTalk*, *YouTube*, Skype, *AOL* en *Apple*.[252] Dit word bedryf onder die magtiging van artikel 702, en die doel is om alle *inhoudelike* inligting van buitelanders te versamel.[253] Asof hierdie inligting nie erg genoeg is nie, is daar ook aangetoon dat 'n tweede been van die program daargestel is onder die naam "Upstream", en dat dit ten doel het om direk vanuit die Internet-ruggraat *inhoudelike* inligting van VSA-persone te verkry.[254] Donohue verduidelik:

> It monitors all traffic crossing cables — not just information targeted at specific Internet protocol addresses or telephone numbers. By 2011, the NSA was acquiring around 26.5 million Internet transactions per year through upstream collection.[255]

Die Direkteur van Nasionale Intelligensie, James Clapper, het dadelik die koerantberigte gekritiseer:

> In particular, the surveillance activities published in The Guardian and The Washington Post are *lawful and conducted under authorities widely known and discussed*, and fully debated and authorized by Congress. Their purpose is to obtain foreign intelligence information, including information necessary to thwart terrorist and cyber attacks against the United States and its allies.[256]

---

251 Colonna 2013 *Journal of Information Technology and Privacy Law* 227.

252 Donohue L K "The Dawn of Social Intelligence (SOCINT)" 2015 *Drake Law Review* 1061 1086. Colonna 2013 *Journal of Information Technology and Privacy Law* 227 en 231. Hierdie diensverskaffers is deur FISC-hofbevele gedwing om inligting beskikbaar te stel, en om alles te kroon is hulle onder 'n sogenaamde "gag-order", of nie-bekendmakingsklousule, geplaas waarvolgens hulle nie die bekendmaking van data aan die NSA aan hulle gebruikers kon bekendmaak nie. Balkin J M "Old School/New School Speech Regulation" 2014 *Harvard Law Review* 2296 2331 vn 149.

253 Daar sal onthou word vanuit die vorige afdeling se bespreking van artikel 215 van FISA dat *nie-inhoudelike* metadata-inligting versamel is. Hierteenoor word artikel 702 ingespan om *inhoudelike* data van buitelanders (nie-VSA persone) te vergader.

254 Donohue 2015 *Drake Law Review* 1087. Sy skryf: "The second, 'upstream' collection under Section 702, amounts to collection from the servers of U.S. service providers. It allows the NSA to acquire Internet communications 'as they transit the 'internet backbone' facilities'".

255 Donohue 2015 *Drake Law Review* 1087.

256 My kursivering. Clapper J R "DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" 2013 *Office of the Director of National Intelligence* 1.

Clapper het ook bygevoeg dat die gebruikmaking van artikel 702 was "vital to keeping the nation and our allies safe".[257]

Privaatheidsgroepe was nie beïndruk nie, en het gemeen dat die trefwydte van artikel 702 te wyd was, en dat bykans enige persoon geteiken kon word, wat die onderskeid tussen grootmaat-inligtingsinwinning en geteikende inligting laat vervaag.[258] Dit het tot 'n hofgeding aanleiding gegee wat uiteindelik in die hooggeregshof van Amerika 'n draai gaan maak het. In *Clapper v Amnesty International*[259] het die respondent, wat 'n groot organisasie sonder winsbejag en 'n kampvegter vir menseregte is, die direkteur van Nasionale Intelligensie gedagvaar oor die verreikende gevolge wat artikel 702 inhou. Die respondent het aangevoer dat sy werknemers, wat kwalifiseer as "VSA persone", gedurig met mense kommunikeer wat as "nie-VSA persone" beskou word, en wat dus onder artikel 702 ondersoek kan word.[260] Hierdie internasionale kommunikasie is van 'n sensitiewe aard, aldus die respondent.[261] Gevolglik het die respondent gevra dat die bepalings van artikel 702 van FISA (wat as § 1881a USC gekodifiseer is) onkonstitusioneel verklaar moet word.[262]

Die respondente het tydens die hofaansoek nog geen bewys gehad dat daar inderdaad op hulle internasionale kommunikasies inbreuk gemaak is nie, maar het aangevoer dat hulle "can establish injury in fact because there is an objectively reasonable likelihood that their communications will be acquired under § 1881a at some point in the future".[263] Die hof het egter bevind dat hierdie toekomstige nadeel te spekulatief is, en dat dit nie voldoen aan die vereiste van "certainly impending" wat in die Amerikaanse reg geld nie.[264] Selfs as daar veronderstel word dat die respondent se nadeel

257 Clapper 2013 *Office of the Director of National Intelligence* 1.

258 Margulies 2015 *Washington and Lee Law Review* 1294.

259 133 S Ct 1138 — Supreme Court 2013.

260 *Clapper v Amnesty International* 1142.

261 *Clapper v Amnesty International* 1142.

262 *Clapper v Amnesty International* 1142.

263 *Clapper v Amnesty International* 1143.

264 Op 1143 vind die hof dat: "respondents' theory of future injury is too speculative to satisfy the

"certainly impending" is, kan daar nie aangetoon word dat die nadeel toe te skryf is aan artikel 702 (§ 1881) nie.[265] Gevolglik is die saak van die hand gewys, aangesien die respondent nie *locus standi* het nie.[266]

Met hierdie bevinding het die hof dit vaardig reggekry om die werklike aangeleentheid onbeantwoord te laat, wat 'n jammerte is.[267]

Colonna verduidelik vanuit 'n Europese perspektief dat *PRISM* 'n fundamentele probleem vir nie-VSA persone skep omdat 'n magdom van hulle inligting in die VSA 'n draai maak.[268] Webdienste soos *Facebook* en *Google* produkte soos Gmail word deur die VSA geroeteer ten spyte daarvan dat die versender of ontvanger nie in die VSA teenwoordig is nie.[269] Colonna maak die geldige punt dat: "the U.S. government is able to engage in 'extra-territorial surveillance from domestic soil'".[270]

Die algemene publiek was net so ontevrede met hierdie uitlatings as wat hierbo onder artikel 215 van FISA bespreek is. President Obama het in Januarie 2014 in 'n toespraak gesê dat persone regoor die wêreld 'n belang in hul eie privaatheid het, en onderneem om die net van inligtingsinwinning te vernou.[271] Die USA FREEDOM-wet is gewysig om die vyf beperkings hierbo genoem, in te sluit.[272] Wanneer die inligting wat volgens artikel 702 ingewin is, ondersoek word, mag dit net gedoen word deur van sekere gemagtigde "search terms" gebruik te maak.[273] Indien ingewinde inligting in

well-established requirement that threatened injury must be 'certainly impending'. ... And even if respondents could demonstrate that the threatened injury is certainly impending, they still would not be able to establish that this injury is fairly traceable to § 1881a".

265 *Clapper v Amnesty International* 1143.

266 *Clapper v Amnesty International* 1143.

267 Met hierdie stelling word daar nie beweer dat die hof gefouteer het nie, want op 'n bloot tegniese punt het die hof tot 'n korrekte beslissing gekom. Die nadeel waarvan die respondent melding gemaak is, is inderdaad verwyder van werklike nadeel. Tog is dit 'n jammerte dat die hoogste hof in die VSA nie die geleentheid gekry het om die werklike aangeleentheid van artikel 702 onder die loep te kon neem nie.

268 Colonna 2013 *Journal of Information Technology and Privacy Law* 228.

269 Colonna 2013 *Journal of Information Technology and Privacy Law* 238.

270 Colonna 2013 *Journal of Information Technology and Privacy Law* 228.

271 Margulies 2015 *Washington and Lee Law Review* 1289–1290.

272 Ombres D "NSA Domestic Surveillance From the PATRIOT Act to the FREEDOM Act: The Underlying History, Constitutional Basis, and the Efforts at Reform" 2015 *Seton Hall Legislative Journal* 27 43.

273 Margulies 2015 *Washington and Lee Law Review* 1291. Die gebruikmaking van "search terms" word

'n geregshof of administratiewe proses gebruik wil word, moet die persoon *vooraf* daarvan verwittig word[274]

Die proses wat gevolg moet word om op artikel 702 te steun, is soos volg: Die intelligensie-owerheid rig 'n aansoek aan die FISC wat die teikenprosedure sowel as die "minimization procedures" uiteensit.[275] Die FISC sal dit dan *ex parte* oorweeg, wat beteken dat geen eksterne bronne of mosie geraadpleeg hoef te word nie, en sal dan die aansoek óf toestaan óf afwys.[276]

Litt wys daarop dat inligting wat volgens artikel 702 ingewin is, "oor die algemeen" binne vyf jaar vernietig word tensy daar gelykwaardige inligting van 'n VSA persoon behou kan word.[277] Skynbaar is die retensie van nie-VSA persone gekoppel aan dié van VSA persone, alhoewel die regverdiging daarvoor onduidelik is, en nie deur die outeur verduidelik word nie.[278]

6.4.1.5.5 *Foreign Intelligence Surveillance Court*

Daar is reeds hierbo heelwat geskryf oor die en watter rol hul speel in die Intelligensiegemeenskap — en veral ten opsigte van FISA (wat die FISC in die lewe geroep het). Die FISC is 'n hof wat in die geheim sit omdat die sake wat hulle aanhoor, van nasionale intelligensie kom, en dit is uiteraard alles geklassifiseer. Meeste van die FISC besluite beland in die openbare domein nadat dit uitlek in die media. Die beste voorbeeld hiervan is die Verizon-beslissing wat elders bespreek is. Die vraag wat onwillekeurig

gerieflikheidshalwe gedoen "wherever practicable", wat lyk asof dit bloot gedoen word om teenkanters van die wetgewing se monde te snoer. Margulies 2015 *Washington and Lee Law Review* 1291; Litt R S "US Intelligence Community Surveillance One Year After President Obama's Address" 2015 *National Security Law Journal* 210 224 beskryf die soekkriteria as "identifiers".

274 Deeks 2015 *Virginia Journal of International Law* 346.

275 Margulies 2015 *Washington and Lee Law Review* 1288. wys daarop dat die data wat ingewin wil word, moet slaan op nasionale sekuriteit, soos 'n werklike of potensiële aanval, asook ernstige vyandige optrede van 'n ander moondheid of agent daarvan.

276 Margulies 2015 *Washington and Lee Law Review* 1288.

277 Litt 2015 *National Security Law Journal* 228.

278 Die skrywer, Robert Litt, word beskryf as die "Second General Counsel of the Office of the Director of National Intelligence". Litt 2015 *National Security Law Journal* 210.

opduik wanneer die omvangryke bepalings van artikels 215 en 702 van FISA beoordeel word, asook die vrye teuels wat in die verlede aan die NSA en FBI gegee is, is dit vreemd dat die FISC, wat 'n uitvoerige waghond-funksie het, nie meer gedoen het om die intelligensiediens aan bande te lê nie.

Donohue verskaf antwoorde op hierdie vraag.[279] In 'n breedvoerige bespreking oor die samestelling en werking van die FISC verduidelik sy hoe die FISC agteroor gebuig het om die NSA tegemoet te kom ten spyte daarvan dat hulle die FISC se uitdruklike bevele verontagsaam het deur nie gebruik te maak van die kriteria wat dit neergelê het vir die deursoeking van die metadata wat verkry is nie.[280] Dit is ongehoord dat die metadata-program nie deur die FISC gekelder is nie, aangesien die NSA by meerdere male die FISC totaal geïgnoreer het.[281]

Ruger[282] suggereer dat die FISC dalk nie so onpartydig is as waarvoor dit geskep is nie wanneer hy sê dat dié hof "a government success rate unparalleled in any other American court" het.[283] Die feite spreek vanself: sedert die hof se bestaan van 1978 tot 1999 het die hof bykans 12000 ondersoek-lasbriewe toegestaan en *geen* geweier nie.[284] Slegs een keer sedert daardie tyd (tot met die skrywe van die artikel in 2007) het die FISC 'n ondersoek-lasbrief geweier, en daardie aangeleentheid is op hersiening deur die FISC-hersieningshof ten gunste van die regering beslis.[285] Omdat die regering die enigste party is wat 'n saak op hersiening kan neem, is die

279 Donohue 2014 *Harvard Journal of Law and Public Policy* 817–836.

280 Die FISC het bepaal dat alvorens die NSA die metadata-databasis mag deursoek, hulle eers 'n aansoek aan 'n geselekteerde groep hoëvlak-amptenare by die NSA moet rig wat uitwys dat die voorgenome soektog "reasonable, articulable suspicion" bevat. Dit is verkort na die akroniem RAS-kriteria. Slegs as die betrokke amptenare bevind het dat daar aan die RAS-kriteria voldoen word, mag die metadata-databasis deursoek word. Donohue 2014 *Harvard Journal of Law and Public Policy* toon op 812 aan dat bykans 90% van soektogte in die metadata-databasis nie aan die RAS-kriteria voldoen het nie.

281 Donohue 2014 *Harvard Journal of Law and Public Policy* 813–816.

282 Ruger T W "Chief Justice Rehnquist's Appointments to the FISA Court: An Empirical Perspective" 2007 *Northwestern University Law Review* 239 239.

283 Ruger 2007 *Northwestern University Law Review* 245.

284 Ruger 2007 *Northwestern University Law Review* 245.

285 Ruger 2007 *Northwestern University Law Review* 245.

proses — aldus Ruger — ernstig skeefgetrek in die guns van die regering.[286]

Dit wil dus voorkom asof die oorsigfunksie wat die FISC het, geensins na wense funksioneer nie.

6.4.1.5.6 Effektiwiteit

Ter afsluiting van hierdie deel van die studie kan daar gevra word of die omvattende stappe wat deur artikel 215 en 702 gemagtig word, die gewenste uitwerking gehad het? Volgens die Amerikaanse direkteur van Nasionale Intelligensie, Keith Alexander, is die antwoord bevestigend. Hy het voor die "Senate Approriations Committee" getuig dat die *PRISM* en Upstream-programme "helped prevent more than 50 terrorist attacks in over 20 countries".[287] Senator Patrick Leahy het hierdie uitlatings bevraagteken nadat hy die lys ondersoek het wat Alexander aan hom verskaf het. Leahy het bevind dat "it simply does not reflect dozens or even several terrorist plots that Section 215 helped thwart or prevent, let alone 54, as some have suggested".[288]

Die *Privacy and Civil Liberties Oversight Board* het soortgelyke bevin-

---

286 Ruger 2007 *Northwestern University Law Review* 245.

287 Donohue 2015 *Drake Law Review* 1099; The Guardian "NSA Chief Says Exposure of Surveillance Programs Has 'Irreversible' Impact" http://www.theguardian.com/world/2013/jun/18/nsa-chief-house-hearing-surveillance-live (besoek op 11 Maart 2016); The Guardian "NSA Chief Claims 'Focused' Surveillance Disrupted More Than 50 Terror Plots" http://www.theguardian.com/world/2013/jun/18/nsa-surveillance-limited-focused-hearing (besoek op 11 Maart 2016).

288 Die volledige teks van hierdie verklaring van Senator Leahy skets 'n beter prentjie van wat hy eintlik gesê het, en word vervolgens gegee:

> ...but I asked General Alexander about the effectiveness of the Section 215 phone records program in an Appropriations Committee hearing last month. He agreed to provide a classified list of terrorist events that Section 215 helped to prevent, and I've reviewed that list. Although I agree that it speaks to the value of the overseas content collection implemented in Section 702, it does not do the same for Section 215; it simply does not reflect dozens or even several terrorist plots that Section 215 helped thwart or prevent, let alone 54, as some have suggested.
>
> And these facts matter. This bulk collection program has massive privacy implications. ... just because we have the ability to collect huge amounts of data does not mean that we should be doing so.

IC on the Record "Hearing of the Senate Judiciary Committee on Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs" http://icontherecord.tumblr.com/post/57811913209/hearing-of-the-senate-judiciary-committee-on (besoek op 11 Maart 2016).

dings gemaak. In ’n 238-bladsy verslag oor die spioenasieprogram wat ingevolge artikel 215 van die PATRIOT-wet plaasgevind het, het dié raad bepaal dat die metadata-program nie die verlangde uitwerking gehad het nie:

> We have concluded, based on the evidence provided by the government, that the NSA’s Section 215 program has not proven useful in identifying unknown terrorists or terrorist plots, in part because the program often merely corroborates information about connections among individuals that have already been obtained independently through other means. Yet we also conclude that telephone calling records, if used in more expansive ways than the government currently employs them, can reveal a great deal about an innocent person’s habits, private affairs, and network of social, familial, and professional connections. This capability is magnified when calling records are aggregated across customers and carriers and over a long period of time. The very power that inheres in the analysis of telephone calling records — a power that the government has emphasized in defending the intelligence value of the NSA’s Section 215 program — illustrates the depth of the privacy implications entailed by the program without proving its effectiveness as a counterterrorism tool.[289]

Daar is meerdere studies wat aantoon dat grootmaat-inligtingversameling soos die metadata-program van artikel 215 en 702 van FISA nie regtig suksesvol is nie. Die *New America Foundation* het byvoorbeeld 225 persone wat deur *Al Qaeda* gewerf is en uiteindelik deur die Amerikaanse owerhede van terrorisme aangekla is, geneem en bepaal hoe hulle geïdentifiseer en aangekeer is, en daardie data verder analiseer.[290] Daar is bevind dat met die oorgrote meerderheid van gevalle die persone met tradisionele ondersoekmetodes, soos die gebruikmaking van informante, die plaaslike gemeenskap en geteikende intelligensie-inwinning, aangekeer is.[291] Slegs in 1.8 persent van die gevalle wil dit voorkom asof metadata-analise ’n bydrae gelewer het.[292]

---

289 Privacy and Civil Liberties Oversight Board *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* (2014) 158.

290 Bergen P, Sterman *et al* “Do NSA’s Bulk Surveillance Programs Stop Terrorists?” 2014 *New America Foundation* 1 1.

291 Bergen *et al* 2014 *New America Foundation* 1.

292 Bergen *et al* 2014 *New America Foundation* 2.

Dit wil dus voorkom asof die programme wat ingevolge artikels 215 en 702 van FISA vir etlike jare (en huidig nog) bedryf word, nie die gewenste uitwerking het nie ten spyte daarvan dat dit erge privaatheidskendings meebring. Die enigste partye wat op die effektiwiteit van die spioenasieprogramme aandring, is die NSA en FBI.

6.4.1.6 Samevatting

As skepper van die Internet was die VSA die eerste staat wat met die regulering daarvan moes worstel.[293] Verskeie wette, soos die *Communications Decency Act,*[294] die *Digital Millennium Copyright Act,*[295] en die *Lanham Act*[296] is uitgevaardig om hierdie oogmerk te bewerkstellig.

Artikel 230 van die CDA beskerm ISP's teen eise deur te bepaal dat hulle nie as publiseerders van inligting wat op hulle bedieners te vinde is, beskou sal word nie.[297] Hierdie artikel blyk baie effektief te gewees het, aangesien twee-derdes van alle hofsake tussen 1996 en 2010 teen ISP's in hulle guns beslis is.[298]

Paragraaf 512 van die DMCA is 'n baie meer omvattende stuk wetgewing as die CDA, en dit is in meer besonderhede bespreek.[299] Hier word verskillende ISP's in vier kategorieë verdeel, en aanspreeklikheid volg na aanleiding van die tipe diens wat hulle verskaf.[300] Die vier kategorieë is:

- ISP as geleidingsbuis;[301]
- ISP wat inligting in kasgeheue berg;[302]

293 Afd 6.4.1.1.

294 47 USC § 230 (2006).

295 17 USC § 512 (2012).

296 15 USC § 1114(2)(B) en (C) (2006).

297 Afd 6.4.1.2.

298 Afd 6.4.1.2, veral Ardia se navorsing. Sien vn 124.

299 Afd 6.4.1.3.

300 Afd 6.4.1.3.

301 Afd 6.4.1.3.1.

302 Afd 6.4.1.3.2.

- ISP's wat inligting van die gebruiker stoor, en nie bewus is daarvan dat sulke kopieregskendende materiaal op hulle bedieners te vinde is nie, sal nie vir kopieregskending aanspreeklik wees nie,[303] en

- Inligtingsopsporingsgereedskap.[304]

Dit is belangrik om daarop te let dat die DMCA slegs van toepassing is op gevalle van kopieregskending.

Ter volledigheid is die *Lanham*-wet ook bespreek, en dit hanteer nie-aanspreeklikheid van ISP's in gevalle van handelsmerkskending.[305] Hierdie wet benodig ernstige opdatering, aangesien dit 'n 1946-wet is wat bloot vir die digitale-era aangepas is, maar nie die Internet sinvol aanspreek nie.[306]

Daar is in hierdie afdeling aangetoon dat regulering van ISP's slegs die helfte van die reguleringsprentjie in die VSA skets. Die ander helfte bestaan uit sekuriteitswetgewing wat oor die laaste halfeeu deur die VSA uitgevaardig is. In hierdie konteks is veral die *Foreign Intelligence Surveillance Act,* die *PATRIOT-Act* en die *USA FREEDOM Act* van belang.[307]

Daar is aangetoon hoe die FISA omvorm is van 'n wet wat poog om die VSA-intelligensiediens te reguleer, tot 'n drakoniese wet wat ingrypend op die vryhede van beide VSA-burgers en internasionale persone inbreuk maak.[308] Die metadata-program wat enorme hoeveelhede data van algemene Amerikaanse burgers, asook nie-VSA-persone bymekaar maak, is veral kommerwekkend.[309]

In 'n poging om hierdie wetgewing reg te stel, is die *USA-Freedom Act* gepromulgeer.[310] Dit het die metadata-program gekelder, en die

303 Afd 6.4.1.3.3.

304 Afd 6.4.1.3.4.

305 Afd 6.4.1.4.

306 Afd 6.4.1.4, veral die laaste gedeelte daarvan waar Powell se aanbevole wetswysigings bespreek word — sien vn 187.

307 Afd 6.4.1.5.

308 Afd 6.4.1.5.1.

309 Afd 6.4.1.5.2.

310 Afd 6.4.1.5.3.

onderskepping van VSA-burgers én nie-VSA-persone op ’n meer gesonde voet geplaas.[311]

Die *Foreign Intelligence Surveillance Court* en die effektiwiteit daarvan is ook bespreek.[312] Daar is aangetoon hoe die FISC as waghond vir die VSA se intelligensiedienste moes dien, maar hoe hierdie rol grootliks onvervuld gebly het.

Die bespreking in hierdie afdeling het ’n baie interessante faset van die VSA se beleid oor Internetregulering openbaar. Die Internet het in die VSA ontstaan, en die grootste ruggraatnetwerke is steeds in die VSA te vinde. Dit is daarom nie vreemd nie, dat bykans die hele wêreld se kommunikasie deur Amerikaanse netwerke vloei. Dit het ’n interessante geleentheid geskep om onderskepping op ’n vlak mee te bring wat nog nooit vantevore bestaan het nie. Deur die Internet “oop” te hou — soos wat die VSA wil hê — word daardie onderskeppingsgeleentheid bevorder en versterk. As dit nie was vir die Snowden-spioenasieskandaal nie, sou hierdie “voordeel” wat die VSA geniet het, waarskynlik nie aan die lig gekom het nie. Die uiteindelike gevolgtrekking is dus dat ’n “oop” Internet ’n strategiese voordeel vir die VSA inhou, en dat die VSA ’n voortsetting van die *status quo* sal voorstaan.[313]

Daar word nou wegbeweeg van die VSA se reguleringsisteem na dié van Sjina, wat vervolgens bespreek word.

311 Afd 6.4.1.5.4.

312 Afd 6.4.1.5.5.

313 Hierdie tendens word bevestig in die houding wat die VSA inslaan teenoor ICANN en beheer oor die basis-DNS. Laasgenoemde is steeds binne die beheer van die VSA. Afd 2.3.4, afd 3.4.1 en afd 5.4.1.

6.4.2 Die Volksrepubliek van Sjina

6.4.2.1 Inleiding

Die Volksrepubliek van Sjina (hierna Sjina) is die digsbevolkte land in die wêreld, met bykans 1.4 miljard[314] mense.[315] Alhoewel daar na bewering 298 tale in Sjina gepraat word,[316] is eenvoudige Sjinees by verre die taal wat die meeste in gebruik is.[317] Die Sjinese bevolking is trots op hulle taal, en daarom is dit nie vreemd dat meer as 'n driekwart van die hele Sjinese bevolking nie Engels magtig is nie.[318] Hierdie feit is krities om in ag te neem wanneer die regulering van die Internet in Sjina bespreek word. Die taal- en alfabetverskille wat daar tussen Oosterlinge en Westerlinge is, het dit baie makliker gemaak om die Sjinese intranet van die groter Internet af te skei. Tsui wys byvoorbeeld daarop dat die oorgrote meerderheid van Sjinese die Internet in hul eie taal lees, wat beteken dat enige webblad wat nie Sjinees is nie, vir hulle ontoeganklik is.[319]

Voordat die regulering van die Internet in Sjina beoordeel word, is dit raadsaam om vlugtig te wys dat die Sjinese bevolking tans die grootste Internetgebruiker in die wêreld is. Die land is in 1994 aan die

---

314 In Afrikaans word miljard en biljoen maklik met mekaar verwar, aangesien die woord "billion" in Engels algemeen gebruik word om eenduisend miljoen aan te dui. Maroela Media "Taaltoffie: Miljarde, Biljoene, en Triljoene" http://maroelamedia.co.za/afrikaans/taaltoffie/taaltoffie-miljarde-biljoene-en-triljoene/ (besoek op 15 Maart 2016).

315 Wikipedia "List of Countries and Dependencies by Population" https://en.wikipedia.org/wiki/List_of_countries_and_dependencies_by_population (besoek op 15 Maart 2016); National Bureau of Statistics in China "National Data" http://data.stats.gov.cn/english/ (besoek op 15 Maart 2016);

316 Ethnologue "China" http://www.ethnologue.com/country/CN (besoek op 15 Maart 2016). Volgens dié statistiek is 274 tale inheems en 24 is uitheems.

317 Lidi W "The Spread of English in China and its Implications" 2011 *Australian Review of Applied Linguistics* 32.1 32.2; Wikipedia "Standard Chinese" https://en.wikipedia.org/wiki/Standard_Chinese (besoek op 15 Maart 2016).

318 Wei R en Su J "The Statistics of English in China" 2012 *English Today* 10 12. Hulle noem dat "...21% reported possession of a spoken competence in English which allowed them to sustain a conversation beyond initial greetings...". Lidi 2011 *Australian Review of Applied Linguistics* 32.1.: "It is estimated that the number of learners of English in China exceeds 300 million, which takes up about a quarter of the country's 1.3 billion people".

319 Tsui L "The Panopticon as the Antithesis of a Space of Freedom: Control and Regulation of the Internet in China" 2003 *China Information* 65 72.

Internet gekoppel, en teen 2000 was daar reeds 22 miljoen gebruikers.[320] Hierna het Internetgroei in Sjina geweldig uitgebrei: teen 2005 was daar reeds 111 miljoen Internetgebruikers, en teen 2011 het Internetgebruik op 485 miljoen gebruikers gestaan.[321] Die mees onlangse syfers van 2015 wys dat daar nou reeds 668 miljoen Internetgebruikers in Sjina is,[322] en dat die meeste van hierdie persone die Internet uitsluitlik vir vermaak gebruik.[323]

Sjina word sedert 1949[324] deur die kommunistiese Party van Sjina regeer.[325] Die party is daarvoor bekend om nie enige vorm van politieke teëstand te duld nie, en die bekendste voorbeeld hiervan is sekerlik die 1989 studente-optogte wat in 'n bloedbad op Tiananmen-plein geëindig het.[326]

Internetregulering in Sjina kan volgens Yang in drie stadiums verdeel word: die eerste is van 1994 tot 1999, en dit is gekenmerk deur die skepping van administratiewe- en regsraamwerke om sekuriteitsaangeleenthede op die Internet te skep.[327] Dit behels maar eintlik die skepping van regulasies en sisteme om Internetregulering moontlik te maak, en etlike van hierdie regulasies sal binnekort bespreek word.[328] Die tweede stadium van Internetregulering is van 2000 tot 2002, en dit behels die fisiese regulering van Internet-diensverskaffers en gebruikers.[329] In hierdie fase word persone se *gebruik* van die groter Internet beperk, en ontoelaatbare gedrag word

320 Hua J J "Establishing Certainty of Internet Service Provider Liability and Safe Harbor Regulation" 2014 *National Taiwan University Law Review* 1 5.

321 Hua 2014 *National Taiwan University Law Review* 5.

322 Cui D en Wu F "Moral Goodness and Social Orderliness: An Analysis of the Official Media Discourse about Internet Governance in China" 2015 *Telecommunications Policy* 265 265.

323 Kuo K *TEDxHonolulu Technology, Entertainment and Design Conference* 5 November 2009. Die voorlegging is beskikbaar by *YouTube* "TEDxHonolulu — Kaiser Kuo — 11/05/09" https://www.*YouTube*.com/watch?v=M-jqGmc6xKI (besoek op 15 Maart 2016). Kuo noem dat die meeste Sjinese die Internet gebruik as die "entertainment superhighway". Sien ook Sivan Y (red) "Escaping the World: A Chinese Perspective on Virtual Worlds" 2012 *Journal of Virtual Worlds Research* 1 6 en Inkster N "China in Cyberspace" 2010 *Survival* 55 fig 1 57 wat dieselfde tendens bevestig.

324 Ebrey P B *The Cambridge Illustrated History of China* (2010) 321.

325 'n Volledige bespreking van hoe die Kommunistiese Party in Sjina aan bewind gekom het, is te vinde in Ebrey *The Cambridge Illustrated History of China* 286.

326 Ebrey *The Cambridge Illustrated History of China* 342.

327 Yang G *The Power of the Internet in China: Citizen Activism Online* (2013) 47–51.

328 Afd 6.4.2.2.1.

329 Yang *The Power of the Internet in China* 47–51.

gestraf.[330] Die derde stadium van Internetregulering het volgens Yang in 2003 begin, toe die regering die land se Internetbeheer versterk en uitgebrei het.[331]

'n Seleksie van regulasies sal vervolgens bespreek word. Let egter daarop dat aangesien Sjina nie 'n demokrasie is nie, is die status van wetgewing heel anders as in die weste. Die Kongres van die "People's Republic of China" maak belangrike landswette, maar die oorgrote meerderheid van wetgewing is in die vorm van regulasies wat deur ander staatsorgane uitgevaardig word.[332] Hierdie regulasies lyk glad nie soos wetgewing nie, maar vertoon eerder die eienskappe van 'n memorandum wat sekere beginsels stapsgewys uiteensit.

Die eerste fase van Internetregulering het begin met 'n verskeidenheid

330 Afd 6.4.2.2.2.

331 Yang *The Power of the Internet in China* 47–51.

332 Sien Guan S Y *China's Telecommunications Reforms: From Monopoly Towards Competition* (2003) 70 vir meer inligting oor die proses waardeur wetgewing gaan om uiteindelik aanvaar te word. Die kern van hierdie proses word egter goed opgesom: "Most parts of this legislative process are kept confidential". Sien ook Zhao J *Corporate Social Responsibility in Contemporary China* (2014) 130 waar daar gesê word dat "... the legislative process in China is not transparant".

regulasies[333] wat voor die draai van die eeu uitgevaardig is om die basis van Internetregulering daar te stel.[334] Die *Temporary Regulation for the Management of Computer Information Network International Connection*, (hierna MCI)[335] het die basis gelê vir regulering, die *Measures for Security Protection Administration of the International Networking of Computer Information Networks* (hierna PINN)[336] het dit verstewig, en die *Security Management Procedures in Internet Accessing* (hierna SMP)[337] het die eerste fase van regulering afgesluit toe dit in 1997 uitgevaardig is. Dit word vervolgens bespreek.

---

333 Voorbeelde hiervan is:

- 1994: Ordinance of the People's Republic of China on the Protection of Computer Information System Security
- 1994: Rules of Security Protection of Computer Information Systems
- 1996: Temporary Regulation for the Management of Computer Information Network International Connection
- 1997: Security Management Procedures in Internet Accessing
- 1997: Computer Information Network and Internet Security, Protection and Management Regulations
- 2000: State Council Order No. 292, "Measures on Internet Information Services"
- 2000: Administration of the Maintenance of Secrets in the International Networking of Computer Information Systems Provisions
- 2000: Administration of Engagement by Internet Sites in the Business of News Publication Tentative Provisions

Saamgestel uit Rust S, Monani S en Cubitt S *Ecomedia: Key Issues* (2015) 216; Sohmen P "Taming the Dragon: China's Efforts to Regulate the Internet" 2001 *Stanford Journal of East Asian Affairs* 17 19; Chueng A S Y en Zhao Y "An Overview of Internet Regulation in China" 2013 *University of Hong Kong Faculty of Law Research Paper* 1 3 en Liang B en Lu H "Internet Development, Censorship, and Cyber Crimes in China" 2010 *Journal of Contemporary Criminal Justice* 103 108.

334 Let daarop dat ál die wetgewing wat onder hierdie afdeling bespreek word, die Engelse weergawe van die Sjinese teks gebruik. Daar is egter gepoog om by elke regulasie die mees akkurate weergawe van die teks op te spoor.

335 Qiu J L "Virtual Censorship in China: Keeping the Gate Between the Cyberspaces" 2000 *International Journal of Communications Law and Policy* 1 10 en Kissel 2007 *Indiana International and Comparative Law Review* 234.

336 World Intellectual Property Organization "Measures for Security Protection Administration of the International Networking of Computer Information Networks" http://www.wipo.int/edocs/lexdocs/laws/en/cn/cn115en.pdf (besoek op 15 Maart 2016).

337 Qiu 2000 *International Journal of Communications Law and Policy* 11. Rust, Monani en Cubitt *Ecomedia: Key Issues* 216.

6.4.2.2 Eerste-fase Regulering

6.4.2.2.1 *Temporary Regulation for the Management of Computer Information Network International Connection (MCI)*

Die MCI is in Januarie 1996 reeds uitgevaardig, en het die basis vir Internetregulering neergelê.[338] Artikel 1 het dit duidelik gemaak dat die doel daarvan is "strengthening the control on the computer information networks connecting to the international network"[339] Dit is noodsaaklik om daarop te let dat by ál die regulasies wat bespreek word, verwys die Engelse teks na die Internet as die "international network". Sjinese regulasies onderskei dus reeds vanuit die staanspoor tussen die plaaslike netwerk, en die internasionale netwerk,. Die plaaslike netwerk verwys na 'n Sjinese *intranet*, wat dit afskei van die groter Internet en wat beperk word deur tegnologiese hekpoorte (of in Engels gateways). In die bespreking wat hieronder volg, sal daar dikwels na die Sjinese Internet as 'n *intranet* verwys word ten einde dit van die groter Internet te onderskei.

Artikel 2 van die regulasie stipuleer dat *elke netwerk* wat binne Sjina is, aan hierdie vereistes moet voldoen.

Dit is die taak van die regering om alle beplanning, standaarde, en ontwikkeling van die "international connection" te behartig.[340] Geen privaat skakeling met die groter Internet word toegelaat nie, maar slegs die gemagtigde openbare telekommunikasienetwerk mag gebruik word.[341] Alle toegangspunte na die internasionale netwerk word aktief beheer.[342]

---

338 Qiu 2000 *International Journal of Communications Law and Policy* 10.

339 MCI art 1. Die teks van die Engelse weergawe is beskikbaar by: Laws of the People's Republic of China "Interim Provisions Governing the Management of Computer Information Network International Connection" http://www.asianlii.org/cn/legis/cen/laws/ipgtmotcinitproccttin1488/ (besoek op 15 Maart 2016). International Business Publications *China Telecom Industry Business Opportunities Handbook Volume 3 Strategic Information, Developments, Regulations* (2007) 146–151.

340 Art 4.

341 Art 6, 8 en 10.

342 Art 7 bepaal dat vier entiteite in beheer van die toegangspunte na die groter Internet sal wees, naamlik die ministerie van pos- en Telekommunikasiewese; die ministerie van Elektriese Industrie; die Staatskommissie en die Sjinese Wetenskapsakademie.

In artikels 9 en 10 word Internet-diensverskaffers gemagtig om aan die Sjinese intranet te skakel.[343] Enige persoon wat aan die groter Internet wil skakel, móét dit deur 'n ISP doen.[344] ISP's is verantwoordelik vir die opleiding van gebruikers, met ander woorde hoe om die "internasionale netwerk" op 'n gepaste wyse te gebruik.[345] Artikel 13 meld uitdruklik dat geen persoon die skakeling met die groter Internet mag gebruik om die regering op enige manier te benadeel nie.[346] Indien 'n persoon hierdie reëls verontagsaam, kan hy met 'n bedrag van tot 15 000 Yuan gevonnis word.[347]

Die volledige regulasie bevat slegs 17 artikels, maar met hierdie kort dokument is daar vroeg reeds 'n ystergreep op Sjina se stukkie Internet gekry.

6.4.2.2.2 *Measures for Security Protection Administration of the International Networking of Computer Information Networks*

Die PINN is in Desember 1997 gepromulgeer, en bevat 'n verskeidenheid artikels wat die regering se greep op die Sjinese intranet verstewig.[348] Verskeie artikels herhaal (en bevestig) die MCI, wat direk hierbo bespreek is.[349]

---

343 Om as ISP toegelaat te word, moet dit volgens art 9: (a) 'n regspersoon wees; (b) 'n rekenaarnetwerk besit wat onderhou word deur tegnici en bestuurspersoneel; (c) 'n volledige "confidential management system" in plek hê, en (d) enige ander vereistes wat deur die staat bepaal mag word. Wat bedoel word met 'n "confidential management system" word nie verder in die regulasie uiteengesit nie.

344 Art 10.

345 Art 12.

346 Die Engelse teks maak melding dat 'n persoon "shall not take advantage of the international connection to conduct criminal acts such as endangering the safety of the state [and], leaking state secrets". In dieselfde asem word daar ook gesê dat enige soektog na pornografie op die groter Internet verbode is.

347 Art 14 van die MCI. 15 000 Yuan is in 2016 ongeveer ses maande se lone in die privaat sektor in Sjina. CNN Money "Global Wage Calculator" http://money.cnn.com/interactive/news/economy/davos/global-wage-calculator/ (besoek op 15 Maart 2016).

348 Die Engelse teks van hierdie regulasie is beskikbaar by: World Intellectual Property Organization "Measures for Security Protection Administration of the International Networking of Computer Information Networks" http://www.wipo.int/edocs/lexdocs/laws/en/cn/cn115en.pdf (besoek op 14 Maart 2014).

349 Art 2 van die MCI bevat bv ongeveer dieselfde inhoud as art 2 van die PINN en art 13 van die MCI bevat ongeveer dieselfde inhoud as art 5(2) van die PINN. Hierdie is slegs voorbeelde en nie 'n volledige lys nie.

Artikel 5 verklaar dat daar nege handelinge is wat op die Internasionale Internet verbode is.[350] 'n Persoon mag nie die groter Internet gebruik om vir enige van die volgende te soek, of inligting daaromtrent te berg nie:

(1) teenkanting van die Grondwet;

(2) ondergrawing van staatsmag;

(3) aanstigting van sabotasie of nasionale eenheid;

(4) aanstigting van haat en diskriminasie tussen nasionaliteite;

(5) inligting wat die sosiale orde in gedrang bring;

(6) inligting aangaande "feudalistic superstitions",[351] pornografie, dobbelary en die aanstigting van misdaad;

(7) inligting wat ander persone beledig;

(8) inligting wat enige staatsorgane se reputasie in gedrang stel, en

(9) enige ander inligting wat die Grondwet, wette van die land en administratiewe regulasies ondermyn.

Net soos die MCI is hierdie lys baie omvattend, en veral die laaste punt van "enige ander inligting" maak regs*on*sekerheid 'n gegewe.

Interessant genoeg bepaal artikel 7 dat die privaatheid van gebruikers se Internet-kommunikasie beskerm word. Geen *gebruiker* mag 'n ander

350 Art 5 van die PINN.

351 Wat presies met hierdie term bedoel word, is ietwat onduidelik, maar dit wil voorkom asof bygelowe steeds 'n belangrike plek in Sjinese kultuur speel. Randi wys bv daarop dat 'n ene Mnr Liu, wat die voormalige minister van spoorweë was, afgedank is weens die feit dat hy 'n "feng shui master" geraadpleeg het om die korrekte datum te bepaal vir wanneer die bouwerk van 'n belangrike spoorwegnetwerk begin moes word. Randi J "China and Superstitions" http://archive.randi.org/site/index.php/swift-blog/2120-china-and-superstitions.html (besoek op 15 Maart 2015). Skynbaar word persone ook van hierdie misdryf aangekla wanneer hulle die vryheid van Tibet ondersteun. Harrison L "Beijing Shakes Fist at 'Cults and Feudal Superstition' Online" http://www.theregister.co.uk/2000/10/14/beijing_shakes_fist_at_cults/ (besoek op 15 Maart 2016). Overmeyer D L "From 'Feudal Superstition' to 'Popular Beliefs': New Directions in Mainland Chinese Studies of Chinese Popular Religion" 2001 *Cahiers d'Extrême-Asie* 103 103–126.

gebruiker se kommunikasie op die Internet moniteer nie. Ongelukkig bepaal die volgende artikel[352] dat Internet-diensverskaffers en individue "should accept security supervision, inspection and guidance of public security organs"! Onderskepping van enige kommunikasie tussen gebruikers is onwettig, maar dieselfde gedrag is toelaatbaar wanneer dit van staatsweë af kom.

6.4.2.2.3 *Security Management Procedures in Internet Accessing*

Die SMP is deur die Ministerie van Openbare sekuriteit in 1997 uitgevaardig. Net soos die PINN bevat dit 'n lys handelinge wat sekere gedrag op die Internet verbied — en net soos die vorige twee regulasies is dit 'n lys wat verskeie wyses van optrede verbied wat reeds deur daardie twee regulasies gedek is. Potter[353] noem dat die SMP die volgende gedrag op die Internet verbied:

(1) oortredings van die Grondwet, wetgewing, of regulasies van Sjina;

(2) inligting wat aanhitsing van die regering of die sosialistiese stelsel bewerkstellig;

(3) inligting wat separatisme bevorder of die nasionale eenheid benadeel;

(4) inligting wat die eenheid van nasionaliteite benadeel;[354]

(5) inligting wat valshede of gerugte bevat;

(6) inligting wat die sosiale orde ondermyn;

(7) inligting wat terrorisme ondersteun, en

(8) inligting wat die reputasie van enige staatsorganisasies benadeel.

352 Art 8.

353 Potter P *China's Legal System* (2013) 154.

354 Dit wil voorkom asof die woord "nationalities" hier eintlik die verskillende etniese groepe in Sjina aandui.

Let daarop dat die blote soek en toegang tot enige van hierdie onderwerpe verbode is.

Tot dusver is daar aangetoon dat die blote soek en die verkryging van toegang van sekere tipes inligting verbode is. Die SMP is egter die eerste dokument wat ook ander tipe gedrag verbied wat ook in die weste as 'n misdryf beskou word, naamlik ongemagtigde toegang tot rekenaarstelsels.[355] Dit is die sogenaamde "hacking" klousules wat mens byvoorbeeld ook in artikel 86 van die Wet op Elektroniese Kommunikasies en Transaksies[356] kry.[357]

Die drie bovermelde regulasies het Sjina se Internet-landskap van 1994 tot 1999 geskep. Hierna sou die tweede fase van Internetregulering begin — 'n era waar die klem verskuif van 'n poging tot direkte regulering na een van wetgewing wat Internet-diensverskaffers en gebruikers noop om te *self-reguleer* sodat die regering se vae wette en regulasies nie verbreek word nie. Chueng voer aan dat "... the legislation represents an attempt to contract out responsiblity to the business sector to accomplish the most effective monitoring of the Internet and to achieve the twin goals of power maintenance and economic growth in the midst of the globalizing effect of the Internet".[358]

6.4.2.3 Tweede-fase Regulering

Die tweede fase van Internetregulering in Sjina word gekenmerk deur 'n reeks regulasies en wette wat daarop gemik is om die doelwitte van ISP- en gebruiker-selfmonitering te bereik. Omdat daar soveel regulasies

355 Art 6.

356 25 van 2002.

357 Ongemagtigde toegang van rekenaarsisteme word nie in hierdie studie onder die loep geneem nie, maar 'n verduideliking van art 6 van die SMP kan gevind word by Qiu 2000 *International Journal of Communications Law and Policy* 11. Art 285 van die Sjinese Strafkode bevat ook 'n volledige verbod om ongemagtigde toegang tot rekenaarsisteme. Qiu 2000 *International Journal of Communications Law and Policy* 11.

358 Chueng A S Y "The Business of Governance: China's Legislation on Content Regulation in Cyberspace" 2006 *International Law and Politics* 1 19.

uitgevaardig is, is dit nie sinvol om in hierdie beperkte studie elkeen daarvan in besonderhede te bespreek nie.[359] Waar van toepassing sal die belangrikste regulasies bespreek word, maar in ander gevalle sal regulasies saam gegroepeer word om die doel daarvan, uit te lig.

6.4.2.3.1 *Telecommunications Regulations of the People's Republic of China*

Die *Telecommunications Regulations of the People's Republic of China*[360] (hierna TRPC) is op die 25e September 2000 gepromulgeer, en is een van die belangrikste Internetreguleringsmaatstawwe in Sjina.[361] Hierdie is die eerste regulasie wat soos wetgewing lyk, en bevat behoorlike definisies en bepalings. Dit is deur die Staatsraad uitgereik, wat die hoogste administratiewe orgaan in Sjina is.[362]

---

[359] Daar is bv in 2000 sewe regulasies uitgereik wat min of meer dieselfde strekking het. Hulle is:

Datum van Promulgering	Uitreikingsgesag	Wetgewing of Regulasie
25 Januarie 2000	Staatsgeheime-buro	Administration of the Maintenance of Secrets in the International Networking of Computer Information Systems Provisions
1 September 2000	Staatsadministrasie van Handel en Nywerheid	Interim Procedures on the Regulation and Filing of Online Business Operation
25 September 2000	Staatsraad	Regulation on Internet Information Service of the People's Republic of China
25 September 2000	Staatsraad	Telecommunications Regulations of the People's Republic of China
8 Oktober 2000	Ministerie van Inligting	Management Provisions on Electronic Bulletin Services in the Internet
7 November 2000	Perskantoor van die Staatsraad	Administration of Engagement by Internet Sites in the Business of News Publication Tentative Provisions
28 Desember 2000	Staande komitee van die "National People's Congress"	Decision of the Standing Committee of the National People's Congress People's Congress Concerning Maintaining Internet Security

Chueng 2006 *International Law and Politics* 16–17, opgedateer.

[360] Die volledige teks van hierdie regulasie is te vinde by ChinaITLaw "Telecommunications Regulations of the People's Republic of China" http://www.china.org.cn/business/laws_regulations/2010-01/20/content_19273945.htm (besoek op 17 Maart 2016).

[361] Ziccardi G *Resistance, Liberation Technology and Human Rights in the Digital Age* (2012) 254.

[362] Wikipedia "State Council of the People's Republic of China" https://en.wikipedia.org/wiki/State_Council_of_the_People's_Republic_of_China (besoek op 17 Maart 2016).

Uit die staanspoor word daar genoem dat hierdie wetgewing die hele telekommunikasiemark in Sjina beheers,[363] en almal (insluitend buitelanders) wat enige aktiwiteit verrig wat met telekommunikasie in Sjina te make het, moet hulle aan hierdie vereistes hou.[364] Artikels 3–5 sit dan 'n organogram uiteen van hoe die gesagstrukture in Sjina sal lyk — die Staatsraad bo is in beheer van die hele telekommunikasiewese, en daardie gesag word dan afgewentel na hulle "onderskeie jurisdiksies".[365]

Artikels 7 tot 16 verduidelik hoe die intranet van Sjina gestruktureer sal word, en wat die regering se rol daarin is. In die eerste plek word daar onderskei tussen twee soorte dienste, naamlik basiese- en toegevoegde-waarde-dienste.[366] Eersgenoemde sluit in die fisiese Internet-argitektuur, soos die beskikbaarstelling van data- en basiese stemdienste.[367] Laasgenoemde het te doen met die aanbieding van inligtingsdienste wat deur die netwerk vloei.[368]

Die rede waarom die onderskeid belangrik is, is dat alle maatskappye wat basiese dienste lewer, slegs 'n permit[369] sal kry om te kan funksioneer as die regering ten minste 'n beherende aandeel van 51% in die maatskappy het.[370] Deur dit te doen behou die regering totale beheer oor die fisiese argitektuur van Sjina se intranet.[371]

Afdeling 5 van die TRPC bevat die gewraakte bepalings wat, net soos die vorige regulasies, ontoelaatbare gedrag op Sjina se nasionale netwerk uiteensit. In hierdie afdeling is daar nie slegs een lys nie, maar drie: die eerste verbied die *verspreiding* van ontoelaatbare inligting; die tweede verbied

363 Art 1.

364 Art 2.

365 Art 3.

366 Art 8.

367 Art 8 par 2.

368 Art 8 par 2.

369 Geen persoon mag sonder 'n permit enige telekommunikasiedienste in Sjina bedryf nie. Dit word gereguleer deur art 7–16.

370 Art 10(1).

371 Art 17–22 reguleer selfs die interne skakeling *tussen* verskillende diensverskaffers, en verskaf die regering mikrobeheer oor die totale Sjinese intranet.

inligting wat die *sekuriteit* van die netwerk bedreig, en die derde verbied die *ontwrigting* van die netwerk.[372]

Artikel 57 bepaal dat geen organisasie of individu die Sjinese telekommunikasienetwerk mag gebruik om enige van die volgende te produseer, reproduseer of te versprei nie: inligting wat

(1) teen die beginsels van die Grondwet indruis;

(2) staatsveiligheid en staatsgeheime openbaar maak;

(3) die belange van die Staat benadeel;

(4) rassediskriminasie of inter-etniese eenheid aanhits;

(5) staatsbeleid aangaande godsdiens saboteer, asook "feudal superstitions";[373]

(6) gerugte versprei of die sosiale orde of -stabiliteit ontwrig;

(7) pornografie, dobbel, geweld, moord of vrees of die aanstigting van misdade bevorder;

(8) beledigings of kwaadpratery teen 'n derde party of die inbreukmaking op die regte en belange van die derde party; of

(9) deur enige ander wet of administratiewe regulasies verbied word.

Met hierdie nege verbiedinge is dit duidelik dat daar gepoog word om die regering se belange en die sosiale orde te beskerm.[374] Soos hierbo genoem is die verbode handeling die *opsoek* en *verspreiding* van verbode materiaal.

Die volgende artikel[375] het ten doel om die sekuriteit van die nasionale netwerk te beskerm. Let daarop hoe die verbode gedrag spesifiek te doen het met manipulering van data *op die netwerk*. Die gedrag wat verbied word is:

372 Art 57–59.

373 Vn 351.

374 Art 67 bepaal dat dit 'n misdryf is wanneer art 57 oortree word.

375 Art 58.

(1) verwydering of verandering van sagteware wat die netwerk laat werk, of manipulering van data wat versend word;

(2) die gebruik van die netwerk om inligting van iemand anders te steel en sodoende sy regte en belange te benadeel

(3) die skepping en verspreiding van rekenaar-virusse of die gebruik van enige ander metodes om die telekommunikasienetwerk of enige telekommunikasie-fasiliteite aan te val, of

(4) die verrigting van enige handeling wat die sekuriteit van 'n telekommunikasienetwerk in gevaar stel.[376]

Hierdie is almal handelinge wat in westerse lande ook verbied word. Punt 3 hierbo maak melding van enige metode om 'n telekommunikasienetwerk aan te val, en dit is 'n interessante bepaling wat oorkoepelend met 'n menigte handelinge te doen het wat netwerke kan lam lê. Verskeie lande het byvoorbeeld spesifiek "denial-of-service" handelinge verbied[377] — so ook Suid-Afrika[378] — maar hierdie algemene vereiste is so wyd dat dit maklik enige metodes wat huidig nog onbekend is om netwerke binne te dring, kan omvat.

Artikel 59 bevat die derde lys van handelinge wat verbode is, maar dit gaan nie volledig genoem word nie aangesien dit bloot enige handeling verbied wat daarop gerig is om 'n skakeling tussen enigiemand binne Sjina met iemand buite Sjina te verbind.[379]

Artikel 63 bepaal dat enige gebruiker van 'n telekommunikasiediens aanspreeklik gehou word vir enige inhoud wat hulle daarop versend. Indien

376 Art 67 bepaal dat dit 'n misdryf is wanneer art 58 oortree word.

377 In die VSA word hierdie tipe gedrag verbied deur USC §1030, en in die Verenigde Koninkryk bepaal art 2 van die Computer Misuse Act van 1990 dat sulke gedrag 'n misdryf sal wees. Om meer te lees oor wat 'n "denial-of-service" aanval behels, sien Dittrich D, Mirkovic J *et al Internet Denial of Service: Attack and Defense Mechanisms* (2004), veral hfst 2 getiteld Understanding Denial of Service.

378 Art 86(5) van die Wet op Elektroniese Kommunikasies en Transaksies 25 van 2002.

379 Sien die Internetskakel by vn 360 om meer inligting hieroor te bekom.

dit staatsgeheime bevat, moet die nodige stappe geneem word om dit te beskerm teen ongemagtigde gebruik.

6.4.2.3.2 *Measures for Managing the Internet Information Services*

Die *Measures on Internet Information Services*[380] (hierna MIIS) is op dieselfde dag as die TRPC uitgevaardig.[381] Dit poog om spesifiek inligtingsdienste, of — soos artikel 1 bepaal — "Internet Information services" te reguleer.

Die MIIS bevat presies dieselfde lys van verbode gedrag wat in artikel 57 van die TRPC verbied word, en dus word dit nie weer genoem nie.[382] Wat wél nuut is, is die onderskeid wat getref word tussen kommersiële en nie-kommersiële Internet-diensverskaffers.[383] Eersgenoemde is diensverskaffers wat vergoeding ontvang, óf dienste verskaf wat webblaaie ontwerp.[384] Nie-kommersiële diensverskaffers is diensverskaffers wat "open source" en gratis (algemeen-beskikbare) inligting verskaf sonder vergoeding.[385]

Die rede vir die onderskeid is dat nie-kommersiële Internet-diensverskaffers rekord van hulle dienste moet hou, sodat verslag daaroor gedoen kan word.[386] Beide kommersiële- en nie-kommersiële diensverskaffers moet gelisensieerd wees alvorens hulle enigsins mag funksioneer.[387]

Artikel 13 van die MIIS maak verreikende ingrepe op ISP's deur te bepaal

---

380 Die teks van die MII kan verkry word by City U "Measures for Managing Internet Information Services" http://newmedia.cityu.edu.hk/cyberlaw/gp9/pdf/lr01.pdf (besoek op 17 Maart 2016). Sien ook Ziccardi *Resistance, Liberation Technology and Human Rights in the Digital Age* 254.

381 Stevenson C "Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World" 2007 *Boston College International and Comparative Law Review* 531 537 vn 55.

382 In die MIIS is die lys van verbode gedrag in art 15 vervat.

383 Art 3.

384 Art 3 par 2.

385 Art 3 par 3.

386 Art 8 noem dat die volgende inligting bewaar moet word: "1. Basic facts about the sponsor and the person in charge; 2. The Web site address and the services it provides; and 3. Proof of concurrence from the relevant authorities if its services fall within the scope of Article 5". Wat hiermee bedoel word, is egter onduidelik, aangesien geen bronne gevind kon word wat spesifiek hierdie artikel aanspreek nie. Wie die "sponsor" is, is ook onduidelik.

387 Art 4 par 2.

dat dit die ISP se verantwoordelikheid is om toe te sien dat alle gebruikers se optrede wettig is.[388] Net so word ISP's verplig om rekords vir 60 dae te hou oor die nuus wat hulle versprei het. Chueng wys op die omvang van dié regulasie:

> ISP's that offer news coverage and bulletin board services are required to keep a sixty-day record of the information that they distribute, when it is distributed, and the Web address where the information is located. IISPs are similarly required to keep records of the time of use, accounts of Internet addresses or domain names, and dial-in telephone numbers of online users for 60 days. The Regulations are considered to be the prime model for the strict control of Internet administration.[389]

Dit is dus duidelik dat die MIIS geweldige streng vereistes vir ISP's neerlê om te kan funksioneer. Chueng wys hoe daar ook soortgelyke reëls vir elektroniese bulletin-diensverskaffers[390] en Internet-nuusverskaffers[391] gemaak is. In die geval van bulletin-diensverskaffers word hulle vereis om 'n rekord van al hulle gebruikers te hou, en hulle ook te moniteer. Internet-nuusverskaffers word verbied om na enige internasionale nuus-skakels te verbind, en slegs die nuus wat deur die amptelike staatsmedia-kanaal versprei word, mag aan inwoners deurgegee word.[392]

6.4.2.3.3 Tussengangers en Gebruikers geteiken

Nadat die fondament in 2000 gelê is met 'n verskeidenheid regulasies wat ISP's en gebruikers teiken om te self-reguleer, is die net wyer gespan

388 Art 13. Chueng 2006 *International Law and Politics* 19.

389 Chueng 2006 *International Law and Politics* 19.

390 Chueng 2006 *International Law and Politics* 19. Die teks van die "Electronic Bulletin Services Provision" is verkrygbaar by ChinaItLaw "Administrative Provisions for Electronic Bulletin Services on the Internet" http://www.china.org.cn/business/2010-01/20/content_19274960.htm (besoek op 17 Maart 2016). Sien ook Yang K C C "A Comparative Study of Internet Regulatory Policies in the Greater China Region: Emerging Regulatory Models and Issues in China, Hong-Kong SAR, and Taiwan" 2007 *Telematics and Informatics* 30 35 waar reëls aangaande "bulletin-board"-dienste bespreek word.

391 Chueng 2006 *International Law and Politics* 19. Die teks van die "Provisions on the Administration of Newspaper Publication" is verkrygbaar by LawInfoChina "Provisions on the Administration of Newspaper Publication" http://www.lawinfochina.com/display.aspx?lib=law&id=4716&CGid=# (besoek op 17 Maart 2016).

392 Chueng 2006 *International Law and Politics* 20.

om meer industrieë onder dieselfde sisteem in te forseer. In 2001 is die *Measures on the Administration of Business Sites of Internet Access Services* uitgevaardig met die doel om Internetkafee's te reguleer.[393] Die wye aanwending van hierdie regulasie het egter tot gevolg gehad dat enige besigheid wat Internetskakeling verskaf — soos Internet-kroeë en rekenaar-sitkamers — ook onder die regulasie geval het.[394] Die regulasie is spoedig in 2002 uitgebrei met die *Regulations on the Administration of Business Sites of Internet Access Services* wat bepaal het dat van alle sodanige besighede vereis word om monitering-sagteware te installeer, en ook aktiewe monitering te bewerkstellig.[395] Alle wangedrag moet dan aan owerhede deurgegee word.[396] Besighede wat onder hierdie regulasie val, is verder verplig om rekords van die identiteit van elke gebruiker te bewaar, asook alle aktiwiteit wat die gebruiker op die netwerk uitgevoer het, vir 'n tydperk van minstens 60 dae te bewaar.[397] Minderjariges word geheel-en-al verbied om enigsins van sulke dienste gebruik te maak.[398] Chueng wys daarop dat as gevolg van die groot las wat hierdie regulasies op Internetkafee's en verwante besighede geplaas het, die aantal besighede wat sulke dienste lewer, binne twee jaar van 200 000 na ongeveer 110 000 verlaag het.[399]

Dieselfde metodes is gebruik om Internet-publikasies te reguleer. Die *Interim Provisions on the Administration of Internet Publication* is in 2002 uitgevaardig, en dit het bepaal dat alle Internet-publikasies[400] slegs gepubliseer mag word indien daar vooraf toestemming deur die relevante

393 Chueng 2006 *International Law and Politics* 21.

394 Chueng 2006 *International Law and Politics* 19.

395 Chueng 2006 *International Law and Politics* 19.

396 Art 19.

397 Art 23.

398 Art 21.

399 Chueng 2006 *International Law and Politics* 22. Sy noem verder op 22–23 dat "Those that are still in operation must install software to filter out more than 500,000 banned sites that are considered by the authorities to be offensive or subversive".

400 'n Internet-publikasie word volgens hierdie regulasie beskou as "online transmission acts by Internet information service providers of posting on the Internet, or sending to user terminals through the Internet, after selection and editing, works created by themselves or others for browsing, reading, use or downloading by the public". Art 5.

owerhede verleen is.[401] Net soos die ander regulasies hierbo bespreek, word daar van Internet-publiseerders verwag om vir ten minste 60 dae rekords te hou van enige materiaal wat op die Internet gepubliseer word,[402] en die Internet-uitgewer se redakteur word aanspreeklik gehou vir die "legality of content" wat geplaas word.[403] Artikel 21 van hierdie regulasie bepaal dat werknemers van Internet-publiseerders opleiding oor geskikte gedrag moet ondergaan voordat hulle hulle take mag verrig.

Chueng som die *legio* Internetregulasies op deur te verduidelik hoe die regering dit reggekry het om elkeen oor sy eie skouer te laat kyk en onderling almal mekaar te reguleer: "the picture of Internet regulation in China is composed of Internet cafe managers patrolling their own shops and *Yahoo* monitoring its own chat rooms and screening the e-mail messages of its users".[404]

Wanneer hierdie regulasies onder die vergrootglas geplaas word, is dit duidelik dat daar in alle gevalle twee groepe geteiken word: die eerste is die eienaar of beherende persoon van die maatskappy wat aanspreeklik gehou word vir inligting wat op sy netwerk te vinde is, of inligting wat deur sy besigheid geplaas word, en die tweede teiken is eindgebruikers wat eweneens verantwoordelik gehou word vir hulle Internetgebruik.

Voordat die bespreking verder geneem word, is dit nodig om die groter konteks van dit wat sopas bespreek is, te omlyn. Daar is reeds hierbo genoem[405] dat Yang van mening is dat Internetregulering in Sjina in drie fases verdeel kan word: die eerste was tussen 1994 en 1999, en dit het die groter landskap van Internetregulering in Sjina daargestel met die uitvaardiging van regulasies wat die Internet in Sjina oorkoepelend gedek het. Die tweede fase is sopas bespreek, en daar is aangetoon hoe daar tussen 2000 en 2002 'n rits regulasies uitgevaardig is om spesifieke Internet-

401 Art 6.

402 Art 22.

403 Art 21.

404 Chueng 2006 *International Law and Politics* 26.

405 Afd 6.4.2.1.

industrieë te teiken met reëls wat besonder op hulle van toepassing is.[406] Die volgende fase het in 2003 begin, maar soos dit spoedig sal blyk, is die grens tussen die tweede en derde fase eerder 'n gelykmatige oorloop van een sisteem na die ander. Regulasies wat spesifieke Internet-industrieë teiken is steeds uitgevaardig — maar met groter tussenposes — en dit het gepaard gegaan met tegnologie wat al hoe beter geword het en wat nou regulering op 'n bloot tegnologiese vlak moontlik begin maak het.[407] Hiermee saam is polisiëring van die Sjinese intranet verskerp, en is daar dus van meer mense gebruik gemaak om 'n verskeidenheid reguleringsfunksies te verrig.[408]

6.4.2.4 Derde-fase Regulering

Die derde fase van Internetregulering in Sjina gaan gepaard met twee oorhoofse strategieë: die eerste is steeds die uitvaardiging van regulasies om spesifieke industrieë te reguleer, maar die tweede strategie het te doen met tegnologiese regulering. Dit het nou moontlik geword om Internet-toegang in spesifieke gebiede te beperk of selfs geheel en al af te sny, terwyl ander nabygeleë gebiede se Internet-toegang onaangeraak bly.[409] Persone kan selfs op 'n individuele basis geteiken word.[410] Hierdie aspekte sal spoedig verder toegelig word. Voordat dit egter gedoen word, moet vier regulasies uitgelig word wat voortgegaan het om, soos in die vorige fase, spesifieke industrieë te teiken.

406 Afd 6.4.2.3.

407 Afd 6.4.2.4

408 Afd 6.4.2.4.5.

409 Afd 6.4.2.4.5.

410 Dit wil voorkom asof menseregte-aktiviste dikwels op 'n individuele basis geteiken word. Sien British Broadcasting Corporation "Human Rights: What is China Accused Of?" http://www.bbc.com/news/magazine-34592336 (besoek op 28 Maart 2016); Quartz "The Seven Tweets That Could Cost a Chinese Human Rights Lawyer Eight Years in Jail" http://qz.com/569370/the-seven-tweets-that-could-cost-a-chinese-human-rights-lawyer-eight-years-in-jail/ (besoek op 28 Maart 2016; The Wall Street Journal "China Targets Human-Rights Lawyers in Crackdown" http://www.wsj.com/articles/china-targets-human-rights-lawyers-in-crackdown-1436715268 (besoek op 28 Maart 2016) en British Broadcasting Corporation News "China Internet: Ren Zhiqiang's Account Blocked After Xi Criticism" http://www.bbc.com/news/world-asia-china-35682030 (besoek op 28 Maart 2016).

6.4.2.4.1 *Provisions for the Administration of Internet News Information Services*

Hierdie regulasie het persone wat *blogs* bedryf asook diegene wat bulletin-dienste[411] lewer geteiken. Die *Provisions for the Administration of Internet News Information Services* (hierna PANS) wat in 2005 uitgevaardig is, het 'n nuwe lys van gedrag wat op die Internet verbode is, bevat.[412] Hierdie keer word die volgende verbied:

(1) die oortreding van basiese beginsels soos dit bevestig is in die Grondwet;

(2) benadeling van die nasie se veiligheid, die bekendmaking van staatsgeheime, ondergrawing van die nasionale regering of in gevaarstelling van die eenheid van die nasie;

(3) benadeling van die eer of die belange van die nasie;

(4) aanhitsing van haat teen mense, rassisme, of ontwrigting van eenheid tussen mense;

(5) ontwrigting van nasionale beleid oor godsdiens of die verkondiging van kultusse en "feodal superstitions";[413]

(6) die verspreiding van gerugte, versteuring van die sosiale orde, of ontwrigting van sosiale stabiliteit;

(7) die verspreiding van pornografie, dobbelary, geweld, of verlening van bystand by die pleeg van 'n misdryf;

411 Sogenaamde "bulletin board services".

412 Congressional Executive Commission on China "Provisions on the Administration of Internet News Information Services (Chinese Text and CECC Full Translation)" http://www.cecc.gov/resources/legal-provisions/provisions-on-the-administration-of-internet-news-information-services (besoek op 22 Maart 2016); Human Rights Watch *Race to the Bottom: Corporate Complicity in Chinese Internet Censorship* (2006) 18.

413 Vn 351.

(8) belediging of laster teen derde partye, of die inbreukmaking op die regte en belange van ander:

(9) aanhitsing van onwettige byeenkomste, -verenigings, -optogte, betogings, of byeenkomste wat die sosiale orde versteur;

(10) die uitvoering van aktiwiteite in die naam van 'n onwettige burgerlike organisasie; en

(11) enige ander inhoud wat deur die landswette of reëls verbied word.[414]

Alle Internet-nuusdienste word verplig om 'n "content administration responsible system" in werking te stel. [415] Dit beteken dat enige Internet-nuusdiens verbied word om enige inligting aangaande enige aspek in die lys hierbo te dek of te versprei.[416] Sou die Internet-nuusdiens agterkom dat dit wél 'n berig geplaas het wat verbode is, moet dit dadelik uitgevee word, en 'n rekord daarvan moet aan owerhede deurgegee word.

Volledige rekords moet ook gehou word: artikel 21 bepaal uitdruklik dat die inhoud van elke berig, die tyd wat dit geplaas is en die Internet-adres (URL) daarvan, moet op rekord gehou word vir 'n periode van 60 dae. Volgens Human Rights Watch is die hoofdoel van hierdie regulasie om enige nuus wat nie in lyn is met die amptelike siening van die regerende party nie, te verban.[417]

Die PANS skep 'n geweldige streng sisteem ten aansien van nuuslewering, aangesien elke nuusverskaffer by die regering geregistreer moet word.[418] Wanneer dit gedoen is, mag die nuusverskaffer ook net nuus wat

414 Art 19. Human Rights Watch *Race to the Bottom* 19.

415 Art 20.

416 Art 20.

417 Human Rights Watch *Race to the Bottom* 19 meld: " such provisions are implemented in a way to prohibit all reporting that reflects a line different from the official government position, or contains information that the government deems too embarrassing, or is too candid in its discussion of particularly entrenched social problems".

418 Art 5. Sien ook Human Rights Watch *Race to the Bottom* (2006) 20 vir 'n volledige verduideliking van die proses waardeur daar gegaan moet word om as nuusverskaffer te kan registreer.

van die amptelike regeringskanale verkry word, verder versprei.[419] Human Rights Watch beskryf dit tereg as 'n sisteem waar die gewone nuuskanale bloot 'n "extension(s) of currently-existing news units" is.[420] Dit is egter te verwag, aangesien die PANS dit baie duidelik maak dat nuusverskaffers se funksie is "toward serving the people and serving socialism".[421]

6.4.2.4.2 *Measures for the Administration of the Publication of Audio-Visual Programs through the Internet or other Information Network*

Alle Internetdienste wat oudio-visuele programme deur die Internet beskikbaar stel, word gereguleer deur die *Measures for the Administration of the Publication of Audio-Visual Programs through the Internet or other Information Network* van 2004.[422] Die belangrikste bepaling by hierdie regulasie is dat sulke verskaffers geregistreer moet wees,[423] en dat 'n volledige bestuurstelsel geïmplementeer moet word wat inhoud moniteer.[424] Die hoofredakteur word aanspreeklik gehou vir enige materiaal wat gepubliseer word.[425] 'n Lys van onwettige gedrag word eweneens in artikel 19 gegee, maar dit word nie hier herhaal nie aangesien dit in wese met die lys van die PANS (direk hierbo) ooreenstem.[426]

---

419 Art 5. Qui J L "Virtual Censorship in China: Keeping the Gate Between the Cyberspaces" 2000 *International Journal of Communications Law and Policy* 1 17–18.

420 Human Rights Watch *Race to the Bottom* 19.

421 Art 3.

422 Weber R H en Burri M *Classification of Services in the Digital Economy* (2012) 115. Vir 'n volledige teks van die regulasie, sien Lehman, Lee en Xu "Measures for the Administration of the Publication of Audio-Visual Programs Through the Internet or Other Information Network 2004" http://www.lehmanlaw.com/resource-centre/laws-and-regulations/information-technology/measures-for-the-administration-of-the-publication-of-audio-visual-programs-through-the-internet-or-other-information-network-2004.html (besoek op 22 Maart 2016).

423 Art 6–16.

424 Art 20.

425 Art 20.

426 Lehman, Lee en Xu "Measures for the Administration of the Publication of Audio-Visual Programs through the Internet or Other Information Network 2004" http://www.lehmanlaw.com/resource-centre/laws-and-regulations/information-technology/measures-for-the-administration-of-the-publication-of-audio-visual-programs-through-the-internet-or-other-information-network-2004.html (besoek op 22 Maart 2016).

6.4.2.4.3 *Measures for the Administrative Protection of Internet Copyright*

Die *Measures for the Administrative Protection of Internet Copyright* van 2005 (hierna MAPC) het 'n nuwe kopieregsisteem vir Internet-diensverskaffers ingelui.[427] Hiervolgens moet 'n Internet-diensverskaffer enige kopieregskendende materiaal verwyder indien dit 'n afhaalkennisgewing van die kopiereghouer kry.[428] Op die oog af lyk dit baie soortgelyk aan artikel 512 van die USC wat hierbo bespreek is.[429] Die skepper van die materiaal wat na bewering kopiereg skend, kan selfs 'n teen-kennisgewing stuur aan die ISP wat die materiaal op sy bediener gehuisves het, asook die persoon wat die afhaalkennisgewing gestuur het, wat aandui waarom die materiaal *nie* kopiereg skend nie.[430] In so 'n geval mag die ISP dan die materiaal wat hy verwyder het, weer plaas sonder vrese van enige vervolging.[431] Indien 'n ISP geen kennis dra van enige kopieregskending nie, sal dit eweneens nie aanspreeklik gehou kan word nie.[432] Net soos die vorige regulasies is daar 'n regsplig op 'n ISP om sulke kennisgewings en alle verwante dokumente vir 'n tydperk van 60 dae te bewaar.[433]

Die MAPC duld egter geen vorm van roofkopieëring[434] nie, en meld uitdruklik in artikel 14 dat persone wat hulle met "piracy activities" besig hou, gestraf kan word. Die tweede deel van die artikel meld dat daar van Internet-diensverskaffers verwag word om hulle volle samewerking te

427 Die volledige teks van hierdie regulasie is beskikbaar by World Intellectual Property Organization "Measures for the Administrative Protection of Internet Copyright" http://www.wipo.int/edocs/lexdocs/laws/en/cn/cn034en.pdf (besoek op 23 Maart 2016).

428 Art 5.

429 Afd 6.4.1.3 hierbo.

430 Art 7.

431 Art 7.

432 Art 12.

433 Art 6 par 2.

434 "Piracy" is die algemene term wat in Engels gebruik word. Karaganis wys daarop dat daar geen algemeen-aanvaarbare definisie van roofkopieëring bestaan nie, en definieer dit eenvoudig as: "the ubiquitous, increasingly digital practices of copying that fall outside the boundaries of copyright law" Karaganis J *Media Piracy in Emerging Economies* (2011) 2. Sien ook Honick R *Software Piracy Exposed* (2005) 20 vir 'n volledige historiese oorsig van digitale roofkopieëring.

gee om sulke gebruikers aan die pen te laat ry.[435] Indien dit blyk dat die ISP hom op enige wyse aan 'n misdryf skuldig gemaak het, sal die saak aan die relevante owerhede deurgegee word waar die ISP dan strafregtelik aanspreeklik gehou sal word.[436]

6.4.2.4.4 *China Internet Domain Name Regulations*

Die *China Internet Domain Name Regulations* is in 2004 uitgevaardig en in 2006 hersien.[437] Vir doeleindes van hierdie studie is dit slegs nodig om daarop te wys dat die regulasies uitvoerige vereistes neerlê vir domeinnaam-registrateurs ten aansien van die opstel van basisnaambedieners.[438] Die kritieke werking van basisnaambedieners is reeds in afdeling 2.3.4 bespreek.[439] Met hierdie stap het die Sjinese regering volle beheer oor die Sjinese intranet, asook alle ruggraatskakels wat dit aan die groter Internet koppel, bevestig. Indien 'n organisasie 'n basisnaambediener wil installeer, moet daar vooraf toestemming van die Ministerie van Inligtingsindustrie[440] verkry word.[441]

---

435 Art 14 verwag van ISP's: "the Internet access service provider shall, provide cooperation in implementing the corresponding punishment measures".

436 Art 16.

437 Die teks van die 2004 *China Internet Domain Name Regulations* is beskikbaar by: World Intellectual Property Organization "China Internet Domain Name Regulations" http://www.wipo.int/wipolex/en/text.jsp?file_id=182419 (besoek op 23 Maart 2016). Die 2006-wysigings is beskikbaar by: China Patent Agent "China Internet Domain Name Regulations (2006)" http://www.cpahkltd.com/EN/static/20100315155837187932.html (besoek op 23 Maart 2016). Sien ook Smith G J H *Internet Law and Regulation* (2007) 223 vir 'n volledige verduideliking van die registrasieproses van 'n domeinnaam in Sjina, asook American Bar Association *China Law Deskbook: A Legal Guide for Foreign-invested Enterprises* (2005) 248–250 vir die hantering van dispute rakende domeinname in Sjina.

438 Art 8–10.

439 Sien ook fig 2.8 vir 'n skematiese uiteensetting van hoe die DNS en basisnaambedieners funksioneer.

440 Die Ministerie van Inligtingsindustrie word as 'n "superministerie" beskryf aangesien dit die Ministerie van Pos- en Telekommunikasie, die Ministerie van Elektroniese Nywerheid en die Ministerie van Radio, Film en Televisie vervang en hulle werksaamhede onder een ministerie verenig. FindLaw "China's Telecommunications Industry: The New Ministry of Information Industry (MII) and Foreign Investment Opportunities" http://corporate.findlaw.com/law-library/china-s-telecommunications-industry-the-new-ministry-of.html (besoek op 23 Maart 2016).

441 Art 8.

6.4.2.4.5 Direkte Tegnologiese Regulering

Daar is reeds in die begin van afdeling 6.4.2.4 aangetoon dat die derde fase van Internetregulering in Sjina uit twee strategieë bestaan. Die eerste was 'n voortsetting van skepping van regulasies, waarvan die belangrikste sopas bespreek is. Die tweede strategie was nuut, en dit het behels dat individue geteiken word, asook programme aangebied word om ondersteuning vir die regering se planne te verkry. Etlike van hierdie ingrepe sal toegelig word om vir die leser 'n blik te verskaf van wat hierdie strategie behels.

- Op 10 Junie 2004 word die webwerf net.china.cn geloods met die titel *Illegal and Inappropriate Information Report Center*. Die doel daarvan is om burgers aan te moedig om enige ongepaste of onwettige inligting op die netwerk te rapporteer.[442]

- Op 1 Januarie 2006 word die amptelike webwerf van die Volksrepubliek van Sjina geloods. Die doel daarvan is om regerings-inligting aan burgers deur te gee.[443]

- Op 21 Februarie 2006 word die "Sunshine Green Network Campaign" geloods.[444] Die doel daarvan is om "morele goedheid" op die Internet te bevorder.[445]

- Op 15 Februarie 2007 word 'n algemene omsendbrief uitgevaardig wat virtuele geld in Internetkafee's reguleer.[446]

---

442 China Internet Network Information Center "The Internet Timeline of China 2004–2006" http://www1.cnnic.cn/IDR/hlwfzdsj/201209/t20120904_36017.htm (besoek op 23 Maart 2016).

443 China Internet Network Information Center "The Internet Timeline of China 2004–2006" http://www1.cnnic.cn/IDR/hlwfzdsj/201209/t20120904_36017.htm (besoek op 23 Maart 2016).

444 China Internet Network Information Center "The Internet Timeline of China 2004–2006" http://www1.cnnic.cn/IDR/hlwfzdsj/201209/t20120904_36017.htm (besoek op 23 Maart 2016).

445 Cui en Wu 2015 *Telecommunications Policy* 268–271 gee 'n volledige verduideliking van die "Groen Netwerk"-beweging.

446 China Internet Network Information Center "The Internet Timeline of China (2007)" http://www1.cnnic.cn/IDR/hlwfzdsj/201209/t20120904_36018.htm (besoek op 23 Maart 2016).

- Op 30 September 2007 word die hele intranet-ruggraat van Sjina onder een nasionale netwerk geplaas.[447]

- In Mei 2008 versprei die Ministerie van Inligtingsindustrie[448] rekenaarsagteware (getiteld "Green Dam Youth Escort") wat die jeug teen onwettige Internet-optrede sou beskerm. Dit word gratis beskikbaar gestel ten spyte daarvan dat dit teen US$ 6 miljoen ontwikkel is.[449] Dit word swak deur die jeug ondersteun.[450]

- Op 19 Mei 2009 neem die Ministerie van Inligtingindustrie verdere stappe om die "Green Dam Youth Escort" sagteware op Sjina se rekenaars te kry deur 'n kennisgewing aan alle rekenaarvervaardigers te stuur met die opdrag dat die sagteware op alle nuwe rekenaars geïnstalleer moet word. Rekenaarkundiges het egter vinnig aangetoon hoe dit nie jeugdiges beskerm nie, maar eerder moniteer,[451] en dit het soveel teëkanting ontlok dat die regering die projek laat vaar het.[452]

- In Desember 2009 word 530 webwerwe wat roofkopieëring bedryf, van die Sjinese intranet verwyder.[453]

- In Desember 2009 kondig die Sjinese domeinregistrasie-owerheid aan dat geen individu meer domeinname mag registreer nie, en dat die *.cn* topvlakdomein slegs vir maatskappye en organisasies

447 China Internet Network Information Center "The Internet Timeline of China (2007)" http://www1.cnnic.cn/IDR/hlwfzdsj/201209/t20120904_36018.htm (besoek op 23 Maart 2016).

448 Vn 440.

449 Zheng 2013 *Beijing Law Review* 38.

450 Zheng 2013 *Beijing Law Review* 38.

451 MacKinnon R "China's Networked Authoritarianism" 2011 *Journal of Democracy* 32 39.

452 Zheng 2013 *Beijing Law Review* 38.

453 China Internet Network Information Center "The Internet Timeline of China (2009)" http://www1.cnnic.cn/IDR/hlwfzdsj/201209/t20120904_36020.htm (besoek op 23 Maart 2016). In 2012 het die hoogste hof in Sjina, die Supreme People's Court, 'n uitvoerige beleid uitgereik oor hoe kopieregskending deur howe geïnterpreteer moet word. Dit heet die *Provisions of the Supreme People's Court on Certain Issues Related to the Application of Law in the Trial of Civil Cases Involving Disputes over Infringement of the Right to Network Dissemination of Information.* Hua J *Toward A More Balanced Approach: Rethinking and Readjusting Copyright Systems in the Digital Network Era* (2014) 30; Hua 2014 *National Taiwan University Law Review* 16.

beskikbaar is. Gevolglik word meer as 130 000 persone se web-domeins gederegistreer.[454] Hierdie besluit word vroeg in 2010 in heroorweging geneem wanneer dit aan die lig kom dat vele vryskut-werkers en eenmansake negatief deur die besluit geraak is. Sulke persone kan nou wél 'n domein registreer, maar dit word slegs toegelaat indien die persoon homself positief kan identifiseer met 'n geldige identiteitsdokument en foto.[455]

- Sedert ten minste Julie 2009 het die Sjinese regering die vermoë om spesifieke areas se Internet-toegang af te sny of ernstig in te kort. Hierdie vermoë is getoon toe daar opstand in die provinsie Xinjiang was en die hele provinsie se Internet-toegang en selfoonnetwerke vir ses maande afgesny was.[456] Geen e-pos- of Internetkommunikasie was dus moontlik nie.[457]

- In Oktober 2010 het 'n bestuurder by *Sina Weibo*, wat Sjina se grootste sosiale platform is, aangedui dat dit ongeveer een miljoen inskrywings per dag verwyder.[458]

- Op die 30e Mei 2011 word kletskamers, gespreksforums, blogs en kitsboodskap-platforms, sowel as sommige SMS-dienste in Mongolië vir ongeveer 'n maand afgeskakel nadat geweld losgebars het weens 'n Mongoolse herder wat vermoor is.[459]

- Vroeg in 2012 het erge binnegevegte in die Sjinese Kommunistiese party plaasgevind. Die stad Chongqing se polisiehoof het gepoog om na die weste oor te loop, en gedurende hierdie tyd is verskeie

454 MacKinnon *Journal of Democracy* 40.

455 MacKinnon *Journal of Democracy* 40.

456 MacKinnon *Journal of Democracy* 40; Kelly, Cook en Truong (red) *Freedom on the Net 2015* 194.

457 MacKinnon *Journal of Democracy* 40.

458 Kelly en Cook (red) *Freedom on the Net 2011* 94; Committee to Protect Journalists "Read and Delete: How *Weibo*'s Censors Tackle Dissent and Free Speech" https://cpj.org/blog/2016/03/read-and-delete-how-weibos-censors-tackle-dissent-.php (besoek op 28 Maart 2016).

459 Kelly, Cook en Truong (red) *Freedom on the Net 2012* 129.

politici uit die kussings gelig. Op hierdie stadium was ál hierdie politici se name op die verbode lys, en het Internet-soektogte daarna geen resultate opgelewer nie.[460]

- In November 2014 het dit aan die lig gekom dat Sjina die grootste gebruiker van *Virtual Private Network*-produkte (hierna VPN) in die wêreld is. Hiervolgens word alle verkeer geënkripteer en geherroeteer om tegniese regulering te ontduik. Bykans 93 miljoen persone maak van hierdie tegnologie gebruik om die Kommunistiese Party se regulering te ontduik.[461]

- In Januarie 2015 het Sjinese owerhede aangekondig dat die nasionale moniteringstelsel opgegradeer word om verskeie internasionale *VPN*-verskaffers te blokkeer.[462] Dit was waarskynlik in reaksie op die November 2014 gewaarwording dat soveel Sjinese burgers van *VPN*-dienste gebruik maak.

Die insidente wat hierbo genoem word, is maar net 'n klein uittreksel van vele voorbeelde waar die Sjinese regering poog om direkte tegnologiese regulering te bewerkstellig.[463] Die punt wat egter gemaak word is dat die tweeledige strategie van wetgewing en direkte monitering 'n baie hoë vlak van sukses teweeg gebring het. [464]

460 Kelly, Cook en Truong (red) *Freedom on the Net 2012* 136.

461 Kelly, Cook en Truong (red) *Freedom on the Net 2015* 196; Global Web Index "90 Million VPN Users in China Have Accessed Restricted Social Networks" http://www.globalwebindex.net/blog/vpn-in-china (besoek op 24 Maart 2016).

462 Kelly, Cook en Truong (red) *Freedom on the Net 2015* 197.

463 Vir volledige lyste van Internet-sensorskap in Sjina, sien: China Internet Network Information Center "The Internet Timeline of China 2004–2006" http://www1.cnnic.cn/IDR/hlwfzdsj/201209/t20120904_36017.htm (besoek op 23 Maart 2016); China Internet Network Information Center "The Internet Timeline of China (2007)" http://www1.cnnic.cn/IDR/hlwfzdsj/201209/t20120904_36018.htm (besoek op 23 Maart 2016); China Internet Network Information Center "The Internet Timeline of China (2009)" http://www1.cnnic.cn/IDR/hlwfzdsj/201209/t20120904_36020.htm (besoek op 23 Maart 2016); Kelly en Cook (red) *Freedom on the Net 2011* 88–108; Kelly, Cook en Truong (red) *Freedom on the Net 2012* 126–151; Kelly S en Truong M (red) *Freedom on the Net 2013* (2013) 181–214; Kelly S en Truong M (red) *Freedom on the Net 2014* (2014) 191–215; Kelly, Cook en Truong (red) *Freedom on the Net 2015* 190–213.

464 Hierdie sukses is baie duidelik wanneer daar besef word hoe die Sjinese regering geslaag het om Sjinese burgers amper alles op hul eie intranet in Sjinees te gee wat in die Weste beskikbaar is. Alhoewel *YouTube*

6.4.2.4.6 Die Tweede Wêreld Internet-konferensie

'n Gepaste wyse om die bespreking van Sjina se Internetreguleringspogings af te sluit is die verwysing na die Tweede Wêreld Internet-konferensie wat in Desember 2015 in Sjina gehou is.[465] Ten spyte daarvan dat verskeie menseregtegroepe versoek het dat hierdie jaarlikse konferensie geboikot word, is dit iets waarvan deeglik kennis geneem moet word.[466] In die konteks van Sjina is dit so belangrik dat die Sjinese president, Xi Jinping sélf in 2015 die hoof spreker was.[467] Sy toespraak het heelwat lig gewerp op wat Sjina se planne vir hulle intranet én die groter Internet is.[468]

Die belangrikste hiervan is dat president Jinping 'n nuwe konsep voorgehou het dat nasies van die wêreld mekaar se kubersoewereiniteit — of cyber sovereignty — moet respekteer.[469] Om dit te wettig hou hy die

byvoorbeeld in Sjina verbied word, is daar die Sjinese ekwivalent *You Ku* en *iQiyi*; *Google* is sedert 2010 nie meer in Sjina aanwesig nie (Quelch J en Jocz K E *Google in China* (2010) 1), maar die gewilde *Baidu* het vinnig sy plek ingeneem, en *Facebook* en *Twitter* is eweneens nie in Sjina beskikbaar nie — maar *Sina Weibo* het beide hierdie organisasies se plek ingeneem. Daar is as't ware geen rede vir 'n Sjinese burger om buite die skynbare "veiligheid" van die Sjinese intranet te gaan nie. (Sien Tsui 2003 *China Information* 65 wat op 72 daarvan melding maak dat die Sjinese bevolking die Sjinese afskeiding van die groter Internet beskou as 'n "safe sandbox environment".) Die enigste probleem (beskou vanuit 'n westerse perspektief) is dat daar nie persvryheid in Sjina is nie, maar dit is iets wat die meeste Sjinese burgers (wat meestal a-polities is) nie veel pla nie (Wang S S en Hong J "Discourse Behind the Forbidden Realm: Internet Surveillance and its Implications on China's Blogosphere" 2009 *Telematics and Informatics* 67 76).

465 World Internet Conference — Wuzhen Summit "An Interconnected World Shared and Governed by All" http://www.wicwuzhen.cn/english/ (besoek op 26 Maart 2016); World Internet Conference — Wuzhen Summit "An Interconnected World Shared and Governed by All" http://www.wuzhenwic.org/ (besoek op 26 Maart 2016).

466 Groepe soos Amnesty International en Reporters without Borders het versoek dat hierdie konferensie geboikot moet word. Dit wil voorkom asof daar nie aan hierdie versoek gehoor gegee is nie, aangesien groot maatskappye soos onder andere *Microsoft, Facebook*, *IBM* en *Netflix* almal die konferensie bygewoon het. Carsten P "China Calls for Internet Front to Fight Hacking, Cyber 'Arms Race'" http://www.reuters.com/article/us-china-internet-idUSKBN0TZ09920151216 (besoek op 26 Maart 2016).

467 Griffiths J "Chinese President Xi Jinping: Hands Off Our Internet" http://edition.cnn.com/2015/12/15/asia/wuzhen-china-internet-xi-jinping (besoek op 26 Maart 2016).

468 Die volledige Engelse teks van Xi Jinping se toespraak is beskikbaar by: Ministry of Foreign Affairs of the People's Republic of China "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference" http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml (besoek op 26 Maart 2016).

469 Ministry of Foreign Affairs of the People's Republic of China "Remarks by H.E. Xi Jinping President of

Handves van die Verenigde Nasies[470] voor waar daar in artikels 2(1) en 78 staan dat lande van die wêreld se verhouding op wedersydse respek vir soewereine gelykheid, of "sovereign equality" sal geskied. Elke land het aldus Jinping 'n reg om sy eie kubersoewereiniteit uit te oefen, en hy stel dit so:

> We should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries' national security.[471]

Hierdie stelling is baie interessant aangesien dit 'n verskeidenheid aspekte aanspreek wat Sjina se strategie van Internetregulering aandui. In die eerste plek bevestig dit Sjina se siening is dat "hulle" intranet onafhanklik van die Internet is. Dit is iets waarna daar reeds sydelings in afdeling 6.4.2.2.1 verwys is, en wat reeds in die 1996 MCI[472] voorkom. Sjina huldig die mening dat elke staat se "intranet" — of eie stukkie van die Internet — iets is waaroor daar sélf besluit kan word aangesien dit deel vorm van die betrokke staat se soewereiniteit. Jinping gaan selfs sover deur 'n nuwe term daarvoor te skep — *cyber sovereignty.*

Jinping noem verder wat hy onder hierdie nuwe term van hom verstaan: dit behels dat elke staat uitsluitlik die gesag het om oor sy eie intranet-*ontwikkeling* te besluit, *regulering* en *openbare beleide* vas te stel, en op *gelyke voet op internasionale vlak daaroor te onderhandel.* Laasgenoemde

the People's Republic of China At the Opening Ceremony of the Second World Internet Conference" http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml (besoek op 26 Maart 2016); Lindsay J R, Cheung T M en Reveron D S *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (2015) 132 en Jensen E T "Cyber Sovereignty: The Way Ahead" 2015 *Texas International Law Journal* 273 276 vir meer oor "cyber sovereignty".

470 United Nations Treaty Collection "Charter of the United Nations" https://treaties.un.org/doc/publication/ctc/uncharter.pdf (besoek op 26 Maart 2016).

471 Ministry of Foreign Affairs of the People's Republic of China "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference" http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml (besoek op 26 Maart 2016) asook Griffiths J "Chinese President Xi Jinping: Hands off our Internet" http://edition.cnn.com/2015/12/15/asia/wuzhen-china-internet-xi-jinping/ (besoek op 26 Maart 2016).

472 Afd 6.4.2.2.1.

is 'n duidelike boodskap aan die VSA dat Sjina geensins die *status quo* van Internetregulering aanvaar nie. In die eerste plek het die VSA steeds beheer oor die basis-DNS, ten spyte daarvan dat die skyn bestaan dat dit onder ICANN-bestuur word.[473] In die tweede plek het die Snowden-spioenasieskandaal[474] duidelik aangetoon in watter mate die VSA en die "Five Eyes"[475] die Internet gebruik om internasionale spioenasie te verrig. Volgens hierdie stelling beskou Jinping sulke optrede as "conniv(ing)" en ondermyning van ander state se nasionale sekuriteit.[476]

Jinping het ook duidelik aangetoon hoe Sjina se toekomstige regulering van sy intranet sal ontvou. 'n "Internet-Plus"-plan is huidig besig om uitgerol te word, en dit behels om 'n "digitale Sjina" te bou wat Internet toegang vir almal te verseker en sodoende die krimpende Sjinese ekonomie te stimuleer.[477] Plaaslike Internet-besighede sal versterk word, en daar is veral 'n groot beweging om Sjina se afhanklikheid van buitelandse invoere en -besighede te beperk. Op hierdie vlak het Sjina reeds daad by die woord gevoeg met die kontroversiële beleid om vanaf 10 Maart 2016 *alle* buitelandse nuusagentskappe binne Sjina te verbied.[478] Wat die gevolg van

473 Afd 2.3.4en 3.4.2.

474 Sien afd 5.3.2.4 en 6.4.1.5.2 asook Farrell H en Finnemore M "The End of Hypocrisy: American Foreign Policy in the Age of Leaks" 2013 *Foreign Aff*airs 22 22 vir meer inligting oor die Snowden-spioenasieskandaal.

475 Die "Five Eyes" het sy oorsprong in die tweede wêreldoorlog waar die VSA en Brittanje 'n geheime verdrag gesluit het om intelligensie onder mekaar uit te ruil. Hierdie verdrag het later bekend gestaan as die *UKUSA-agreement*. Dit is in 1955 uitgebrei om Australië, Kanada en Nieu-Zeeland in te sluit, en is dus vandag die grootste intelligensiesamewerkingsooreenkoms in die Engelsprekende wêreld. Dixon P *Surveillance in America: An Encyclopedia of History, Politics, and the Law* (2016) 171 meld: "Many of the documents released by Snowden showed the extent to which the Five Eyes members routinely shared sensitive, top secret surveillance intelligence with one another. Since then, officials familiar with the Five Eyes operations have come forward to defend the program's value and practices. "The benefits of membership are immense, say intelligence experts"".

476 Sien die laaste stelling van die aanhaling direk hierbo.

477 Ministry of Foreign Affairs of the People's Republic of China "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference" http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml (besoek op 26 Maart 2016). Sien ook IBP.Inc *Macao Information Strategy, Internet and E-Commerce Development Handbook — Strategic Information, Programs, Regulations* (2015) 43 waar die "Internet Plus"-plan kortliks verduidelik word as: "Apart from Chinese government's goal of upgrading China into a 'powerful industrial country', the 'Internet Plus' strategy will, most importantly, produce new economic forms and create suitable environment for the general public to make innovations or start their own business".

478 Internasionale nuusagentskappe mag slegs nuus in Sjina verskaf indien hulle saam met

hierdie nuwe regulasie is, is nog nie duidelik nie.

Die Internet-Plus plan het ook ten doel om Sjina se sekuriteit van hulle intranet te verskerp teen virusse en ander aanvalle wat mag voorkom,[479] en interessant genoeg sal dit die gevolg hê dat hulle baie maklik geïsoleer kan word indien 'n globale vergiftiging van die basis-DNS sou voorkom.[480] In so 'n geval sal Sjina bykans onaangeraak wees en hulle Internetdienste kan voortsit sonder enige probleme, terwyl dit verreikende gevolge vir meeste ander wêreldlande sou inhou.

Die laaste punt van Jinping se toespraak wat hier relevant is, is dat Sjina sal streef om 'n meer gelyke speelveld in die Internetregulering-sfeer te skep. Hy sê:

> There should be no unilateralism. Decisions should not be made with one party calling the shots or only a few parties discussing among themselves. All countries should step up communication and exchange, improve dialogue and consultation mechanism on cyberspace, and study and formulate global Internet governance rules, so that the global Internet governance system becomes more fair and reasonable and reflects in a more balanced way the aspiration and interests of the majority of countries.[481]

'n staats-geregistreerde nuusagentskap saamwerk. Li D "The Expanding Great Firewall of China: A New Rule Banning All Foreign Media from Publishing Online Goes Live Today" http://www.usnews.com/news/best-countries/articles/2016-03-10/the-expanding-great-firewall-of-china (besoek op 26 Maart 2016); Quartz "Beijing is Banning All Foreign Media From Publishing Online in China" http://qz.com/620076/beijing-is-banning-all-foreign-media-from-publishing-online-in-china/ (besoek op 26 Maart 2016).

479 The Diplomat "'Internet Plus' and the Salvation of China's Rural Economy" http://thediplomat.com/2015/07/internet-plus-and-the-salvation-of-chinas-rural-economy/ (besoek op 28 Maart 2016).

480 Virgiftiging van die basis-DNS, oftewel "DNS-poisoning" in Engels, word treffend in Steward J M, Chapple M en Gibson *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide* (2015) 543 beskryf as: "DNS poisoning occurs when an attacker alters the domain-name-to-IP-address mappings in a DNS system to redirect traffic to a rogue system or to simply perform a denial-of-service against a system".

481 Ministry of Foreign Affairs of the People's Republic of China "Remarks by H E Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference" http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml (besoek op 26 Maart 2016).

6.4.2.5 Samevatting

Die regulering van die Sjinese intranet is die gesofistikeerdste in die hele wêreld. Sedert Sjina se skakeling met die groter Internet was die Sjinese regering se uitgangspunt altyd om nie die groter Internet ongekwalifiseerd toe te laat in die deursnee Sjinese burger se huis nie.[482] Hierdie isolering het relatief vreedsaam geskied, omdat die taal- en alfabet faktor altyd 'n probleem vir die deursnee Sjinese persoon was, wat in elk geval nie Engels magtig was nie.[483]

Die afskeiding van die Internet het in drie fases plaasgevind.[484] Die eerste was tussen 1994 en 1999, waartydens die groter reguleringsisteem in 'n verskeidenheid regulasies tot stand gebring is. Slegs die belangrikstes hiervan is bespreek.[485] Die eerste hiervan was die MCI, en daar is aangetoon hoe die Sjinese regering reeds vanuit die staanspoor besluit het om die Sjinese intranet as 'n afsonderlike deel van die Internet te ontwikkel en te reguleer.[486]

Die PINN het 'n lys bevat van sekere gedrag wat op die Sjinese intranet (asook die groter Internet) verbode is.[487] Ander regulasies het hierdie trant voortgesit deur soortgelyke — en dikwels meer uitgebreide — lyste te bevat.[488]

Die MCI het Sjina se reguleringsisteem versterk deur sekere handelinge, soos teëspraak teen die regerende party se beleide, te verbied. Die trant van hierdie regulasies is algemene stellings wat regonsekerheid teweeg bring.

Die tweede fase van Internetregulering, wat tussen 2000 en 2003

---

482 Afd 6.4.2.

483 Afd 6.4.2.

484 Afd 6.4.2.2.1.

485 Die *Temporary Regulation for the Management of Computer Information Network International Connection, Measures for Security Protection Administration of the International Networking of Computer Information Networks* en die *Security Management Procedures in Internet Accessing* is as voorbeelde van die eerste fase van regulering bespreek. Afd 6.4.2.2.1.

486 Afd 6.4.2.2.1.

487 Afd 6.4.2.2.2.

488 Afd 6.4.2.2.3 ev.

geskied het, het gepaard gegaan met regulasies wat spesifieke Internet-industrieë en -besighede geteiken het om ongewenste gedrag te beperk.[489] Die *Telecommunications Regulations of the People's Republic of China,* en *Measures for Managing the Internet Information Services,* as voorbeelde van hierdie fase se regulasies bespreek.[490] Nie-nakoming van gelyste gedrag word gestraf met de-registrasie of boetes. Gedwonge selfregulering word dus van hierdie industrieë en besighede vereis. Dit het ook tot gevolg dat gedwonge selfregulering van gebruikers geverg word, aangesien hulle eweneens met opskorting van Internetdienste of boetes gedreig word indien ongewenste gedrag geopenbaar word.[491]

Die derde fase van Internetregulering in Sjina is vandag steeds aan die gang. Dit behels verskerpte optrede teen besighede en gebruikers, asook nuut-ontwikkelde tegnologiese maatreëls wat ingestel word om regulering te verseker.[492] Die *Provisions for the Administration of Internet News Information Services,*[493] *Measures for the Administration of the Publication of Audio-Visual Programs through the Internet or other Information Network,*[494] *Measures for the Administrative Protection of Internet Copyright,*[495] en *China Internet Domain Name Regulations,*[496] is as voorbeelde van hierdie fase se regulasies bespreek. Die algemene trant is dat die Sjinese intranet al hoe fyner gereguleer word, byvoorbeeld Internet-nuusdienste wat gemoniteer word,[497] maatskappye wat oudio-visuele inligting oor die Internet versprei, geregistreer moet word,[498] ISP's vir kopieregskending aanspreeklik gehou kan word,[499] en verskaffers van basisnaambedieners

489 Afd 6.4.2.3.

490 Afd 6.4.2.3.1 en 6.4.2.3.2.

491 Afd 6.4.2.3.1 en 6.4.2.3.2.

492 Afd 6.4.2.4.

493 Afd *6.4.2.4.1.*

494 Afd *6.4.2.4.2.*

495 Afd *6.4.2.4.3.*

496 Afd *6.4.2.4.4.*

497 Afd *6.4.2.4.1.*

498 Afd *6.4.2.4.2.*

499 Afd *6.4.2.4.3.*

streng gereguleer word.[500]

Die derde fase van regulering in Sjina gaan ook gepaard met direkte tegnologiese regulering, en dit is in afdeling 6.4.2.4.5 aangespreek. Besighede en individue word nou direk geteiken, en etlike voorbeelde hiervan is genoem. Die inkorting van Internetdienste in spesifieke geografiese gebiede, terwyl ander gebiede nie geraak word nie, is die algemene reël.[501]

Al hierdie maatreëls val binne die groter plan van die Sjinese regering, soos in afdeling 6.4.2.4.6 bespreek is toe president Xi Jinping se toekomsplanne vir die Sjinese intranet uiteengesit is. Sjina se strukturering van sy intranet is van so 'n aard dat dit al hoe makliker word om sy intranet te beskerm teen gevare van die groter Internet, en dit beteken dat kuber-soewereiniteit 'n al hoe groter realiteit word. Sjina gaan ongetwyfeld in die toekoms 'n groot rolspeler in die Internetreguleringsdebat word, ten spyte van teëkanting wat die westerse wêreld mag ophaal. Dit wil voorkom asof die nuwe strukturering van die Internet mag neig na kuber-soewereiniteit.[502]

Sjina is 'n voorbeeld van buitengewone intranet-regulering. Die hantering van ISP-aanspreeklikheid in die Europese Unie word vervolgens bespreek, en soos spoedig sal blyk, word dit heel anders as in Sjina hanteer.

6.4.3 Die Europese Unie

6.4.3.1 Totstandkoming

Ná die tweede wêreldoorlog was sommige Europese lande[503] van mening dat die gemeenskaplike gebruik van steenkool en staal die beste manier sou wees om enige verdere oorloë te vermy.[504] Dit het aanleiding gegee tot die

500 Afd *6.4.2.4.4.*

501 Afd 6.4.2.4.5.

502 Afd 6.4.2.4.6.

503 Hierdie lande was Frankryk, Wes-Duitsland, Italië, Nederland, België en Luxemburg. European Union "The Schuman Declaration — 9 May 1950" http://europa.eu/about-eu/basic-information/symbols/europe-day/schuman-declaration/index_en.htm (besoek op 16 Februarie 2016).

504 Klaarblyklik was die siening dat indien Frankryk en Duitsland hulle steenkool- en staalproduksie sou saamspan, die waarskylikhioed van oorlog "becomes not merely unthinkable, but materially

Schuman-deklarasie van 1950 waar die steenkool- en staalindustrieë van Frankryk en Duitsland verenig is.[505] Hierdie eerste stap was die voorloper tot die skepping van die Europese Unie.[506]

Die tweede stap na 'n Europese eenheid het gekom in die vorm van die Verdrag van Rome, wat in 1957 geteken is.[507] Dit het 'n Europese Ekonomiese Gemeenskap geskep,[508] en België, Frankryk, Italië, Luxemburg en Nederland was ondertekenaars daarvan.[509] Die derde — en belangrikste — stap na 'n Europese Unie het gekom in die totstandkoming van die verdrag van Maastricht wat in 1992 gesluit is.[510] Hiermee is die Europese Unie formeel geskep.

Die Europese Unie het sewe eenhede wat die regulering daarvan beheer,[511] waarvan die Europese parlement en Geregshof van die Europese Unie die belangrikste regsorgane is. Dit sal hieronder in meer besonderhede bespreek word.

Volgens artikel 288 van die Verdrag van die Werking van die Europese

impossible" — aldus die woorde van die Schuman Declarasie van 9 Mei 1950. Sien vn 503.

505 Vn 503; Craig P en De Búrca G *EU Law: Text, Cases, and Materials* (2011) 5.

506 Die Schuman-deklarasie maak dit duidelik dat die doel van hierdie stap 'n verenigde Europa is:

> The pooling of coal and steel production should immediately provide for the setting up of common foundations for economic development as a first step in the *federation of Europe*, and will change the destinies of those regions which have long been devoted to the manufacture of munitions of war, of which they have been the most constant victims.
>
> The setting up of this powerful productive unit, open to all countries willing to take part and bound ultimately to provide all the member countries with the basic elements of industrial production on the same terms, will lay a true foundation for their economic unification. (My kursivering). Vn 503.

507 Nsour M F *Rethinking the World Trade Order: Towards a Better Legal Understanding of the Role of Regionalism in the Multilateral Trade Regime* (2010) 189.

508 Volgens hierdie verdrag het lidlande ooreengekom om alle oorgrens-tariewe vir 'n periode van twaalf jaar op te skort. Nsour *Rethinking the World Trade Order* 189.

509 Nsour *Rethinking the World Trade Order* 189 vn 1032.

510 Folsom R, Lake R B en Nanda V P *European Union Law After Maastricht: Practical Guide for Lawyers Outside the Common Market* (1996) 600. Die volle teks van die Maastricht-verdrag is beskikbaar by Council of the European Communities "Treaty on European Union" http://europa.eu/eu-law/decision-making/treaties/pdf/treaty_on_european_union/treaty_on_european_union_en.pdf (besoek op 16 Februarie 2016).

511 Die sewe organe is die (1) Europese parlement, (2) Raad van die Europese Unie, (3) Europese Kommissie, (4) Europese raad (5) Europese sentrale bank, (6) Geregshof van die Europese Unie, en (7) Europese hof van Ouditeure. Wikipedia "European Union" https://en.wikipedia.org/wiki/European_Union#Governance (besoek op 16 Februarie 2016).

Unie mag die organe van die Unie regulasies, direktiewe, besluite, aanbevelings en opinies lewer.[512] Die regskrag van elkeen word soos volg verduidelik:

> A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States.
>
> A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods.
>
> A decision shall be binding in its entirety. A decision which specifies those to whom it is addressed shall be binding only on them.
>
> Recommendations and opinions shall have no binding force.[513]

6.4.3.2 Aanspreeklikheid van Internet-diensverskaffers

Die aanspreeklikheid van Internet-diensverskaffers word gereguleer deur die *Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market*[514] (hierna die EU-direktief). Hierdie Europese direktief is in die jaar 2000 uitgevaardig om die ongelykhede in hulle onderskeie lande se wetgewing aan te spreek.[515]

Die algemene beginsels rakende die aanspreeklik van ISP's vir inhoud wat op hul bedieners geplaas word, word in artikels 12–15 uiteengesit.[516]

---

512 Consolidated Version of the Treaty on the Functioning of the European Union (2007), art 288. Die volteks van die verdrag is beskikbaar by Wikisource "Consolidated Version of the Treaty on the Functioning of the European Union (2007)" https://en.wikisource.org/wiki/Consolidated_version_of_the_Treaty_on_the_Functioning_of_the_European_Union (besoek op 16 Februarie 2016).

513 Art 288.

514 Direktief 2000/31/EC van die Europese Parlement en die Raad van 8 Junie 2000 oor "Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market" (Directive on electronic commerce) 2000 OJ L178/1. Lodder A R en Van der Meulen N S "Discussion of Dutch Pirate Bay Case Law and Introducing Principles on Directness, Effectiveness, Costs, Relevance, and Time" 2012 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 130 132 verduidelik dat hierdie direktief geformuleer is om die kernpilaar van e-handel in die Europese Unie te vorm.

515 Par (40) van die inleiding tot die Direktief 2000/31/EC stel dit duidelik: "Both existing and emerging disparities in Member States' legislation and case-law concerning liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition".

516 Baistrocchi P A "Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce" 2002 *Santa Clara High Technology Law Journal* 111 118.

Die algemene reël word in artikel 15 uitgestippel, en behels eenvoudig dat lidlande nie 'n algemene plig om te moniteer op ISP's sal plaas nie.[517] Dit beteken dus dat wanneer 'n ISP aan die vereistes van artikels 12–14 voldoen, dit aanspreeklikheid vir onwettige optrede kan vryspring.

Vervolgens word die vereistes van artikels 12–14 bespreek.[518]

Die EU-direktief onderskei tussen drie "soorte" Internet-diensverskaffers, te wete daardie diensverskaffers wat bloot 'n geleibuis is wat data déúr hulle netwerke stuur sonder om dit te monitor,[519] diegene wat data tydelik berg voordat dit aangestuur word,[520] en dié wat gasheer tot data is.[521] Die onderskeid is belangrik omdat die verskillende diensverskaffers aan verskillende vereistes moet voldoen om op nie-aanspreeklikheid staat te kan maak.[522]

Volgens artikel 12 van die EU-Direktief sal 'n diensverskaffer wat bloot as 'n geleibuis dien, nie aanspreeklik gehou kan word vir enige data wat deur sy netwerk beweeg nie, mits hy aan die volgende drie vereistes voldoen — die diensverskaffer mag nie:

(a) die oordrag inisieer nie;

(b) die ontvanger van die oordrag kies nie; en

(c) mag nie die inligting wat in die oordrag vervat is, kies of verander nie.[523]

Dit is duidelik dat hierdie drie vereistes daarop geskoei is om te verseker dat die "blote geleibuis"-diensverskaffer juis dít is — slegs 'n geleibuis

---

517 Baistrocchi 2002 *Santa Clara High Technology Law Journal* 126.

518 Die EU-direktief is vanselfsprekend ook op sellulêre kommunikasie van toepassing. Vir 'n volledige bespreking ten aansien hiervan, sien Jakobsen S S "Mobile Commerce and ISP Liability in the EU" 2010 19 *International Journal of Law and Information Technology* 29 33.

519 Die Engelse term "mere conduit" word hier bedoel. Sien art 12 van die EU Direktief 2000/31/EC.

520 Die Engelse term "caching" word hier bedoel. Sien art 13 van die EU Direktief 2000/31/EC, asook Baistrocchi 2002 *Santa Clara High Technology Law Journal* 118.

521 Die Engelse term "hosting" word hier bedoel. Sien art 14 van die EU Direktief 2000/31/EC. Sien ook Kryczka K "Ready to Join the EU Information Society — Implementation of E-Commerce Directive 2000/31/EC in the EU Acceding Countries — The Example of Poland" 2004 *International Journal of Law and Information Technology* 55 65 vir 'n voorbeeld van 'n lidland (in hierdie geval Poland) wat die EU-direktief net so in hul eie wetgewing vervat het.

522 Leistner M "Structural Aspects of Secondary (Provider) Liability in Europe" 2014 *Journal of Intellectual Property Law and Practice* 75 76.

523 Art 12(1)(a)–(c) van die Direktief.

wat op geen wyse die inligting verander nie, maar dit bloot deur sy rekenaarnetwerke roeteer.

Artikel 12(2) maak voorsiening dat die diensverskaffer wel vir ’n kortstondige tydperk die data op sy netwerk mag stoor, mits dit gedoen word in die proses waar die data geroeteer word.[524]

Artikel 13 hanteer die geval waar diensverskaffers data tydelik in ’n kasgeheue berg. Dit kan met die eerste oogopslag met artikel 12(2) (hierbo) verwar word, maar wanneer artikel 13 in meer besonderhede bestudeer word, word die onderskeid duidelik. Artikel 12(2) hanteer die tydelike berging van data met die uitsluitlike doel om dit verder aan te stuur, en hierdie berging mag dalk vir ’n paar sekondes duur. In teenstelling hiermee het artikel 13 ten doel om data te hanteer wat vir ’n langer tyd geberg word. ’n Voorbeeld hiervan is die algemene gebruik van diensverskaffers om gewilde webwerwe in hul eie kasgeheue te berg om dit vinniger aan intekenaars aan te bied. Die gewilde webwerf se blad word elke paar uur uit die kasgeheue van die diensverskaffer verwyder en met ’n nuwe weergawe vervang.

Artikel 13 lê meer reëls neer vir diensverskaffers wat van ’n kasgeheue gebruik maak. Dit is:

(a) die verskaffer mag nie die inligting verander nie;

(b) die verskaffer moet voldoen aan vereistes tot toegang tot die inligting;[525]

(c) die verskaffer moet aan reëls oor die opdatering van die inligting voldoen op ’n wyse wat deur die betrokke industrie in gebruik is,

(d) die verskaffer mag nie inmeng met die wettige gebruik van tegnologie

---

524 Art 12(2) maak bv melding van “transient storage” en “in so far as this takes place for the sole purpose of carrying out the transmission in the communication network”. Blote tydelike berging is dus hier in gedagte.

525 Hierdie vereiste klink aanvanklik vreemd op die oor, maar daar word bedoel dat die vereistes wat vir die oorspronklike webblad voorgeskryf word, ook deur die diensverskaffer nagekom moet word. As die webblad wat in die kasgeheue van die diensverskaffer is, byvoorbeeld slegs vir betalende intekenaars beskikbaar is, mag die diensverskaffer nie die dokument in die kasgeheue gratis beskikbaar stel nie. Lodder H W K en Kaspersen A R *e-Directives: Guide to European Union Law on e-Commerce: Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection* (2002) 88.

soos gebruik in die betrokke industrie om data oor die gebruik van die inligting te bekom nie; en[526]

(e) die verskaffer moet vinnig optree om toegang tot inligting te beperk indien dit nie meer beskikbaar is op die oorspronklike netwerk nie, of indien 'n hof of administratiewe gesag sodanige verwydering van die inligting beveel het.[527]

Ál hierdie vereistes het ten doel om die kopie van die inligting in die ISP se kasgeheue op datum te hou. Soos in die voorbeelde hierbo[528] verduidelik, is die inligting in die ISP se kasgeheue altyd ouer as die nuwe opgedateerde inligting van die webwerf self, en het die vyf vereistes hierbo genoem ten doel om die industrie se beste praktyke ten aansien van opdatering van kasgeheue tot uitvoering te bring. Indien die kasgeheue dus op datum bly, kan nie-aanspreeklikheid op dieselfde wyse volg as wat vir "gewone" diensverskaffers geld.

Artikel 14 van die EU-direktief hanteer die derde "soort" diensverskaffer, naamlik gevalle waar 'n ISP as 'n gasheer vir die inligting optree. Hier word die ISP eweneens vrygestel van aanspreeklikheid, mits hy aan twee vereistes voldoen, te wete:

(a) die verskaffer nie werklike kennis van onwettige aktiwiteite of inligting het nie, en met betrekking tot eise vir skadevergoeding, nie bewus is van enige feite of omstandighede waaruit die onwettige aktiwiteit of inligting spruit nie, of [529]

(b) op die verkryging van sodanige kennis of bewusmaking daarvan, vinnig op te tree om toegang tot die inligting te verwyder of te deaktiveer.[530]

Lodder en Kaspersen meen dat artikel 14(a) daarop dui dat 'n ISP geen

---

526 'n Voorbeeld hiervan is waar webwerwe sekere tellerprogramme gebruik om te bepaal hoeveel gebruikers hulle webwerwe besoek het, en watter webblaaie die meeste gelees is. Soms beïnvloed die hoeveelheid besoeke ("hits") die betrokke webblad se inkomste uit advertensies, en diensverskaffers wat webblaaie in hul kasgeheue berg moet sorg dat die werking van die tellerprogramme op die oorspronklike webblaaie nie beïnvloed word nie. Lodder en Kaspersen *e-Directives* 88.

527 Art 13(1)(a)–(e) van die Direktief.

528 Vn 525 en 526 direk hierbo.

529 Art 14(1)(a) van die Direktief.

530 Art 14(1)(b) van die Direktief.

aanspraak op nie-aanspreeklikheid kan maak in siviele en strafregtelike sake wanneer hy werklike kennis van die onwettige aktiwiteite het nie.[531] Daar word aangevoer dat hierdie afleiding duidelik te vinde is in die teks, veral waar dit met siviele sake te doen het. Om die artikel egter sonder meer op die Strafreg van toepassing te maak, mag dalk effe te ver gaan. Die EU-direktief bepaal duidelik in paragraaf 26 van die aanhef dat elke lidland by magte is om te bepaal of hierdie direktief ook ten opsigte van strafsake sal geld.[532] Dus sal die werking van artikel 14 van land tot land verskil in die mate waarop die Strafreg toepassing vind.[533]

6.4.3.3 Regspraak

Bogenoemde bepalings het sedert hul ontstaan tot verskeie interessante hofsake aanleiding gegee. Die eerste hiervan is die saak van *Google France v Louis Vuitton*.[534] Die Geregshof van die Europese Unie het daar beslis dat

531 Lodder en Kaspersen *e-Directives* 88.

532 Die direktief bepaal in paragraaf 26 van die aanhef: "Member States, in conformity with conditions established in this Directive, may apply their national rules on criminal law and criminal proceedings with a view to taking all investigative and other measures necessary for the detection and prosecution of criminal offences, without there being a need to notify such measures to the Commission".

533 Die doel van hierdie afdeling is om aan te toon in watter wys die Europese Unie poog om diensverskaffers te reguleer. In hierdie konteks is dit sinvol om die generiese bepalings van die EU-direktief voor te hou. Wanneer spesifieke lidlande se wetgewing beoordeel word, kan regsaanspreeklikheid van ISP's ongelukkig baie vinnig uitkring tot 'n bespreking wat nie in hierdie studie hanteer kan word nie. ISP-aanspreeklikheid dek areas soos aanlyn-laster, kopieregskending en die gebruik en deelname aan sogenaamde "peer-to-peer" netwerke. (Vir 'n volledige bespreking van laasgenoemde sien Conradi M, Baker en McKenzie "ISP Liability — UK: Liability of an ISP for Allowing Access to File Sharing Networks" 2003 *Computer Law and Security Review* 289 289–294).

Al hierdie areas is wyd en uiteenlopend, en ten spyte daarvan dat dit insny op die onderwerp van regsaanspreeklikheid van Internet-diensverskaffers, kan dit nie aangespreek word nie omdat dit eerder op die plaaslike regsfront aanwending geniet, en nie soseer op die globale, internasionaalregtelike vlak nie.

Om dit te illustreer kan die Britse "Defamation Act" van 2013 as voorbeeld gebruik word. Hierdie wetgewing het verreikende gevolge op die Britse lasterreg gehad, aangesien dit bepaal dat 'n Engelse (en Walliese) hof nie meer jurisdiksie het ten aansien van lastersake teen derde partye (soos ISP's) in gevalle waar dit moontlik en redelikerwys prakties is om die aksie teen die outeur, redakteur of uitgewer van die lasterlike uitsprake in te stel nie (art 10 van die wet). Die wetgewing bied beskerming aan ISP's in geval van lastersake in Engeland en Wallis, maar word nie in die hoofteks bespreek nie, aangesien dit slegs op laster van toepassing is, en nie die groter aangeleentheid van die aanspreeklikheid van diensverskaffers *per se* aanspreek nie.

534 *Google France SARL v Louis Vuitton Malletier SA* 2010 E C R I 2417 (2010).

kommersiële soekenjins, soos *Google*, nie op artikel 14 kan staat maak tensy hulle rol "neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores" is nie.[535] Dit bevestig die letter van die wet van artikel 14, naamlik dat die diensverskaffer nie werklike kennis van die misdryf moet hê nie, en dat hul spoedig sou optree om enige ongeruimdheid op te klaar. Op die feite het die hof beslis dat *Google* wél aan artikel 14 se twee subvereistes voldoen.[536]

L'Oreal v eBay[537] het die twee subvereistes van artikel 14 bevestig, maar dit getemper in die konteks van handelsmerkskending. (By handelsmerke bestaan daar 'n regsplig op 'n lidland om handelsmerkhouers te beskerm.)[538] Die hof het genoem dat artikel 14 van die EU-direktief geïnterpreteer moet word dat die diensverskaffer nie 'n "aktiewe rol" moes gespeel het in die berging van die data nie — in so 'n geval sal die diensverskaffer wél op artikel 14 kan steun.[539]

Die Geregshof van die EU het in die uitspraak genoem dat Brittanje se hof, wat die saak na die EU-geregshof verwys het, sélf moet bepaal of *eBay* daarvan bewus was dat hy L'Oreal se handelsmerk skend. In die oorweging daarvan moet die hof *a quo* die vraag vra of 'n redelike ekonomiese operateur (diensverskaffer) die onwettige optrede raakgesien het, en in ooreenstemming met artikel 14(1)(b) van die direktief opgetree het.[540] Slegs

535 Par 114 van die uitspraak.

536 Par 115 van die uitspraak.

537 *L'Oreal v eBay* C-324/09.

538 Art 5(1)(a) van die Handelsmerkdirektief 95/2008 en art 9(1)(a) van die Handelsmerkregulasie 207/2009.

539 Par 6 van die uitspraak lees soos volg:

> Article 14(1) of Directive 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce") must be interpreted as applying to the operator of an online marketplace when that operator has not played an active role allowing it to have knowledge or control of the data stored.

540 Die hof bepaal:

> it is sufficient, in order for the provider of an information society service to be denied entitlement to the exemption from liability provided for in Article 14 of Directive 2000/31, for it to have been aware of facts or circumstances on the basis of which a *diligent economic operator should have identified the illegality in question* and acted in accordance with Article 14(1)(b) of Directive 2000/31. (My kursivering). Par 120 van die uitspraak.

dan sal nie-aanspreeklikheid ingevolge artikel 14 volg.

Hieruit blyk dit duidelik dat die L'Oreal uitspraak nie meer aan die eenvoudige letter van die wet voldoen nie. Daar bestaan nou 'n strenger vereiste dat die betrokke diensverskaffer se optrede gemeet word aan 'n "redelike diensverskaffer". Dit strook eenvoudig nie met die res van die direktief nie, want artikel 15 bepaal juis dat daar nie 'n algemene plig om te moniteer, bestaan nie.

Om sake in die EU verder te bemoeilik wil dit voorkom asof lidlande hul eie koers inslaan wanneer dit met die nie-aanspreeklikheid van Internet-diensverskaffers te make het. In die Britse saak *Tamiz v Google*[541] moes die hof beslis of *Google* aanspreeklik gehou kon word vir inhoud wat deur 'n derde party op sy Blogger-webtuiste geskep is. Nadat *Google* die klagte ontvang het, het dit binne drie dae die *blogger* versoek om die inligting te verwyder, maar dit is eers na 'n periode van vyf weke gedoen. In die Engelse hooggeregshof[542] het regter Eady *Google* se posisie vergelyk met "the owner of a wall which has been festooned overnight with defamatory graffiti". In so 'n posisie sou *Google* kon "acquire scaffolding and have it all deleted with whitewash", maar selfs as *Google* dit nie sou doen nie, kon dit nie die uitgewer (publisher) van die materiaal wees nie. *Google* se optrede is deur die regter as 'n blote passiewe rol beskou. Hiermee het die regter konsekwent opgetree aangesien hy in die saak van *Bunt v Tilley*[543] 'n soortgelyke uitspraak gemaak het dat die ISP "a degree of awareness or at least an assumption of general responsibility"[544] uitgeoefen het. Dus was die regter van mening dat 'n Internetdiensverskaffer geensins aanspreeklik gehou kan word vir inligting op sy bedieners as hy nie ten minste bewus was van die materiaal nie, en 'n algemene verantwoordelikheid vir die materiaal geneem het nie. In beide *Tamiz v Google* en *Bunt v Tilley* was regter Eady se

541 *Tamiz v Google Inc* 2013 E W C A Civ 68 2012 E W H C 449 (2013).

542 2012 E W H C 449 (QB) par 39.

543 2006 E W H C 407 (QB).

544 Par 22 van die uitspraak.

houding dat "an ISP who performs no more than a passive role in facilitating postings on the internet cannot be deemed to be a publisher at common law".[545]

Interessant genoeg is kennis van die sogenaamde lasterlike skrywe op die bedieners van die diensverskaffers verskillend in die twee sake. In die *Bunt*-saak was daar geen bewys dat die drie ISP-verweerders kennis van die gewraakte inligting gehad het nie. Regter Eady se uitspraak van "passiewe en onwetende diensverskaffers" was dus heeltemal gegrond in die *Bunt*-saak, maar nie in die *Tamiz*-saak nie. By laasgenoemde was *Google* vir bykans vyf weke bewus van die skynbaar-lasterlike pos.[546] Dit is daarom nie vreemd dat die *Tamiz*-saak op appèl geneem is nie.

Die Engelse hof van appèl[547] was van mening dat regter Eady gefouteer het: "In my view the judge was wrong to regard *Google* Inc's role in respect of Blogger blogs as a purely passive one and to attach the significance he did to the absence of any positive steps by *Google* Inc in relation to continued publication of the comments in issue."[548] Die hof gaan voort deur te verduidelik dat *Google* wél beheer het oor die *blogger* deur spasie op sy bediener beskikbaar te stel. Trouens, *Google* gebruik die *blogger* se webblad om sy eie advertensies te plaas, en dit maak hom 'n fasiliteerder van die publikasie van blogs.[549] Tóg het *Google* nie beheer oor die *inhoud* van die blog nie, en dit onderskei hom juis van 'n uitgewer (publisher): "It does not create the blogs or have any prior knowledge of, or effective control over, their content. It is not in a position comparable to that of the author or editor of a defamatory article".[550] Dit is dus interessant om op te merk dat die hof dieselfde gevolgtrekking ten opsigte van die saak maak, (en uiteindelik die appèl af te wys), maar dat die redenasie heeltemal verskillend is.

545 *Bunt v Tilley* par 36.

546 Die woord "pos" word gebruik vir die Engelse werkwoord "post".

547 *Tamiz v Google* 2013 E W C A Civ 68 par 51.

548 Par 23.

549 Par 25 van die uitspraak meld: "By the provision of that service *Google* Inc plainly facilitates publication of the blogs (including the comments posted on them)".

550 Par 25.

Daar word aangevoer dat die hof van appèl hierdie punt korrek bereg het. Regter Eady het wél gefouteer deur *Google* as 'n passiewe rolspeler te beskou, terwyl die hof van appèl daardie fout reggestel het.

Dit is egter nie die einde van die saak nie. Die aangeleentheid oor *Google* se versuim om op te tree nadat dit bewus geword het van die lasterlike spraak, moet bereg word. Regter Richards was nie beïndruk met regter Eady se analogie van die muur wat met graffiti vervuil is nie, en het gemeen die 1937-saak van *Byrne v Deane*[551] was meer gepas. In daardie saak is lasterlike stellings op 'n kennisgewingbord by die plaaslike gholfklub aangebring, en die eienaars en sekretaris van die gholfklub het geen poging aangewend om dit te verwyder nie, ten spyte daarvan dat hulle daarvan bewus was. Regter Richards kwoteer *Davison v Habeeb and Others,*[552] wat sê dat: "It might be seen as analogous to a gigantic noticeboard which is in [*Google* Inc's] control, in the sense that [*Google* Inc] provides the noticeboard for users to post their notices on, and it can take the notices down (like the club secretary in *Byrne v Deane* ...) if they are pointed out to it".[553] Dus is Regter Richards daarmee eens dat *Google* se Blogger-diens eintlik maar 'n reusagtige kennisgewingbord is, en dat dit lasterlike publikasies goedkeur indien dit bewus word daarvan, en niks doen om dit te verwyder nie — nes die geval in *Byrne v Deane*.

Die laaste — en waarskynlik die deurslaggewendste punt — wat regter Richards maak, het te doen met die aard van 'n "blog" op die Internet. Hy verduidelik dit so: "By the very nature of a blog, they will have been followed by numerous other comments in the chain and, whilst still accessible, will have receded into history."[554] Die skynbaar lasterlike uitlatings sou so vinnig deur ander inligting begrawe word, dat volgehoue publikasie daarvan op 'n *blog* onbeduidend en gering sou wees.[555] Gevolglik is die appèl van die hand

551 1937 1 KB 818.

552 2011 E W H C 3031 (QB).

553 Par 31 van die *Tamiz*-uitspraak.

554 Par 50.

555 "It follows, as the judge clearly had in mind, that any damage to the appellant's reputation arising

gewys.

Die appèlbeslissing in *Tamiz v Google* het in 2013 plaasgevind. In dieselfde jaar het die EU-geregshof 'n verreikende beslissing in *Delfi v Estonia*[556] gemaak wat lynreg teen die Britse *Tamiz*-appèlbeslissing ingaan. Delfi was 'n aanlyn-nuusverskaffer wat tot 330 nuusberigte per dag gepubliseer het.[557] Een berig het aangetoon hoe 'n maatskappy met die naam SLK van plan was om ysroetes, wat eilande in die winter met mekaar verbind het, met 'n ysbreker te breek en sodoende die publiek te forseer om van hulle eie veerbootdienste gebruik te maak. Delfi se nuusportaal het dit moontlik gemaak dat lesers hulle kommentaar op die berig kan lewer, en die negatiewe berig het hewige reaksie by lesers ontlok — soveel so dat sommige van die kommentaar lasterlik was. SLK het Delfi daarvan in kennis gestel dat daar lasterlike bewerings op die nuusportaal was, en het hulle op die koop toe daarvoor aanspreeklik gehou. Delfi het dadelik die kommentaar verwyder toe hulle daarvan bewus geword het, maar het geweier om die €32000 in skadevergoeding te betaal.

Die saak het in die hof gaan draai, en daar is beslis dat Delfi se nuusportaal nie binne die sfeer van artikel 14 van die EU-regulasies val nie. Die rede hiervoor is die eng wyse waarop die reg in Estonië Internet-diensverskaffers beoordeel. Die hof het genoem dat ten spyte daarvan dat die hoofberig nie lasterlik was nie, dit leser-kommentaar bevat het wat lasterlik was, en dat Delfi dus 'n uitgewer van die hele berig was. Gevolglik is Delfi aanspreeklik gehou.[558] Die Estonië-appèlhof het hiermee akkoord gegaan en die hof *a quo* se beslissing bevestig.[559]

Die saak is na die EU-geregshof geneem, en die nie-aanspreeklikheids-klousule van artikel 14 (soos hierbo bespreek in 6.4.3.2) is opgehaal. Delfi het

out of continued publication of the comments during that period will have been trivial; and in those circumstances the judge was right to consider that 'the game would not be worth the candle'". Par 50.

556 ECtHR 64659/09.

557 Par 11 van die *Delfi*-saak.

558 Par 26 en 27 van die EU-geregshof uitspraak.

559 Par 28 van die EU-geregshof uitspraak.

aangevoer dat as nuusportaal voldoen dit aan die vereistes van artikel 14, en gevolglik moet dit nie aanspreeklik gehou word vir die kommentaar wat lesers op die betrokke blad geplaas het nie. Die EU-geregshof se uitspraak was baie interessant deurdat dit die aard van die EU-direktief voor oë gehou het en beslis het dat dit (die EU-geregshof) nie by magte is om nasionale wetgewing te oorskadu nie. Gevolglik het die EU-geregshof die nou-interpretasie van die Estonië-appèlhof aanvaar dat Delfi 'n *uitgewer* was, en nie 'n *gasheer-diensverskaffer* soos wat die EU-direktief voor oë het nie.[560] Hierdie siening was die doodsteek vir Delfi se saak, want artikel 14 van die EU-direktief was nie op uitgewers nie, maar slegs op gasheer diensverskaffers van toepassing.

In die konteks van die Internasionale reg wil dit voorkom asof die *Delfi*-saak korrek bereg is. Die soewereiniteit van 'n staat en sy wette behoort die hoogste prioriteit te geniet, maar ongelukkig het dit in hierdie konteks tot 'n baie ongelukkige gevolg aanleiding gegee: die indruk word geskep dat diensverskaffers aanspreeklik gehou kan word vir die inligting wat gebruikers op hulle webwerwe plaas, en dit druis lynreg teen die EU-direktief se bepalings in.

Juis hierdie laaste punt het daartoe aanleiding gegee dat die *Delfi*-saak nie goed ontvang is nie. In Januarie 2014 het 69 Internetmediamaatskappye, soos onder andere *Google*, *Forbes*, *Reuters* en die *New York Times* 'n ope brief aan die president van die EU-geregshof gestuur waarin daar versoek word dat hy die saak op hersiening neem (volgens 'n aansoek wat die applikant *Delfi* aan die EU-geregshof gerig het).[561]

560 Par 65 van die uitspraak.

561 La Quadrature Du Net "Civil Society Calls on the ECHR's Grand Chamber to Overturn Delfi v Estonia Ruling" https://www.laquadrature.net/en/civil-society-calls-on-the-echrs-grand-chamber-to-overturn-delfi-v-estonia-ruling (besoek op 23 Februarie 2016).

6.4.3.4 Samevatting

Die aanspreeklikheid van Internet-diensverskaffers in die EU word gereguleer deur die *"Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market"*[562] Veral artikels 12–15 verduidelik hoe die aanspreeklikheid van Internet-diensverskaffers hanteer behoort te word. Hierdie artikels skep — net soos die DMCA — sekere kategorieë ISP's en elkeen se aanspreeklikheid is gebaseer op die tipe funksie wat hul verrig.[563] Die eerste kategorie is ISP's wat as geleibuise dien, en hulle is volgens artikel 12 nie aanspreeklik vir inligting wat deur hulle netwerke vloei nie.[564] Die tweede kategorie is ISP's wat van netwerke met kasgeheues gebruik maak, en hulle is eweneens nie aanspreeklik vir inligting in hulle netwerke se kasgeheues nie, mits hulle aan sekere vereistes voldoen.[565] Die derde kategorie word in artikel 14 geskep, en dit hanteer ISP's wat as gasheer van inligting optree. Hiervolgens moet daar bepaal word of ISP's bewus was van inligting op hulle netwerke, en afhangend van die antwoord kan hulle óf aanspreeklik gehou word, óf nie.[566]

Uit dit wat in hierdie afdeling oor die EU bespreek is, wil dit voorkom asof regsaanspreeklikheid van Internet-diensverskaffers in die EU op die oomblik redelik problematies is. Die EU-direktief van 2000 is in *Google France v Louis Vuitton* baie letterlik geïnterpreteer toe daar bepaal is dat 'n Internetdiensverskaffer op artikel 14 kan staat maak indien dit 'n neutrale en passiewe rol speel.[567] Dit was 'n baie goeie begin vir die direktief.

Ongelukkig het *L'Oreal v eBay,* artikel 14 van die EU-direktief uitgebrei deur die vereiste van die "redelike diensverskaffer" daar te stel.[568]

---

562 Direktief 2000/31/EC van die Europese Parlement en die Raad van 8 Junie 2000 oor "Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market" (Directive on electronic commerce) 2000 OJ L178/1.

563 Afd 6.4.3.2.

564 Daar is uitsonderings, maar dit word nie in hierdie samevatting bespreek nie. Afd 6.4.3.2.

565 Afd 6.4.3.2.

566 Afd 6.4.3.2.

567 Afd 6.4.3.3.

568 Afd 6.4.3.3.

Die Britse regspraak onderskei tussen gevalle waar Internet-diensverskaffers nog nie bewus is van wangedrag op hulle bedieners nie, en daardie gevalle waar hulle reeds daarvan kennis gekry het. In eersgenoemde geval sal Internet-diensverskaffers nie aanspreeklik gehou word nie (net soos artikel 14 van die EU-regulasies bepaal), maar sodra 'n ISP kennis ontvang van die gewraakte gedrag, sal hulle vinnig moet ingryp om aanspreeklikheid te vermy.[569] In *Tamiz v Google* het regter Richards hierdie beginsel getemper deur te bepaal dat die aard van *blogs* van verbygaande aard is, en dat die nie-verwydering in so 'n geval nie noodwendig tot ISP-regsaanspreeklikheid sal lei nie.[570]

Delfi v Estonia het weer eens getoon watter premie op soewereiniteit geplaas word.[571] Ten spyte van die duidelike bepalings van die EU-direktief, was die EU-geregshof nie bereid om 'n lidland se eng interpretasie van wat as 'n uitgewer beskou kan word, opsy te skuif nie. Dit wil dus voorkom asof die EU-direktief tweede viool speel teenoor die regbank van lidlande, alhoewel die EU-direktief juis bepaal dat lidlande hulle wetgewing in lyn daarmee (die direktief) behoort te kry.[572]

Die algemene trant van die Europese Unie se hantering van ISP-aanspreeklikheid is dat dit reeds vroeg in die ontstaan van die Internet baie duidelike reëls neergelê het van hoe sulke situasies hanteer moet word, maar dat lidlande steeds nie hulle eie wetgewing aangepas het om hierdie beginsels te weerspieël nie. Die gevolg is 'n inkonsekwente toepassing van relatief duidelike reëls, wat 'n jammerte is.

Die laaste staat waar ISP-aanspreeklikheid ondersoek word, is Suid-Afrika. Die skakel met die Europese Unie sal onmiddellik duidelik word wanneer dit vervolgens bespreek word.

---

569 Dit skep 'n situasie waar vryheid van spraak maklik beperk kan word.

570 Afd 6.4.3.3.

571 Afd 6.4.3.3.

572 Par (3) tot (6) van die EU-direktief.

6.4.4 Die Republiek van Suid-Afrika

6.4.4.1 Algemeen

Internetregulering in Suid-Afrika word deur verskeie stukke wetgewing hanteer.[573] Die Wet op Elektroniese Kommunikasies en Transaksies[574] is sekerlik die omvattendste hiervan. Dit is 'n stuk wetgewing wat in 'n onstuimige politieke klimaat geformuleer is, soos wat reeds in besonderhede in afdeling 3.5 uiteengesit is. Die ANC-regering was vasbeslote om die .ZA-domein uit "privaat beheer" te kry, en op die koop toe is daar besluit om dié wetgewing so omvattend moontlik te maak. Ongelukkig was die hele proses baie haastig afgehandel, en die gevolg daarvan kan in die EKT-wet raakgesien word.[575]

6.4.4.2 Die Wet op Elektroniese Kommunikasies en Transaksies

Internet-tussengangers word in Suid-Afrika deur hoofstuk XI van die Wet op Elektroniese Kommunikasies en Transaksies[576] gereguleer. Dit bevat 10 artikels wat Internet-diensverskaffers se optrede beheers.[577] Met

573 Die Wet op Elektroniese Kommunikasies en Transaksies 25 van 2002 is die mees omvattende hiervan. Ander stukke wetgewing wat ook van belang is, is die Wet op die Reëling en Onderskepping van Kommunikasies en Verstrekking van Kommunikasie-Verwante Inligting 70 van 2002, die Wet op Films en Publikasies 65 van 1996 (veral art 27(3), wat spesifiek aanlyn-kinderpornografie strafbaar stel), die Wet op Elektroniese Kommunikasie 36 van 2005 (veral artikels 1 en 74), die "Consumer Protection Act" 68 van 2008 (wat slegs in Engels uitgevaardig is) asook art 71(5) van die Suid-Afrikaanse Polisiedienswet 68 van 1995; Watney M "State Surveillance of the Internet: Human Rights Infringement or E-security Mechanism?" 2007 *International Journal of Electronic Security and Digital Forensics* 42 51.

574 Wet 25 van 2002.

575 Ten spyte daarvan dat verskeie "nuwe" maatreëls met die 2002-wetgewing voorgeneem is om die Suid-Afrikaanse Internet beter te reguleer, is heelwat daarvan nog nie behoorlik geïmplementeer nie. Dit sal in meer besonderhede hieronder bespreek word, maar die sprekendste voorbeeld hiervan is sekerlik Hfst XII van die wet. Daarin word bepaal dat kuberinspekteurs aangestel moet word om 'n polisiëringsfunksie te verrig, maar tot op datum (meer as dertien jaar later) is daar steeds nog steeds geen kuberinspekteurs aangestel nie. (S v *Miller and Others* 2016 (1) SASV 251 (WCC) 267J). Netsó bepaal art 28(2) van die EKT-wet dat die Suid-Afrikaanse Poskantoor as die voorkeurdiensverskaffer beskou sal word wanneer 'n waarmerkdiensverskaffer gebruik moet word. Ook hierdie vereiste is nie geïmplementeer nie. 'n Laaste voorbeeld is dat Hfst V van die wet, wat spesifiek die kwessie van kriptografieverskaffers hanteer, baie lomp is, en steeds tot op hede nie in algemene gebruik is nie.

576 Wet 25 van 2002. Roos A en Slabbert M "Defamation on *Facebook*: *Isparta v Richter* 2013 6 SA 529" 2014 *Potchefstroom Electronic Reserves* 2844 2857.

577 Artikels 70–79 van die Wet; Coetzee J "The Electronic Communications and Transactions Act 25 of 2002: Facilitating Electronic Commerce" 2004 *Stellenbosch Law Review* 501 507.

die lees van die gemelde artikels blyk dit duidelik dat die wetgewer ’n selfreguleringsisteem in gedagte gehad het toe die wet geformuleer is.[578] Artikel 71 bepaal byvoorbeeld dat ’n verteenwoordigende liggaam geskep sou moes word om as waghond vir Internet-diensverskaffers te dien.[579] Dan word daar uiteengesit dat Internet-diensverskaffers onder sekere omstandighede[580] immuun teen enige vervolging sou wees. Die verteenwoordigende liggaam sou dus die spil wees waarom selfregulering deur lede (die individuele Internet-diensverskaffers) draai.

Ongelukkig het hierdie ideaal nie gerealiseer nie, aangesien die minister ’n omvattende regulasie uitgevaardig het wat die vereistes van verteenwoordigende liggame uiteengesit het, en waar die minister die reguleringsisteem verander het na ’n mede-reguleringsisteem waar die staat die reëls neerlê, en die verteenwoordigende liggaam dit moet toepas. Dit word hieronder in besonderhede onder die loep geneem.[581] Voordat dit egter gedoen word, moet die grondwerk gelê word met die bespreking van die relevante artikels in die EKT-wet, en dit begin met ’n omskrywing van wat ’n “diensverskaffer” sal wees.

6.4.4.2.1 Omskrywing van “Diensverskaffer”

Artikel 70 is die eerste artikel van hoofstuk XI en is ’n woordomskrywingsartikel wat “diensverskaffer” definieer as “enige persoon wat inligtingstelseldienste verskaf”. “Inligtingstelseldienste” word in artikel 1 beskryf as:

> ook die verskaffing van verbindings, die bedryf van fasiliteite vir inligtingstelsels, die verskaffing van toegang tot inligtingstelsels, die uitsending of roetering van databoodskappe tussen punte wat deur ’n gebruiker gespesifiseer word, en die prosessering en berging van data op die individuele versoek van die ontvanger van die diens.[582]

[578] Afd 6.4.4.2.2.

[579] Afd 6.4.4.2.2.

[580] Art 73–76 en 78–79.

[581] Afd 6.4.4.2.2.

[582] Art 1 van die EKT-wet.

Hierdie mondvol-definisie beteken dat 'n reeks handelinge 'n persoon of maatskappy as 'n Internetdiensverskaffer sal kan laat kwalifiseer:

- As 'n derde party aan die Internet gekoppel word, sal die koppelaar 'n Internetdiensverskaffer wees. Dit beteken eenvoudig dat 'n maatskappy wat enige gebruiker aan die Internet koppel 'n Internetdiensverskaffer is (dit is die algemeenste vorm van koppeling).

- As iemand enige fasiliteite bedryf wat aan die Internet gekoppel sal word, is hy eweneens 'n diensverskaffer — dit sal byvoorbeeld gebeur wanneer 'n persoon 'n bedienerplaas[583] bedryf.

- So ook sal 'n entiteit as 'n diensverskaffer beskou word as dit data-boodskappe op die Internet roeteer. Alle maatskappye wat ruggraat-Internetdienste aan kleiner Internet-diensverskaffers verskaf, val onder hierdie kategorie. In praktiese terme sal slegs 'n handjievol verskaffers onder hierdie kategorie val, en Telkom is sekerlik die beste voorbeeld hiervan.

- Laastens sal iemand wat data berg en prosesseer — soos iemand wat "cloud"-dienste verskaf — ook as 'n diensverskaffer beskou word. Voorbeelde hiervan is *Google* en Amazon.

Die ongelukkige gevolg van hierdie definisie is dat dit ontsettend wyd is: die resultaat is dat bykans *alle* persone en entiteite wat 'n kommersiële Internet-diens verskaf, as 'n diensverskaffer gereken sal word. Die plaaslike restaurant of koffiewinkel wat *Wi-Fi* toegang verskaf, is nou skielik 'n Internetdiensverskaffer. Net so kring dit ook uit tot nie-kommersiële sfere, soos byvoorbeeld gemeenskapsbiblioteke wat Internetkiosks op hul persele verskaf. So ook sal privaat individue wat *Wi-Fi* toegang aan ander op 'n nie-winsbejag-metode verskaf, as 'n Internetdiensverskaffer beskou word. Die uiteinde is dat mens amper met 'n sinnelose definisie te make het.

583 'n Bedienerplaas, oftewel "server farm" in Engels, word gewoonlik deur groot maatskappye bedryf wat webdienste soos "website hosting" lewer. Dit is nie vreemd om webwerwe van regoor die wêreld op 'n enkele bedienerplaas te hê nie. Bidgoli H *The Internet Encyclopedia, Volume 3* (2003) 713.

6.4.4.2.2 Verteenwoordigende Liggaam as Reguleerder

Nadat die gebruiklike definisies in artikel 70 afgehandel is, begin die wetgewer om in artikel 71 die Suid-Afrikaanse stelsel van regulering van Internet-diensverskaffers uiteen te sit. Artikel 71 magtig die minister[584] om een of meer verteenwoordigende liggame te erken as die waghond om diensverskaffers in plek te hou.[585] Hieruit kan daar dadelik afgelei word dat die wetgewer 'n selfreguleringsisteem in gedagte gehad het — Internet-diensverskaffers affilieer met een of meer verteenwoordigende liggame, en dan word hulle optrede deur die verteenwoordigende liggaam gereguleer.

Daar word egter in artikel 71(2) bepaal dat die minister slegs die verteenwoordigende liggaam mag erken indien dit aan vier vereistes voldoen, te wete (a) sy lede aan 'n gedragskode onderworpe is; (b) lidmaatskap aan voldoende kriteria onderworpe is; (c) die gedragskode voortdurende ondersteuning van voldoende standaarde van gedrag vereis; en (d) die verteenwoordigende liggaam in staat is om sy gedragskode voldoende te moniteer en af te dwing.[586] Terme soos "voldoende kriteria" (punt (b) hierbo) en "voldoende standaarde" (punt (c) hierbo) is baie vaag, en dit het dadelik tot probleme aanleiding gegee.

Om dit behoorlik te verstaan, moet die tyd vlugtig teruggedraai word om die ontstaan van die *Internet Service Providers Association,*[587] (hierna ISPA) uiteen te sit. Dan sal artikel 71(2) se tekortkominge duidelik sigbaar word.

ISPA is reeds in 1996 deur 'n groep diensverskaffers gestig met die doel om op korporatiewe vlak na hulle belange om te sien. Dit is dus etlike

584 Die minister van Kommunikasie — sien art 1.

585 Art 71(1).

586 Art 71(2).

587 Die *Internet Service Providers Association* is reeds in 1996 gestig. Etlike mylpale sluit in die skepping van die *Johannesburg Internet Exchange,* wat die sentrale punt is waaruit Internet-verkeer vanuit Suid-Afrika beweeg (1996); hulp met die totstandkoming van die *Industry Representative Body*-regulasies (IRB) in 2006, asook die enigste organisasie in Suid-Afrika wat uiteindelik as 'n IRB geregistreer is (2009). ISPA "Key Milestones and Victories for ISPA" http://ispa.org.za/about-ispa/key-milestones/ (besoek op 15 Februarie 2016). Sien ook Ketler Investments Cc T/A Ketler Presentations v Internet Service Providers' Association 2014 (2) SA 569 (GJ) 570 E-G waar die magte van ISPA oor sy lede en dié se gebruikers uiteengesit word.

jare vóór die totstandkoming van van die EKT-wet gestig. Trouens, ISPA het advies verleen in die aanvanklike formulering van die EKT-wet, en was by uitstek die organisasie om as verteenwoordigende liggaam vir Internet-diensverskaffers op te tree.[588] Dit het dan kort ná die promulgering van die EKT-wet aansoek gedoen om as verteenwoordigende liggaam erken te word, maar die aansoek is afgekeur aangesien die minister nog nie riglyne uitgevaardig het vir die erkenning van verteenwoordigende liggame nie, en daar dus nie 'n meetstok was waarteen ISPA gemeet kon word nie.[589] Dit is presies die probleem wat in die voorafgaande paragraaf met artikel 71(2) uitgelig is — die vereistes is so vaag dat dit aan die een kant moeilik vir die minister is om te bepaal of 'n verteenwoordigende liggaam aan die wet se vereistes voldoen, en andersyds dat 'n voornemende verteenwoordigende liggaam geen konkrete maatstaf het waarteen dit gemeet kan word nie.

Die nie-erkenning van ISPA het verreikende gevolge vir ISP's gehad, soos direk hieronder aangetoon word.

6.4.4.2.3 Kwalifisering vir die Voordeel van Nie-Aanspreeklikheid

Artikels 73–76 en 78–79 van die EKT-wet bied 'n verskeidenheid beperkings op aanspreeklikheid vir ISP's, wat uiteraard vir hulle baie aanloklik is. Om egter op enige van hierdie regsbepalings aanspraak te kan maak, bepaal artikel 72 dat die beperkings op aanspreeklikheid slegs op diensverskaffers van toepassing sal wees indien (a) die diensverskaffer 'n lid van die verteenwoordigende liggaam is, (soos wat in artikel 71 uiteengesit is), en (b) die betrokke diensverskaffer die gedragskode van die verteenwoordigende liggaam aanvaar het.

Uit die verduideliking hierbo is dit duidelik dat ISP's in Suid-Afrika hul ná die inwerkingtreding van die EKT-wet in 'n baie netelige posisie bevind het: om op die bepalings in die gemelde artikels aanspraak te kan maak, moet

588 Marx F E en O'Brien N "To Regulate or to Overregulate? Internet Service Provider Liability: The Industry Representative Body in Terms of the ECT Act and Regulations" 2011 *Obiter* 537 548.

589 Marx en O'Brien 2011 *Obiter* 548.

hulle lede van die verteenwoordigende liggaam wees en die gedragskode daarvan aanvaar, maar daar het geen verteenwoordigende liggaam na die inwerkingtreding van die wet bestaan nie aangesien die riglyne daarvoor nog nie uitgevaardig was nie! Dit was dus 'n saak van onmoontlikheid om op enige manier op die beskerming in artikels 73–76 en 78–79 staat te kon maak.

Om hierdie uiters ongunstige posisie te probeer beredder, het ISPA baie druk op die minister geplaas om wél die regulasies uit te vaardig, sodat hulle daaraan aandag kan gee om as verteenwoordigende liggaam te kon registreer. Twee jaar na die inwerkingtreding van die EKT-wet is die regulasies uitgevaardig, en ISPA het weer aansoek gedoen om as verteenwoordigende liggaam geregistreer te word. Hierdie keer was hul aansoek suksesvol.[590] Tot op datum is ISPA steeds die enigste verteenwoordigende liggaam ingevolge die wet.[591]

Die huidige regsposisie is dus dat indien 'n ISP 'n lid van ISPA is en sy gedragskode aanvaar, daar op artikels 73–76 en 78–79 van die EKT-wet aanspraak gemaak kan word.

Op die oog af lyk dit asof ISPA se registrasie as verteenwoordigende liggaam darem nou die deur oopgemaak het vir ISP's om op artikels 73–76 en 78–79 te kan steun. Die saak van *Tsichlas and Another v Touch Line Media (Pty) Ltd*[592] dui daarop dat dit ongelukkig nie noodwendig die geval is nie. Die saak het oorwegend met aanlyn-laster te doen, maar daar sal nie in hierdie konteks daarop gefokus word nie, behalwe vir 'n vlugtige bespreking van die feite om die groter konteks te gee.[593] Die verweerder

590 ISPA is op 22 Mei 2009 as verteenwoordigende liggaam aanvaar. Dit is bykans sewe jaar ná die inwerkingtreding van die wet! *Recognition of the Internet Service Provider's Association as an Industry Representative Body for Internet Service Provider* GN 588 in GG 32252 van 2009-05-22.

591 IT-Online "ISPA Gets Minister's Recognition" http://it-online.co.za/2009/05/21/ispa-gets-ministers-recognition/ (besoek op 15 Februarie 2016).

592 2004 (2) SA 112 (W).

593 Rens A "*Tsichlas and Another v Touch Line Media (Pty) Ltd*" 2005 *South African Law Journal* 740 740 bespreek die saak volledig. Sien ook Nel S "Problematic Issues Surrounding Transborder Cybersmear" 2010 *South African Mercantile Law Journal* 360 369 en Collier D "Freedom of Expresion in Cyberspace: Real Limits in a Virtual Domain" 2005 *Stellenbosch Law Review* 21 23.

het 'n webwerf gehad waar sokkeraangeleenthede bespreek is. Die eiser is op hierdie webwerf deur een van die gebruikers daarvan belaster, met ander woorde 'n gebruiker van die webblad het lasterlike uitlatings op die verweerder se webblad gemaak, terwyl die verweerder nie daarvan bewus was nie. Die eiser het die verweerder aanspreeklik gehou vir die uitlatings wat die gebruiker gemaak het.[594] Die respondent het aan die einde van sy antwoordende eedsverklaring die stelling gemaak dat hy op die relevante nie-aanspreeklikheidsklousules van die EKT-wet kan steun, aangesien hy 'n ISP is, asook 'n lid van die "Online Publishers Association". Regter Kuny het dit as 'n "throw-away defence" beskou, aangesien dit nie in besonderhede in die antwoordende eedsverklaring bespreek is nie, en as't ware as 'n nagedagte bygevoeg is.[595]

Die regter se bevinding hieroor is insiggewend:

> It seems that the respondent does not have much confidence in this possible defence, because nowhere else in its papers do I find mention made of this, and understandably so. The whole basis on which its website operates seems to be that of a principal purveyor of information. It is clearly not, nor does it fall within the definition of, a service provider. Indeed, it has a service provider in the form of Small World Digital (Pty) Ltd and that service provider, as I understand the technology, holds the information to which access is gained via the respondent's website. My conclusion in regard to this purported defence, if one can call it that, is that all the evidence in the papers before me points towards the respondent being a principal purveyor of information; in my view it is not entitled to the protection afforded by the Act to service providers.[596]

Die regter kom dus tot die gevolgtrekking dat die verweerder nie 'n Internet-diensverskaffer is nie, aangesien hy 'n *ander* ISP het wat die gasheer van sy webwerf is. Roos kritiseer hierdie deel van die beslissing deur te sê dat die regter gefouteer het, en dat die verweerder wél as 'n ISP volgens die EKT-wet beskou kan word.[597] Daar word aangevoer dat Roos heeltemal korrek

---

594 115H van die uitspraak.

595 123B.

596 123D–E van die beslissing.

597 Roos A "Freedom of Expression" in Van der Merwe D, Roos A *et al Information and Communications Technology Law* (2008) 432.

is,[598] maar dit illustreer dan ook die groter probleem: die verweerder was 'n lid van die "Online Publishers Association", wat die groot oorkoepelende organisasie vir Internet-uitgewers is, en nie van ISPA nie. Aangesien ISPA die enigste verteenwoordigende liggaam ingevolge artikel 71 van die EKT-wet is, beteken dit dat die verweerder *nie* op die nie-aanspreeklikheidsklousules van hoofstuk XI kan staat maak nie. Die gevolgtrekking is dus dat regter Kuny gefouteer het deur te bepaal dat die verweerder nie 'n ISP ingevolge die EKT-wet is nie (soos Roos aanvoer), maar het uiteindelik *tóg* tot die korrekte gevolgtrekking gekom dat die verweerder se verweer ingevolge die EKT-wet nie kan staan nie (omdat dit nie 'n lid van ISPA is nie).

Die probleem is duidelik: Artikel 71 van die EKT-wet (asook die regulasies daarvan) maak dit so moeilik om as 'n verteenwoordigende liggaam geregistreer te word dat slegs ISPA dit kon regkry om geregistreer te word — maar ISPA is 'n liggaam wat die belange van ISP's dien wat hoofsaaklik toegang aan gebruikers tot die Internet gee. Die verweerder is die eienaar van 'n webwerf wat aanlyn-uitgewery bedryf, en dit is te verstane dat dit nie by ISPA sou affilieer nie, maar eerder by sy eie organisasie wat *sý* belange bevorder. Hierdie beslissing illustreer hoe tradisionele ISP's — wat toegang tot die Internet verskaf — op die nie-aanspreeklikheidsvereistes van die EKT-wet kan staat maak (omdat dit ISPA-lede is), maar ander Internet-besighede geheel en al van die beskerming van die EKT-wet uitgesluit word omdat hulle oorkoepelende waghond-organisasies nie as verteenwoordigende liggame ingevolge artikel 71 van die EKT-wet geregistreer is nie.[599]

6.4.4.2.4 Tipes Internet-diensverskaffers

Voordat enige van die nie-aanspreeklikheidsklousules in die EKT-wet bespreek word, is dit nodig om te verstaan dat artikels 73–75 geskoei is op

[598] Afd 6.4.4.2.5, en veral art 75(1).

[599] Die nie-aanspreeklikheidsvereistes van die EKT-wet word in fyner besonderhede in afd 6.4.4.2.5 bespreek.

die *"Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market"*[600] (hierna die EU-direktief). Hierdie Europese direktief is in meer besonderhede in afdeling 6.4.3.2 bespreek. Volledigheidshalwe word daar nou weer oorsigtelik daarna verwys.

Die EU-direktief is in die jaar 2000 uitgevaardig om die ongelykhede in hulle onderskeie lande se wetgewing aan te spreek.[601] Die EKT-wet is slegs twee jaar hierna uitgevaardig, en daarom is dit nie vreemd nie dat die Suid-Afrikaanse wetgewer by sy Europese eweknie gaan kers opsteek het om die beste praktyke in hierdie jong area van die reg te ontwikkel.

Soos in afdeling 6.4.3.2 bespreek, onderskei die EU-direktief tussen drie "soorte" Internet-diensverskaffers. Elkeen van hierdie diensverskaffers word afsonderlik deur 'n artikel van die EU-direktief gereguleer. Dit is belangrik om tussen die verskillende soorte diensverskaffers te onderskei, aangesien die verskillende diensverskaffers aan verskillende vereistes moet voldoen ten einde op nie-aanspreeklikheid staat te kan maak.

Die drie soorte diensverskaffers met die artikels van die EU-direktief wat hul reguleer, is naamlik:

1. Daardie diensverskaffers wat bloot 'n geleibuis is wat data déúr hulle netwerke stuur sonder om dit te monitor.
   Volgens artikel 12 van die EU-direktief sal hierdie soort diensverskaffer nie aanspreeklik gehou kan word vir enige data wat deur sy netwerk beweeg nie, mits hy aan die volgende drie vereistes voldoen — die diensverskaffer mag nie:

   (a) die oordrag inisieer nie;

[600] Direktief 2000/31/EC van die Europese Parlement en die Raad van 8 Junie 2000 oor "Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market" (Directive on electronic commerce) 2000 OJ L178/1.

[601] Par (40) van die inleiding tot die Direktief 2000/31/EC stel dit duidelik: "Both existing and emerging disparities in Member States' legislation and case-law concerning liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition".

(b) die ontvanger van die oordrag kies nie; en

(c) mag nie die inligting wat in die oordrag vervat is, kies of verander nie.[602]

Hierdie drie vereistes is daargestel om te verseker dat die "blote geleibuis"-diensverskaffer juis dít is — slegs 'n geleibuis wat op geen wyse die inligting verander nie, maar dit bloot deur sy rekenaarnetwerke roeteer.

Volgens artikel 12(2) mag hierdie diensverskaffer die data wel vir 'n kort tydperk op sy netwerk mag stoor. Dit mag egter slegs gedoen word in die proses waar die data geroeteer word.[603] [604]

2. Diensverskaffers wat data tydelik berg, voordat dit aangestuur word.
Artikel 13 van die EU-direktief is van toepassing op diensverskaffers wat data tydelik in 'n kasgeheue berg. Artikel 13 kan maklik met artikel 12(2) (hierbo) verwar word. Die onderskeid tussen hierdie twee artikels (artikel 13 en artikel 12(2)) word egter duidelik wanneer artikel 13 meer besonderhede bestudeer word. Artikel 12(2) hanteer die tydelike berging van data met die uitsluitlike doel om dit verder aan te stuur, en hierdie berging mag dalk vir 'n paar sekondes duur. Artikel 13 hanteer data wat vir 'n langer tyd geberg word. Die algemene gebruik van diensverskaffers om gewilde webwerwe in hul eie kasgeheue te berg om dit vinniger aan intekenaars aan te bied, is 'n voorbeeld hiervan. Die gewilde webwerf se blad word dan elke paar uur uit die kasgeheue van die diensverskaffer verwyder en met 'n nuwe weergawe vervang.

Artikel 13 lê verdere reëls neer vir diensverskaffers wat van 'n kasgeheue gebruik maak:

602 Art 12(1)(a)–(c) van die Direktief.

603 Art 12(2) maak bv melding van "transient storage" en "in so far as this takes place for the sole purpose of carrying out the transmission in the communication network". Blote tydelike berging is dus hier in gedagte.

604 Die Engelse term "mere conduit" word hier bedoel. Sien art 12 van die EU Direktief 2000/31/EC.

(a) die inligting mag nie deur die verskaffer verander word nie;

(b) die verskaffer moet voldoen aan vereistes tot toegang tot die inligting;[605]

(c) die verskaffer moet aan reëls oor die opdatering van die inligting voldoen soos deur die betrokke industrie in gebruik is,

(d) die verskaffer mag nie inmeng met die wettige gebruik van tegnologie soos gebruik in die betrokke industrie om data oor die gebruik van die inligting te bekom nie;[606] en

(e) die verskaffer moet vinnig optree om toegang tot inligting te beperk indien dit nie meer beskikbaar is op die oorspronklike netwerk nie. Die verskaffer moet ook vinnig optree indien 'n hof of administratiewe gesag sodanige verwydering van die inligting beveel het.[607]

Die doel van al hierdie vereistes is om die kopie van die inligting in die ISP se kasgeheue op datum te hou. In die voorbeelde hierbo[608] is verduidelik dat die inligting in die ISP se kasgeheue altyd ouer is as die nuwe opgedateerde inligting van die webwerf self. Die vyf vereistes hierbo genoem, het dit ten doel om die industrie se beste praktyke ten aansien van opdatering van kasgeheue tot uitvoering te bring. Indien die kasgeheue dus op datum bly, kan nie-aanspreeklikheid op dieselfde wyse geld as wat dit vir "gewone" diensverskaffers die geval is.[609]

605 Hierdie vereiste klink aanvanklik vreemd op die oor, maar daar word bedoel dat die vereistes wat vir die oorspronklike webblad voorgeskryf word, ook deur die diensverskaffer nagekom moet word. As die webblad wat in die kasgeheue van die diensverskaffer is, byvoorbeeld slegs vir betalende intekenaars beskikbaar is, mag die diensverskaffer nie die dokument in die kasgeheue gratis beskikbaar stel nie. Lodder en Kaspersen *e-Directives* 88.

606 'n Voorbeeld hiervan is waar webwerwe sekere tellerprogramme gebruik om te bepaal hoeveel gebruikers hulle webwerwe besoek het, en watter webblaaie die meeste gelees is. Soms beïnvloed die hoeveelheid besoeke ("hits") die betrokke webblad se inkomste uit advertensies, en diensverskaffers wat webblaaie in hul kasgeheue berg moet sorg dat die werking van die tellerprogramme op die oorspronklike webblaaie nie beïnvloed word nie. Lodder en Kaspersen *e-Directives* 88.

607 Art 13(1)(a)–(e) van die Direktief.

608 Vn 605 en 606 direk hierbo.

609 Die Engelse term "caching" word hier bedoel. Sien art 13 van die EU Direktief 2000/31/EC.

3. Diensverskaffers wat gasheer tot data is.[610]
   Volgens Artikel 14 van die EU-direktief word 'n ISP wat as 'n gasheer vir die inligting optree, vrygestel van aanspreeklikheid indien hy aan twee vereistes voldoen. Hierdie vereistes is:

   (a) die verskaffer dra nie werklike kennis van onwettige aktiwiteite of inligting nie. Met betrekking tot eise vir skadevergoeding, is die verskaffer nie bewus is van enige feite of omstandighede waaruit die onwettige aktiwiteit of inligting spruit nie,[611] of

   (b) wanneer die verskaffer wel sodanige inligting bekom of bewus gemaak word daarvan, die verskaffer vinnig op te tree om toegang tot die inligting te verwyder of te deaktiveer.[612]
   Volgens Lodder en Kaspersen dui artikel 14(a) daarop dat 'n ISP geen aanspraak op nie-aanspreeklikheid kan maak in siviele en strafregtelike sake wanneer hy werklike kennis van die onwettige aktiwiteite het nie.[613] Daar word aangevoer dat hierdie afleiding van Lodder en Kaspersen duidelik te vinde is in die teks, veral ten opsigte van siviele sake. Dit kan dalk ietwat verregaande wees om egter die artikel egter sonder meer op die Strafreg van toepassing te maak. Die EU-direktief bepaal duidelik in paragraaf 26 van die aanhef dat elke lidland by magte is om te bepaal of hierdie direktief ook ten opsigte van strafsake sal geld.[614] Gevolglik sal die werking van artikel 14 van land na land verskil soos dit op die Strafreg toepassing vind.

Noudat daar aangetoon is hoe die EU-direktief verskillende diensverskaffers

610 Die Engelse term "hosting" word hier bedoel. Sien art 14 van die EU Direktief 2000/31/EC.

611 Art 14(1)(a) van die Direktief.

612 Art 14(1)(b) van die Direktief.

613 Lodder en Kaspersen *e-Directives* 88.

614 Die direktief bepaal in par 26 van die aanhef: "Member States, in conformity with conditions established in this Directive, may apply their national rules on criminal law and criminal proceedings with a view to taking all investigative and other measures necessary for the detection and prosecution of criminal offences, without there being a need to notify such measures to the Commission".

hanteer, kan die bepalings van die EKT-wet verder bespreek word.

6.4.4.2.5 Nie-Aanspreeklikheidsklousules

Artikel 73 van die EKT-wet is sekerlik een van die belangrikste bepalings vir Internet-diensverskaffers deurdat hierdie artikel bepaal dat 'n diensverskaffer bloot 'n geleibuis van die data sal wees indien hy aan sekere vereistes voldoen.[615] Dus kan die diensverskaffer nie aanspreeklik gehou word vir enige onwettige of ongunstige handelinge van sy gebruikers nie. Die vereistes wat gestel word sodat daar op dié artikel gesteun kan word is dat die diensverskaffer:
(a) nie die versending moes begin het nie;[616]
(b) nie die geadresseerde gekies het nie;[617]
(c) die proses van diensverskaffing moes geoutomatiseerd gewees het,[618] en
(d) die data mag nie verander gewees het nie.[619]

Wanneer hierdie vereistes oorweeg word, is dit duidelik dat die wetgewer in gedagte gehad het dat die data bloot op die "gewone" wyse — soos wat Internet-diensverskaffers gewoonlik besigheid doen — moes gevloei het. Die aard van 'n Internetdiensverskaffer se besigheid is dat daar 'n magdom hoeveelheid inligting op enige gegewe tyd deur sy rekenaarstelsels vloei, en dit sou onbillik wees om van 'n diensverskaffer te verwag om álle data te monitor.

Wanneer artikel 73 van die EKT-wet met artikel 12 van die EU-direktief[620] vergelyk word, is dit dadelik merkbaar hoe dit bykans woord-vir-woord ooreenstem. Die enigste verskil is dat artikel 73(1)(c) by die EKT-wet gevoeg is. Daar word aan die hand gedoen dat hierdie byvoegings effe geforseerd is, aangesien dit nie duidelik is wat die wesenlike verskil tussen artikel 73(1)(c)

615 Visser C "A New Online Service Provider Liability Regime" 2007 *Juta's Business Law* 40 41.

616 Art 73(1)(a).

617 Art 73(1)(b).

618 Art 73(1)(c).

619 Art 73(1)(d).

620 Afd 6.4.3.2 hierbo.

en artikel 73(1)(d) is nie. Eersgenoemde meld dat die data nie geselekteer mag word nie, maar dit is onduidelik waarom die data geselekteer sal word sonder die bedoeling om dit te verander. Blote selektering behoort nie tot nie-nakoming van die artikel te lei nie, aangesien selektering sonder die doel om enigiets met die data te doen, eintlik onsinnig is. Die *crux* van die saak is dat die effek van artikel 73 in alle opsigte dieselfde as artikel 12 van die EU-direktief is.

Artikel 73(2) het ten doel om artikel 73(1) verder te omlyn, en maak dit duidelik dat selfs indien die datavloei tot gevolg het dat die Internetdiensverskaffer die data vir ’n kortstondige tydperk moet stoor (op sy eie rekenaarnetwerk), dit steeds aan die diensverskaffer beskerming sal bied. In praktiese terme beteken dit dat ’n diensverskaffer byvoorbeeld immuun teen vervolging sou wees indien ’n kinder-pornografiese foto kortstondig op sy bediener gestoor word wanneer dit “op pad” is na die misdadige gebruiker.

Volledigheidshalwe kan genoem word dat artikel 73(3) bepaal dat ten spyte van die bepalings wat in artikels 73(1) en 73(2) bevat is, ’n hof wél by magte is om ’n diensverskaffer aan te sê om onwettige bedrywighede te staak of te verhinder. Dit beteken eenvoudig dat as ’n hof ’n diensverskaffer aansê om onwettige aktiwiteite wat op sy rekenaarnetwerk gebeur, te staak, die diensverskaffer nie op artikels 73(1) en 73(2) kan staatmaak om die hof se bevel te fnuik nie.[621]

Artikel 74 hanteer die gevalle waar ISP’s data in hul bedieners se kasgeheue berg. Uit dit wat reeds oor die EU-direktief bespreek is, is dit duidelik dat hierdie artikel dieselfde gevalle hanteer as wat artikel 13 van die EU-direktief doen.

621 ’n Diensverskaffer sou byvoorbeeld op artikels 73(1) en 73(2) kon staat maak om hulself van enige onwettige gedrag te verontskuldig, selfs al was hul bewus daarvan (dit is nie vereiste volgens hierdie artikels dat die diensverskaffers nie bewus moes gewees het van die gedrag nie). As ’n hof nou ’n bevel uitvaardig dat die diensverskaffers die gedrag moet monitor, kan dit finansiële gevolge vir die diensverskaffer inhou. As die diensverskaffer artikels 73(1) en 73(2) as regverdigingsgronde kon inbring om te verhinder dat hulle hoef te monitor, sou dit die gesag van die regbank kon ondermyn. Daar word aan die hand gedoen dat die skepping van art 73(3) bloot ’n wyse is om enige misbruik van die regsproses te voorkom.

Artikel 74(1) bepaal dat 'n diensverskaffer nie verantwoordelik gehou sal word vir die outomatiese en tussentydse berging van (onwettige) data op sy eie stelsel nie.[622] Om duplisering te voorkom kan daar eenvoudig genoem word dat die vereistes van artikel 74(1) bykans woord-vir-woord ooreenstem met artikel 13 van die EU-direktief. Die enigste verskil is dat die EU-direktief in artikel 13(1)(e) bepaal dat data verwyder moet word wanneer die ISP daarvan bewus word ("actual knowledge") dat die oorspronklike webwerf die data verwyder het. Hierteenoor bepaal artikel 74(1)(e) van die EKT-wet dat data deur die ISP verwyder moet word indien dit 'n afhaalkennisgewing ontvang het.[623]

Die bepaling van die EKT-wet blyk beter te wees as dié wat in die EU-direktief te vind is, aangesien dit ISP's se taak om te monitor vergemaklik.

Artikel 75(1) hanteer die geval waar 'n diensverskaffer as 'n gasheer van data optree. Waar artikels 73 en 74 grootliks met die ooreenstemmende bepalings in die EU-direktief ooreenstem, is daar by artikel 75 'n effense wegbeweeg van die ooreenstemmende artikel 14 van die EU-direktief. Artikel 14 van die EKT-wet bepaal dat 'n diensverskaffer nie aanspreeklik sal wees vir skade wat ontstaan weens data-berging namens die ontvanger van die diens nie, mits die diensverskaffer:

(a) nie werklike kennis het dat die databoodskap of 'n bedrywigheid in verband met die databoodskap die regte van 'n derde party skend nie; of[624]

(b) nie bewus is van feite of omstandighede waaruit die skendende

622 Om op hierdie bepaling aanspraak te kan maak, bepaal die wet dat die diensverskaffer aan vyf vereistes moet voldoen, te wete: Die diensverskaffer mag (a) nie die data verander nie; (b) voldoen aan die voorwaardes van toegang tot die data; (c) voldoen aan reëls met betrekking tot die opdatering van die data, uiteengesit op 'n wyse wat wyd erken en gebruik word deur die bedryf; (d) nie inmeng met die wettige gebruik van tegnologie, wat wyd erken en gebruik word deur die bedryf, om inligting oor die gebruik van die data te verkry nie; en (e) toegang tot data wat geberg is, verwyder of ongeskik maak by ontvangs van 'n afhaalkennisgewing bedoel in art 77. Hierdie vereistes is identies aan art 13 van die *"Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market"*.

623 Afhaalkennisgewings word deur art 77 van die EKT-wet hanteer, en word hieronder verder bespreek.

624 Art 75(1)(a) van die EKT-wet.

bedrywigheid of die skendende aard van die databoodskap blyk nie; en[625]

(c) by ontvangs van ’n afhaalkennisgewing bedoel in artikel 77, spoedig optree om toegang tot die data te verwyder of ongeskik te maak.[626]

Dit is opmerklik dat waar die EU-direktief in artikel 14 van “information” praat, die EKT-wet in artikel 75 dit met “data” vervang. Die EKT-wet omskryf data in artikel 1 as “elektroniese voorstellings van inligting in enige formaat”. Die term “inligting” word nie in die EKT-wet omskryf nie, maar “inligtingstelsel” wél, en word gedefinieer as “’n stelsel om databoodskappe voort te bring, te stuur, te ontvang, te berg, te vertoon of andersins te prosesseer, en sluit die Internet in”. Uit hierdie definisies wil dit voorkom asof die EKT-wet “data” beskou as ’n wyse om inligting elektronies voor te stel. Die inligting is dus die primêre nut vir die gebruiker, maar die “data” is die rekenaar se meganisme om die inligting, wat in elektroniese vorm is, voor te stel. Dit wil voorkom asof die uiteinde en -doel van artikel 75 van die EKT-wet en artikel 14 van die EU-direktief dieselfde is: om gasheer-diensverskaffers te beskerm teen aanspreeklikheid indien hulle vir derde partye data — of elektroniese inligting — berg.

Artikel 75(2) plaas ’n verantwoordelikheid op die diensverskaffer om ’n agent aan te stel om kennisgewings van skendings te ontvang. Die artikel gaan dan verder en spesifiseer ook dat die betrokke diensverskaffer die naam, adres, telefoonnommer en e-posadres van die agent op ’n prominente plek op sy “webwerwe of plekke wat vir die publiek toeganklik is”, moet aanbring.[627]

Interessant genoeg is hierdie vereiste nie aanwesig in die EU-direktief nie, maar kom dit eerder ooreen met afdeling 512 van die *Digital Millennium Copyright Act* (hierna DMCA) van die VSA.[628] Dáár word

625 Art 75(1)(b) van die EKT-wet.

626 Art 75(1)(c) van die EKT-wet.

627 Art 75(2) van die EKT-wet.

628 Afd 17 USC § S512 (Die Digital Millenium Communications Act) bepaal in (c)(2): Designated agent.

bepaal dat 'n diensverskaffer wat 'n gasheer is, 'n agent moet aanstel om aanspreeklikheid te vermy.[629]

In hierdie bepaling blyk dit weer duidelik hoe slordig die EKT-wet geformuleer is. Dit is onduidelik wat die doel van die agent is, aangesien die diensverskaffer wat 'n gasheer is, tog sélf kan optree om die inligting te verwyder sodra dit 'n afhaalkennisgewing kry (trouens, dit is wat die diensverskaffer móét doen wanneer die agent hom inlig van die afhaalkennisgewing).[630] Roos[631] wys byvoorbeeld daarop dat 'n agent in artikel 75(2) vereis word, maar brei nie uit waarom dit nodig is nie. Net so wys Marx[632] op dieselfde bepaling, maar brei eweneens nie uit waarom 'n agent nodig blyk te wees nie.

Verskeie regsartikels wat die DMCA bespreek, is ook geraadpleeg vir 'n verklaring van waarom 'n agent (as blote tussenganger tussen die klaer en die diensverskaffer) nodig blyk te wees. Seltzer[633] kon nie 'n verklaring gee nie. Bretan[634] gee 'n volledige verduideliking van hoe die prosedure werk om behoorlik kennis te gee, maar verduidelik eweneens nie waarom 'n agent in die eerste plek nodig is nie.

Omdat die aanstelling van 'n agent in die DMCA te vinde is en die EKT-wet dit bloot vandaar geneem het, sou dit logies wees om die nodigheid van 'n agent in die DMCA te probeer vind. Dan sal dit duidelik word waarom 'n agent ook in die EKT-wet gebruik behoort te word. Uit die bespreking

— The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information: (A) the name, address, phone number, and electronic mail address of the agent.

Hieruit blyk dit duidelik dat die bepalings van art 75(2) van die EKT-wet op hierdie paragraaf geskoei is.

629 17 USC § S512.

630 Art 75(1)(c) van die EKT-wet.

631 Roos "Freedom of Expression" 432.

632 Marx F "Hate Speech on Social Network Sites: Perpetrator and Service Providers' Liability" 2011 *Obiter* 322 337.

633 Seltzer W "Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment" 2010 *Harvard Journal of Law and Technology* 171 178–179.

634 Bretan J "Harboring Doubts About the Efficacy of 512 Immunity under the DMCA" 2003 *Berkeley Technolgy Law Journal* 43 50–51; Chang 2010 *Cardozo Arts and Entertainment Law Journal* 200.

hierbo is Suid-Afrikaanse- sowel as VSA-regsbronne geraadpleeg, maar dit het geen oplossing gelewer nie. Na my mening is hierdie saak nie in die regsliteratuur aangespreek nie aangesien die antwoord waarskynlik voor-die-hand-liggend was in 1996, toe die DMCA uitgevaardig was. Die kommersiële Internet was op daardie stadium nog in sy kinderskoene, en die groter publiek was nog nie gewoond aan die gedagte om inligting eerstehands op die Internet te gaan soek nie. Dit was nog die tyd waar daar primêr ag geslaan is op die sentrale registrasie van inligting, soos notarieël-verlyde kontrakte, aktekantore en registrasies van maatskappye in 'n sentrale register. Die DMCA meld byvoorbeeld dat die Registrateur van kopiereg 'n register van alle ISP-agente moet hou,[635] en dit wys daarop dat agente nodig is om die bepalings van die DMCA tot uitvoering te bring in 'n Internet-ongeletterde wêreld. Indien hierdie argument waar is, is die vereiste dat agente aangestel moet word in vandag se Internet-wêreld, waarskynlik onnodig.

Interessant genoeg wys die EKT-wet self na die onsinnigheid van artikel 75(2), want artikel 77, wat afhaalkennisgewings hanteer, bepaal dat die klaer die kennisgewing aan die "diensverskaffer of sy of haar aangewese agent" moet rig.[636] Dus, volgens artikel 77 hoef die klaer nie eers gebruik te maak van die agent wat in artikel 75(2) gespesifiseer word nie! Daar word ook nie enige vereistes vir die aanstelling van 'n agent voorgeskryf nie, en eweneens hoef die naam, adres en ander inligting van die agent nie in 'n sentrale register aangeteken te word nie (soos wat in die VSA vereis word). Artikels 75(2) en 77 is die enigstes wat van agente melding maak,[637] en dit is reeds uit die bespreking hierbo duidelik dat die agent nie eers geraadpleeg hoef te word met die uitreik van 'n afhaalkennisgewing nie. Na my mening is die

635 17 USC § 512(c)(2)(b): "The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, and may require payment of a fee by service providers to cover the costs of maintaining the directory."

636 Art 77(1).

637 Volledigheidshalwe moet genoem word dat die EKT-wet in art 1 en 20 van "elektroniese agente" melding maak, maar dit is nie ter sprake in hierdie konteks nie.

vereiste van ’n agent in die konteks van hierdie artikels, sinneloos.

Artikel 76 het ten doel om diensverskaffers se aanspreeklikheid te beperk waar die inligting wat op die diensverskaffer se bediener is, skakels bevat wat lei na onwettige webwerwe, of rekenaarprogrammatuur wat gebruik word om onwettige optrede uit te voer. Die diensverskaffer kan op hierdie artikel staat maak mits hy:
(a) nie werklik kennis het dat die databoodskap of ’n bedrywigheid in verband met die databoodskap die regte van daardie persoon skend nie;[638]
(b) nie bewus is van feite of omstandighede waaruit die skendende bedrywigheid of die skendende aard van die databoodskap blyk nie;[639]
(c) nie ’n finansiële voordeel ontvang wat regstreeks aan die skendende bedrywigheid toegeskryf kan word nie; en[640]
(d) die verwysing na of koppeling aan die databoodskap of bedrywigheid verwyder of toegang daartoe ongeskik maak binne ’n redelike tyd nadat hy of sy ingelig is dat die databoodskap of die bedrywigheid wat met die databoodskap verband hou, die regte van ’n persoon skend.[641]

Dit is belangrik om daarop te let dat artikel 76 nie van ’n afhaalkennisgewing melding maak nie. Die diensverskaffer moet bloot die webskakel verwyder wanneer hy daarvan bewus word dat dit die regte van ’n persoon skend (artikel 76(c)). Verder behoort ’n diensverskaffer daarop te let dat hy nie enige finansiële voordeel uit die webskakel behoort te kry nie, anders sal hy nie op hierdie artikel kan steun nie (artikel 76(c)).

Artikel 77 hanteer die afhaalkennisgewing, en is uiteraard baie belangrik aangesien dit die spil is waarom artikels 74 en 75 draai. Die vereistes waaraan die afhaalkennisgewing moet voldoen, word in hierdie artikel

638 Art 76(a).
639 Art 76(b).
640 Art 76(c).
641 Art 76(d).

uiteengesit. Dit moet byvoorbeeld skriftelik wees,[642] moet onder andere[643] die volle name en adres van die klaer bevat,[644] en moet die reg wat na bewering geskend is, bevat. [645]

Indien 'n klaer bedrieglike inligting in die afhaalkennisgewing weergee — en dus 'n "wesenlike wanvoorstelling van die feite"[646] maak — sal hy vir skadevergoeding vir die onregmatige verwydering aanspreeklik wees.[647] Die diensverskaffer sal uiteraard nie aanspreeklik gehou kan word vir die onregmatige verwydering nie.[648]

Artikel 78 bevat 'n bepaling dat ISP's nie onder enige algemene verpligting staan om die data op hulle netwerke te moniteer nie. Dit is 'n bepaling wat ook in die EU-direktief voorkom.[649] Die minister kan egter prosedures vir spesifieke diensverskaffers voorskryf om monitering te doen,[650] of owerhede te help om spesifieke oortreders te identifiseer.[651] Dit is eweneens 'n bepaling wat van die EU-direktief geneem is.[652]

Uit die bespreking hierbo is daar aangetoon hoe die wetgewer gepoog

---

642 Art 77(1). Die vereiste van skriftelikheid beteken dat 'n e-pos wat aan ál die vereistes voldoen, aanvaarbaar sal wees. Art 12 van die EKT-wet bepaal byvoorbeeld uitdruklik dat 'n dokument wat (a) in die vorm van 'n databoodskap is, en (b) later toeganklik is, as 'n skriftelike dokument beskou sal word.

643 Die volledige lys van vereistes van die afhaalkennisgewing in art 77 is:
(a) die volle name en adres van die klaer;
(b) die skriftelike of elektroniese handtekening van die klaer;
(c) identifisering van die reg wat na bewering geskend is;
(d) identifisering van die materiaal of bedrywigheid wat na bewering die onderwerp van onwettige bedrywigheid is;
(e) die vereiste regstellende optrede wat deur die diensverskaffer ingestel moet word ten opsigte van die klagte;
(f) telefoniese en elektroniese kontakbesonderhede, as daar is, van die klaer;
(g) 'n verklaring dat die klaer te goeder trou optree; en
(h) 'n verklaring deur die klaer dat na sy of haar wete die inligting in die afhaalkennisgewing waar en korrek is.

644 Art 77(1)(a).

645 Art 77(1)(c).

646 Dit is die presiese bewoording wat art 77(2) gebruik.

647 Art 77(2).

648 Art 77(3).

649 Art 15 van die EU-direktief.

650 Art 78(2)(a).

651 Art 78(2)(b).

652 Art 15(2) van die EU-direktief.

het om met die EKT-wet Suid-Afrikaanse ISP's te beheers. Insette is vanuit wetgewing in Europa en die VSA geneem, maar dit is omvorm om 'n Suid-Afrikaanse inslag te lewer, soos waar die minister by sekere aangeleenthede betrokke moet wees om magtiging te verleen. 'n Ander aangeleentheid wat op hierdie studie betrekking het en waar die minister eweneens betrokke moet wees, is die bepalings in die EKT-wet dat 'n nasionale e-strategie ontwikkel moet word. Dit word vervolgens bespreek.

6.4.4.2.6 Nasionale E-strategie

Deel 1 van hoofstuk II van die EKT-wet bevat vyf artikels waar daar uiteengesit word dat die minister 'n nasionale e-strategie moet formuleer. Wanneer die betrokke artikels gelees word, is dit duidelik dat die wetgewer besef het dat die Internet in die toekoms 'n belangrike rol in mense se lewens sou speel, en dat dit die regering se taak is om die bevolking in staat te stel om daardie rol te vervul. Die insluiting van hierdie hoofstuk is ook te verstane indien daar in gedagte gehou word dat die EKT-wet agt jaar na die nuwe regeringsbestel in Suid-Afrika gepromulgeer is, en dat dit 'n tydperk was waar daar baie klem gelê is op die ontwikkeling van agtergeblewe Suid-Afrikaners. Die EKT-wet sélf maak dit duidelik dat dit die doel van hoofstuk II is, aangesien artikel 7 byvoorbeeld spesifiek noem dat wanneer die e-strategie geformuleer word, die minister voorsiening moet maak om "die voordele van elektroniese transaksies vir histories benadeelde persone en gemeenskappe te maksimeer".[653] Op dieselfde wyse verklaar artikel 9 dat die minister 'n nuwe infrastruktuur vir "Klein, Medium en Mikro Ondernemings" moet ontwikkel om handel tussen hierdie rolspelers te vergemaklik.[654] Die artikel het dus 'n baie duidelike opheffingsdoel.

Artikel 5 van die EKT-wet bepaal dat die minister hierdie nasionale e-strategie as 'n driejaarplan moet ontwikkel, en dat dit binne 24 maande na die inwerkingtreding van die wet aan die Kabinet vir goedkeuring voorgelê

653 Art 7 van Wet 25 van 2002.

654 Art 9 van Wet 25 van 2002.

moet word.[655] Die Kabinet moet dan, nadat dit die e-strategie aanvaar het, dit tot 'n nasionale prioriteit verklaar.[656] Ongelukkig is niks hiervan tot op hede tot uitvoering gebring nie.

Daar word aan die hand gedoen dat die konsep van 'n e-strategie 'n baie goeie idee is. Artikel 5(4)(c) van die EKT-wet bepaal dan ook wat in so 'n e-strategie ingesluit moet word: enersyds is dit duidelik dat die e-strategie die elektroniese dienste van die regering insluit, want artikel 5(4)(c)(v) maak byvoorbeeld melding van "bestaande regerings-inisiatiewe wat regstreeks of onregstreeks relevant is tot, of 'n invloed het op, die nasionale e-strategie". Andersyds is dit duidelik dat die e-strategie nie beperk is tot die regering nie, want artikel 5(4)(c)(vi) maak melding van die rol wat die privaat sektor sal kan speel om die doelwitte van die nasionale e-strategie te bereik.

Die konsep van die nasionale e-strategie soos dit in die EKT-wet vervat is, is egter nog nie voldoende nie. Die e-strategie moet ook konsepte soos effektiewe netwerk-ontwerp insluit, soos die "end-to-end"-beginsel[657] en aspekte van netwerk neutraliteit.[658] Die vrye vloei van data op 'n Suid-Afrikaanse intranet asook die groter Internet is van kardinale belang vir 'n toekoms van ekonomiese ontwikkeling vir die land.

Dit wil voorkom asof die belang van die formulering van die nasionale e-strategie tog iewers inslag gevind het, want in 2012 is die "Electronic Communications and Transactions Amendment"-wetsontwerp in die staatskoerant gepubliseer.[659] Daarin word die nasionale e-strategie weer opgehaal, en die voorgenome wysiging aan artikel 5 van die EKT-wet, wat die minister opdrag gee om die nasionale e-strategie te ontwikkel, word gewysig as:

> The Minister must, within 24 months after the promulgation of this Electronic Communications and Transactions Amendment Act, 2012, de-

655 Art 5(1) van Wet 25 van 2002.

656 Art 5(2) van Wet 25 van 2002.

657 Afd 4.2.3.2.

658 Afd 4.2.3.1.

659 Staatskoerant no 35821 van 26 Oktober 2012.

> velop a three-year national e-strategy for the Republic, which must be submitted to the Cabinet for approval.[660]

In die memorandum wat op die wetsontwerp volg, word daar spesifiek melding gemaak dat die nasionale e-strategie ten doel het om die "digital divide" te probeer oorbrug, en dat die e-strategie so ontwikkel moet word dat daar duidelik identifiseerbare tydsraamwerke ontwikkel moet word waarin die e-strategie uitgerol sal word.[661] Die memorandum verklaar dan verder:

> This strategy has not yet been developed, however the Minister considers that it is necessary and will prioritise the development of such a strategy within 24 months after the promulgation of this Amendment Act. The strategy must deal with those matters that are globally being addressed, and in which endeavours South Africa is participating.[662]

Hierdie wetsontwerp is eweneens nie deurgevoer nie, en die gevolg is dat die nasionale e-strategie steeds nie geformuleer is nie. Die minister het egter aangedui dat die formulering van 'n nasionale e-strategie 'n prioriteit vir 2016 is.[663] Daar word aan die hand gedoen dat dit belangrik is om die nasionale e-strategie te formuleer, en dat dit uitgebrei word om sinvolle netwerk-ontwerp te omvat.

***

Die beginsels ten aansien van regsbeheer van die Internet wat in die EKT-wet vervat is en wat relevant vir hierdie studie is, is nou volledig bespreek. Die regulering van ISP's se aanspreeklikheid het die grootste deel hiervan beslaan, maar eienaardig genoeg het die wetgewer dit goedgedink om in dieselfde jaar wat die EKT-wet uitgevaardig is, 'n afsonderlike stuk wetgewing te gebruik om spesifiek die onderskepping van data deur ISP's te

660 Op 13 van die Staatskoerant 35821.

661 Op 43 van die Staatskoerant 35821.

662 Op 43 van die Staatskoerant 35821.

663 Business Day "ICT Document Goes to Cabinet Ahead of Policy Finalisation" http://www.bdlive.co.za/business/technology/2016/04/06/ict-document-goes-to-cabinet-ahead-of-policy-finalisation (besoek op 22 Mei 2016) meld dat 'n "key objective for the current year, Mr Cwele said, would be the drafting of an e-strategy and a strategy for the provision of e-services by the government".

beheer — ten spyte daarvan dat dit ook grootliks in die EKT-wet sélf hanteer is. Dit word vervolgens bespreek.

6.4.4.3 Die Wet op die Reëling van Onderskepping van Kommunikasies en Verstrekking van Kommunikasie-verwante Inligting

6.4.4.3.1 Magtiging van Onderskepping

Die Wet op die Reëling van Onderskepping van Kommunikasies en Verstrekking van Kommunikasie-verwante Inligting[664] (hierna die RICA-wet)[665] vervat 'n magdom artikels wat elke denkbare geval van onderskepping van inligting beheers. Die fokus van hierdie studie bly egter op makro-vlak,[666] en slegs die regulering van Internet-diensverskaffers sal onder die loep geneem word.

Ongelukkig wil dit voorkom asof dieselfde haastige formulering van regsvoorskrifte wat by die EKT-wet te vinde is,[667] ook by die RICA-wet aanwesig is (beide wette is in dieselfde jaar uitgevaardig). Daar word regdeur die wet na verskillende tipes diensverskaffers verwys, maar sommiges word nie omskryf nie, terwyl ander weer saamgegroepeer word. Byvoorbeeld, telekommunikasiediensverskaffers, wat 'n sentrale rol in die wet speel, word nie omskryf nie, terwyl Internet-diensverskaffers in twee kontekste in artikel 1 omskryf word. In die eerste plek word Internet-diensverskaffers omskryf as:

> enigiemand wat toegang verskaf tot, of enige ander diens verskaf met betrekking tot, die Internet, aan iemand anders, hetsy sodanige toegang of diens verskaf word kragtens en ooreenkomstig 'n elektroniese kommunikasiedienslisensie aan eersgenoemde persoon uitgereik kragtens Hoofstuk 3 van die Wet op Elektroniese Kommunikasie of nie.[668]

664 Wet 70 van 2002.

665 Omdat hierdie wet so 'n lang en ongemaklike titel het, word dit in die regsliteratuur (wat gewoonlik Engels is), bloot as RICA verwys. Die akroniem kom van die Engelse "(R)egulation of (I)nterception of (C)ommunications and Provision of Communication-related Information (A)ct 70 of 2002" (hakies dui die oorsprong van die akroniem aan).

666 Afd 6.4.

667 Afd 6.4.4.2.5.

668 Art 1 van die RICA-wet.

Andersyds word "Internetdiensverskaffer" saamgegroepeer met "elektroniese kommunikasiediensverskaffer".[669] [670] Die resultaat is 'n produk wat onafgerond voorkom en tot regsonsekerheid lei, soos wat uit die bespreking hieronder sal blyk.

Die RICA-wet skep in hoofstukke 5 en 6 'n omvattende sisteem wat bykans alle vorms van elektroniese kommunikasies van Suid-Afrikaners ín die land én daarbuite kan monitor.[671] Artikel 30[672] bepaal dat 'n telekommunikasiediensverskaffer[673] sy diens so moet inrig dat dit moontlik is om daardie diens te kan onderskep.[674] Verder moet die telekommunikasiediensverskaffer in staat wees om die inligting wat onderskep word, vir 'n vasgestelde tyd te kan bewaar[675] en moet dit in staat wees om dadelik —

669 In art 1 word "kommunikasiediensverskaffer" gedefinieer as:
(a) persoon wat 'n elektroniese kommunikasiediens verskaf kragtens en ooreenkomstig 'n elektroniese kommunikasiedienslisensie aan so iemand uitgereik kragtens hoofstuk 3 van die Wet op Elektroniese Kommunikasie; of

(b) Internetdiensverskaffer.

670 Hierbo is aangetoon dat "kommunikasiediensverskaffer" nie gedefinieer is nie. Dit mag dan voorkom dat hierdie stelling verkeerd is, aangesien die wet wél "elektroniese kommunikasiediensverskaffer" definieer. Tog maak die wet geen melding daarvan dat die twee terme enigsins as sinonieme beskou kan word nie. Uit die lees van die wet wil dit ook voorkom asof hierdie terme nie wisselvorme is nie, aangesien daar soms bloot na "kommunikasiediensverskaffer" verwys word, en andermale na "elektroniese kommunikasiediensverskaffer". Die feit dat hierdie terme nie deurgaans konsekwent gebruik word nie, skep die indruk dat die wetgewer tóg een of ander onderskeid wou tref.

671 Die RICA-wet gebruik nie die term monitering nie, maar verkies eerder die term "meeluistering". Laasgenoemde mag dalk suiwerder Afrikaanse vaktaal wees, maar pas dikwels nie in die konteks van hierdie afdeling se verduidelikings in nie. 'n Voorbeeld hiervan is juis hierdie voorafgaande sin. Om "kommunikasies ín die land én daarbuite mee te luister", maak eenvoudig nie sin nie. Gevolglik word "monitering" en "meeluistering" in hierdie deel van die studie as sinonieme gebruik.

672 Art 30 is te vinde in Hfst 5 van die Wet.

673 Soos reeds genoem word "telekommunikasiediensverskaffer" nie omskryf nie, maar uit die konteks van die wet wil dit voorkom asof 'n telekommunikasiediensverskaffer beskou kan word as 'n versamelterm vir enige verskaffer van elektroniese kommunikasies. Art 7(2) bepaal byvoorbeeld dat die telekommunikasiediensverskaffer 'n duplikaatsein van onregstreekse kommunikasie na die onderskeppingsentrum moet kan kanaliseer. Hierdie bepaling kan enersyds van toepassing wees op 'n selfoonsein wat onderskep word en andersyds op 'n webgebruiker se webdiens wat gemonitor word. Art 8(3) meld dat 'n telekommunikasiediensverskaffer 'n wetstoepassingsbeampte moet verwittig van die "posisie van die sender", wat op geografiese plasing van 'n selfoongebruiker dui. Dus is die presiese betekenis van "telekommunikasiediensverskaffer" glad nie duidelik nie.

674 Art 30(1)(a). Hofman J "Electronic Evidence in Criminal Cases" 2006 *South African Journal of Criminal Justice* 257 271. Dit geld ook vir Internetdienste wat per selfoon gelewer word: In *S v Cwele and Another* 2011 (1) SASV 409 (KZP) op 416E vind regter Koen dal *alle tipes* kommunikasie inderskep kan word, en dus ook selfoonkommunikasie. Dit is in *S v Jwara and others* 2015 (2) SASV 525 (SCA) op 531E bevestig.

675 Art 30(1)(b). Bilchitz D "Privacy, Surveillance and the Duties of Corporations" 2015 *Tydskrif vir die Suid-*

in sogenaamde "real time" — die inligting na 'n onderskeppingsentrum te kanaliseer.[676]

Wanneer die telekommunikasiediensverskaffer geregistreer word, moet die registrasie 'n klousule bevat wat aantoon watter tipe kommunikasie onderskep moet word, en vir hoe lank dit gehou moet word.[677] Die vereistes kan dus gewysig word na gelang van die tipe telekommunikasiediensverskaffer waarmee daar te make is, of watter tipe diens verskaf word. Die telekommunikasiediensverskaffer word tussen drie en ses maande gegun om hierdie moniteringsnetwerk in plek te stel.[678]

Die net word selfs wyer in hoofstuk 6 van die wet gespan waar artikel 32 bepaal dat die minister onderskeppingsentrums tot stand moet bring,[679] en dat dit permanent aan die onderskeppingsisteme van die telekommunikasiediensverskaffers (wat hierbo uiteengesit is), gekoppel moet word.[680] Hierdie onderskeppingsentrums is reeds vir etlike jare in gebruik.[681]

Dus, die RICA-wet skep 'n netwerksisteem waarin 'n sentrale staatsbeheerde onderkeppingsentrum aan die kern staan, en dit word dan sywaarts aan individuele kommunikasiediensverskaffers — wat ook Internet-

Afrikaanse Reg 45 45 vn 1.

676 van Rensburg J "Intercepting Communications and Providing Communication Related Information" 2003 *Juta's Business Law* 90 91.

677 Art 30(2).

678 Art 30(2)(b).

679 Art 32(1)(a). Hofman 2006 *South African Journal of Criminal Justice* 270.

680 Art 32(1)(c).

681 Die amptelike webblad van die kantoor vir onderskeppingsentrums is http://www.oic.gov.za/. Volgens 'n artikel in die Sunday Times van 23 Junie 2013 het die onderskeppingsentrum tussen 2006 en 2010 ongeveer 826 hofbevele om te onderskep, ontvang, en het dit ongeveer drie miljoen oproepe en e-posse in die ooreenstemmende tyd onderskep. Dit beteken dat ongeveer 80 000 kommunikasies per maand onderskep word. Defenceweb "State Can Spy on Citizens — Report" http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=30932:state-can-spy-on-citizens–report&catid=90:science-a-defence-technology&Itemid=204 (besoek op 4 April 2016); Legalbrief "Extent of State Spying on Individuals Revealed" http://legalbrief.co.za/story/extent-of-state-spying-on-individuals-revealed/ (besoek op 4 April 2016); Mail and Guardian "Secret state: How the Government Spies on You" http://mg.co.za/article/2011-10-14-secret-state/ (besoek op 4 April 2016); ITWeb "State Can Spy On Citizens — Report" http://www.itweb.co.za/index.php?option=com_content&view=article&id=65120 (besoek op 4 April 2016).

diensverskaffers kan wees — gekoppel.

Internet-diensverskaffers word op ’n eienaardige wyse in die wet hanteer. Die eerste melding van Internet-diensverskaffers is te vinde in artikel 38(1), waar daar bloot genoem word dat: “Daar is ’n fonds bekend as die Internet-diensverskaffers-hulpfonds”. Artikel 38(2) verwys dan hoe dit befonds word,[682] en in artikel 38(3) word die doel van die fonds bekend gemaak:

(3) Die geld in die Fonds word aangewend vir—

(a) verkryging, hetsy deur koop of huur, van fasiliteite en toestelle vir die doeleindes van artikel 46(7)(b); en

(b) die uitgawes betrokke by die beheer en bestuur van die Fonds.

Artikel 46(7) bepaal dat Internet-diensverskaffers wat vrygestel is om hulle eie moniteringsfasiliteite en -toestelle aan te skaf, deur die minister gehelp kan word, en dat die fonds gebruik sal word om daardie moniteringsfasiliteite en -toestelle aan te skaf.

Die hele verduideliking van Internet-diensverskaffers maak tot op hede ongelukkig nie sin as mens nie reeds die groter konteks van die RICA-wet verstaan nie. Artikel 46(1)(a)(i) bepaal byvoorbeeld dat ’n Internetdiensverskaffer vrygestel kan word van sy moniteringsverantwoordelikhede, maar nêrens in die wet word daar uitdruklik gemeld dat Internet-diensverskaffers ’n moniteringsverantwoordelikheid het nie. Die kort en lank van die saak is dat die vrystellings in artikel 46 wys dat Internet-diensverskaffers ’n moniteringsverantwoordelikheid het, en indien hy dit nie kan nakom nie, kan die minister die fonds wat hierbo uitgewys is, gebruik om fasiliteite en toerusting aan te skaf om die Internetdiensverskaffer in staat te stel om die nodige monitering te doen.

Die vraag wat ontstaan is in watter omstandighede is ’n Internet-diensverskaffer verplig om te moniteer? Die antwoord op hierdie vraag word net duidelik wanneer die EKT-wet en die RICA-wet saamgelees en

[682] Die fonds het drie bronne van inkomste, te wete (a) bydraes van Internet-diensverskaffers, (b) rente verkry uit die fonds, en (c) toevallings uit enige ander bron. Sien art 38(2)(a)-(c).

geïnterpreteer word. Daar is reeds hierbo[683] genoem dat artikel 78 van die EKT-wet meld dat 'n diensverskaffer onder geen algemene verpligting staan om te moniteer nie. Tog is daar sopas aangetoon dat die RICA-wet wél so 'n moniteringsverantwoordelikheid op ISP's plaas. Is hierdie twee wette teenstrydig?

Daar word aangevoer dat die antwoord "nee" is. Die RICA-wet skep 'n sisteem waarbinne die ISP wettig mag — en soms móét — moniteer, maar vereis nie enige *algemene aktiewe* monitering nie. Watney verduidelik treffend dat ISP's in Suid-Afrika volgens die RICA-wet oor drie bevoegdhede moet beskik.[684]

In die eerste plek moet 'n ISP in staat wees om kommunikasies te kan onderskep.[685] (Die algemene reël is dat kommunikasies *nie* onderskep mag word nie, en daardie basis word in artikel 2 van die RICA-wet gelê.) Die vermoë om te kan onderskep[686] word uitdruklik in artikel 3 en 30(1)(a) van die RICA-wet uitgestippel, en die regsproses wat gevolg moet word om onderskepping te magtig, word in artikel 16 uitgespel.

In die tweede plek — aldus Watney — moet 'n ISP oor die vermoë beskik om data te kan stoor.[687] Artikel 30(2)(a)(iii) van die RICA-wet bepaal dat kommunikasie-verwante inligting vir 'n tydperk van drie tot vyf jaar nadat

---

683 Afd 6.4.4.2.5.

684 Watney 2007 *International Journal of Electronic Security and Digital Forensics* 51.

685 Watney 2007 *International Journal of Electronic Security and Digital Forensics* 51.

686 Onderskepping en meeluistering/monitering (sien vn 671) is twee verskillende konsepte aldus die RICA-wet. Monitering is die nouer konsep, terwyl onderskepping die wyer konsep is wat ook monitering insluit. Art 1 van die RICA-wet beskou "onderskep" as:

> die deur middel van gehoor of ander verkryging van die inhoud van enige kommunikasie deur die gebruik van enige middel, met inbegrip van 'n onderskeppingstoestel, ten einde sommige van, of die hele inhoud van, 'n kommunikasie beskikbaar te maak aan iemand anders as die sender of ontvanger of bedoelde ontvanger van daardie kommunikasie, en ook die—
>
> (a) meeluistering na so 'n kommunikasie deur middel van 'n meeluistertoestel;
>
> (b) besigtiging, ondersoeking of inspektering van die inhoud van enige onregstreekse kommunikasie; en
>
> (c) afwending van enige onregstreekse kommunikasie van sy bedoelde bestemming na enige ander bestemming,
>
> en het "onderskepping" 'n ooreenstemmende betekenis.

687 Watney 2007 *International Journal of Electronic Security and Digital Forensics* 51.

dit versend is, geberg moet word.[688]

Die derde bevoegdheid waaroor 'n ISP moet beskik, is om regsowerhede te kan help om inligting te bekom aangaande kubermisdaad.[689] Dit is 'n juiste afleiding, want artikels 30, 39, 40 en 47 magtig juis hierdie optrede. Artikel 30 handel oor die vermoë van die ISP om te kan onderskep, asook die berging van kommunikasie-verwante inligting. Artikel 39 handel oor die inligting wat ISP's van hulle kliënte moet ontvang, en slaan duidelik op die identifisering van individue vir 'n moontlike regsproses. Artikel 40 handel oor die verkryging van inligting voordat 'n selfoon se simkaart geaktiveer word, en artikel 47 hanteer die gebruik van inligting in strafregtelike verrigtinge.

Nou is die prentjie aangaande 'n algemene onderskeppingsverpligting geskets, en dit werk eintlik maar soos 'n reuse media-opnemer. Die "sisteem" is so ontwikkel dat dit kommunikasieverwante inligting kan "opneem" (amper soos 'n ou video-opnemer) en bewaar vir die tyd waar dit dalk nodig mag wees om dit weer "terug te speel". Hierdie eenvoudige verduideliking gee, na my mening, tog die nodige konteks om die skynbare teenstrydigheid tussen die EKT-wet se nie-verpligting om te moniteer en die RICA-wet se positiewe verpligting om wél te moniteer met mekaar te kan versoen.

6.4.4.3.2 Oorsigfunksie

Uit die bespreking van die RICA-wet hierbo[690] is dit duidelik dat dié wet omvattende magte aan die Suid-Afrikaanse intelligensiedienste verskaf. Daar is reeds in die bespreking van Internetregulering in die VSA aangetoon hoe 'n soortgelyke vermoë om die breë publiek te kan moniteer, tot

688 Wanneer die betrokke ISP se telekommunikasiedienslisensie uitgereik word, moet 'n voorskrif daarin vervat word wat uitstippel presies hoe lank die bergingproses vir daardie spesifieke diensverskaffer moet wees (art 30(2)(a)(iii)).

689 Watney 2007 *International Journal of Electronic Security and Digital Forensics* 51.

690 Afd 6.4.4.3.

erge skending van privaatheid en menseregte gelei het.[691] Die vraag wat noodwendig na vore tree, is watter oorsigfunksie bestaan daar in Suid-Afrika? Die antwoord is te vinde in twee dele, naamlik oorsig geskep in die RICA-wet self, en oorsig oor die intelligensiedienste.

Die RICA-wet is baie duidelik daaroor dat monitering van kommunikasie in beginsel nie mag plaasvind nie.[692] Hierop bestaan daar 'n hele lys uitsonderings, soos waar 'n persoon self 'n party by die kommunikasie is,[693] of waar onderskepping geskied in die normale verloop van 'n besigheid,[694] soos wat daagliks by inbelsentrums gebeur. In artikels 16 en 17 kan 'n aansoeker by 'n regter aansoek doen om die kommunikasie te onderskep.[695] (Artikel 16 maak voorsiening vir die uitreiking van 'n onderskeppingslasbrief, terwyl artikel 17 voorsiening maak vir intydse onderskepping.)[696] Die term "aansoeker" word wel in die wet omskryf, en dit sluit lede van die polisiediens, die weermag en intelligensiedienste in.[697] Dit is duidelik dat die RICA-wet so geformuleer is dat onderskepping nie sommer na willekeur deur staatsdepartemente soos die intelligensiedienste mag plaasvind nie.

Hierdie formulering is suiwer, maar die probleem word geskep waar die RICA-wet onderskeppingsentrums — wat permanent aan ISP's gekoppel is — magtig.[698] Die intelligensiedienste word nou 'n "oop" kommunikasielyn na *alle* ISP's gegee, en dit is iets wat baie maklik tot misbruik kan

691 Afd 6.4.1.5 en spesifiek afd 6.4.1.5.2.

692 Art 2.

693 Art 4.

694 Art 6

695 Die onderskepping van inligting op 'n elektroniese apparaat deur 'n lid van die polisie, die weermag of intelligensiedienste word ingevolge art 16 of 17 van die RICA-wet gedoen. Hierteenoor word inligting aangaande die eienaarskap van die foon of die simkaart ingevolge art 205 van die Strafproseswet 51 van 1977 verkry (*S v Brown* 2015 JDR 1929 (WCC) op 6: "he had obtained the RICA details relating to the registration/ownership of the phone and SIM card from the service provider ... by applying to a magistrate for a subpoena in terms of sec 205 of the CPA requiring the service provider to provide such information"). Let daarop dat hierdie inligting tydens kontraksluiting tussen die ISP en gebruiker verkry moet word (art 39 van die RICA-wet).

696 Intydse onderskepping is die ekwivalent van die Engelse "real time surveillance".

697 Art 1 omskrywing van "aansoeker".

698 Art 30(1)(a) saamgelees met art 32(1)(c).

lei. Intydse monitering sou immers ook moontlik gewees het deurdat die betrokke ISP deur die intydse moniteringslasbrief aangesê word om intelligensiedienspersoneel te magtig om monitering op hulle netwerke te doen. Dan sou die privaatbeheerde ISP's 'n buffer kon vorm wat misbruik kon verhinder. Soos die wet nou staan, is die moontlikheid van misbruike eenvoudig te groot.[699]

Wanneer artikels 16 en 17 van die RICA-wet gelees word, wil dit voorkom asof oorsig voldoende is, maar wanneer die gevolge van permanent-gekoppelde onderskeppingsentrums deurskemer, word die effektiwiteit van hierdie artikels twyfelagtig.

Die RICA-wet is egter nie die enigste meganisme om 'n oorsigfunksie van onderskepping van kommunikasie deur intelligensiedienste daar te stel nie. Woolman en Bishop verduidelik dat daar ten minste vier ander oorsigmeganismes van die intelligensiedienste in Suid-Afrika bestaan.[700]

Die eerste bestaan uit parlementêre oorsig.[701] In besonder bestaan daar 'n Gesamentlike Staande Komitee oor Intelligensie[702] wat die funksie het om die intelligensiedienste te moniteer. Dit word gemagtig ingevolge artikel 2 van die Wet op Toesig oor Intelligensiedienste.[703] Hierdie komitee word saamgestel volgens verteenwoordiging in die parlement, en is nie toeganklik vir die publiek nie.[704] Die land se verskeie intelligensie-afdelings moet op 'n jaarlikse basis verslae aan die komitee voorlê, wat dit dan ondersoek. Dit is ook moontlik vir 'n lid van die publiek om 'n saak by die komitee aanhangig

699 Dit wil voorkom asof die skrywers van die RICA-wet deeglik bewus was van die geweldige invloed wat 'n permanent-gekoppelde onderkeppingsentrum kan hê, want art 37(2)(ii) meld dat alle misbruike aan die Direkteur van Onderskeppingsentrums deurgegee moet word, en dat die direkteur dit dan weer onder die aandag van die Gesamentlike Staande Komitee oor Intelligensie (sien verduideliking direk hieronder) moet voorlê (art 37(3)). Net soos in die VSA-geval het die Direkteur van Onderskeppingsentrums 'n baie goeie rede om *nie* die nodige inligting rugbaar te maak nie, aangesien dit sy sentrum — waarvan hy die bestuurder is — in 'n swak lig stel.

700 Woolman S en Bishop M *Constitutional Law of South Africa (2nd Edition)* (2014) 54. Let daarop dat hierdie 'n losbladreeks is, en dat bladsyverwysings van toekomstige opdaterings van die huidige nommers kan verskil.

701 Woolman en Bishop *Constitutional Law of South Africa* 56.

702 "Joint Standing Committee on Intelligence" in Engels.

703 40 van 1994.

704 Art 2(2).

te maak, wat dan ondersoek kan word.[705]

Woolman verduidelik dat die tweede meganisme van oorsig die inspekteur-generaal is.[706] Dit word gemagtig ingevolge artikel 210 van die Grondwet van die Republiek van Suid-Afrika.[707] Daar word eweneens verslae deur die land se verskeie intelligensiedienste aan die inspekteur-generaal voorgelê, wat dan ondersoek word. Die inspekteur-generaal kan klagtes van die publiek ondersoek, en is by magte om enige intelligensiediensperseel te betree om die nodige inligting vir sy ondersoek te kry.[708]

Die probleem met hierdie amp is dat die kantoor van die inspekteur-generaal beman word deur intelligensiepersoneel wat deur die minister van Intelligensie verskaf word.[709] Hierdie reëling skep sonder twyfel 'n konflik van belange, en Woolman meld:

> It seems obvious that such an assignment of intelligence staff undercuts the IG's independence. The IG can hardly be called independent when he or she takes direction or relies on operational assistance from the very executive entities he or she may be called upon to investigate.[710]

Die derde wyse waarop oorsig oor die intelligensiedienste in Suid-Afrika bereik word, is deur die Nasionale Intelligensiekoördineringskomitee, wat deur die Wet op Nasionale Strategiese Intelligensie[711] geskep word.[712] In wese is dit 'n komitee wat bestaan uit die hoofde van die land se verskeie intelligensiedienste[713] met die doel om beleidsmakers — spesifiek die president en ministers — in staat te stel om besluite te neem met die beste inligting tot hulle beskikking.[714] Deur die verskillende

705 Woolman en Bishop *Constitutional Law of South Africa* 56.

706 Woolman en Bishop *Constitutional Law of South Africa* 57.

707 1996.

708 Art 7(8) van die Wet op Toesig oor Intelligensiedienste 40 van 1994.

709 Art 7(12).

710 Woolman en Bishop *Constitutional Law of South Africa* 58.

711 39 van 1994.

712 Art 4.

713 Art 4(1).

714 Woolman en Bishop *Constitutional Law of South Africa* 61.

intelligensierolspelers te betrek, word die waarskynlikheid na bewering verminder om intelligensie-inligting te manipuleer.[715]

Die vierde wyse waarop oorsig van intelligensiedienste in Suid-Afrika verkry word, is deur uitvoerende beheer en oorsig.[716] Hiermee word bedoel dat die president en die ministers van Intelligensie, Polisie en Verdediging direkte beheer oor hulle departemente uitoefen. Alhoewel Woolman uitvoerende beheer en toesig as 'n oorsigfunksie lys, wys hy uit hoe interne probleme en politiekery 'n groot probleem skep wat oorsig minimaliseer.[717]

Dit wil voorkom asof nie een van hierdie vier oorsigstrukture na wense funksioneer nie. Die Gesamentlike Staande Komitee oor Intelligensie werk bloot met verslae wat deur intelligensiedienste aan hulle verskaf word, en dit skep dieselfde probleem as die VSA-kongres se oorsigfunksie — meeste senators was nie eens bewus van die bestaan van die metadata-program totdat dit deur Snowden onthul is nie.[718] Net so sal die Gesamentlike Staande Komitee oor Intelligensie nie bewus wees van enige ongeruimdhede as die intelligensiedienste dit nie aan hulle openbaar nie — wat uiteraard nie sal gebeur sonder 'n Snowden-tipe onthulling nie.

Daar is reeds aangetoon hoe die oorsigfunksie van die inspekteur-generaal gebrekkig is — hierdie kantoor kan eenvoudig nie onafhanklik wees as die minister van Intelligensie die personeel verskaf nie.[719] Dieselfde geld vir die Nasionale Intelligensiekoördineringskomitee, waar die waghond bestaan uit 'n komitee met lede wat daarby sal baat dat ongeruimdhede nie openbaar gemaak word nie.[720] Die vierde wyse van oorsig is eweneens nie

715 Woolman en Bishop *Constitutional Law of South Africa* 61.

716 Woolman en Bishop *Constitutional Law of South Africa* 61.

717 Woolman en Bishop *Constitutional Law of South Africa* 61 toon aan hoe die saak van *Masetlha v The President of the Republic of South Africa & Another* (2006) ZAGPHC 107 en *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services: in re Masetlha v President of the Republic of South Africa and Another* 2008 (5) SA 31 (CC) die onderstominge in die verskeie intelligensiedienste blootgelê het.

718 Afd 6.4.1.5.2.

719 Vn 710.

720 Art 4(1).

na wense nie, met interne struwelinge en politiekery wat so 'n oorsigfunksie belemmer.[721]

Die enigste gevolgtrekking wat gemaak kan word is dat die RICA-wet met die skepping van onderskeppingsentrums die Suid-Afrikaanse intelligensiedienste 'n geweldig kragtige sisteem verskaf het waarmee burgers gemoniteer kan word.

6.4.4.4 Struktuur van die Suid-Afrikaanse Intranet

Dit is belangrik om te bepaal hoe die Suid-Afrikaanse intranet gestruktureer is, aangesien dit 'n baie goeie aanduiding kan gee van hoe maklik totale regulering moontlik is. Indien die inkomende kabelnetwerk relatief klein is, kan die Suid-Afrikaanse intranet ook soos die voorval in Egipte gemanipuleer word om toegang te beperk of af te skakel.[722]

Suid-Afrika word aan die Internet gekoppel met behulp van vyf onderssee kabels:[723]

1. Suid-Atlanties 3 / Wes-Afrika Onderwater kabel / Suid-Afrika Verre Ooste (SAT-3 / WASC / SAFE): Hierdie kabel skakel Suid-Afrika aan Europa en die verre ooste (Indië en Maleisië) en is sedert 2002 in gebruik.[724]

2. Seacom (SEACOM): Hierdie kabel skakel Suid-Afrika sedert 2009 met Mosambiek, en dan met Egipte en Saudi Arabië, waarna dit verdeel na Indië en die Verenigde Koninkryk.[725] In Julie 2010 het SEACOM

721 Vn 717.

722 Afd 6.3.5.2.

723 Die eerste kabel wat Suid-Afrika aan die Internet gekoppel het, was die SAT-2 kabel ("South Atlantic 2"). Dit het van 1993 tot 2013 diens gedoen. Information Gatekeepers Inc *Repeatered Submarine Fiber Optics Systems* (1998) 76; Wikipedia "SAT-2" https://en.wikipedia.org/wiki/SAT-2 (besoek op 4 April 2016).

724 Irvine C en Armstrong H *Security Education and Critical Infrastructures* (2003) 120 asook Wikipedia "Internet in South Africa" https://en.wikipedia.org/wiki/Internet_in_South_Africa (besoek op 4 April 2016).

725 Seacom "Seacom" http://seacom.mu/network/ (besoek op 4 April 2016); Dwivedi Y K *Adoption, Usage, and Global Impact of Broadband Technologies: Diffusion, Practice and Policy* (2010) 17.

probleme met hulle kabel ondervind, en groot dele van Suid-Afrika se Internet-beskikbaarheid het daaronder gelei.[726]

3. Oos-Afrika Onderwater Kabelsisteem (EASSy): Hierdie kabel koppel Suid Afrika aan verskeie oos-Afrika lande sedert 2010.[727]

4. Wes-Afrika kabelsisteem (WACS): Hierdie kabelsisteem verbind Suid-Afrika sedert Mei 2012 met die Verenigde Koninkryk.[728]

5. Afrika-kus na Europa (ACE): Hierdie kabelsisteem verbind Suid-Afrika sedert Desember 2012 aan verskeie lande aan die weskus van Afrika, en eindig in die Verenigde Koninkryk.[729]

'n Sesde kabel is tans onder ontwikkeling. Dit is die "South Atlantic Express (SAEx), en behoort teen middel 2018 in gebruik gestel te word. Dit sal die eerste direkte skakeling tussen Suid-Afrika en die VSA bewerkstellig.[730]

Figuur 6.5 bevat 'n visuele voorstelling van hierdie Kabelkoppelings.

Let ook daarop dat daar slegs vier plekke in Suid-Afrika is waar inkomende kabels land, te wete Yzerfontein, Melkbosstrand, Kaapstad (al drie in die suid-Kaap), en Mtunzini (Kwa-Zulu Natal).

6.4.4.5 Samevatting

In hierdie afdeling is daar aangetoon hoe Suid-Afrika sy stukkie van die Internet probeer beheers. Die studie is beperk tot die algemene aanspreeklikheid van Internet-diensverskaffers, omdat dit juis hierdie

726 Salon "Choke Points Leave Us Vulnerable" http://www.salon.com/2010/07/06/yes_technology_fails_sometimes/ (besoek op 4 April 2016).

727 EASSy "What is EASSy" http://www.eassy.org/about.html (besoek op 4 April 2016); Dwivedi *Adoption* 17.

728 Ali K D *Maritime Security Cooperation in the Gulf of Guinea* (2015) 53; Wikipedia "WACS (cable system)" https://en.wikipedia.org/wiki/WACS_%28cable_system%29 (besoek op 4 April 2016).

729 Telegeography "Submarine Cable Map" http://www.submarinecablemap.com/#/submarine-cable/africa-coast-to-europe-ace (besoek op 4 April 2016).

730 Telegeography "Submarine Cable Map" http://www.submarinecablemap.com/#/submarine-cable/south-atlantic-express-saex (besoek op 4 April 2016).

tussengangers is wat 'n sleutelrol speel om die groter publiek toegang tot die Internet te gee, en indien daardie tussengangers deur regsweë beperk word, wys dit watter ideologie die staat inspan om sy doel te verwesenlik.

Daar bestaan vele stukke wetgewing wat Internetgedrag beheer,[731] maar in die konteks van ISP's in Suid-Afrika is dit die Wet op Elektroniese Kommunikasies en Transaksies [732] en die Wet op die Reëling van Onderskepping van Kommunikasies en Verstrekking van Kommunikasie-verwante Inligting [733] wat belangrik is.

Die EKT-wet reguleer die aanspreeklikheid van Internet-diensverskaffers in hoofstuk XI.[734] Toe artikels 70–79 deur die Suid-Afrikaanse wetgewer geformuleer is, is die CDA, die DMCA en veral die EU-regulasies bestudeer, en gevolglik stem sekere van die Suid-Afrikaanse artikels bykans woord-vir-woord met veral die EU-regulasies ooreen.[735] Dit is daarom nie vreemd nie dat dieselfde kategorieë diensverskaffers wat in die EU-regulasie uiteengesit word, ook in die Suid-Afrikaanse wetgewing voorkom.[736] Nie-aanspreeklikheid van ISP's is in wese dieselfde as die EU-regulasies, maar die klein verskille wat wel te bespeur is, is uitgewys.[737]

Die grootste probleem met die nie-aanspreeklikheidsklousules van die EKT-wet is dat dit relatief ontoeganklik is. Artikel 71 van die wet vereis dat daar slegs op die nie-aanspreeklikheidsvereistes staatgemaak kan word indien die ISP aan 'n verteenwoordigende liggaam behoort. In *Tsichlas v Touch Line Media* is aangetoon dat 'n beroep op hierdie vereistes in vele

731 Voorbeelde hiervan is die Wet op die Beskerming van Persoonlike Inligting 4 van 2013 en Wet op Verbruikersbeskerming 68 van 2008. Vir 'n bespreking van eersgenoemde wet, sien Luck R "POPI – Is South Africa Keeping up With International Trends?" 2014 *De Rebus* 44 44. Laasgenoemde wet word onder die loep geneem in Coertse N "Navigating ht Consumer Protection Act 68 of 2008" 2014 *De Rebus* 27 27.

732 25 van 2002. Afd 6.4.4.2.

733 70 van 2002. Afd 6.4.4.3.

734 Afd 6.4.4.2.

735 Afd 6.4.4.2.4.

736 Art 73–75; Afd 6.4.4.2.4.

737 Afd 6.4.4.2.5. Sien bv art 73(1)(c) op bl 388 waar so 'n verskil aangetoon word.

gevalle sal misluk.[738]

Die ontwikkeling van 'n nasionale e-strategie, soos in die EKT-wet voorgestel, is bespreek, en daar is vasgestel dat dit nooit deur die minister ontwikkel is nie, ten spyte daarvan dat dit 'n nasionale prioriteit is. Daar is aangevoer dat die ontwikkeling van so 'n strategie belangrik is, en dat dit uitgebrei moet word om netwerk-ontwerp in te sluit.[739]

Die RICA-wet is ook onder die loep geneem.[740] Ten spyte daarvan dat die RICA-wet telekommunikasiediensverskaffers — en dus ook Internet-diensverskaffers — reguleer, is die trant van die RICA-wet heel anders as van die EKT-wet, aangesien eersgenoemde 'n sisteem skep waarmee *alle* ISP's in Suid-Afrika gemoniteer kan word.[741] Dit is 'n sisteem wat 'n eenvoudiger kombinasie is van dié wat in Sjina en die VSA gevind word. Daarmee word bedoel dat die RICA-wet 'n sisteem skep wat soortgelyk is aan Sjina, deurdat 'n sentrale stelsel, wat deur die Suid-Afrikaanse intelligensiedienste gemoniteer kan word en aan alle ISP's gekoppel is, ontwikkel is.[742] Ongelukkig is daar min inligting beskikbaar oor hoe hierdie stelsel deur die Suid-Afrikaanse geheime diens aangewend word, en die gebrek aan openbare oorsig ("public oversight") is uiters kommerwekkend.[743] Hierteenoor vertoon die Suid-Afrikaanse stelsel ook eienskappe van die VSA-model, aangesien die Suid-Afrikaanse intranet redelik vry is om aan die groter Internet te koppel, en daar geen vorm van inligtingsregulering — soos wel in Sjina die geval is — te vinde is nie.[744] Die Suid-Afrikaanse intranet bestaan uit relatief min in-en-uitgangspoorte, en daarom behoort dit tegnies moontlik te wees om dit van die Internet te ontkoppel — net soos wat Egipte gedoen het — indien dit nodig sou

738 Afd 6.4.4.2.3.

739 Afd 6.4.4.2.6.

740 Afd 6.4.4.3.

741 Afd 6.4.4.3.

742 Afd 6.4.4.3.

743 Afd 6.4.4.3.2.

744 Kelly, Cook en Truong (red) *Freedom on the Net 2015* 702.

wees.[745] Gelukkig het so 'n situasie van anargie hom nog nooit in Suid-Afrika voorgedoen om so 'n stap te noodsaak nie.

6.5 Gevolgtrekking

Die doel van hierdie hoofstuk was om aan te toon hoe soewereine state van die wêreld tans besig is om die Internet te reguleer. Dit is gedoen deur die hoofstuk in twee afdelings te deel: die eerste was om met 'n meer teoretiese verduideliking aan te toon hoe dit vir 'n staat moontlik is om buite sy grense te kan reguleer, en die tweede afdeling toon aan hoe state van die wêreld tans besig is om regulering in plek te sit.[746]

Die eerste afdeling van die hoofstuk het aangetoon dat daar altyd ten minste drie partye by 'n Internet-kommunikasie of -transaksie betrokke is, te wete die bron, 'n tussenganger en 'n teiken.[747] Gewoonlik is al drie hierdie rolspelers binne die jurisdiksie van die staat, maar deur gebruik te maak van veilige hawens is dit moontlik dat een of meer van die rolspelers die jurisdiksie van die staat kan ontduik. Indien dit gebeur, het die staat steeds die vermoë om te reguleer, aangesien slegs *één* van die rolspelers nodig is om die hele proses te manipuleer. Wanneer al drie rolspelers die staat se regsgebied verlaat, is dit emigrasie, en hoef die staat nie meer die betrokke aktiwiteit te reguleer nie.[748]

Die eerste afdeling het ook aangetoon wie die Internet se tussengangers is. Sommige van hierdie rolspelers — soos Internet-diensverskaffers[749] — is voor-die-hand-liggend, maar ander — soos die netwerk sélf[750] — was meer subtiel. Voorbeelde is gebruik om aan te toon hoe sulke tussengangers gereguleer kan word.

745 Afd 6.4.4.4.

746 Afd 6.1.

747 Afd 6.2.1.

748 Afd 6.2.1.

749 Afd 6.3.1.

750 Afd 6.3.5.2.

Die tweede afdeling van die hoofstuk het spesifieke state se reguleringspogings beoordeel.[751] Die VSA, Sjina, Europese Unie en Suid-Afrika is bespreek.

Die VSA se reguleringsisteem vertoon teenstrydighede. Enersyds staan dit 'n vrye Internet met wette soos die CDA en DMCA voor,[752] maar andersyds bedryf dit 'n verskeidenheid koverte operasies op sy eie burgers en nie-burgers.[753] Dit is anders as wat verwag sou word, aangesien die VSA oor die algemeen as 'n vrye land beskou word. In die konteks van Internetregulering is dit veral interessant aangesien dit blyk dat die VSA se buitelandse beleid van 'n oop Internet juis sy koverte operasies bemagtig deurdat meeste van die wêreld se Internetkommunikasie deur die enorme VSA-Internetruggraat vloei en dit op hierdie wyse maklik deur die VSA-regering gemoniteer kan word.[754]

Sjina se reguleringsisteem is — soos te verwag van 'n kommunistiese regeringstelsel — baie beperkend.[755] Dit is ewe insiggewend dat Sjina reeds vanuit die staanspoor besluit het om sy nasionale intranet van die groter Internet af te skei, en dat dit nie 'n latere wysiging was nie.[756] Dit het tot 'n verrassende gevolg gelei — Sjina is waarskynlik die staat wat die beste toegerus is om sy eie intranet te beskerm en dit ongestoord te laat voortgaan indien daar 'n rampspoedige gebeurtenis met die groter Internet sou plaasvind.

'n Verdere aangeleentheid wat uit die bespreking in hierdie hoofstuk duidelik geword het, is die deursnee Sjinese burger se siening oor Internetregulering, naamlik dat dit 'n beskermende funksie verrig, en dat plaaslike ekwivalente van gewilde webwerwe en sosiale platforms die

751 Afd 6.4.

752 Afd 6.4.1.2 en afd 6.4.1.3.

753 Afd 6.4.1.5.

754 Afd 6.4.1.

755 Afd 6.4.2.

756 Afd 6.4.2.2.1.

plaaslike ekonomie bevorder asook nasionalisme aanwakker.[757]

Die Europese Unie se regulasies oor Internet-diensverskaffers is vroeg in die bestaan van die Internet uitgevaardig,[758] en dit het 'n geweldige groot invloed gehad op ander lande, soos Suid-Afrika,[759] waar soortgelyke reëls ingevoer is. Tog word hierdie reëls steeds nie goed ontvang deur die howe van EU-lidlande nie.[760] Die gevolg is verwarring en teenstrydighede tussen lidlande.

Suid-Afrika se Internetreguleringsbeginsels word grotendeels in die EKT-wet en RICA-wet vervat.[761] Eersgenoemde het baie van die EU-beginsels geïnkorporeer, maar byvoegings soos artikel 71 van die EKT-wet — wat onnodige vereistes neerlê wat moeilik is om na te kom — veroorsaak dat vele Internet-diensverskaffers nie op die nie-aanspreeklikheidsklousules wat in die wet vervat word, kan staatmaak nie.[762] Die saak van *Tsichlas v Touch Line Media* het hierdie punt duidelik geïllustreer.[763]

Die EKT-wet bevat verskeie bepalings ten aansien van die ontwikkeling van 'n nasionale e-strategie, maar dit is steeds nie deurgevoer nie, en daar word aangevoer dat dit 'n belangrike kwessie is wat aangespreek moet word. Beginsels van sinvolle netwerk-ontwerp behoort ook by die e-strategie ingesluit te word.[764]

Die RICA-wet het 'n sisteem geskep waar alle ISP's intyds gemoniteer kan word. Dit is maklik vatbaar vir misbruik, en die gevolgtrekking word gemaak dat regshervorming in dié verband ernstig oorweeg behoort te word.[765]

***

Uit die bespreking in hierdie hoofstuk is dit duidelik dat state van die wêreld hulle eie nasionale intranette reguleer volgens die ideologiese

757 Afd 6.4.2.4.5. Sien ook vn 464.

758 Afd 6.4.3.2.

759 Afd 6.4.4.2.4.

760 Afd 6.4.3.3.

761 Afd 6.4.4.2 en afd 6.4.4.3.

762 Afd 6.4.4.2.3.

763 Afd 6.4.4.2.3.

764 Afd 6.4.4.2.6.

765 Afd 6.4.4.3.1.

beginsels wat die betrokke staat voorstaan. Dit verklaar dan ook waarom regulering van die groter Internet so ’n omslagtige proses is. Die oorhoofse gevolgtrekking wat uit die bestudering van hierdie hoofstuk gemaak kan word, is dat state van die wêreld — en ook internasionale organisasies soos in hoofstuk 5 bespreek — daarby sal baat om slegs sake van gemeenskaplike belang te probeer reguleer. Aangeleenthede wat binne die staat se soewereiniteit en ideologiese standpunte val, kan nie sinvol op internasionale vlak gereguleer word nie. Dit sou byvoorbeeld nie sinvol wees om menseregte in Sjina op ’n internasionale reguleringsvlak aan te spreek nie, ten spyte daarvan dat hierdie ’n belangrike saak is. Dit is ’n aangeleentheid wat binne die land se eie soewereiniteit val, en die Internet is reeds so gefragmenteer in nasionale intranette dat daar nie op internasionale vlak sinvolle inspraak in ’n land se regulering van sy intranet kan wees nie. Die ongelukkige waarheid is dat uitsprake soos dié van president Xi Jinping van Sjina korrek is — kubersoewereiniteit is ’n konsep wat in die moderne era van die Internet deur state toegepas kan word,[766] aangesien die Internet lank nie meer een enkele globale netwerk is nie. Die konsep van kubersoewereiniteit en jurisdiksie is die aangeleentheid wat in hoofstuk 7 bespreek sal word.

[766] Afd 6.4.2.4.6.

(a) SAT-3

(b) EASSy

(c) WACS

(d) SEACOM

(e) SAFE

(f) SAEx

Bron: Telegeography "Submarine Cable Map" http://www.submarinecablemap.com (besoek op 4 April 2016).

Figure 6.5: Internetkoppeling in Suid-Afrika

Hoofstuk 7

Kubersoewereiniteit

> *[The] concept of sovereignty is today much misunderstood. The main reason derives from its intrinsic political and legal dimensions. Sovereignty is a fundamental concept of both political and legal thought, expressing the autonomous nature of the State's political power and its specific mode of operation in a distinctively juristic form.*[1]
>
> Richard Rawlings

7.1 Inleiding

SOEWEREINITEIT IS 'N konsep wat tydens die verligting van die laat middeleeue begin ontwikkel het. In sy werk getiteld *Leviathan*,[2] het Thomas Hobbes aangetoon dat mense se lewenskwaliteit kan verbeter indien daar 'n sterk en soewereine heerser is wat inwoners kan beskerm.[3] Die basis van so 'n verhouding is die gedagte van die *sosiale kontrak*. Jean Bodin,[4] 'n Franse juris en filosoof, het soortgelyke uitsprake gemaak.[5]

---

1 Rawlings R, Leyland P en Young A *Sovereignty and the Law: Domestic, European and International Perspectives* (2013) 35.

2 Hobbes T *Leviathan* (1651).

3 Tuck R (red) *Hobbes Leviathan Revised Student Edition* (1996) 155–156.

4 Jean Bodin (1530–1596) word veral onthou vir sy werk oor soewereiniteit. Hy was 'n lid van die parlement van Frankryk en professor in die Regte in Toulouse, Frankryk. Franklin J H (red) *Bodin on Sovereignty* (1992) 1–3 asook Franklin J H *Jean Bodin and the Sixteenth-century Revolution in the Methodology of Law and History* (1977) 61.

5 Pocock J G A *The Ancient Constitution and the Feudal Law: A Study of English Historical Thought in the Seventeenth Century* (1987) 80.

Hierdie skrywers se sienings het geweldige aanhang geniet totdat die Franse rewolusie van 1789 die begin van soewereine state ingelei het.[6]

Die wêreld, soos dit vandag bestaan, is volledig gebou op die beginsels van territoriale soewereiniteit.[7] Ten spyte daarvan dat territoriale soewereiniteit die basis van die moderne staat vorm, is dit 'n konsep wat verbasend ontwykend is. Wendt en Duvall verwoord die frustrasie van vele regskenners:

> Few ideas today are as contested as sovereignty, in theory or in practice. In sovereignty theory scholars disagree about almost everything — what sovereignty is and where it resides, how it relates to law, whether it is divisible, how its subjects and objects are constituted, and whether it is being transformed in late modernity.[8]

Lauterpacht stel dit effens sagter:

> The concept of sovereignty is still with us today. The question is whether it means anything. In particular, we must ask ourselves whether the use of the word "sovereignty" really contributes significantly to contemporary political debate — especially on the plane of international relations.[9]

Dit is buite die trefwydte van hierdie studie om enige pogings aan te wend om teenstrydige standpunte oor soewereiniteit aan te spreek of te ontleed. Kubersoewereiniteit as 'n *species* van soewereiniteit sal in hierdie hoofstuk bestudeer word, en daar sal bepaal word of dit enigsins regtens bestaanbaar kan wees. Sou so 'n konsep nuttig kon wees in die soeke na 'n Internetregulerings-*regime* wat meer toepaslik is as die huidige een? Ten einde nader aan 'n antwoord op hierdie vraag te kom, word die konsepte van soewereiniteit en staatskap vervolgens bespreek.

---

6 Sien ook Schultz T "Carving up the Internet: Jurisdiction, Legal Orders, and the Private/public International Law Interface" 2008 *European Journal of International Law* 799 807 vir 'n verdere bespreking oor die invloed wat hierdie twee skrywers op die *psige* van die mense van hul tyd gehad het.

7 Schultz 2008 *European Journal of International Law* 807.

8 Wendt A en Duvall R "Sovereignty and the UFO" 2008 *Political Theory* 607 607.

9 Lauterpacht E "Sovereignty-myth or Reality?" 1997 *International Affairs* 137 138.

7.2 Soewereiniteit en Staatskap

Die enkele grootste probleem met die konsep van soewereiniteit is dat dit ’n verskeidenheid konsepte ondervang. Gallie noem byvoorbeeld dat soewereiniteit kan “appraisive, complex, elusive, and evolving characteristics” hê.[10] Hobbes en Bodin het soeweriniteit nog beskou as ’n konsep waar ’n regeerder absolute mag en gesag het, en geensins aan sy eie wette onderdanig is nie.[11] Hierdie konsep van soewereiniteit is aldus Jovanović nie meer in die moderne wêreld van veel nut nie.[12]

In die konteks van hierdie studie is dit belangrik om te begryp dat soewereiniteit en staatskap (“statehood”) nie sinonieme is nie. Die klassieke (en steeds aanvaarde) omskrywing van staatskap is te vinde in die *Montevideo Convention on the Rights and Duties of States* van 1935.[13] Artikel 1 bepaal:

> The state as a person of international law should possess the following qualifications: (a) a permanent population; (b) a defined territory; (c) government; and (d) capacity to enter into relations with the other states.[14]

’n Staat wat aan hierdie vereistes voldoen, kan sonder inmenging van ’n ander staat outonoom funksioneer.[15] Dit sal funksies insluit soos om mag uit te oefen oor burgers van die land, besluite te neem oor buitelandse beleid,[16] oorlogs- en vredesverklarings te maak[17] en oor die algemeen te beslis oor aspekte wat die grondgebied van die staat sal beïnvloed.[18] Kortom, die staat

10 Gallie W B “Essentially Contested Concepts” 1955 *Proceedings of the Aristotelian Society* 167 167–198.

11 Jovanović M en Henrard K (red) *Sovereignty and Diversity* (2008) 2.

12 Jovanović en Henrard *Sovereignty and Diversity* 2–3 noem voorbeelde van gevalle in die een-en-twintigste eeu waar dit blyk dat Hobbes en Bodin se oorspronklike konsep van soewereiniteit nie meer water hou nie.

13 *Inter-American Convention on the Rights and Duties of States* LNTS Vol 165 19.

14 *Montevideo Convention on the Rights and Duties of States* 1935 art 1.

15 Oppenheim L F L *International Law* (2008) 384 en Shaw M N *International Law* (2008) 180 en 183.

16 Shaw *International Law* 147.

17 Shaw *International Law* 812; Jackson R H *Quasi-States: Sovereignty, International Relations and the Third World* (1993) 39.

18 Shaw *International Law* 355.

is volgens die Internasionale reg 'n regspersoon in eie reg,[19] is outonoom,[20] en alle state van die wêreld is gelyk voor die reg.[21] State mag nie in mekaar se sake inmeng nie.[22]

Soewereiniteit is egter iets anders. Duursma verduidelik dat:

> Sovereignty is considered a consequence of statehood, not a prerequisite thereof. It is the 'totality of international rights and duties recognized by international law' vested in States.[23]

As die konsep van soewereiniteit tot op die been gesny word — soos Duursma dit hier doen — blyk dit dat soewereiniteit die *regte, verpligtinge* en *magte* is wat 'n staat kan uitoefen. Indien hierdie eenvoudige verklaring van 'n moeilike onderwerp moontlik vreemd voorkom, kan daar aangetoon word dat Duursma nie die enigste skrywer is wat hierdie sienswyse huldig nie. Barker verduidelik dat soewereiniteit die "rights and obligations of nations" is,[24] terwyl Fowler en Bunck aantoon hoe 'n staat internasionale verpligtinge opdoen wanneer dit op soewereiniteit staat maak.[25] Hulle verduidelik dan verder dat: "Sovereignty is a declaration of *political responsibility* for governing, defending, and promoting the welfare of a human community".[26] Die voorbeeld word genoem van hoe Argentinië tydens die Falkland-oorlog die internasionale gemeenskap se roede op die hals gehaal het deurdat hulle hul "regte" wou uitoefen, maar nie die resulterende verpligting nakom om vir die mense van die eiland te sorg

19 Rai D *Statehood and the Law of Self-Determination* (2002) 19.

20 Oppenheim *International Law* 384 en Shaw *International Law* 180 en 183.

21 Rai *Statehood and the Law of Self-Determination* 31; art 4 van die *Montevideo Convention on the Rights and Duties of States.*

22 Art 8 van die *Montevideo Convention on the Rights and Duties of States.*

23 Duursma J *Fragmentation and the International Relations of Micro-states: Self-determination and Statehood* (1996) 121.

24 Barker J *Sovereignty Matters: Locations of Contestation and Possibility in Indigenous Struggles for Self-determination* (2005) 2.

25 Fowler M R en Bunck L M *Law, Power, and the Sovereign State: The Evolution and Application of the Concept of Sovereignty* (2010) 12: "What may be less frequently recognized is that to claim sovereignty is also to incur international obligations".

26 My kursivering. Fowler en Bunck *Law, Power, and the Sovereign State* 12.

nie.[27]

Lauterpacht som dit mooi op wanneer hy sê dat soewereiniteit is:

> ... the term used to describe the right of a state freely to exercise its *power* under customary international law without the permission of any other state in relation to *persons, things and relationships within its territory.*[28]

In 'n neutedop omvat staatskap dus die *wese* van die staat, terwyl jurisdiksie die *regte, verpligtinge* en *magte* van die staat uiteensit.

Taylor is van mening dat hierdie siening van staatskap en jurisdiksie korrek is, maar dat dit as die tradisionele siening van die Internasionale reg beskou moet word.[29] In die moderne era het verskeie nuwe rolspelers op die internasionale front begin funksioneer, naamlik internasionale organisasies.[30] Hulle is tot stand gebring deur internasionale ooreenkomste in die vorm van verdrae, en hulle tree dikwels namens state op. Voorbeelde hiervan is *legio*, soos die Internasionale Telekommunikasie Unie[31] en die Organisasie vir Internasionale Burgerlugvaart.[32]

Taylor meen verder dat die konsepte van staatskap en soewereiniteit nie dieselfde is nie (soos vroeër in hierdie afdeling bespreek), en dat 'n duideliker onderskeid getref moet word om 'n meer praktiese en werkbare sisteem te skep.[33] In die konteks van die werking van internasionale organisasies het 'n staat 'n "bundle of powers" wat hy kan uitgee aan internasionale organisasies.[34] Hierdie "bundle of powers" is eintlik maar die regte, verpligtinge en magte van soewereiniteit.[35] Indien 'n staat van

27 Fowler en Bunck *Law, Power, and the Sovereign State* 13.

28 My kursivering. Lauterpacht 1996 *International Affairs* 140.

29 Taylor C R "A Modest Proposal: Statehood and Sovereignty in a Global Age" 1997 *University of Pennsylvania Journal of International Economic Law* 745 752.

30 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 752.

31 Afd 5.3.3.

32 Afd 4.2.2.2.4.

33 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 753.

34 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 754–755; Mcveigh S *Jurisprudence of Jurisdiction* (2007) 68 meen eweneens dat soewereiniteit "verdeelbaar" is: "Sovereignty is at once divisible, temporal and contingent. It is capable of being divided and held by an 'occupying power'".

35 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 754–755.

sy bevoegdhede aan ’n internasionale organisasie afwentel, delegeer die staat sekere dele van sy soewereiniteit, maar deur dit te doen word die staat se staatskap nie negatief beïnvloed nie — die staat bly ’n staat met staatsgesag — en die internasionale organisasie word eweneens nie skielik ’n staat omdat hy een van die staat se ontbondelde soewereiniteitsfunksies verrig nie. Taylor verduidelik dit soos volg:

> A State may allocate portions of its bundle of powers to other actors without becoming any less a State and that those actors receiving direct or indirect allocations of power do not thereby become “States”.[36]

Om hierdie konsep te illustreer, gebruik Taylor die voorbeeld van die eiendomsreg van grond.[37] ’n Grondeienaar kan ’n servituut aan ’n buurman toestaan sodat laasgenoemde by sy pypsteel-erf kan uitkom. Deur dit te doen kan die buurman nou regmatig die servituut betree, en het die buurman die reg om die servituut te gebruik, maar die eienaar bly die eienaar van die grond — ook die deel met die servituut op. Deur die servituut toe te staan het die grondeienaar nie nou minder grond nie — die hele erf behoort steeds aan hom ten spyte van die bestaan van die servituut. Net so sal ’n staat nie enige van sy verdeelbare soewereiniteitsregte, -verpligtinge en magte prysgee wanneer dit sekere funksies aan internasionale organisasies delegeer nie.[38]

Soewereiniteit is dus nie ’n enkele konsep wat ’n enkele inhoud het nie. Dit is eerder ’n bondel van regte, verpligtinge en magte wat oorgedra kan word, en ook herroep kan word.[39] Wanneer enige van die magte oorgedra word, is die nuwe houer nie ’n staat nie, net soos die gebruiker van die servituut nie die eienaar van die grond is nie.[40]

Om die onderskeid tussen die elemente van staatskap en jurisdiksie verder tuis te bring, noem Taylor dat staatskap te doen het met “claim”-

36 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 753.

37 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 754–755.

38 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 755.

39 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 755.

40 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 755.

elemente, terwyl soewereiniteit te doen het met "exercise"-elemente.[41] "Claim"-elemente kan nie uitgedeel word nie, aangesien dit die wese van staatskap raak, maar "exercise"-elemente kan wel aan ander state of internasionale organisasies gedelegeer word.

Die "claim"-elemente bestaan uit die tradisionele siening van staatskap. Dit is die vier elemente wat in die *Montevideo Convention on the Rights and Duties of States* gelys word, en dit bepaal wat 'n staat moet besit om as 'n afsonderlike entiteit in die Internasionale reg beskou te word.[42] Dit is iets wat die staat nie kan uitdeel nie.[43] Taylor bespreek wat met die vier elemente van staatskap in die *Montevideo Convention on the Rights and Duties of States* bedoel word. Hierna bespreek sy ook 'n aantal "exercise"-elemente. Die wyse waarop sy dit identifiseer is deur die feit dat sulke magte wel aan ander state en organisasies uitgedeel kan word sonder om die staatskap van die staat te beïnvloed. Die "exercise"-elemente is: (a) outonomie, (b) ondeurdringbaarheid en (c) gelykheid.[44]

Outonomie verwys na 'n staat se vermoë om onafhanklik van buitelandse beheer te kan funksioneer, tensy dit uitdruklik toestem dat inmenging kan plaasvind.[45] 'n Voorbeeld hiervan is die funksies van die *International Civil Aviation Organisation*, aangesien state van die wêreld aan hierdie organisasie die bevoegdheid delegeer om sake van gemeenskaplike belang in die lugruim te reël. Taylor voer aan dat state in vandag se wêreld nie totaal outonoom is nie, aangesien daar dikwels aan ander state in die *forum* van die Verenigde Nasies verslag gedoen moet word.[46] Tog kan 'n staat sekere bevoegdhede uitdeel, soos waar 'n internasionale ooreenkoms geteken word en die staat se gesag daarmee

41 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 756.

42 Artikel 1 van die *Montevideo Convention on the Rights and Duties of States* bepaal: "The state as a person of international law should possess the following qualifications: (a) a permanent population; (b) a defined territory; (c) government; and (d) capacity to enter into relations with the other states".

43 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 761.

44 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 762–767.

45 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 762.

46 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 762.

verminder word, of waar ’n staat gesag oorgee aan ’n internasionale organisasie.[47]

Ondeurdringbaarheid as “exercise”-element het te doen met die vermoë van ’n staat om teen enige indringing weerstand te bied. Die belangrikste aangeleentheid hier is sekerlik die territoriale grense van die staat. Binne die grense daarvan het die staat uitsluitlike gesag.[48] Dit kan egter ook gedelegeer of beperk word, soos waar menseregte-skendings aan die Verenigde Nasies gerapporteer word.[49]

Die laaste “exercise”-element wat Taylor bespreek, is gelykheid.[50] Taylor voer aan dat, ten spyte van die Verenigde Nasies se grondwet wat bepaal dat alle state gelyk is,[51] dit in werklikheid nie die geval is nie. Sekere lande is groter en sterker en het meer gesag as ander, en dit beïnvloed hulle status teenoor mekaar in die internasionale arena.[52]

***

Die vraag mag ontstaan waarom daar so ’n groot gewag gemaak word van die onderskeid tussen staatskap en soewereiniteit, en ook waarom Taylor se artikel so breedvoerig bespreek is. Die antwoord daarop is dat hierdie onderskeid tussen konsepte krities belangrik is vir die bespreking wat volg. Die term kubersoewereiniteit is op die oomblik ’n mode-woord (“buzz-word”) in die media, maar daar bestaan min regsartikels wat die basis daarvan probeer vasstel. Daar moet begryp word dat kubersoewereiniteit byvoorbeeld slegs deur bestaande state van die wêreld gevestig kan word, want soewereiniteit is ’n gevolg van staatskap.[53] Gevolglik kan die inhoud van kubersoewereiniteit slegs sover strek as wat die regte, verpligtinge en magte van die staat strek — staatskap beperk

47 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 762.

48 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 764.

49 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 765.

50 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 766.

51 Art 2(1) van die “Charter of the United Nations”.

52 Taylor 1997 *University of Pennsylvania Journal of International Economic Law* 766.

53 Vn 23.

kubersoewereiniteit.[54] Die "claim"-elemente van staatskap soos in die *Montevideo Convention on the Rights and Duties of States* uiteengesit, sal grootliks nie sin maak in die konteks van kubersoewereiniteit nie. Wat beteken die konsep van 'n permanente bevolking by kubersoewereiniteit? Wat is 'n bepaalde grondgebied in die kuberruim, en hoe word dit bepaal? Die antwoord word baie eenvoudiger wanneer daar begryp word dat hierdie laaste twee vrae nie deel vorm van kubersoewereiniteit nie, maar eerder 'n kwalifikasie is van die entiteit (die staat) wat op kubersoewereiniteit aanspraak maak. Let op hoe 'n stelling soos hierdie dadelik onjuis klink wanneer die konsepte van staatskap en kubersoewereiniteit verwar word:

> [C]yberspace changes the face of nations' sovereignty by introducing the notion of the cyber-sovereignty of nations and thus expanding the entirety of nations' sovereignty. In other words, territorial sovereignty within national boundaries has been transferred to *a*-territorial sovereignty without boundaries in cyberspace.[55]

Die kuberruim is geen "plek" nie, en 'n staat se grense kan nie na die kuberruim "skuif" nie. Dit is alles deel van staatskap, en die staat wat kubersoewereiniteit vestig, se staatskap is reeds gevestig en staan onafhanklik van sy kubersoewereiniteit.[56] Die enigste dimensie wat bygevoeg word wanneer state kubersoewereiniteit vestig, is om nouer beheer te neem oor die staat se regte, verpligtinge en magte ten aansien van Internetkommunikasie van sy nasionale bevolking.

Hierdie stelling is moontlik die belangrikste in hierdie bespreking en word dus weer herhaal: ál wat state doen wanneer hulle kubersoewereiniteit

---

54 Lindsay J R, Cheung T M en Reveron D S *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (2015) 132 formuleer dit korrek dat: "In sum, one should set cyber rules on the ground of respecting cyber sovereignty, not only that of one's own country but also that of other countries".

55 Zekos G I "Cyber-Territory and Jurisdiction of Nations" 2012 *Journal of Internet Law* 3 10.

56 McGhee J E "Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy" 2013 *Journal of Law & Cyber Warfare* 64 85 verwar die konsep van staatskap en kubersoewereiniteit wanneer hy sê dat "although no State may claim sovereignty over cyberspace *per se*, States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure". Die eerste stelling is foutief, want kubersoewereiniteit is bloot 'n uitoefening van die staat se regte, verpligtinge en magte in die kuberruim. Die tweede stelling is korrek, want 'n staat het inderdaad uitsluitlike bevoegdheid om oor aangeleenthede binne sy fisiese grondgebied te beslis (in hierdie geval intranet-infrastruktuur). Dit is egter 'n gevolg van staatskap, en nie kubersoewereiniteit nie.

vestig, is om nouer beheer te neem oor hulle regte, verpligtinge en magte ten aansien van Internetkommunikasie van hulle bevolking.

In die konteks van Taylor se konstruksie is "claim"-elemente deel van staatskap, en behoort dit nie aanwending te vind by kubersoewereiniteit nie. Hierteenoor is die "exercise"-elemente wel toepaslik by kubersoewereiniteit. Om kubersoewereiniteit te kan vestig, moet 'n staat se intranet outonoom kan funksioneer. Die staat-intranet[57] moet in so 'n mate onafhanklik wees dat buitelandse beheer nie sonder meer kan plaasvind nie.[58] Dieselfde geld vir die "exercise"-element van ondeurdringbaarheid. Kortom beteken dit dat 'n land soos Sjina baie makliker kubersoewereiniteit kan vestig as wat Rusland — wat ook 'n voorstaander van kubersoewereiniteit is — sal kan doen.

7.3 Vestiging van Kubersoewereiniteit

Sjina het by monde van president Xi Jinping in Desember 2015 uitdruklik genoem dat dit 'n voorstander van kubersoewereiniteit is.[59] President Xi Jinping het ongelukkig nie breedvoerig uitgebrei oor wat Sjina daarmee bedoel nie, maar sy toespraak bevat genoeg inligting dat daar bepaal kan word wat kubersoewereiniteit aldus Jinping behoort te behels.

Jinping sê die volgende in sy toespraak by die *Second World Internet Conference*:

> To make progress in the transformation of the global Internet governance system, the following principles must be upheld:
>
> **— Respect for cyber sovereignty.** The principle of sovereign equality enshrined in the Charter of the United Nations is one of the basic norms

[57] Let daarop dat die benaming "staat-intranet" in hierdie studie dui op die netwerk van die land, of staat, wat vir gebruik deur al sy inwoners beskikbaar is, en *nie* die konsep van 'n netwerk wat slegs vir die regering of staats-instansie beskikbaar is nie. "Staat-intranet" word dus volgens die Internasionale reg se konsep van 'n staat beoordeel as die oorkoepelende netwerk wat in 'n betrokke staat of land ontwikkel word om almal te dien.

[58] Voorbeelde van krakery ("hacking") is uitsonderings en hierdie optrede is onregmatig, net soos wat die indring van 'n fisiese gebied onregmatig is.

[59] Afd 6.4.2.4.6. Sjina het egter reeds in 2014 gemeld dat kubersoewereiniteit 'n prioriteit is. Segal A *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (2016) 32.

> in contemporary international relations. It covers all aspects of state-to-state relations, which also includes cyberspace. We should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries' national security. [60]

Hierdie stelling bevat 'n rits stellings oor kubersoewereiniteit in die algemeen — sommige daarvan behandel die konsep van staatskap ("claim"-elemente) en ander bevat aangeleenthede oor kubersoewereiniteit *per se* ("exercise"-elemente). Die elemente wat oor staatskap handel, en wat bloot gerespekteer moet word, is (a) respek vir kubersoewereiniteit; (b) staatsgelykheid volgens die Handves van die Verenigde Nasies; (c) onderhandeling oor kuber-regering (van gemeenskaplike belang) op gelyke voet en (d) nie-inmenging in state se interne sake asook nasionale sekuriteit.[61]

Die eintlike kubersoewereiniteits-aangeleenthede is: (a) die vermoë van 'n staat om oor die ontwikkeling van sy eie intranet te besluit en (b) sy eie model van intranetregulering te kies. Daar sal nou oorgegaan word tot 'n bespreking van hierdie twee aangeleenthede.

7.3.1 Ontwikkeling van 'n Eie Intranet

Met die ontwikkeling van 'n eie intranet het Jinping duidelik in gedagte dat elke staat die bevoegdheid het om sy eie intranet na goeddunke te ontwerp en te struktureer. Dit slaan op die fisiese argitektuur van die netwerk, en sluit in die wyse waarop netwerke aanmekaar gesit word, asook die interkonneksie tussen die netwerke (internetwerk) om uiteindelik die

[60] Ministry of Foreign Affairs of the People's Republic of China "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference" http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml (besoek op 15 April 2016).

[61] Stelling (d) het ongetwyfeld betrekking op die VSA se breedvoerige Internet-afluistertering wat in 2013 deur Snowden ontbloot is. Afd 6.4.1.5.2.

groter intranet van die staat te vorm.[62] Alhoewel Sjina op die wêreldverhoog hierdie stelling as ’n voorstel aanbied, is dit reeds vir dekades besig om juis dié oogmerk tot stand te bring. Reeds in 1996 het Sjina begin om hulle intranet van die groter Internet af te skei,[63] en vandag is die Sjinese intranet so suksesvol dat dit in ’n groot mate ’n kleiner spieëlbeeld van die groter Internet is.[64]

Wanneer die Internasionale reg met betrekking tot kubersoewereiniteit op hierdie aspek toegepas word, is dit duidelik dat Sjina by uitstek die staat is wat aan hierdie vereiste voldoen. Sjina se intranet is volledig van die groter Internet afgeskei deur die *Golden Shield*-sisteem, en daar bestaan ook breedvoerige wetgewing in Sjina wat bepaal hoe netwerke saamgestel moet word, hoe hulle moet skakel aan die groter internetwerk, asook die koppeling aan staatsbeheerde sisteme.[65] Die intranet in Sjina is geografies onafhanklik van die groter Internet. Daar word voldoen aan die “exercise”-element van die ontwikkeling van ’n eie intranet.

Sjina is egter nie die enigste staat wat hierdie roete volg nie. Daar bestaan reeds ’n verskeidenheid projekte wat op ’n meer subtiele wyse poog om ’n vorm van kubersoewereiniteit te vestig, veral waar dit staatsbelange beskerm. Drie projekte sal vervolgens uitgewys word om hierdie verskynsel aan te dui. Eerstens is daar ’n beweging dat state van data-lokalisering gebruik maak om sensitiewe inligting binne die grense van hul state te hou. Tweedens neem state toenemend meer stappe in die internasionale sfeer om hul nasionale intranette te beskerm, en derdens bestaan daar ’n projek wat met ’n alternatiewe basis-DNS eksperimenteer. Dit kan tot gevolg hê dat die Internet in so ’n mate fragmenteer dat state se intranette totaal onafhanklik funksioneer. Hierdie drie projekte naamlik data-lokalisering, beskerming van nasionale intranette en alternatiewe

62 Afd 6.4.2.3.1.

63 Afd 6.4.2.2.1.

64 Afd 6.4.2.4.5 vn 464.

65 Afd 6.4.2.3.1.

basis-DNS eksperimentering word vervolgens bespreek.

7.3.1.1 Data-lokalisering

'n Nuwe ontwikkeling wat sterk eienskappe van kubersoewereiniteit vertoon, is data-lokalisering. Daarmee word bedoel dat die betrokke staat aktiewe stappe neem (gewoonlik deur wetgewing) om data binne die staat te hou. Hill definieer dit soos volg:

> These are laws that limit the storage, movement, and/or processing of data to specific geographies and jurisdictions, or that limit the companies that can manage data based upon the company's nation of incorporation or principal situs of operations and management.[66]

Die behoefte aan data-lokalisering het duidelik geword nadat Edward Snowden in 2013 aangetoon het hoe die VSA 'n spioenasieprogram bedryf wat data kan ontleed wat deur die VSA se Internet-ruggraat vloei.[67] (Omdat die VSA die mees ontwikkelde Internet-tegnologie het, vloei meeste van die wêreld se data deur die VSA.)[68]

Daar is huidig ten minste vier voorstelle om data-lokalisering 'n werklikheid te maak.[69] Die eerste is in Duitsland, waar kanselier Angela Merkel na die Snowden onthullings aangedui het dat sy van mening is dat sulke stappe nodig is, "so that you don't have to go across the Atlantic with emails and other things, but can build up communications networks also within Europe."[70] *Deutsche Telecom* werk reeds aan hierdie voorstel.[71] Net so is daar in Brasilië 'n soortgelyke program van stapel gestuur nadat

66 Hill J F "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for US Policymakers and Industry Leaders" 2014 *The Lawfare Institute, Lawfare Research Paper Series* 1 3.

67 Afd 6.4.1.5.2, veral bl 314.

68 Afd 6.4.1.5.2, veral bl 314.

69 Hill 2014 *The Lawfare Institute, Lawfare Research Paper Series* 9.

70 New York Times "Merkel Backs Plan to Keep European Data in Europe" http://www.nytimes.com/2014/02/17/world/europe/merkel-backs-plan-to-keep-european-data-in-europe.html?hp&_r=0 (besoek op 15 April 2016).

71 New York Times "Merkel Backs Plan to Keep European Data in Europe" http://www.nytimes.com/2014/02/17/world/europe/merkel-backs-plan-to-keep-european-data-in-europe.html?hp&_r=0 (besoek op 15 April 2016).

dit geblyk het dat die VSA die Brasiliaanse president se kommunikasie gemonitor het, asook die netwerk van die land se grootste oliemaatskappy, *Petrobas*, geïnfiltreer het.[72] Dieselfde tipe reaksie het ook in Indië voorgekom nadat die Snowden-onthullings aangetoon het dat Indië een van Amerika se grootste teikens vir data-inwinning is.[73]

Die vierde voorstel om data te lokaliseer, is dié van die Europese Unie, waar gebruikersdatabeskerming reeds lank 'n belangrike aangeleentheid is.[74] Die EU se *Data Protection Directive* is reeds in 1995 aanvaar, en dit behels dat sensitiewe inligting oor persone in die EU — soos mediese inligting — nie sonder meer buite Europa moet vloei nie.[75] Hierdie direktief het vroeg reeds probleme gegee met handel in die VSA omdat laasgenoemde nie aan die vereistes van die direktief voldoen het nie.[76] Die oplossing van die probleem was dat maatskappye in Europa direk met handelsvennote in die VSA kon ooreenkom om sisteme in plek te sit wat die nodige beskerming bied, en dus aan die direktief se vereistes voldoen.[77]

---

72 Hill 2014 *The Lawfare Institute, Lawfare Research Paper Series* 16.

73 Hill 2014 *The Lawfare Institute, Lawfare Research Paper Series* 19.

74 Hill 2014 *The Lawfare Institute, Lawfare Research Paper Series* 12.

75 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data.* Deacon J *Global Securitisation and CDOs* (2004) 476 verduidelik dat: "The Directive set out certain requirements for dealing with "personal data", including the requirement that personal data should not be transferred outside the European Economic Area unless the recipient territory has adequate personal data protection provisions".

76 Rustad M *Global Internet Law* (2013) 125 verduidelik:

> The US. did not satisfy the European Commission's (EC) standard for adequate privacy precautions in the 1990s after the Data Protection Directive was enacted. ... Under the current EU Data Protection Directive, a company is required to get explicit consent from data subjects as to the collection of data on race, ethnicity, political opinions, union membership, physical health, mental health, sexual preferences, and criminal records. ... Member States prohibit the transfer of personal information across national borders unless the receiving country has implemented an adequate level of protection. The United States' sectorial privacy protection did not comply with the European standard of adequately protecting consumer privacy.

Sien ook De Busser E *Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters Between Judicial and Law Enforcement Authorities* (2009) 116 vn 394.

77 Rustad *Global Internet Law* 126 verduidelik: "The safe harbor relies almost completely on self-policing and almost no empirical evidence exists on whether US. companies comply with the safe harbor principles".

Daar is egter oor die laaste dekade besef dat die uitvoering van hierdie direktief problematies is, en gevolglik het die Europese Parlement begin werk aan 'n nuwe direktief wat die *Data Protection Directive* kon vervang.[78] Na die Snowden-onthullings het hierdie pogings nuwe *impetus* gekry, en die nuwe *General Data Protection Regulation* is op die 8ste April 2016 aanvaar.[79] Dit is 'n geweldig omvangryke stuk wetgewing wat in die fynste besonderhede persoonlike data-inwinning, -versending en -berging hanteer. Hoofstuk V van die direktief, getiteld "Transfer of Personal Data to Third Countries or International Organisations" bevat byvoorbeeld breedvoerige inligting oor die vereistes waaraan voldoen moet word voordat sensitiewe persoonlike inligting elektronies buite die EU versend mag word.[80] Omdat die direktief so omvangryk is, sal dit eers binne twee jaar (dus middel-2018) in werking tree, sodat diensverskaffers en ander rolspelers die nodige sekuriteitsmaatreëls in plek kan sit om aan die direktief te kan voldoen.[81] 'n Voorbeeld hiervan is dat die data-inwinner nie slegs moet toesien dat die data veilig bewaar en versend word nie, maar selfs ook sisteme in plek moet sit wat *aantoon* dat die data korrek hanteer is — sisteme wat owerhede in staat sal stel om 'n ouditfunksie te kan verrig.[82]

7.3.1.2 Beskerming van Nasionale Intranet

Die wortels van kubersoewereiniteit is eweneens te vinde in die onlangs aangepaste ITU-grondwet, (wat in 2011 tydens die ITU-gevolmagtigde

78 Wikipedia "General Data Protection Regulation" https://en.wikipedia.org/wiki/General_Data_Protection_Regulation (besoek op 16 April 2016)

79 European Commission *Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection* (14 April 2014) Statement/16/1403.

80 Council of the European Union *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* (2016) hfst V.

81 European Commission *Joint Statement on the Final Adoption of the New EU rules for Personal Data Protection* (14 April 2014) Statement/16/1403.

82 Art 22(1) van die finale konsep-*General Data Protection Regulation* bepaal byvoorbeeld dat "the controller shall implement appropriate technical and organisational measures to ensure *and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation*". (My kursivering.)

vergadering aangeneem is en op 1 Januarie 2012 in werking getree het).[83] Artikel 34(2) meld byvoorbeeld dat:

> Member States also reserve the right to cut off, in accordance with their national law, any other private telecommunications which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency.[84]

Die gronde vir blokkering van enige telekommunikasie — dus ook ontkoppeling van die groter Internet — is duidelik, te wete staatsveiligheid, miskenning van wetgewing van die staat, en selfs beskerming van die openbare orde.

Artikel 35 gaan selfs verder deur te bepaal dat:

> Each Member State reserves the right to suspend the international telecommunication service, either generally or only for certain relations and/or for certain kinds of correspondence, outgoing, incoming or in transit, provided that it immediately notifies such action to each of the other Member States through the Secretary-General.[85]

In noodsituasies mag state selfs hulle *hele* internasionale telekommunikasiedienste van die groter netwerk verwyder. Dus sal optrede soos deur Egipte, wat tydens ernstige burgerlike oproer hulle hele land van die groter Internet ontkoppel het, volgens hierdie bepaling regmatig wees.[86]

7.3.1.3 Alternatiewe Basis-DNS

Een van die kommerwekkendste uitdrukkings van kubersoewereiniteit is projekte waar daar met alternatiewe basis-DNS-dienste geëksperimenteer

---

83 International Telecommunications Union *Collection of the Basic Texts of the International Telecommunication Union Adopted by the Plenipotentiary Conference: Edition 2011* (2011) ongenommerde bl — "Message from the Secretary General".

84 *Constitution of the International Telecommunication Union* Art 34(2) in International Telecommunications Union *Collection of the Basic Texts of the International Telecommunication Union Adopted by the Plenipotentiary Conference: Edition 2011* (2011) 37.

85 *Constitution of the International Telecommunication Union Art* 35 in International Telecommunications Union *Collection of the Basic Texts of the International Telecommunication Union Adopted by the Plenipotentiary Conference: Edition 2011* 38.

86 Afd 6.3.5.2 bespreek die geval waar Egipte hulle hele telekommunikasiestelsel van die Internet ontkoppel het.

word. Die werking van die basis-DNS is reeds in afdeling 2.3.4 bespreek, en daar is aangetoon hoe dit die kern van die hele Internet vorm. Indien die basis-DNS bedieners ontkoppel word, sal die hele Internet binne ure nie meer ander netwerke kan opspoor nie.

Die sogenaamde *Yeti*-projek is daargestel om 'n toetsplatform te wees vir nuwe tegnologieë wat op die Internet geïnkorporeer kan word, maar wat nog nie gereed is om op die werklike Internet geplaas te word nie.[87] Toetsing kan op *Yeti* plaasvind sonder om die groter Internet te beïnvloed. Dit is 'n uitstekende toetsplatform, maar die wyse waarop *Yeti* funksioneer, is om 'n kopie van die basis-DNS bediener te maak, die sekurtiteitsprotokolle daarvan af te sny, en dit met nuwe *Yeti*-protokolle te stempel. Die gevolg is dat 'n alternatiewe basis-DNS gevorm word.[88] Indien die twee bedieners identies bly, is daar nie 'n probleem nie, maar indien die inskrywings verskil en *Yeti* aan die groter Internet gekoppel sou word, sou dit die basis-DNS bedieners "vergiftig" met foutiewe inligting.[89] Dan kan dit gebeur dat dieselfde IP-adres na twee verskillende bedieners wys.

Hierdie is 'n hipotetiese geval, maar die werklikheid is soos volg: die skepper van die *Yeti*-projek, Paul Vixie, het *Yeti* geskep in noue samewerking met die Sjinese regering.[90] Die gedagte is dat 'n basis-DNS bediener met sy eie staatgelokaliseerde basis-DNS geskep kan word, en *daardie* basis-DNS bediener aan die groter Internet gekoppel word. Elke staat van die wêreld sal dan 'n intranet hê wat soos 'n graansilo werk — elke staat se intranet is *totaal* afgesluit van die groter Internet. Dan sal stellings soos dié van ICANN se president, Fadi Chehadé 'n werklikheid wees:

> The moment we fragment the Internet it is possible there will be tariffs between borders, there will be rules ... it will not be the Internet as we know

87 Yeti DNS Project "A Live Root DNS Server System Testbed" https://yeti-dns.org/ (besoek op 16 April 2016).

88 World Economic Forum *Internet Fragmentation: An Overview* (2016) 28.

89 World Economic Forum *Internet Fragmentation* 34.

90 Internet Governance Project "Alternate DNS Roots and the Abominable Snowman of Sovereignty" http://www.internetgovernance.org/2016/04/07/alternate-dns-roots-and-the-abominable-snowman-of-sovereignty/ (besoek op 16 April 2016).

it.[91]

Die alombekende Vinton Cerf stel dit in 'n verslag van die *World Economic Forum* so:

> More generally, if ever leading governments or intergovernmental organizations were to implement an alternate root — a possibility that was sometimes raised in the highly charged geopolitical context of the WSIS negotiations — the results could be a game changer. Indeed, the establishment of an alternate root that has significant government backing arguably would be the *mother of all fragmentations*.[92]

Hierdie voorbeelde is alles wyses waarop die "exercise"-elemente van kubersoewereiniteit gevestig kan word. Dit is alles maniere waarop die betrokke staat van die wêreld — wie se staatsgesag reeds vasstaan — sy regte, verpligtinge en magte van kubersoewereiniteit uitoefen om 'n meer direkte beheer oor die netwerk wat geografies binne sy grondgebied is, uit te oefen.[93]

7.3.2 Eie Model van Intranetregulering

'n Verdere uitlating van Xi Jinping oor kubersoewereiniteit tydens sy toespraak by die *Second World Internet Conference,* was dat elke staat die bevoegdheid het om sy eie model van intranetregulering te kies.[94] Dit verwys na 'n kwessie wat reeds vir dekades in die internasionale Internetreguleringsdebat woed: dat alle state van die wêreld meer direkte seggenskap moet hê oor Internet-aangeleenthede wat van gemeenskaplike belang is.[95] Dit verwys ook spesifiek na die kwessie van die basis-DNS en die VSA se hantering daarvan om dit nie te wil prysgee nie.[96]

---

91 Huffpost Business "Fadi Chehadé: If We Fragment The Internet, 'It Will Not Be The Internet As We Know It'" http://www.huffingtonpost.com/2014/01/24/fadi-chehade-davos_n_4635949.html (besoek op 14 April 2016).

92 My kursivering. World Economic Forum *Internet Fragmentation* 28.

93 Afd 7.2.

94 Afd 7.3.

95 Afd 4.2.4.

96 Afd 3.4.1.

Hierdie stelling word duidelik vanuit ’n diplomatieke posisie gedoen, want Sjina het reeds sedert sy aansluiting by die groter Internet dit duidelik gemaak wat sy voorkeurmetode van Internetregulering is — ’n *legio* regulasies is sedert die middel-negentigerjare uitgevaardig wat baie duidelik aandui wat Sjina se standpunt hieroor is.[97] As “exercise”-element van kubersoewereiniteit staan dit Sjina vry om sy eie intranetreguleringsmetode te kies, en geen ander staat kan enigiets daaroor sê nie aangesien dit binne die regsfeer van Sjina se eie bevoegdhede val.

Al wat Xi Jinping met sy uitlatings oor hierdie aspek in sy toespraak maak, is om die wêreld te versoek om Sjina se keuse van intranetreguleringsmodel te respekteer.[98] Sjina word (met reg) geweldig daaroor gekritiseer, veral vanweë die feit dat sy intranetreguleringsmodel veral menseregte tot ’n groot mate aan bande lê. Dit is egter alles in lyn met Sjina se kommunistiese ideologie, en net soos wat state van die wêreld nie oor Sjina se kommunistiese bestel invloed het nie, is die keuse van ’n bepaalde model van intranetregulering wat aan sy ideologie voldoen, ook nie binne die seggenskap van wêreldstate nie.

7.3.3 Samevatting

Kubersoewereiniteit is ’n aangeleentheid wat al hoe meer op die wêreldverhoog aandag begin geniet. Die staatshoof van Sjina, Xi Jinping, het tydens die *Second World Internet Conference* in 2015 verskeie uitlatings gemaak en daarmee aangetoon dat kubersoewereiniteit vir Sjina ’n nasionale prioriteit

97 Afd 6.4.2 verduidelik volledig Sjina se wyse van Internetregulering.

98 Valls A *Ethics in International Affairs: Theories and Cases* (2000) 117 noem byvoorbeeld: “Embedded in the international system is a commitment on the part of *states to respect state sovereignty*. In addition, the United Nations affirms in Article 2(7) a principle of nonintervention...”. (My kursivering.) International Commission on Intervention and State Sovereignty *The Responsibility to Protect: Research, Bibliography, Background : Supplementary Volume to the Report of the International Commission on Intervention and State Sovereignty* (2001) 5 noem hierteenoor dat “Empirically, *sovereignty has routinely been violated by the powerful*. In today’s globalizing world, it is generally recognized that cultural, environmental, and economic influences neither respect borders nor require an entry visa. ... territorial boundaries have come under stress and have diminished in significance as a result of contemporary international relations”. (My kursivering.)

is.[99] Twee "exercise"-elemente van kubersoewereiniteit is geïdentifiseer, te wete die vermoë van 'n staat om oor die ontwikkeling van sy eie intranet te besluit en om sy eie model van intranetregulering te kies.[100]

Daar is aangetoon dat die vermoë van 'n staat om oor die ontwikkeling van sy eie intranet te besluit tot 'n groot mate afhang van die mate waarin hy sy intranet struktureer. In die geval van Sjina is netwerkbeheer al so ver gevorder dat dit relatief maklik op kubersoewereiniteit kan aanspraak maak.[101]

Ander state van die wêreld is ook besig om op 'n mindere of meerdere mate in die rigting van kubersoewereiniteit te beweeg. Na die Snowden-onthullings het state soos Duitsland, Brasilië, Indië en die groter Europese Unie begin om data-lokalisering in werking te stel om optrede soos dié van die VSA te probeer fnuik.[102]

State begin ook besef dat 'n groter beheer oor hulle nasionale telekommunikasiedienste belangrik word — veral in die konteks van handhawing van wet en orde in noodsituasies. Gevolglik is die ITU-grondwet reeds in 2011 aangepas om hierdie behoefte te regverdig, en staan dit state vry om die nodige stappe te neem om sulke maatreëls in werking te stel.[103]

'n Kommerwekkende verwikkeling in die elektroniese onafhanklikheid van state is die eksperimentering met alternatiewe basis-DNS-dienste. Dit het die vermoë om die Internet fundamenteel te omvorm in totaal geïsoleerde nasionale netwerke met nasionale smoorpunte ("choking points").[104]

'n Tweede "exercise"-element van kubersoewereiniteit is bespreek, naamlik die vermoë van 'n staat om 'n eie model van intranetregulering te kies. Daar is aangetoon dat dit 'n staat vry staan om so 'n model te kies en in

99 Afd 7.3.

100 Afd 7.3.

101 Afd 7.3.1.

102 Afd 7.3.1.1.

103 Afd 7.3.1.2.

104 Afd 7.3.1.3.

werking te stel, soos wat Sjina reeds vir dekades mee besig is.[105]

***

Enige Internasionaalregkundige sal weet dat die onderwerp van soewereiniteit — en in hierdie geval kubersoewereiniteit — oneer aangedoen sal word indien jurisdiksie nie ook saam met dit bespreek word nie.[106] Dit is twee onderwerpe wat hand aan hand gaan, en Crawford stel dit mooi wanneer hy sê: "'Jurisdiction is ... a consequence of sovereignty'".[107] Dit is egter eweneens waar dat jurisdiksie net so 'n omvattende konsep soos soewereiniteit is, en om te probeer om die *nuances* daarvan in hierdie studie te bespreek, sal nie sinvol wees nie.[108] Tog is dit nodig om enkele aangeleenthede van jurisdiksie te bespreek, maar dit sal slegs gedoen word in die mate wat dit op kubersoewereiniteit te doen het, en dit sal eweneens slegs in die konteks van die Internasionale reg bespreek word.

7.4 Jurisdiksie

In die konteks van die Internasionale reg is dit baie moeilik om 'n spesifieke definisie van jurisdiksie[109] neer te pen. Ten spyte hiervan word jurisdiksie gewoonlik beskou as die bevoegdheid van 'n staat om gesag oor 'n bevolking uit te oefen.[110] Handl stel dit so: "Jurisdictional authority may be asserted to

105 Afd 7.3.2.

106 Die twee konsepte hou nou verband: Dromgoole S *Underwater Cultural Heritage and International Law* (2013) 18 meld byvoorbeeld dat: "Two interrelated concepts of major significance in the field of international law are sovereignty and jurisdiction". Net so sê Farer T J (red) *Beyond Sovereignty: Collectively Defending Democracy in the Americas* (1996) 32 dat "the common theme is that matters pertaining to exclusive domestic jurisdiction are closely related to the sovereignty of the state".

107 Crawford J *Brownlie's Principles of Public International Law* (2012) 456–457.

108 Tsagourias N en Buchan R *Research Handbook on International Law and Cyberspace* (2015) 34 verduidelik treffend die verskillende vorme van jurisdiksie: jurisdiksie in die internasionale privaatreg bepaal of 'n hof die bevoegdheid het om 'n saak aan te hoor; wetgewende jurisdiksie ("legislative jurisdiction") hanteer die vraag of die staat wetgewing oor 'n saak mag maak en beregtende jurisdiksie ("adjudicative jurisdiction") bepaal of 'n hof in 'n strafsaak mag verhoor.

109 Die term jurisdiksie word verkry van die samevoeging van die twee Latynse terme *iuris* en *dicere* wat onderskeidelik "reg" en "om te spreek/praat" beteken. Handl G, Zekoll J en Zumbansen P *Beyond Territoriality: Transnational Legal Authority in an Age of Globalization* (2012) 14 vn 9.

110 Dromgoole *Underwater Cultural Heritage and International Law* 18; Fowler en Bunck *Law, Power, and the Sovereign State* 12.

protect a community from an internal or external threat to its coherence".[111] Jurisdiksie word binne 'n geografiese gebied uitgeoefen,[112] en state sal oor die algemeen baie huiwerig wees om jurisdiksie buite daardie gebied te vestig.[113]

Uit hierdie beskrywing is dit duidelik dat jurisdiksie en territorialiteit baie nou saamhang. Wanneer hierdie beginsels egter op die Internet toegepas word, skep dit probleme aangesien territorialiteit in die fisiese wêreld en dié van die kuberruim in die meeste gevalle nie ooreenstem nie. By state met 'n goed afgebakende intranet soos Sjina sal die kuberruim se territorialiteit en die fisiese wêreld s'n grootliks ooreenstem, maar elders in die wêreld vloei data steeds relatief maklik oor landsgrense.[114] Wat is die algemene beginsels wat by territorialiteit en jurisdiksie op die Internet ter sprake kom?

Die antwoord is moontlik eenvoudiger as wat met die eerste oogopslag mag blyk, aangesien die vrae aangaande territorialiteit en jurisdiksie reeds dekades gelede in die Internasionale reg deurgetrap is — die beginsels wat uitgekristalliseer het, behoort slegs vir die kuberruim aangepas te word. 'n Studie daarvan begin met die alombekende *SS Lotus-saak,* wat reeds in 1927 deur die *Permanent Court of International Justice* beslis is.[115]

Op die 2de Augustus 1926 het die Franse skip genaamd die *SS Lotus* met 'n Turkse skip genaamd die *Boz-Court* op die oop see gebots.[116] Die *Boz-Court* het gesink, en die *Lotus* se bemanning kon sommige van die drenkelinge red. Ongelukkig was daar agt *Boz-Court*-matrose wat in die ongeluk omgekom het. Die *Lotus* het dadelik na die hawe in Konstantinopel (Turkye) gevaar, waar 'n ondersoek geloods is. Die Franse bemanningslid

111 Handl, Zekoll en Zumbansen *Beyond Territoriality* 14.

112 Dromgoole *Underwater Cultural Heritage and International Law* 18.

113 Reinold T *Sovereignty and the Responsibility to Protect: The Power of Norms and the Norms of the Powerful* (2013) 84 meld dat state "do not believe that they have a legal obligation to protect civilians in areas outside of their jurisdiction".

114 'n Goeie voorbeeld hiervan is die VSA, wat relatief min beperkings op data-vloei plaas. Afd 6.4.1.

115 Publications of the Permanent Court of Internatrional Justice Series A no 10 1927.

116 Op 10 van die uitspraak.

wat tydens die botsing die uitkyk-nagwag was, is gearresteer en in 'n Turkse hof van strafbare manslag aangekla. Die beskuldigde het hierteen kapsie gemaak en aangevoer dat die Turkse hof nie jurisdiksie gehad het nie. Die hof het hierdie pleit van die hand gewys en hom aan strafbare manslag skuldig bevind.[117]

Volgens die Turkse owerhede het hulle die volste reg gehad om die beskuldigde aan te kla, aangesien artikel 6 van die Turkse Strafkode van 1926 uitdruklik bepaal het dat 'n buitelandse burger in Turkye vervolg mag word, mits hy in Turkye gearresteer is.[118] Dit is belangrik om daarop te let dat die Turkse Strafkode regverdiging vir die vervolging van 'n buitelandse burger verkry, deur te bepaal dat indien die *gevolg* van die misdryf vir Turkye of 'n Turkse burger raak, dit jurisdiksie sal vestig.[119]

Frankryk het teen hierdie optrede kapsie gemaak en aangevoer dat die bemanningslid tydens die ongeluk aan boord van die *Lotus* was — wat die vlag van Frankryk gewaai het en aan Frankryk behoort het — en dat Frankryk dus die uitsluitlike jurisdiksie gehad het om die bemanningslid te verhoor en te vonnis.[120] Frankryk het aangevoer dat Turkye foutiewelik opgetree het om jurisdiksie te vestig en die bemanningslid te verhoor. Die saak is na die Internasionale Geregshof[121] verwys. Daar het die hof duidelike uitsprake oor jurisdiksie en territorialiteit gemaak.

In die eerste plek het die hof verduidelik dat die Internasionale reg die verhoudings tussen outonome state reguleer, en dat enige reëls wat bindend

---

117 Op 11 van die uitspraak.

118 Art 6 van die Turkse Strafkode bepaal soos volg:

> Any foreigner who, apart from the cases contemplated by Article 4, commits an offence abroad *to the prejudice of Turkey or of a Turkish subject*, for which offence Turkish law prescribes a penalty involving loss of freedom for a minimum period of not less than one year, shall be punished in accordance with the Turkish Penal Code *provided that he is arrested in Turkey*. The penalty shall however be reduced by one third and instead of the death penalty, twenty years of penal servitude shall be awarded. (My kursivering.)

119 Vn 118. Op 15 van die uitspraak.

120 Op 8 van die uitspraak.

121 "Permanent Court of International Justice" in Engels.

op ’n staat is, uit óf konvensies óf gevestigde gebruike tussen lande spruit.[122] Lande kom deur gebruikmaking van ooreenkomste ooreen om sekere sake op ’n spesifieke manier te reguleer, en dus tree die staat uit eie vrye wil op. Die hof meld spesifiek dat: “Restrictions upon the independence of States cannot therefore be presumed”.[123]

Die hof maak dan die volgende belangrike beslissing:

> Now the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.[124]

Die beginsel is baie duidelik — ’n staat mag nie sy jurisdiksie buite die staat uitoefen nie, tensy daar een of ander magtigende reël bestaan wat dit toelaat.

Die hof kwalifiseer dan hierdie stelling deur te bepaal dat ’n staat *binne sy grense* die vryheid het om jurisdiksie uit te oefen selfs al is daar nie ’n volkeregtelike beginsel wat dit spesifiek magtig nie:

> Far from laying down a general prohibition to the effect that States may not extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, it leaves them in this respect a wide measure of discretion, which is only limited in certain cases by prohibitive rules; as regards other cases, every State remains free to adopt the principles which it regards as best and most suitable. This discretion left to States by international law explains the great variety of rules which they have been able to adopt without objections or complaints on the part of other States … In these circumstances all that can be required of a State is that it should not overstep the limits which international law places upon its jurisdiction; within these limits, its title to exercise jurisdiction rests in its sovereignty.[125]

Met die eerste oogopslag wil dit lyk asof hierdie twee uitsprake van die hof teenstrydig is. Tog word daar twee basisbeginsels neergelê, te wete:

---

122 Op 18 van die uitspraak.

123 Op 18 van die uitspraak.

124 18–19.

125 Op 19. Hierdie beginsel is in die onlangse opinie van die Internasionale Geregshof in *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo* (2010) bevestig.

1. 'n Staat kan nie mag *buite sy grondgebied* uitoefen nie tensy daar 'n Internasionaalregtelike beginsel is wat dit magtig.

2. 'n Staat het 'n vrye diskresie om jurisdiksie *binne sy grondgebied* te vestig.[126]

Die hof som dan die beginsels wat neergelê is, soos volg op:

> all that can be required of a State is that it should not overstep the limits which international law places upon its jurisdiction; within these limits, its title to exercise jurisdiction rests in its sovereignty.[127]

Die reëls wat hierdeur neergelê is, vorm die basis van jurisdiksie en territorialiteit. Daar is egter 'n uitsondering wat spesiale aandag verg, te wete *strafregtelike* jurisdiksie. Die hof verduidelik dat bykans alle moderne regstelsels die konsep van jurisdiksie uitbrei wanneer dit by die Strafreg kom.[128] In sulke gevalle is die uitoefening van jurisdiksie *wyer* as territorialiteit. Die hof stel dit so:

> The territoriality of criminal law, therefore, is not an absolute principle of international law and by no means coincides with territorial sovereignty.[129]

Die hof verklaar hierdie uitsondering aan die hand van twee beginsels in die Internasionale reg. In die eerste plek het state algehele vryheid om wette te maak wat binne hulle regsgebied val. Dit sluit wette in wat jurisdiksie buite hulle regsgebied vestig. Die enigste beperking op wetgewing van dié aard is dat dit nie teen beginsels van die Internasionale reg moet indruis nie.[130] Die ander verklaring wat die hof aanbied, is dat bykans alle state van die wêreld wetgewing uitvaardig wat ekstra-territoriale werking het, en dit 'n algemene gebruik van die Internasionale reg is.[131]

---

126 *R v Pienaar* 1948 1 SA 925 (A) op 929–930; *Commissioner of Taxes, Federation of Rhodesia v McFarland* 1965 1 SA 470 (W) op 473F; *Coin Security Group (Pty) Ltd v Smit* 1991 2 SA 315 (T).

127 Op 19.

128 Op 20.

129 Op 20.

130 Op 20.

131 Op 20.

Wat sal dan die basis wees om ekstra-territoriale jurisdiksie te vestig? Die hof verduidelik dat indien die *gevolg* van die misdryf wat in die buiteland gepleeg is, in die staat wat die ekstra-territoriale wetgewing bevat, gevoel word, kan dit strafregtelike jurisdiksie vestig.[132] In die huidige geval is die Turkse wetgewing juis so geformuleer, en beslis die hof dat Turkye korrek opgetree het in hulle vervolging van die beskuldigde.[133]

Ten spyte daarvan dat hierdie 'n baie ou beslissing is, is daar vele toepassings wat op die kuberruim gemaak kan word.

Die eerste beginsel wat die hof neerlê, is dat 'n staat nie sy mag buite sy grondgebied mag uitoefen nie.[134] Dit is 'n beginsel wat algemeen aanvaar word — indien een staat die grondgebied van 'n ander staat wil inval, sal dit in die internasionale gemeenskap veroordeel word. Net so is dit onverantwoordbaar om bedieners of rekenaarstelsels in ander state binne te dring.[135]

In die tweede plek het state vrye diskresie om jurisdiksie binne hulle grondgebied te vestig. Hierdie vorm van jurisdiksie het 'n geweldige wye omvang. State kan jurisdiksie vestig oor fisiese intranet-argitektuur soos rekenaarstelsels, bedieners en telefoon- en telekommunikasienetwerke. Dan kan bestaande en nuut gestigte sisteme gereguleer word, soos die registrasie van domein-name of registrasieprosedures wat neergelê word om netwerke te gebruik. Tsagourias verduidelik dit so:

> With regard to cyberspace, a State can exercise jurisdiction over cyber infrastructure located on its territory and over its nationals when engaged in cyber activities. It can also do so over non-nationals located in its territory. A State can exercise jurisdiction over information circulated

132 Op 23.

133 Op 23, 30 en 31.

134 Op 18–19.

135 'n Voorbeeld hiervan is kuber-spioenasie. Smeby L C, Chapple M en Seidl D *Cyberwarfare* (2014) 5 definieer dit so:

> Cyberespionage involves intrusions onto computer systems and networks designed to steal sensitive information that may be used for military, political, or economic gain. Cyberespionage is akin to traditional intelligence-gathering operations that seek to gain access to protected information.

> through cyberspace at the point of delivery as well as the point of reception or when the information crosses through wires and lines falling within its jurisdiction. A State can exercise jurisdiction over web addresses to the extent they are registered in a specific country. In sum, the State can exercise its prescriptive and enforcement jurisdiction over cyberspace and over cyber activities on the basis of nationality and territoriality.[136]

Hier is Sjina ongetwyfeld die beste voorbeeld. Daar is in hoofstuk 6 aangetoon hoe Sjina sy intranet-argitektuur tot in die fynste besonderhede reguleer.[137] Die fisiese argitektuur word beheer, en registrasieprosedures word neergelê om anonieme gebruik van die intranet aan bande te lê.[138]

Ander minder gesofistikeerde state maak ook tot 'n minder mate van binnelandse jurisdiksievestiging gebruik om hulle intranette te reguleer. Suid-Afrika maak gebruik van die kontroversiële onderkeppingsentrums soos deur RICA bepaal,[139] state soos Duitsland, Brasilië, Indië en die Europese Unie stel data-lokalisering in werking om inligting te beskerm[140] — kortom, hierdie tegniek word in elke staat van die wêreld gebruik om sy eie intranet tot 'n mindere of meerdere mate te reguleer.

In die *Lotus*-saak wys die hof hoe state van die wêreld ekstra-territoriale jurisdiksie vestig. Hierdie beginsel is ook in die kuberruim van toepassing. Daar hoef nie eers verder as die Wet op Elektroniese Kommunikasies en Transaksies 25 van 2002 gesoek te word om dit te vind nie. Artikel 90 bepaal dat 'n Suid-Afrikaanse hof ten aansien van enige misdryf op die Internet jurisdiksie kan vestig indien die misdryf (a) in Suid-Afrika gepleeg is; (b) 'n voorbereidingshandeling tot die misdryf of enige deel daarvan in Suid-Afrika gepleeg is, of dit 'n uitwerking in die republiek het; (c) die misdryf deur 'n Suid-Afrikaanse burger gepleeg is, of (d) die misdryf aan boord van 'n Suid-Afrikaanse skip of vliegtuig gepleeg is.[141] Trouens, jurisdiksievestiging

136 Tsagourias en Buchan *Research Handbook on International Law and Cyberspace* 19.

137 Afd 6.4.2.

138 Afd 6.4.2.4.

139 Afd 6.4.4.3.

140 Afd 7.3.1.1.

141 Art 90 van die Wet op Elektroniese Kommunikasies en Transaksies 25 van 2002.

is gewoonlik nie die probleem nie, maar eerder die uitvoering van hofbevele waar die beskuldigde hom nie binne die regsgebied van die hof bevind nie.[142]

Die laaste stelling wat die hof in die *Lotus*-saak gemaak het wat hier bespreek sal word, is dat dit state vry staan om wetgewing te maak wat ekstra-territoriale jurisdiksie vestig, *mits dit nie teen die Internasionale reg indruis nie.*[143] Die Internasionale reg reguleer verhoudings tussen state, en by implikasie die reëls wat geld, sodat daar so min as moontlik konflik tussen state voorkom. Wat die hof hier impliseer is dat 'n staat nie wetgewing met ekstra-territoriale werking kan maak indien dit die belange van ander state negatief beïnvloed nie. Wanneer hierdie aspek in gedagte gehou word, is daar 'n interessante parallel wat getrek kan word met netwerk neutraliteit.[144] Met sy verduideliking van netwerk neutraliteit staan Wu nie 'n absolute vrye netwerk voor nie, maar meen dat die netwerk-eienaar vry is om die netwerk te bestuur (en by implikasie te manipuleer) solank gebruikers, sowel as die groter netwerk nie negatief beïnvloed word nie. In sy oorspronklike artikel oor netwerk neutraliteit stel hy dit so:

> The principle achieves this by adopting the basic principle that broadband operators should have full freedom to "police what they own" (the local network) while restrictions based on inter-network indicia should be viewed with suspicion.[145]

Wanneer jurisdiksie ten aansien van die Internet gevestig word, behoort dieselfde beginsel te geld. Die staat het die diskresie om jurisdiksiewetgewing te skryf na goeddunke, maar die groter integriteit van die Internet moet in gedagte gehou word wanneer dit gedoen word. 'n Hipotetiese voorbeeld hiervan sal wees dat 'n staat soos Sjina 'n alternatiewe basis-DNS-sisteem

142 Grabosky P N en Smith R G "Telecommunications and Crime: Regulatory Dilemmas" 1997 *Law and Policy* 317 327; Tsagourias en Buchan *Research Handbook on International Law and Cyberspace* 34.

143 Op 20 van die *Lotus*-beslissing.

144 Afd 4.2.3.1.

145 Wu T "Network Neutrality, Broadband Discrimination" 2003 *Journal on Telecommunications and High Technology Law* 141 165.

in werking stel,[146] en dít aan die groter Internet koppel met die regverdiging dat die bediener binne sy staat se grense val en daarom binne sy uitsluitlike jurisdiksie. In so 'n geval word die realiteit van vergiftiging van die hele Internet se basisbedieners 'n werklikheid, en kan dit groot skade aan die groter Internet aanbring. Volgens die beginsel van netwerk neutraliteit in die konteks van die *Lotus*-saak, behoort so 'n sisteem nie aanvaar te word nie, aangesien dit die groter netwerk asook die belange van ander state negatief beïnvloed.

***

Aan die begin van afdeling 7.4 is daar aangedui dat jurisdiksie 'n omvangryke onderwerp is. Dit mag daarom voorkom asof die bespreking van jurisdiksie hierbo nie die omvang daarvan na wense illustreer nie. Soos vroeër verduidelik is jurisdiksie in afdeling 7.4 slegs bespreek in die mate waarop dit van toepassing is op kubersoewereiniteit. Dit bly steeds die doel van die bespreking hierbo.

Ander dele van die studie het wel ook sydelings aangetoon hoe jurisdiksie deur state en howe hanteer word. Afdeling 6.3 het byvoorbeeld aangetoon hoe regerings van tussengangers gebruik maak om buite hulle state te reguleer.[147] Dit is 'n indirekte wyse van regulering, maar dit veronderstel die vestiging van jurisdiksie. Net so is daar deurgaans met hierdie studie aangetoon hoe howe die aangeleentheid van jurisdiksie aanspreek om reg in hul staat te laat geskied. Die reeks *Yahoo v Licra*-beslissings[148] is sekerlik die beste voorbeeld hiervan. Aangesien hierdie studie meerendeels te doen het met die Internasionale publiekreg, sou dit nie sinvol wees om die uitgebreide veld van jurisdiksie in die Internasionale

146 Afd 7.3.1.3.

147 Sien ook Tsagourias en Buchan *Research Handbook on International Law and Cyberspace* 31 waar daar aangetoon word dat regulering van tussengangers dikwels die voorkeurmetode is wat state gebruik om te reguleer, en dat jurisdiksievestiging in die gebied van die staat die wyse is waarop dit afgedwing kan word.

148 Afd 2.3.6.2.

privaatreg te probeer bespreek nie.[149] Dit sou die studie in 'n heel ander rigting stuur. Tog is dit belangrik dat hierdie punt wel uitgewys moes word.

7.5 Gevolgtrekking

Staatsoewereiniteit is die basis waarop die moderne wêreld gebou is.[150] Ten spyte hiervan is dit steeds 'n konsep wat verwarrend en moeilik beskryfbaar is. Moontlik is die rede daarvoor dat soewereiniteit 'n verskeidenheid konsepte ondervang.[151]

In hierdie hoofstuk is die konsepte van "soewereiniteit" en "staatskap" nader toegelig, en daar is aangetoon dat dit nie sinonieme is nie.[152] Die algemeen aanvaarde definisie van "staatskap" is te vinde in die *Montevideo Convention on the Rights and Duties of States* van 1935. Dit bevat eienskappe wat eie is aan 'n staat, en daar is aangetoon dat hierdie eienskappe as "claim"-elemente beskou kan word, omdat dit iets is waarop die staat bloot kan staat maak, en dat dit nie verder uitgedeel kan word nie.[153]

Hierteenoor is daar aangetoon dat soewereiniteit te doen het met die regte, verpligtinge en magte van 'n staat. Dit is die sogenaamde "exercise"-elemente, aangesien dit elemente is wat 'n staat kan delegeer, soos byvoorbeeld dat 'n internasionale organisasie sekere sake namens die staat hanteer.[154]

Wanneer die onderskeid tussen staatskap en soewereiniteit begryp word, word dit duidelik dat wanneer 'n staat kubersoewereiniteit vestig, dit slegs besig is om nouer beheer te neem oor sy regte, verpligtinge en

149 Voorbeelde hiervan is Svantesson D J B *Private International Law and the Internet* (2012) 19; Forsyth C F *Private International Law: The Modern Roman Dutch Law Including the Jurisdiction of the High Courts* (2003) 96; Hörnle J *Cross-border Internet Dispute Resolution* (2009) 19; Øren J S T *International Jurisdiction and Consumer Contracts* (2004) 27 (Jurisdiksie in die Europese Unie); Spang-Hanssen H *Cyberspace Jurisdiction in the US* (2001) 75.

150 Afd 7.1.

151 Afd 7.2.

152 Afd 7.2.

153 Afd 7.2.

154 Afd 7.2.

magte ten aansien van sy telekommunikasiedienste. Dit is iets wat nie op internasionale vlak onderhandel hoef te word nie, maar bloot deur die staat uitgeoefen kan word.[155]

In hierdie hoofstuk is daar aangetoon hoe state van die wêreld besig is om kubersoewereiniteit te vestig.[156] Die voorloper hiervan is Sjina,[157] maar aangesien die Snowden-onthullings op internasionale vlak aangetoon het hoe wydverspreid kuber-spioenasie is, het ander state ook begin om in die rigting van kubersoewereiniteit te beweeg. Voorbeelde hiervan is Duitsland, Brasilië, Indië en die Europese Unie, wat almal besig is om planne in werking te stel om meer outonome telekommunikasiedienste te verkry.[158] Data-lokalisering is dus een van die wyses wat gebruik word om meer outonoom ten aansien van Internetdienste te wees.

Hierdie is nie die enigste wyse waarop state nader aan kubersoewereiniteit beweeg nie. Die beskerming van 'n staat se nasionale intranet word al hoe belangriker soos wat dit 'n groter aandrywer van ekonomiese groei word. Die ITU-grondwet is in 2011 gewysig om hierdie realiteit te weerspieël, en dit staan state nou vry om 'n reeks maatreëls in plek te plaas om hulle nasionale intranette te beskerm.[159]

Die ontwikkeling van alternatiewe basis-DNS-dienste is ook onder die loep geneem. Hierdie verwikkeling is uiters kommerwekkend, aangesien dit die Internet so kan fragmenteer dat dit fundamenteel anders sal wees as die huidige Internet. Die ontwikkeling van sulke maatreëls sal kubersoewereiniteit tot sy absolute voleinding bring.[160]

Sjina het by monde van Xi Jinping aangetoon dat dit van die wêreld verwag om sy eie model van intranet-regulering te respekteer. Daar is aangetoon dat hierdie 'n "exercise"-element is, en dat dit Sjina vry staan

155 Afd 7.2.

156 Afd 7.3.

157 Afd 7.3.1.

158 Afd 7.3.1.1.

159 Afd 7.3.1.2.

160 Afd 7.3.1.3.

om sonder enige inmenging van ander state so ’n sisteem in werking te stel. Trouens, Sjina doen dit reeds vir dekades, en hierdie versoek is bloot ’n verklaring aan die res van die wêreld dat Sjina die aangeleentheid van kubersoewereiniteit ernstig opneem.[161]

Die kwessie van jurisdiksie is ook bespreek, maar slegs in die mate waarin dit met kubersoewereiniteit te doen het. Die Internasionale Geregshof-beregte *SS Lotus*-beslissing is voorgehou, en verskeie beginsels wat daar neergelê is, is in die konteks van die Internet toegepas.[162]

’n Belangrike aangeleentheid wat uitgelig is, is dat state van die wêreld die gebruik het om strafregtelike jurisdiksie *wyer* te vestig as wat hulle territorialiteit toelaat, met ander woorde state is geneig om makliker ekstraterritoriale jurisdiksie te vestig in strafsake as in die siviele reg.[163] In die konteks van die Internet is daar aangetoon dat die beginsel van netwerk neutraliteit wel gebruik kan word om sodanige jurisdiksievestiging te magtig, mits dit nie die groter Internet skade aandoen nie.[164]

***

Hierdie hoofstuk het die beginsels van kubersoewereiniteit bespreek. Dit het die laaste gedeelte van die legkaart gevorm voordat ’n meer gepaste Internetreguleringsmodel voorgestel kan word. Dit word in die volgende hoofstuk weergegee.

161 Afd 7.3.2.

162 Afd 7.4.

163 Afd 7.4.

164 Afd 7.4.

Hoofstuk 8

Gevolgtrekkings en Aanbevelings

Anyone who reads detective stories, or anyone who is a scientist, knows that the solution of a complex problem often turns out to be simple, once the problem has been understood.[1]

Sir Colin J Humphreys

8.1 Inleiding

REGSBEHEER VAN DIE Internet is 'n multidimensionele aangeleentheid. Die mensdom het dit reg gekry om 'n sfeer van realiteit in 'n elektroniese sisteem te skep.[2] Deur dit te doen is dit moontlik om nie net die inhoud op die Internet nie, maar die realiteit sélf, te vervorm deur argitektuursveranderinge van die netwerk aan te bring.[3] Alhoewel hierdie vermoë nie met die eerste oogopslag as 'n besondere prestasie mag voorkom nie, stel dit die mensdom in staat om in 'n sekere mate die konteks van die fisiese realiteit te ontsnap — op die Internet kan kinders as volwassenes voorkom, en persone van die een geslag kan ander geslagsrolle uitleef.

---

1 Humphreys C J *The Mystery of the Last Supper: Reconstructing the Final Days of Jesus* (2011) 192.

2 Hfst 2 verduidelik die ontwikkeling van die Internet.

3 Afd 2.3.3.

Hierdie nuwe realiteit skep ook ’n besondere uitdaging vir die regspleging. In die verlede is wetgewing uitgevaardig en geïnterpreteer met ’n verwysingsraamwerk van die fisiese wêreld, en die wete het bestaan dat dit nie fundamenteel verander kan word nie. Die gewaarwording dat hierdie basisbeginsel nie altyd op die Internet aan die werk is nie, het nog nie by vele regsplegers deurgeskemer nie. Die resultaat is regskepping wat op ’n lukraak wyse toegepas word en die gevolg is regs-ingrype wat dikwels nie die bedoelde uitwerking het nie.[4]

Aangesien die Internet in sekere opsigte ’n internasionale karakter vertoon, word die uitdagings vergroot wanneer dit vanuit ’n Internasionaalregtelike konteks beskou word. Verskillende ideologieë veroorsaak dat gespreksforums ten aansien van inhoud op die Internet dikwels sulke uiteenlopende menings tot gevolg het, dat sinvolle konsensus-besluite nie geneem kan word nie.[5] In dieselfde mate verskil state se houding ten aansien van die Internet dikwels só, dat ooreenkomste eweneens nie bereik kan word nie.[6]

Die doel van hierdie studie was om die landskap van Internetregulering te ondersoek, en te poog om ’n nuwe model vir Internetregulering daar te stel. Hierdie hoofstuk neem alles wat tot op hede bestudeer is, saam, en poog om konteks daaraan te verleen.

---

4 Daar is vele voorbeelde hiervan in dié studie. Die VSA het byvoorbeeld met die “Communications Decency Act” probeer om vryheid van spraak op die Internet te reguleer, maar dit is ongrondwetlik verklaar. Sien afd 3.3.2. Net so is argitektuursveranderinge van die Internet deur ’n Franse hof beveel. Sien afd 2.3.6.2. In Duitsland is ’n hofbevel uitgereik wat Internetgebruikers in die VSA beïnvloed het. Sien afd 6.3.1.

5 Hfst 5.

6 Hfst 6 en 7.

8.2 Opsomming van Besprekings, Bevindings en Gevolgtrekkings

8.2.1 Internet-ontwikkeling

In hoofstuk 2 is daar verduidelik hoe die ontwikkeling van die Internet dit vir die eerste keer in die geskiedenis van die mensdom moontlik geword het dat die mens in 'n sfeer kan beweeg wat geheel en al binne sy beheer is. In die fisiese wêreld is die mens gebonde aan die argitektuur daarvan, soos byvoorbeeld die werking van swaartekrag, of 'n persoon se liggaamsbou. Op die Internet is dit egter nie die geval nie. Wanneer 'n persoon die sfeer van die Internet betree, is dit moontlik om die argitektuur van die fisiese wêreld agter te laat.[7]

Die gevolg hiervan is verreikend, veral vir regsgeleerdes en regerings wat die taak het om regulering op 'n ordelike wyse te laat geskied. Die rede waarom dit so 'n moeilike taak is, is juis omdat die argitektuur van die Internet binne die mens se beheer is.[8] Benkler toon aan hoe die "lae" wat die Internet laat funksioneer, vir regsdoeleindes vereenvoudig kan word tot 'n fisiese laag, 'n logiese laag, en 'n inhoud-laag.[9] Net soos met die funksionering van die *Internet Suite* is die "hoër" lae afhanklik van die "laer" lae om behoorlik te kan funksioneer. Indien "laer" lae gereguleer word, sal daardie besluit ook die "hoër" lae beïnvloed. Trouens, dit sal die "hoër" lae in so 'n mate beïnvloed dat enige regulatoriese maatreëls wat daarop aangewend is, sal verdwyn, en slegs die "laer" laag se regulatoriese maatreëls sal van krag bly.[10] Huidig word al die "lae" van die Internet gereguleer — dikwels sonder kennis van die gevolge wat regulering van die fisiese

7 Afd 2.1.

8 Afd 2.3.

9 Afd 2.3.3.

10 Afd 2.3.3.

argitektuur op ander regulatoriese maatreëls kan hê.[11]

Wanneer die definisie van die Internet oorweeg word, word dit duidelik dat dit 'n uiters ingewikkelde sisteem is.[12] Enersyds omskryf sommige definisies die struktuur van die Internet, te wete die rekenaars, drade en netwerke wat die Internet vorm.[13] Tóg is die Internet baie meer as dit, aangesien dit inligting en funksionaliteit meebring wat meer is as die fisiese argitektuur daarvan.[14] Sommige definisies poog om hierdie groter funksionaliteit te beskryf — en tereg so — aangesien dit in wese die werklike karakter van die Internet beskryf.[15] Hoe dit ook al sy, die gevolgtrekking wat hieruit gemaak kan word is dat daar met 'n komplekse sisteem gewerk word, en enige regulatoriese maatreëls behoort goed oorweeg te word voordat dit in werking gestel word. Die feit dat die moderne Internet 'n skakeling tussen verskeie tegnologieë teweeg bring, bevestig hierdie stelling al te meer.[16]

Die huidige studie het in die tweede hoofstuk aangetoon dat die Internet oorspronklik ontwerp is volgens suiwer netwerkbeginsels wat ten doel het om dit so goed as moontlik te laat funksioneer.[17] Dit was oorspronklik 'n verspreide netwerk,[18] maar fragmentering van die Internet het in die vroeë 2000's begin plaasvind in geografiese gebiede wat rofweg staatsgrense verteenwoordig.[19] Hierdie is egter nie 'n absolute reël nie — sulke grense is slegs op die Internet getrek om state se wette te gehoorsaam, soos in die geval van Frankryk wat statutêr verbied dat Nazi-goedere daar verkoop mag word.[20] Tog blyk dit duidelik dat fragmentasie en "individualisasie" van die Internet in "staat-intranette" wél tegnologies moontlik is, en dat dit al hoe

11 Afd 2.3.3.
12 Afd 2.2.1.
13 Afd 2.2.1.1.
14 Afd 2.2.1.3.
15 Afd 2.2.1.3.
16 Afd 2.2.3.
17 Afd 2.2.4.
18 Afd 2.2.4.
19 Afd 2.3.6.
20 Afd 2.3.6.2.

meer in die praktyk gebeur.[21]

Die *Yahoo v Licra*-beslissings het op twee kontinente afgespeel, en hierdie beslissings het aangetoon hoe ingewikkeld regulatoriese vraagstukke van die Internet kan wees. Die Franse hof het besef dat regulering van die Internet nie slegs deur regsweë hoef te geskied nie, maar dat die onderliggende argitektuur daarvan beïnvloed kan word om regulatoriese maatreëls in werking te stel.[22] Dit was dan uiteindelik ook die Franse hof se bevinding.[23]

Die howe in die VSA kon nie eenstemmigheid bereik oor verskeie Internetreguleringsvrae nie.[24] Die gevolg was 'n reeks hofsake wat so lank gesloer het dat die saak tussen die partye grootliks opgelos is deur tegnologiese maatreëls wat ingevoer is.[25] Dit illustreer treffend die beginsel dat argitektuursveranderinge van die Internet dikwels 'n groter regulatoriese invloed kan hê as regsreëls.[26]

8.2.2 Lesse uit Vorige Regulatoriese Pogings

Die vroeë Internet het uitsluitlik gebruik gemaak van selfregulering as voorkeurmetode van Internetregulering.[27] Gebruikersreëls is op netwerke geïmplementeer en afgedwing.[28] Hierdie siening was so gewild dat daar selfs na die Internet as 'n afsonderlike ruimte verwys is.[29] Die regering van die VSA het gedurende hierdie tyd probeer om vryheid van spraak op die Internet te reguleer, maar die betrokke bepalings van die *Communications Decency Act* wat die regulering bewerkstellig het, is in die beslissing van

21 Afd 2.3.6.

22 Afd 2.3.6.2.1.

23 Afd 2.3.6.2.1.

24 Afd 2.3.6.2.2, afd 2.3.6.2.3 en afd 2.3.6.2.4.

25 Afd 2.3.6.2.4.

26 Afd 2.3.6.2.4 asook afd 2.3.3.

27 Afd 3.3.1.

28 Afd 3.3.1.

29 Afd 3.3.2.

American Civil Liberties Union v Reno ongrondwetlik verklaar.[30] Uit hierdie saak het dit voorgekom asof selfregulering van die Internet inderdaad die mees gepaste vorm van regulering bevat.[31] Die Internet was egter op hierdie stadium 'n eenheidsnetwerk. Tog kan die duidelike gevolgtrekking gemaak word dat pogings van state nie suksesvol is om sake van internasionale aard deur nasionale wetgewing te reguleer nie. Internasionale aangeleenthede van die Internet behoort in internasionale *fora* hanteer te word.

Die regering van die VSA het egter sy greep op die Internet verskerp deur beheer te neem oor die basis-DNS.[32] Hierdie was 'n belangrike ingreep aangesien dit die kern van die hele Internet vorm, en veroorsaak het dat die VSA-regering algehele beheer oor die Internet verkry het.[33] Hierdie stap het nie byval gevind by die internasionale gemeenskap nie, en gevolglik het die VSA die *Internet Corporation of Assigned Names and Numbers* (ICANN) gestig om as 'n internasionale organisasie te dien wat die DNS kon beheer.[34] Ongelukkig is hierdie organisasie eensydig deur die VSA in die lewe geroep, en dit het nie aan internasionale vereistes voldoen nie.[35] Gevolglik is die ICANN sedert sy ontstaan in omstredenheid gehul.[36] Dit wil egter voorkom asof vordering gemaak word om die basis-DNS aan ICANN oor te dra.[37] Dit is egter nog onduidelik of hierdie stap die internasionale gemeenskap van state tevrede sal stel.[38]

Dit is duidelik dat beheer oor die basis-DNS die neteligste kwessie tussen state is. Dit wil voorkom asof die enigste wyse waarop hierdie saak beredder kan word, is om die basis-DNS in die internasionale sfeer te plaas.

30 Afd 3.3.2.
31 Afd 3.3.2.
32 Afd 3.4.1.
33 Afd 3.4.1.
34 Afd 3.4.3.
35 Afd 3.4.3.
36 Afd 3.4.3.
37 Afd 3.4.3.
38 Afd 3.4.3.

8.2.3 Modelle van Internetregulering

Die Internet verskil van die fisiese wêreld deurdat die argitektuur daarvan verander kan word.[39] Dit beteken dat — anders as die fisiese wêreld — die fundamentele reëls by die Internet so verander kan word dat dit die hele aard daarvan kan beïnvloed. 'n Analogie in die fisiese wêreld sou wees indien die werking van swaartekrag verander kan word. Dit sal die hele onderbou van die samelewing beïnvloed. In dieselfde mate hou die verandering van die argitektuur van die Internet geweldige gevolge vir die reg in, want wanneer die Internet fundamenteel verander, raak regsbeginsels skielik onbruikbaar.[40] Die regsteorieë van die negentigerjare verskaf die nodige perspektief vir hierdie punt: wanneer artikels soos Johnson en Post — wat vurig aanvoer dat die Internet onreguleerbaar deur state is — vandag gelees word, kom dit bykans naïef voor.[41] Die rede daarvoor is dat die Internet vandag fundamenteel anders is as wat dit in die negentigerjare was.[42] Op daardie stadium het die teorieë geheel-en-al sin gemaak, maar vandag is dit onbruikbaar vir die gefragmenteerde Internet. Die rede daarvoor is eenvoudig: die Internet se argitektuur het verander.[43]

Selfregulering het in die onstaansjare van die Internet baie goeie resultate gelewer.[44] Dit blyk die beste reguleringsisteem van 'n eenheidsnetwerk te wees.[45]

Regulering van spesifieke Internet-aangeleenthede kan deur 'n internasionale organisasie hanteer word.[46] Dit is egter nie die beste metode om die Internet as 'n geheel te probeer reguleer nie, aangesien die reguleringskwessies van die Internet té uiteenlopend is om deur 'n enkele

39 Afd 4.2.1.

40 Afd 4.2.2.

41 Afd 4.2.2.2.

42 Afd 4.2.2.2 saamgelees met hfst 2 .

43 Afd 4.2.3.

44 Afd 4.2.2.2.5 saamgelees met afd 2.3 en afd 2.4.

45 Afd 4.2.2.2.5 saamgelees met afd 2.3 en afd 2.4.

46 Afd 4.2.2.2.4.

organisasie hanteer te word.[47]

Regsbeginsels is nie die enigste wyse waarop regulering geskied nie.[48] Dit gebeur deur ’n verskeidenheid modaliteite wat almal in wisselwerking met mekaar is.[49] Slegs as die rol van die verskeidenheid modaliteite oorweeg word, sal suksesvolle regulering kan volg.[50]

Die beginsel van netwerk neutraliteit is ’n krities belangrike konsep by Internetregulering.[51] Enersyds moet die netwerk so vry as moontlik gehou word om dit in werkende toestand te hou, maar andersyds aanvaar die beginsel van netwerk neutraliteit dat netwerk-eienaars wel hulle netwerke kan manipuleer deur dit in goeie werkende toestand te hou. Sulke manipulering moet egter nie geskied ten koste van verbruikers of van die integriteit van die groter netwerk nie.[52]

Die “end-to-end”-beginsel is ’n belangrike konsep om netwerke behoorlik te laat funksioneer.[53] Wanneer hierdie beginsel verontagsaam word, lei die hele netwerk daaronder. Dit geld ook vir die groter Internet. Ongelukkig het ontwikkelings in die afgelope jare veroorsaak dat hierdie beginsel nie meer algemeen toegepas word nie.[54] Dit kan ’n probleem vir die groter Internet skep, en dit is duidelik dat die “end-to-end”-beginsel weer op die groter Internet gerespekteer moet word.[55]

Die twee heersende reguleringsmodelle van die moderne gefragmenteerde era verskaf geensins enige sinvolle oplossings tot Internetregulering nie.[56] Die multi-belangegroepreguleringsmodel hou ’n edele doel voor oë, te wete dat soveel as moontlik rolspelers by besluitnemingsprosesse

47 Afd 4.2.2.2.4.

48 Afd 4.2.2.4.

49 Afd 4.2.2.4.2 en afd 4.2.2.4.3.

50 Afd 4.2.2.4.4.

51 Afd 4.2.3.1.

52 Afd 4.2.3.1.

53 Afd 4.2.3.2.

54 Afd 2.3.6; afd 5.5.1 en afd 6.4.

55 Afd 4.2.3.2.

56 Afd 4.2.4.

betrek moet word, en dat die konsep van demokrasie daardeur versterk word.[57] Ongelukkig is hierdie ideologie nie maklik in die praktyk uitvoerbaar nie, aangesien werklike besluitneming bykans onmoontlik is wanneer daar soveel rolspelers betrokke is.[58] Hierteenoor het die regeringsbeheerde reguleringsmodel die voordeel dat besluitneming makliker deur 'n kleiner groep state geneem kan word, maar dit geskied ten koste van 'n meer demokratiese proses.[59]

Ongelukkig wil dit voorkom asof die stryd tussen die twee verskillende reguleringstrominge niks goeds vir die groter Internet inhou nie. Dit is bloot 'n magstryd tussen twee faksies wat elk sy eie ideologie wil laat seëvier. Dit word gedoen sonder enige konkrete basis-beginsels om aan te toon watter ideologie voorkeur behoort te geniet.[60]

8.2.4 Nie-regeringreguleringrolspelers

Nie-regeringreguleringrolspelers speel 'n krities belangrike rol by die korrekte funksionering van die Internet sowel as by die effektiewe regulering daarvan. Verskeie van hierdie rolspelers vertoon nie die eienskappe van internasionale organisasies wat algemeen in die Internasionale reg aangetref word nie.[61] Byvoorbeeld, die Internasionale Regskommissie se definisie van 'n internasionale organisasie behels dat die internasionale organisasie deur 'n verdrag in die lewe geroep moes word, dat dit 'n afsonderlike regspersoonlikheid moet beklee, en dat state die lede van die organisasie moet vorm.[62] Die meeste nie-regeringsrolspelers wat binne die internasionale sfeer van die Internet werksaam is, voldoen nie aan hierdie vereistes nie, maar tóg sou die Internet nie sonder daardie rolspelers kon

57 Afd 4.2.4.1.

58 Afd 4.2.4.1.

59 Afd 4.2.4.3.

60 Afd 4.2.4.

61 Afd 5.2.

62 Afd 5.2.

bestaan nie.[63]

Drie nie-regeringreguleringrolspelers wat op die Internet werksaam is en wat deur internasionale instrumente in die lewe geroep is, is geïdentifiseer en bespreek. Dit is die "Internet Governance Forum",[64] die Internasionale Telekommunikasie Unie[65] en die Raad van Europa.[66] Daar is vasgestel dat die Internet Governance Forum 'n uitstekende gespreksforum is, maar dat dit geensins die regulatoriese funksie vervul wat daarvan verwag word nie.[67] Daarteenoor is die ITU 'n organisasie wat gefokus is op die inwerkingstelling van telekommunikasieregulasies, maar dit word nie algemeen in die internasionale sfeer aanvaar as 'n onpartydige rolspeler ten aansien van die Internet nie.[68] Dit wil voorkom asof die stigma van die ITU dit nie 'n kandidaat maak vir die bestuur van basisfunksies van die Internet nie.

Die Raad van Europa is 'n gesaghebbende organisasie wat die primêre funksie van menseregtebeskerming en bevordering van demokrasie uitleef.[69] Dit is dan ook hierdie funksie wat dit effektief vervul met die ontwikkeling van die verdrag op Kubermisdaad wat in vele state se nasionale wetgewing vervat is.[70]

Die "Internet Corporation for Assigned Names and Numbers" is een van die belangrikste rolspelers by Internetregulering, aangesien dit die tegniese basis-DNS-funksie (oftewel die IANA-funksie) vervul.[71] Dit staan huidig steeds onder die oorsig van die VSA, maar 'n aansoek om die IANA-funksie in sy geheel oor te neem, is huidig onder oorweging deur die VSA-owerhede.[72]

---

63 Afd 5.2.

64 Afd 5.3.2.

65 Afd 5.3.3.

66 Afd 5.3.4.

67 Afd 5.3.2.5.

68 Afd 5.3.3.5.

69 Afd 5.3.4.

70 Afd 5.3.4.

71 Afd 5.4.1.

72 Afd 5.4.1.5.

Suiwer tegniese regulering van die Internet word hoofsaaklik deur drie organisasies uitgeoefen. Hulle is die "Internet Society",[73] "Internet Engineering Task Force"[74] en die "World Wide Web Consortium".[75] Al drie hierdie organisasies word gekenmerk deur plat organisatoriese strukture, met vrywillige personeel wat tegniese kwessies op 'n *ad hoc* basis oplos. Al drie organisasies funksioneer effektief sonder enige staatsinmenging.[76]

Een van die belangrikste nie-regeringsreguleerders is Internet-diensverskaffers (ISP's).[77] Hulle is reguleerders in eie reg deurdat hulle van 'n tegnologie genaamd "deep packet inspection" (DPI) gebruik maak om hul netwerke so te manipuleer dat dit groter finansiële voordele vir hul inhou — dikwels ten koste van gebruikers.[78] 'n Belangrike gevolgtrekking is gemaak nadat die gebruik van DPI in twee state, te wete die VSA en Kanada, ondersoek is.[79] Dit het geblyk dat die gebruik van DPI in Kanada toegeneem het omdat regulatoriese ingrepe nie sterk uitsprake téén DPI gemaak het nie.[80] Hierin lê 'n belangrike les vir Suid-Afrika, aangesien die telekommunikasieraamwerk in Kanada soortgelyk is aan Suid-Afrika, met net een groot nasionale rolspeler.[81]

8.2.5 Regulering deur Soewereine State

Soewereine state regeer in 'n gebied deur wetgewing op nasionale vlak uit te vaardig, en dit met mag af te dwing.[82] Hierdie metode is gewoonlik suksesvol wanneer al die rolspelers in die staat aanwesig is. Somtyds bevind sekere

73 Afd 5.4.2.

74 Afd 5.4.3.

75 Afd 5.4.4.

76 Afd 5.4.2, afd 5.4.3 en afd 5.4.4.

77 Afd 5.5.

78 Afd 5.5.1.

79 Afd 5.5.1.2, afd 5.5.1.3 en afd 5.5.1.4.

80 Afd 5.5.1.4

81 Afd 5.5.1.4. Die groot nasionale telekommunikasierolspeler in Kanada is Bell Canada, en in Suid Afrika is dit Telkom.

82 Afd 6.1.

rolspelers hulle buite die regsgebied van die staat en dan word dit moeiliker om regulering deur te voer.[83] Tog is dit steeds moontlik om op 'n indirekte wyse regulering te bewerkstellig indien die verskeie rolspelers geïdentifiseer kan word en hulle funksies bepaalbaar is.[84]

In die reguleringsproses is daar altyd ten minste drie rolspelers ter sprake, te wete 'n bron, tussenganger en teiken.[85] Effektiewe regulering kan ten aansien van enige rolspeler uitgeoefen word.[86] Hierdie is 'n belangrike gevolgtrekking aangesien 'n Staat slegs een rolspeler hoef te beheer om effektiewe regulering te bewerkstellig.[87] Dit is belangrik om die rolspelers ten aansien van die Internet te identifiseer om sodoende effektiewe regulering te verkry.[88]

Internet-diensverskaffers is die belangrikste rolspelers van die Internet.[89] Hulle koppel gebruikers aan die Internet,[90] en vervul self ook 'n reguleringsfunksie op hul eie netwerke.[91]

Inligtingstussengangers soos groot soekenjins kan op 'n kragtige wyse gebruik word om regulering van inligting moontlik te maak.[92] Hierdie tussengangers is al in die verlede deur howe beveel om spesifieke inligting van hulle databasisse te verwyder, en dit het die gevolg dat inligting nie deur algemene gebruikers opgespoor kan word nie, ten spyte daarvan dat dit moontlik nog op die Internet aanwesig kan wees.[93]

Finansiële tussengangers kan gebruik word om betalingstelsels te manipuleer sodat buite-staatlike rolspelers verhinder kan word om onwettige

83 Afd 6.1.

84 Afd 6.2.1.

85 Afd 6.2.1.

86 Afd 6.2.1.

87 Afd 6.2.1.

88 Afd 6.3.

89 Afd 6.3.1 en afd 5.5.

90 Afd 6.3.1.

91 Afd 5.5.

92 Afd 6.3.2.

93 Afd 6.3.2.

goedere binne die grense van ’n bepaalde staat te verkoop.[94] Die VSA het hierdie strategie gebruik met die probleem van buite-staatlike verkoop van sigarette, en dit was so suksesvol dat bykans alle buite-staatlike rolspelers binne weke hulle bedrywighede gestaak het.[95]

Individue word in sommige dele van die wêreld gebruik om as tussengangers ’n kragtige reguleringsfunksie te verrig. Sjina het byvoorbeeld ’n Internet-polisiediens wat ’n wye spektrum van gedrag moniteer.[96]

Omdat die Internet in wese maar net uit ’n reeks netwerke bestaan wat aaneen gekoppel is, is dit voor-die-hand-liggend dat netwerk-eienaars ’n belangrike, maar dikwels ongesiene, rolspeler is. Hierdie rolspelers kan deur manipulasie van die fisiese argitektuur van hulle netwerke regulatoriese ingrepe lewer.[97]

Vier state se reguleringspogings van die Internet is bespreek, te wete die VSA, Sjina, die Europese Unie, en Suid-Afrika. Dit is egter onmoontlik om in ’n studie van hierdie omvang volledig aan *alle* regulerings-ingrepe aandag te gee, en daarom is daar spesifiek beoordeel hoe hierdie state Internet-diensverskaffers reguleer. Deur dit te doen kan die staat se algemene regulatoriese aanslag ten opsigte van sy intranet, sowel as die groter Internet beoordeel word.

Oor die algemeen staan die VSA ’n oop Internet voor waar data vryelik tussen state onderling en ook deur die groter Internet kan vloei.[98] Hierdie sienswyse word in die VSA se wetgewing weerspieël, waar Internet-diensverskaffers ’n baie groot mate van vryheid gegun word om eie sake te reguleer, en hulle geniet wye nie-aanspreeklikheid vir data wat deur hulle stelsels vloei.[99] Trouens, die “Communications Decency Act” van 1996 verskaf sulke wye nie-aanspreeklikheidsbeskerming vir ISP’s dat dit al onder

94 Afd 6.3.3.

95 Afd 6.3.3.

96 Afd 6.3.4.

97 Afd 6.3.5.

98 Afd 6.4.1.

99 Afd 6.4.1.2, afd 6.4.1.3 en afd 6.4.1.4.

fel kritiek deurgeloop het as té liberaal.[100]

Die "Digital Millenium Copyright Act" (DMCA) is 'n goed deurdagte stuk wetgewing wat verskeie kategorieë daarstel om ISP's se aanspreeklikheid te reguleer ten opsigte van die spesifieke funksie wat hul op die Internet vervul.[101] Indien 'n ISP op die nie-aanspreeklikheidsklousules soos vervat in die wet, wil staatmaak, moet daar aan die betrokke kategorie se vereistes voldoen word. Dit hou die voordeel in dat regulatoriese ingrepe ten aansien van spesifieke kategorieë gemaak kan word, wat enersyds die ISP's in staat stel om makliker aan die wet te voldoen deurdat vereistes uitgestippel word, en andersyds die regulatoriese ingreep meer effektief maak deurdat daar nie gepoog word om 'n verskeidenheid van gevalle met 'n breë kwas te probeer hanteer nie.[102]

Die "Lanham"-wet reguleer handelsmerkskending, en dit is so gewysig dat dit ook op die Internet toepassing kan vind.[103] Hierdie is 'n goeie voorbeeld van hoe wetgewing *nie* geformuleer moet word nie, aangesien dit in 'n voor-Internet-era tot stand gebring is, en gewysig is met die oog op die Internet. Dit is inderdaad totaal ontoereikendheid, en wysigings soos deur Powell voorgestel, behoort aangebring te word.[104]

Die donker prentjie van 'n vrye Internet het ontvou toe daar verduidelik is hoe die Amerikaanse intelligensiedienste die "big data" wat oor die Internet vloei, saamvoeg om 'n grootskaalse moniteringsprogram op eie bodem sowel as internasionaal, te bedryf.[105] Gemeet aan die internasionale reaksie is dit duidelik dat verskeie state van die wêreld hierdeur onkant betrap is. Die feit dat die VSA die wêreld se grootste Internet-ruggraat het, het tot gevolg dat meeste state van die wêreld se Internetverkeer

100 Afd 6.4.1.2.

101 Afd 6.4.1.3.

102 Afd 6.4.1.3.

103 Afd 6.4.1.4.

104 Afd 6.4.1.4. Powell C D "The *eBay* Trademark Exception: Restructuring the Trademark Safe Harbor for Online Marketplaces" 2011 *Santa Clara High Technology Law Journal* 1 18–20.

105 Afd 6.4.1.5.

deur die VSA geroeteer word.[106] Die VSA intelligensiedienste het 'n "regmatige" gebruik op hierdie internasionale data verkry deur wetgewing wat so gewysig is dat dit sulke grootskaalse monitering magtig.[107] Die magtigende bepalings van die "Foreign Intelligence Surveillance Act" van 1978 (soos gewysig)[108] is bespreek, en daar is verduidelik hoe die "Foreign Intelligence Surveillance Court", wat 'n oorsigfunksie oor die intelligensiedienste moet verrig, nie na wense gefunksioneer het nie. Hierdie is 'n belangrike gevolgtrekking, aangesien dit ook gevolge vir Suid-Afrika se onderskeppingsentrums inhou.[109]

Die Volksrepubliek van Sjina het besluit om Internetregulering van 'n totaal verskillende hoek as die VSA te benader.[110] Sedert sy koppeling met die groter Internet in 1994 het Sjina aangedui dat die staat-intranet onafhanklik van die groter Internet ontwikkel sou word.[111] Die "Golden Shield"-projek het tot stand gekom, en vandag is Sjina se intranet die mees ontwikkelde — en hoogs gereguleerde — staat-intranet ter wêreld.[112] Die gevolg is die uitvaardiging van 'n magdom regulasies, waarvan slegs die belangrikste in hierdie studie bespreek kon word. Dit is duidelik dat Sjina deeglik daarvan bewus is dat Internetregulering op verskeie vlakke kan geskied.[113] Enersyds bestaan daar regulasies wat noukeurig bepaal hoe die staat-intranet aanmekaar gesit moet word.[114] Daar is regulasies wat die struktuur van netwerke bepaal, en dan is daar verdere regulasies wat die struktuur van koppeling aan ander netwerke — die sogenaamde

106 Afd 6.4.1.5.

107 Afd 6.4.1.5.2.

108 Afd 6.4.1.5.2.

109 Afd 6.4.4.3.1.

110 Afd 6.4.2.

111 Afd 6.4.2.2.1.

112 Afd 6.4.2. Hagestad W *21st Century Chinese Cyberwarfare* (2013) 253 verduidelik wat die "Golden Shield"-program behels: "This project was called the 'Golden Shield Project' and is also known as the 'Great Firewall of China'. Under the direct policy enforcement of the Ministry of Public Security of the People's Republic of China (MPS) 'Golden Shield' provides the People's Republic of China with Internet censorship at the Internet backbone and ISP level".

113 Afd 6.4.2.2.1.

114 Afd 6.4.2.2.1.

internetwerk — uiteensit.[115] Nóg regulasies reguleer die gedrag van verskeie rolspelers op die Internet,[116] en verskeie regulasies reguleer inhoud op die Internet.[117] Vanuit 'n westerse perspektief is dit duidelik dat daar *oorgereguleer* word, maar interessant genoeg word dit allerweë vanuit die Sjinese publiek se oogpunt as beskerming van kulturele- en morele waardes beskou.

Ten spyte daarvan dat Sjina se intranet-regulering wêreldwyd as drakonies en 'n skending van menseregte beskou kan word, is daar vele belangrike lesse te leer oor hoe Sjina hul staat-intranet reguleer. Daar is reeds by verskeie geleenthede in hierdie studie genoem dat die Internet — op nasionale en internasionale vlak — 'n belangrike sleutel tot ekonomiese groei geword het.[118] Sjina is deeglik van hierdie feit bewus, want daar word gereeld stappe geneem om ekonomiese groei op die Internet, plaaslik te hou. Sjinese druk op *Google* het tot gevolg gehad dat hierdie Internet-reus in 2010 uit Sjina onttrek het, en *Baidu* (die Sjinese ekwivalent), het gou sy plek ingeneem en sodoende verhoed dat kapitaal uit die land vloei.[119] Dieselfde het gebeur met *eBay*, en *Taobao* het sy plek ingeneem.[120] Net so is *Facebook* nie in Sjina beskikbaar nie, maar die "mikro-blog"-diens genaamd *Sina Weibo* vervul 'n soortgelyke funksie — en verskaf werksgeleenthede aan duisende mense. Dit geld ook vir *Youtube,* wat in Sjina geblokkeer word ten gunste van sy eie *You Ku* en *iQiyi.*[121] (Hierteenoor is ál hierdie Sjinese maatskappye op die *New York*-aandelemark gelys, wat inkomste aan Sjina toebring.)

Die regulering van Sjina se netwerkstruktuur is eweneens navolgings-

115 Afd 6.4.2.2.1.

116 Afd 6.4.2.3.

117 Afd 6.4.2.4.

118 Bv afd 3.4.2 en afd 5.1.

119 Afd 6.4.2.4.5 vn 464.

120 So S en Westland J *Red Wired: China's Internet Revolution* (2010) 98–100 verduidelik hoe *eBay* in Sjina gefaal het. *Ebay* se bedieners was buite Sjina gestasioneer, en dit het veroorsaak dat die *eBay*-diens gereeld nie beskikbaar was nie. Die Sjinese ekwivalent van *Ebay, Taobao* het die grootste markaandeel verkry en dit behou.

121 Afd 6.4.2.4.5 vn 464.

waardig. Sonder om op mikro-vlak te reguleer, is dit tóg sinvol vir ’n staat om basiese vereistes van netwerkstruktuur neer te lê.[122] Dit geld ook vir koppeling tussen netwerke om die internetwerk te vorm, want as hierdie aangeleenthede totaal ongereguleerd gelaat word, sal finansiële voordeel vanuit die mark veroorsaak dat netwerk-eienaars nie ag slaan op die sinvolste wyse van netwerkontwikkeling nie, en die staat se intranet as geheel sal daaronder ly.

Hierdie studie het ook in besonderhede uitgewys hoe Sjina te werk gaan om inhoud op die staat-intranet te reguleer, en hoe Sjinese burgers grootliks verhinder word om inligting vanuit die groter Internet te verkry.[123] Dit illustreer die hartseer les van Internet-argitektuursveranderinge wat tot gevolg het dat mense deur gebruikmaking van tegnologiese maatreëls in ’n tronk van manipulasie geplaas word. Dit illustreer ook die krag van die Internet om algehele bevolkings se opinies te vorm na die wense van staatsowerhede.[124]

Die Europese Unie se *Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market*[125] is een van die belangrikste stukke wetgewing wat nie-aanspreeklikheid van Internet-diensverskaffers reguleer. Die rede daarvoor is tweërlei: in die eerste plek is die direktief een van die eerste stukke wetgewing wat uitgevaardig is om nie-aanspreeklikheid van ISP’s te reguleer. Dit het tot gevolg gehad dat ander state dié regulasie as voorbeeld gebruik het. Die tweede rede is dat Suid-Afrika spesifiek sy wetgewing aangaande nie-aanspreeklikheid van ISP’s in so ’n groot mate op dié direktief geskoei

122 Afd 6.4.2.2.1.

123 Afd 6.4.2.3 en afd 6.4.2.4.

124 Afd 6.4.2.4.

125 Direktief 2000/31/EC van die Europese Parlement en die Raad van 8 Junie 2000 oor “Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market” (Directive on electronic commerce) 2000 OJ L178/1. Lodder A R en Van der Meulen N S “Discussion of Dutch Pirate Bay Case Law and Introducing Principles on Directness, Effectiveness, Costs, Relevance, and Time” 2012 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 130 132 verduidelik dat hierdie direktief geformuleer is om die kernpilaar van e-handel in die Europese Unie te vorm.

het, dat dit in verskeie aspekte identies is.

Die EU-direktief onderskei tussen drie "soorte" Internet-diensverskaffers, te wete daardie diensverskaffers wat bloot 'n geleibuis is wat data déúr hulle netwerke stuur sonder om dit te monitor,[126] diegene wat data tydelik berg voordat dit aangestuur word,[127] en dié wat gasheer tot data is.[128] Die onderskeid is belangrik omdat die verskillende diensverskaffers aan verskillende vereistes moet voldoen om op nie-aanspreeklikheid staat te kan maak.[129] Wanneer die vereistes beoordeel word, wil dit voorkom asof dit sinvolle beginsels uiteensit wat tot effektiewe regulering behoort te lei. Tóg is hierdie beginsels op 'n verskeidenheid wyses in lidlande se howe geïnterpreteer, en dit wil voorkom asof teenstrydige bepalings in lidlande se wetgewing die duidelike beginsels in die EU-direktief ongedaan maak. Die gevolg is insiggewend vir regulerings-ingrepe op die Internet, want dit is duidelik dat state in bykans elke geval hul nasionale wetgewing sal volg en nie die oorkoepelende streekswetgewing (van die EU) nie. In sulke gevalle word staatsoewereiniteit bo EU-streekseenvormigheid verkies.

In Suid-Afrika word die nie-aanspreeklikheid van ISP's deur artikels 70–79 van die Wet op Elektroniese Kommunikasies en Transaksies[130] gereguleer. Ál hierdie artikels is volledig bespreek.[131] Verskeie van die artikels kom woord-vir-woord ooreen met die ooreenstemmende artikels in die EU-direktief, en waar daar enige verskille was, is dit bespreek en die wenslikheid

126 Die Engelse term "mere conduit" word hier bedoel. Sien art 12 van die EU Direktief 2000/31/EC.

127 Die Engelse term "caching" word hier bedoel. Sien art 13 van die EU Direktief 2000/31/EC, asook Baistrocchi 2002 *Santa Clara High Technology Law Journal* 118.

128 Die Engelse term "hosting" word hier bedoel. Sien art 14 van die EU Direktief 2000/31/EC. Sien ook Kryczka K "Ready to Join the EU Information Society — Implementation of E-Commerce Directive 2000/31/EC in the EU Acceding Countries — The Example of Poland" 2004 *International Journal of Law and Information Technology* 55 65 vir 'n voorbeeld van 'n lidland (in hierdie geval Poland) wat die EU-direktief net so in hul eie wetgewing vervat het.

129 Leistner M "Structural Aspects of Secondary (Provider) Liability in Europe" 2014 *Journal of Intellectual Property Law and Practice* 75 76.

130 Wet 25 van 2002. Roos A en Slabbert M "Defamation on *Facebook*: *Isparta v Richter* 2013 6 SA 529" 2014 *Potchefstroom Electronic Reserves* 2844 2857.

131 Afd 6.4.4.2.

daarvan oorweeg.[132] In wese vervat die Suid-Afrikaanse wetgewing die goedgeformuleerde bepalings van die EU-direktief, maar ongelukkig het die Suid-Afrikaanse wetgewer dit goedgedink om verskeie aangeleenthede te wysig, en dit het tot gevolg gehad dat die wetgewing lomp funksioneer. Die twee belangrikste aangeleenthede is (a) dat daar streng vereistes neergelê word vir ISP's om aan te voldoen om vir die nie-aanspreeklikheidsbepalings in aanmerking te kom,[133] en (b) dat die minister by magte is om regulasies uit te vaardig om bykomende vereistes neer te lê.[134]

Wat die streng vereistes waaraan ISP's moet voldoen om op die nie-aanspreeklikheidsbepalings te steun, betref, bestaan die groot probleem dat artikel 71 van die EKT-wet bepaal dat ISP's aan Verteenwoordigende liggame moet behoort om op enige nie-aanspreeklikheidsbepalings te kan steun.[135] Daar is in die studie aangedui hoe daar in die veertien jaar wat die EKT-wet bestaan, slegs één organisasie dit vermag het om as 'n Verteenwoordigende liggaam erken te word. Hierdie organisasie, die "Internet Providers Association of South Africa" (ISPA), dien egter slegs die belange van kommersiële ISP's, en alle ander entiteite wat as ISP's volgens die breë definisie van ISP's in die EKT-wet beskou word, val buite die sfeer van beskerming van die nie-aanspreeklikheidsbepalings van die EKT-wet.[136] Die gevolg is dat die EKT-wet nie-aanspreeklikheidsbeskerming aan ISP's verleen, maar dit dan dadelik wegneem deur dit buite die bereik van meeste ISP's te plaas as gevolg van nie-bereikbare vereistes waaraan voldoen moet word. Dit is 'n ernstige tekortkoming in die EKT-wet.

Wat die minister se vermoë om regulasies uit te vaardig, betref, behoort hierdie regulasies in ernstige heroorweging geneem te word.[137] Die studie het aangetoon hoe die EKT-wet 'n selfreguleringsisteem vir ISP's tot stand

132 Afd 6.4.4.2.

133 Afd 6.4.4.2.2 en afd 6.4.4.2.3.

134 Afd 6.4.4.2.2 en afd 6.4.4.2.3.

135 Afd 6.4.4.2.2.

136 Afd 6.4.4.2.2.

137 Afd 6.4.4.2.3.

gebring het, maar hoe die regulasies van die minister tot gevolg het dat 'n regeringsbeheerde sisteem tot uitvoering gebring is. Die minister se regulasies gaan lynreg in teen die gees van die selfreguleringsisteem wat in die EKT-wet ontwikkel is.[138]

Artikel 75(2) van die EKT-wet bepaal dat 'n ISP 'n agent moet aanstel om sekere funksies te verrig.[139] Daar is in die studie aangetoon hoe hierdie vereiste van die Amerikaanse DMCA verkry is, en wat die funksie van die agent in daardie staat is. Daar is tot die gevolgtrekking gekom dat hierdie 'n argaïese gebruik vervat, en dat dit in die moderne Internet-era nie nodig is om so 'n agent aan te stel nie aangesien die ISP self sulke funksies kan verrig.[140] Die EKT-wet maak ook op 'n lukraak wyse van die agent gebruik deurdat daar byvoorbeeld in artikel 77 van die EKT-wet bepaal word dat óf die ISP óf sy agent gebruik kan word om sekere kennisgewingsfunksies te verrig, en die gebruikmaking van die agent eweneens nie nodig is nie.[141]

Die gebruik van afhaalkennisgewings in die Suid-Afrikaanse EKT-wet is bespreek, en dit is met dié van die VSA en die EU vergelyk. Die gevolgtrekking kan gemaak word dat die EKT-wet in hierdie geval voldoende is.

Sekere aspekte van die Suid-Afrikaanse Wet op die Reëling van Onderskepping van Kommunikasies en Verstrekking van Kommunikasie-verwante Inligting[142] (hierna die RICA-wet)[143] is bespreek. Daar is verduidelik hoe die RICA-wet 'n gevaarlike sisteem in plek stel waar die Suid-Afrikaanse veiligheidsagentskappe in staat gestel word om intydse monitering op die hele Suid Afrikaanse intranet te bedryf.[144] Die wyse waarop die RICA-

138 Afd 6.4.4.2.3.

139 Afd 6.4.4.2.5.

140 Afd 6.4.4.2.5.

141 Afd 6.4.4.2.5.

142 Wet 70 van 2002.

143 Omdat hierdie wet so 'n lang en ongemaklike titel het, word dit in die regsliteratuur (wat gewoonlik Engels is), bloot as RICA verwys. Die akroniem kom van die Engelse "(R)egulation of (I)nterception of (C)ommunications and Provision of Communication-related Information (A)ct 70 of 2002" (hakies dui die oorsprong van die akroniem aan).

144 Afd 6.4.4.3.1.

wet dit magtig, is om *alle* ISP's in Suid Afrika te verplig om 'n data-moniteringslyn aan die veiligheidsagentskappe te koppel.[145] Die RICA-wet vereis wél dat prosesregtelike stappe geneem moet word om van die data-moniteringslyn gebruik te maak, maar gesien in die lig van hoe eenvoudig dit vir die Amerikaanse veiligheidsmagte was om hierdie kanaal te misbruik,[146] bestaan daar ernstige kommer dat dieselfde in Suid-Afrika gebeur — veral aangesien daar in Suid-Afrika nie enige sterk oorsigstrukture in plek is nie.[147]

Die struktuur van die Suid-Afrikaanse intranet is kortliks bespreek, en daar kan tot die gevolgtrekking gekom word dat dit ongelukkig maklik manipuleerbaar is[148] — veral in samewerking met die verreikende RICA-monitering.[149]

8.2.6 Kubersoewereiniteit

Kubersoewereiniteit is 'n moderne konsep wat al hoe meer aandag begin geniet.[150] Dit is verweef met die konsep van soewereiniteit, maar daar is nog groot onduidelikheid wat met kubersoewereiniteit bedoel word.[151]

Staatskap en soewereiniteit hang eweneens nou saam, maar is nie sinonieme konsepte nie.[152] In die Internasionale reg word daar algemeen aanvaar dat die moderne konsep van staatskap te vinde is in die *Montevideo Convention on the Rights and Duties of States,* en dit behels aspekte waaraan 'n staat moet voldoen om as 'n staat beskou te word.[153] Hierteenoor is die gevolgtrekking bereik dat soewereiniteit in die moderne Internasionale reg

145 Afd 6.4.4.3.1.
146 Afd 6.4.1.5.
147 Afd 6.4.4.3.2.
148 Afd 6.4.4.4.
149 Afd 6.4.4.3.1.
150 Afd 7.1.
151 Afd 7.1.
152 Afd 7.2.
153 Afd 7.2.

die regte, verpligtinge en magte is wat 'n staat uitoefen in die gebied waaroor dit jurisdiksie het.[154] Indien so 'n konstruksie gevolg word, pas dit netjies by die moderne konsep van die Internasionale reg in, naamlik dat die moderne Internasionale reg nie slegs die verhouding tussen state reël nie, maar dat internasionale organisasies ook 'n rol speel om sekere aangeleenthede van gemeenskaplike belang namens state te reguleer.[155] Soewereiniteit is dus die verdeelbare "exercise"-elemente wat 'n staat uitoefen, en dit beteken dat sulke regte, verpligtinge en magte aan internasionale organisasies gedelegeer mag word sonder dat laasgenoemde staatskap verkry.[156]

'n Verdere gevolgtrekking wat in hierdie verband gemaak kan word, is dat soewereiniteit die gevolg is van staatskap. Dit is ook waar van kubersoewereiniteit: laasgenoemde is eweneens 'n gevolg van staatskap.[157]

Daar is verskeie state van die wêreld wat luide uitlatings maak dat kubersoeweiniteit 'n prioriteit in die staat word.[158] Die prominentste hiervan is Sjina,[159] met ander state soos Indië, Brasilië en Rusland wat soortgelyke uitsprake maak.[160] Selfs staatsgroepe soos die Europese Unie het al hul stem by hierdie groep gevoeg.[161] Sulke uitlatings is nie vreemd in die moderne wêreld nie, aangesien staatlike intranet-stabiliteit dikwels 'n voorvereiste vir ekonomiese groei is. Tog het dit die gevolg om die aard van die groter Internet negatief te beïnvloed.

'n Interessante gevolgtrekking wat by die vestiging van kubersoewereiniteit gemaak kan word is dat 'n staat wat 'n goed ontwikkelde en relatief outonome staats-intranet het, makliker kubersoewereiniteit sal kan vestig as 'n staat wat so volledig aan die groter Internet gekoppel is dat dit bykans

154 Afd 7.2.
155 Afd 1.5.
156 Afd 7.2.
157 Afd 7.2.
158 Afd 7.3.
159 Afd 7.3.
160 Afd 7.3.1.1.
161 Afd 7.3.1.1.

ononderskeibaar daarvan is.[162] Dit beteken dat 'n staat soos Sjina makliker kubersoeweiniteit sal kan vestig as 'n staat soos die VSA, wat meerendeels met die groter Internet geïntegreer is.[163] Soos wat nuwe tegnologieë, soos data-lokalisering[164] en alternatiewe basis-DNS-dienste[165] verder ontwikkel, sal dit makliker vir state word om kubersoeweiniteit 'n werklikheid te maak. In dieselfde mate neig onlangse staats-onderhandelinge soos die wysiging van die ITU se grondwet, in die rigting van state se bereidwilligheid om kubersoeweiniteit te vestig.[166]

Wat jurisdiksie betref, is die verrassende gevolgtrekking gemaak dat die algemene beginsels van die Internasionale reg aangaande jurisdiksie grotendeels op die kuberruim van toepassing gemaak kan word.[167] Hardeware soos netwerke, roeteerders, en ander fisiese Internet-argitektuur is binne die beheer van die staat indien dit in sy fisiese gebied (territorium) is. Jurisdiksie kan vryelik daaroor uitgeoefen word.[168]

Daar is bevind dat die Internasionale reg aanvaar dat strafregtelike jurisdiksie dikwels verder strek as die staat se territorialiteit, en dat dit 'n algemeen aanvaarde beginsel is dat state gewillig is om ekstra-territoriale jurisdiksie te vestig in strafregtelike sake.[169] Net soos in die fisiese wêreld is dit dikwels nie die vestiging van jurisdiksie wat die probleem skep nie, maar eerder die uitvoering van hofbevele indien 'n dader hom nie binne die fisiese beheer van die betrokke staat bevind nie.[170]

State maak gereeld van wetgewing gebruik om aangeleenthede rakende hulle nasionale intranette te beheer.[171] Dit is niks vreemd nie, maar dit

162 Afd 7.3.1.

163 Afd 7.3.1.

164 Afd 7.3.1.1.

165 Afd 7.3.1.3.

166 Afd 7.3.1.2.

167 Afd 7.4.

168 Afd 7.4.

169 Afd 7.4 bespreek die *SS Lotus*-beslissing van die Permanente Internasionale Geregshof wat hierdie bevindings gemaak het.

170 Afd 7.4.

171 Afd 7.4.

sal elke staat van die wêreld baat om na te dink oor sy nasionale beleid aangaande sy nasionale intranet en wetgewing op 'n konsekwente wyse in te stel. Hier is Sjina by verre die voorloper, ten spyte daarvan dat dit erge internasionale kritiek op die hals haal weens sy beperkings op persvryheid en menseregte.[172]

Internasionaalregtelike beginsels is eweneens duidelik daaroor dat *mag* nie buite die grense van die staat uitgeoefen mag word nie — ook nie in die kuberruim nie.[173] Dit verklaar waarom optrede soos dié van die VSA met sy kuber-spioenasie erge negatiewe kritiek van ander state ontlok het.[174]

In die breë het state dus 'n groot mate van vryheid wanneer dit kom by die vestiging van kubersoewereiniteit en jurisdiksie. 'n Belangrike gevolgtrekking is gemaak dat dit wenslik sou wees om die beginsels van netwerk neutraliteit in gedagte te hou wanneer nasionale wetgewing oor die kuberruim gemaak word.[175] Die nasionale intranet mag gesmee word na die beleid van die betrokke staat, maar daar moet in gedagte gehou word dat dit steeds gekoppel is aan 'n groter netwerk — die Internet — en sodanige nasionale wetgewing mag nie die beginsels van die groter netwerk so beïnvloed dat dit skade daaraan aanrig nie.[176]

8.3 Aanbevelings

8.3.1 Aanbevelings ten aansien van Globale Internet-hervorming

Die Internet het sy ontstaan te danke aan tegniese personeel, maar spoedig het dit tot 'n kommersiële entiteit ontwikkel. Hierna het sekerlik die ingrypendste ontwikkeling gevolg, naamlik die fragmentering van die

172 Afd 7.4.

173 Afd 7.4.

174 Afd 7.4 saamgelees met afd 6.4.1.5.

175 Afd 7.4.

176 Afd 7.4 saamgelees met afd 4.2.3.1.

Internet. Die doel daarmee was grotendeels om aan state se nasionale wetgewing te voldoen.[177] Die gevolg is dat die Internet soos dit vandag bestaan, in wese uit twee vlakke bestaan. Die eerste vlak bestaan uit 'n staat-intranet waar wette van die staat gehoorsaam word. Die tweede vlak bestaan uit die internasionale Internet, waar data steeds vryelik tussen state vloei, en relatief ongereguleerd bly indien dit aan state se wetgewing voldoen. Die eerste aanbeveling is dat hierdie feitelike werklikheid nie meer ontken word nie. Die aanvanklike aantrekkingskrag van die Internet was inderdaad die feit dat dit internasionaal van aard was en die wêreld se inligting na die algemene gebruiker gebring het. Die Internet van vandag bevat eweneens 'n magdom inligting, maar die waarheid is dat baie daarvan weens fragmentasie nie meer vir die algemene gebruiker beskikbaar is nie. Die argitektuur van die moderne Internet is ingrypend anders as dié van die negentigerjare.

Indien hierdie waarheid in die gesig gestaar word, word reguleringskwessies en -hervormings makliker om te identifiseer. Die sensitiefste hiervan is sekerlik die aard van ICANN. Dit is enig in sy soort onder internasionale organisasies, en voldoen geensins aan die vereistes wat vir internasionale organisasies gestel word nie. Die VSA het dit duidelik gemaak dat dit slegs oorsig van die IANA-funksie aan 'n multi-belangegroep sal oordra, en ICANN is die beste verteenwoordiging daarvan. Daar word voorsien dat hierdie oorsig spoedig aan ICANN toegeken sal word. Dit sal egter kortsigtig wees indien enigeen meen dat dit die einde van ICANN se ontwikkeling sal wees. Die enkele grootste probleem is dat ICANN steeds onder die jurisdiksie van die VSA staan, en ten spyte daarvan dat dit 'n multi-belangegroep van die wêreld verteenwoordig, sal die meeste state dit nie aanvaar tensy dit werklikwaar outonoom is nie. Solank ICANN onder die jurisdiksie van die VSA verkeer, is dit nie waarlik outonoom nie. Daar word aanbeveel dat ICANN onder die jurisdiksie van die VSA uitgeskuif word.

Die vraag wat in hierdie verband gevra word, is hoe dit gestruktureer

[177] Sien yahoo saak.

behoort te word? In 2005 is daar reeds uitgeklaar dat ICANN nie onder die vaandel van die Verenigde Nasies behoort nie. Daar word aan die hand gedoen dat ICANN as ’n internasionale organisasie omvorm word wat aan die vereistes van die Internasionale Regskommissie voldoen. Dit sal beteken dat ’n verdrag tot stand gebring word wat dit omvorm na ’n internasionale organisasie, en dat dit met afsonderlike regspersoonlikheid beklee word. Die struktuur van ICANN behoort onaangeraak gelaat te word, want dit is in elk geval wensliker dat ’n multi-belangegroep ICANN bestuur en nie state wat met verskuilde agendas hul eie belange voorop stel nie. Daar word ook aanbeveel dat ICANN se hoofkantoor nie meer in die VSA gesetel moet wees nie, maar in ’n jurisdiksie wat meer neutraal is, en wat algemeen deur internasionale organisasies gebruik word. Die voor-die-hand-liggendste kandidaat-stad is Genéve, waar meeste internasionale organisasies hulle hoofkantore het.

Om aan die internasionale gemeenskap se vereistes te voldoen, sal ICANN sy eie interne oorsigbeleid moet aanpas om sterker oorsigstrukture daar te stel. Die IANA-funksie onderlê die behoorlike funksionering van die Internet, en dit is van kritiese belang dat hierdie funksie nie aan enige politieke magstryde onderwerp word nie.

Die ontwikkeling van ICANN wat hier voor oë gehou word, is ’n ambisieuse projek, veral gesien in die lig van die Internasionale reg waar sake nie vinnig beredder word nie. Daar word aanvaar dat ’n proses soos hierdie ten minste ’n dekade sal duur, maar uiteindelik sal dit in belang van die groter Internet wees. Dit sal ook tyd vir die VSA verleen om te aanvaar dat die Internet nie meer die eksklusiewe eiendom van die VSA is nie.

Huidig is daar twee teenstrydige teorieë wat voorgehou word om die groter Internet te reguleer. Enersyds is daar die multi-belangegroepreguleringsmodel, en andersyds word die regeringsbeheerde reguleringsmodel deur verskeie state voorgehou. Daar word aan die hand gedoen dat as die tweevlak-sisteem van die Internet voor oë gehou word, beide regulasiesisteme sinvol aangewend kan word. Op nasionale vlak is

dit duidelik dat die regeringsbeheerde reguleringsmodel by staat-intranette gebruik kan word. Dit sal tot 'n groot mate die *status quo* van huidige staat-intranetreguling bevestig. Regerings neem beheer oor die staat-intranet volgens die beginsels van kubersoewereiniteit en jurisdiksie wat in hoofstuk 7 bespreek is, maar twee ander rolspelergroepe, te wete die privaat sektor en burgerlike samelewing, speel hulle onderskeie rolle. Dit kom in wese ooreen met die model wat in die WSIS-I-verslag uiteengesit is.[178]

Reguleringsteorieë van die negentigerjare kan met vrug gebruik word op die staat-intranet, aangesien dit baie ooreenkomste met die eenheids-Internet van die negentigerjare vertoon. Die wyse waarop die privaat sektor en die burgerlike samelewing hulle onderskeie rolle vertolk, is deur gebruikmaking van selfregulering. Die staat se rol is bloot om 'n "enabling environment", of struktuur van effektiewe netwerkbeheer, te ontwikkel. So 'n struktuur sal aspekte van netwerk neutraliteit en goeie netwerkontwikkeling, soos die "end-to-end"-beginsel, as basis gebruik.[179]

Die multi-belangegroepreguleringsmodel kan op die internasionale vlak as reguleringsisteem gebruik word. Die voorbehoud is egter dat sake van gemeenskaplike belang ten aansien van tegniese regulering hier beredder word. Die rede waarom die voorbehoud bestaan, is omdat dit ongelukkig nie moontlik is om sake van inhoudelike aard op die Internet in 'n multi-belangegroep uit te klaar nie. Inhouds-aangeleenthede is bykans altyd gekoppel aan sterk gevestigde ideologieë, en dit kan nie sinvol op 'n multi-belangegroep-platform hanteer word nie. Byvoorbeeld, die aangeleentheid van vryheid van spraak in Sjina wat by 'n IGF-vergadering geopper word, sal nie werklik enige praktiese gevolge vir die algemene Sjinese burger hê nie, aangesien daardie inhoudelike aangeleentheid totaal binne die beheer van die Sjinese regering is (op staatsvlak), en die bespreking daarvan op internasionale vlak gaan geen praktiese uitkoms lewer nie. Die doel van 'n multi-belangegroep sou wees om Internetregulering van gemeenskaplike

178 Afd 4.2.4.3.

179 Afd 4.2.3.2.

tegniese aangeleenthede uit te klaar, soos die ontwikkeling van nuwe topvlakdomeine en kwaliteit van Internetstrukture. Dit beteken dan ook dat inhoudelike aangeleenthede van die Internet die beste op nasionale vlak beredder word.

Daar word nie ontken dat daar somtyds wél die behoefte bestaan om inhoudsaangeleenthede ten aansien van die Internet op 'n internasionale *forum* te bespreek nie. Iets soos die skending van menseregte op die Internet is iets wat wél aangespreek moet word, maar dit is twyfelagtig of die bespreking hiervan in enige van die *fora* wat regulering op die Internet bewerkstellig (en wat in hoofstuk 5 bespreek is), enige werklike resultate sal lewer. Die skrywer is van mening dat daar tans geen so 'n *forum* bestaan nie, en daar word gespekuleer dat die rede daarvoor blyk te wees dat state nie gewillig is om sake wat in die nasionale sfeer is, op 'n internasionale *forum* te bespreek nie.

Wat die werking van internasionale organisasies op die Internet betref, word daar aanbeveel dat die ISOC, IETF en W3C onaangeraak gelaat word. Deur hul selfreguleringsisteem funksioneer hulle reeds vir bykans twee dekades sonder enige regerings-inmenging, en dit behoort aangemoedig te word.

Wat die IGF betref, word daar aangevoer dat hierdie organisasie se belang in die toekoms sal taan. As gespreksforum vorm dit 'n multi-belangegroep, en word daar aanbeveel dat dit sinvol onder ICANN ingeskuif word indien laasgenoemde omvorm word, soos hierbo aanbeveel.

Die ITU se voortgesette rol by Internetregulering word onder verdenking geplaas, aangesien dit nie 'n positiewe beeld in die internasionale gemeenskap by state of internasionale organisasies het nie. Die feit dat dit as 'n orgaan van die Verenigde Nasies funksioneer, tel nie in die ITU se guns nie. Daar word gevolglik aanbeveel dat die ITU nie by regulering van die Internet betrokke moet wees nie.

Hierteenoor staan die Raad van Europa geensins onder verdenking nie, en behoort die rol wat hulle speel, geloof te word en hul werksaamhede

aangemoedig word. Daar word aan die hand gedoen dat die Raad van Europa sy rol ten aansien kubermisdaad uitbrei, asook die skep van verdere verdrae wat hul visie van menseregte en demokrasie, uitbrei.

Wat spioenasie op die Internet betref, blyk dit dat daar twee wyses is waarop dit huidig geskied: enersyds moniteer state data wat vryelik op die internasionale vlak van die Internet voorkom. Dit is die tipe monitering wat die VSA bedryf het met sy metadata-program. Andersyds vind spioenasie plaas waar die groter Internet as ’n kanaal gebruik word om ongemagtigde toegang tot ’n netwerk op ’n staat se intranet te verkry. Verskeie lande maak hul skuldig aan dié praktyk. Daar word aanbeveel dat ’n multilaterale ooreenkoms ontwikkel word om beide praktyke te verbied.

Daar word aanvaar dat so ’n verdrag nie by sommige state byval sal vind nie, en daarom word daar ook aanbeveel dat die praktyk van data-lokalisering aangemoedig word. Dit het vele voordele: die mees voor-die-hand-liggende redes is dat sulke inligting dan veiliger bewaar kan word; daar kan makliker aan nasionale wetgewing voldoen word waar aspekte soos beskerming van persoonlike inligting van belang is. ’n Verdere voor-die-hand-liggende voordeel van data-lokalisering is dat dit die plaaslike ekonomie bevoordeel deurdat daar van plaaslike kundigheid gebruik gemaak word om die data binne die staat te hou: dit skep werk en beperk buitelandse uitgawes.

Daar word verder aanbeveel dat die voorgestelde verdrag wat spioenasie verbied, ’n bepaling bevat wat ondertekende state aanmoedig om sanksies teen state wat hulle aan spioenasie op die Internet skuldig maak, in te stel. Soos wat data-lokaliseringstegnologieë verbeter, bestaan daar geen twyfel dat “elektroniese sanksies” ’n werklikheid gaan word nie. Trouens, in hoofstuk 7 is daar aangedui hoe Duitsland ná die Snowden-onthullings besluit het om data-lokaliseringsmeganismes in werking te stel, en dit is eintlik niks anders nie as “elektroniese sanksies”. Daar bestaan by die skrywer geen twyfel nie dat hierdie tendens sal voortduur vir solank state hulle skuldig maak aan spioenasie op die Internet.

8.3.2 Aanbevelings ten aansien van Nuwe Suid-Afrikaanse Regeringsbeleid

Die ontwikkeling van 'n nasionale staat-intranetbeleid

Verskeie groot state wat die Internet as 'n strategiese hulpbron beskou, soos Sjina, Indië, Brasilië en selfs die Europese Unie begin staat-intranet-ontwikkeling (en dus kubersoewereiniteit) as 'n nasionale prioriteit te beskou.[180] Daar word aanbeveel dat 'n ondersoek by die Suid-Afrikaanse Regskommissie geregistreer word om 'n ondersoek te loods om te bepaal watter wetgewende ingrepe nodig mag wees om die Suid-Afrikaanse intranet te beskerm en te ontwikkel. Dit is duidelik dat van die grootste state van die wêreld ernstig is oor kubersoeweiniteit, en ongelukkig is dit nog geensins 'n prioriteit by Suid-Afrika nie. 'n Ondersoek deur die Suid-Afrikaanse Regskommissie sal die nodige wetgewende insette lewer om hierdie belangrike saak aan te spreek.

Daar word ook aanbeveel dat die Suid-Afrikaanse regering 'n afsonderlike komitee bymekaarbring om die tegniese aangeleenthede van 'n staat-intranet[181] te ondersoek. Die doel daarvan is om 'n sterk en goedwerkende netwerk te skep wat alle rolspelers se belange in Suid-Afrika kan dien. Die komitee sal moet bestaan uit rekenaar- en netwerk *tegnici*, asook regsgeleerdes wat oor die nodige kundigheid van Internetregulering beskik. Sake wat by hierdie *forum* onder bespreking geneem moet word, is die aard van effektiewe netwerkontwerp, asook internetwerkskakeling. Onderliggende beginsels wat so 'n ontwerp onderlê, is netwerk neutraliteit en die "end-to-end"-beginsel. Die sinvolheid van die gebruik van diep-pakket-inspeksie sal ongetwyfeld ook oorweeg moet word. Aangesien Suid-

180 Hfst 7.

181 Let daarop dat die benaming "staat-intranet" in hierdie studie dui op die netwerk van die land, of staat, wat vir gebruik deur al sy inwoners beskikbaar is, en *nie* die konsep van 'n netwerk wat slegs vir die regering of staats-instansie beskikbaar is nie. "Staat-intranet" word dus volgens die Internasionale reg se konsep van 'n staat beoordeel as die oorkoepelende netwerk wat in 'n betrokke staat of land ontwikkel word om almal te dien.

Afrika 'n demokrasie is, is die taak van die regering om 'n netwerk te skep as 'n raamwerk waarvan alle inwoners gebruik kan maak sonder onnodige inmenging van die regering. Dit sal ook die gevolg hê dat die Internet as 'n apparaat van ekonomiese groei gebruik kan word.

Wanneer die bevindings van die regskommissie en tegniese kommissie (wat hierbo aanbeveel word) beskikbaar is, word daar verder aanbeveel dat die regering die nasionale e-strategie, soos in artikel 5 van die EKT-wet uiteengesit is, ontwikkel.[182] Wanneer die nasionale e-strategie geformuleer word, moet daar ernstige aandag gegee word aan meganismes om plaaslike kommersiële netwerke so vry as moontlik te hou sonder dat dit op die eienaars daarvan so 'n groot las plaas dat dit ontwikkeling verhinder. Daar behoort ook baie aandag gegee te word aan beste praktyke ten aansien van koppeling van netwerke om 'n internetwerk te vorm. Suiwer netwerkbeginsels moet in wetgewing vervat word. Dieppakketinspeksie behoort slegs aan die einde van die netwerk gebruik te word, en slegs vir die behoud van die integriteit van die netwerk en nie vir die skep van nuwe produkte deur ISP's nie. Data-lokalisering van sensitiewe inligting behoort aangemoedig te word. Daar word aanbeveel dat ál hierdie aangeleenthede in die nasionale e-strategie ingesluit word.

8.3.3 Aanbevelings ten aansien van Suid-Afrikaanse Regshervorming

8.3.3.1 Wet op Elektroniese Kommunikasies en Transaksies

8.3.3.1.1 Herstrukturering van Verteenwoordigende Liggaam

Hierdie studie het aangetoon hoe die EKT-wet[183] 'n selfreguleringsisteem vir ISP's tot stand gebring het, maar hoe die regulasies van die minister ten aansien van verteenwoordigende liggame tot gevolg het dat 'n

182 Afd 6.4.4.2.6.

183 25 van 2002.

regeringsbeheerde sisteem tot uitvoering gebring is.[184] Die minister se regulasies gaan lynreg in teen die gees van die selfreguleringsisteem wat in die EKT-wet ontwikkel is. Daar is ook verduidelik hoe ISP's wat nie ISPA-lede is nie omdat dit 'n ander tipe Internet-bedryf beoefen, uitgesluit word van die werking van die nie-aanspreeklikheidsbeskerming van Hoofstuk XI van die EKT-wet.[185] Daar word aanbeveel dat artikel 71 van die EKT soos volg gewysig word:

> **71 Verteenwoordigende Liggaam**
>
> (1) 'n Liggaam kan vir doeleindes van hierdie hoofstuk as 'n bedryfsverteenwoordigende liggaam beskou word indien dit in 'n bepaalde industrie as 'n verteenwoordigende liggaam geag word en aan die vereistes soos in subartikel (2) genoem, voldoen.
>
> (2) 'n Liggaam kan as 'n verteenwoordigende liggaam beskou word indien dit aan die volgende vereistes voldoen-
>
> > (a) lidmaatskap van die liggaam gebaseer is op gespesifiseerde kriteria wat in daardie industrie in gebruik is en die kriteria in sy gedragskode uiteengesit is;
> >
> > (b) die liggaam sy lede aan die gedragskode onderwerp het;
> >
> > (c) die gedragskode voortdurende onderwerping van gespesifiseerde standaarde van gedrag vereis; en
> >
> > (d) die verteenwoordigende liggaam in staat is om sy gedragskode voldoende te moniteer en af te dwing.

Hierdie voorgestelde wetswysiging het verskeie veranderinge tot gevolg. In die eerste plek verskuif die voorgestelde wysiging die fokus van 'n regeringsbeheerde sisteem na 'n selfreguleringsisteem. Dit is in lyn met die oorspronklike doel van die wet. Die wyse waarop die verandering bewerkstellig word, is om die bedryfsverteenwoordigende liggaam die sentrale rolspeler te maak, en nie die minister nie.

Die tweede verandering wat so 'n voorgenome wetswysiging teweeg sal bring, is dat meer as een verteenwoordigende liggaam outomaties erkenning sal verkry. Subartikel (1) van die voorgenome wetswysiging

184 Afd 6.4.4.2.2.

185 Die saak van *Tsichlas and Another v Touch Line Media (Pty) Ltd* 2004 (2) SA 112 (W) is gebruik om hierdie punt te illustreer. Sien afd 6.4.4.2.3 vir die bespreking van die beslissing.

bepaal dat die verteenwoordigende liggaam in ’n bepaalde industrie as ’n verteenwoordiger beskou sal word, en dit hou die voordeel in dat ISP’s nie eensydiglik ’n verteenwoordigende liggaam vir homself tot stand kan bring nie. Die organisasie moet ten minste in die industrie as ’n verteenwoordigende liggaam beskou word, en die bepaling daarvan deur ’n hof is ’n eenvoudige feitebeslissing. Die onmiddellike voordeel van so ’n wetswysiging sal byvoorbeeld die probleem wat daar by die *Tsichlas*-saak[186] aangetoon is, uit die weg ruim deurdat die verteenwoordigende liggaam in daardie saak outomaties as ’n verteenwoordigende liggaam volgens die voorgenome wetswysiging beskou sal word.

Die derde gevolg wat die voorgenome wetswysiging meebring, is dat subartikel (2) bepaal dat die verteenwoordigende liggaam aan vier objektief-bepaalbare kriteria moet voldoen. Dit staan in sterk kontras teenoor die huidige artikel wat regsonsekerheid teweeg bring weens die feit dat die minister die uitspraak moet maak of ’n verteenwoordigende liggaam kwalifiseer as sodanige rolspeler.

Die vereiste wat in subartikel (2)(a) gespesifiseer word, bepaal dat lidmaatskap tot die verteenwoordigende liggaam slegs verleen sal word indien die aansoeker aan die vereistes van daardie industrie voldoen. Dit is nie ’n vreemde konsep nie, aangesien enige verteenwoordigende liggaam ’n sekere fokus het om rolspelers, met bepaalde gemeenskaplike belange, te dien. Dit hou ook die voordeel in dat die verteenwoordigende liggaam nie sy funksie te breedvoerig neerlê en sodoende nie meer in staat is om sy gefokusde doel te verrig nie.

Subartikel (2)(a) bepaal ook dat kriteria in die gedragskode gespesifiseer moet word. Dit het die gevolg dat ’n hof bloot ’n feitebeslissing moet maak of die lid aan die kriteria van die verteenwoordigende liggaam voldoen.

Subartikel (2)(b) stem in wese met die huidige artikel 71(2)(a) van die EKT-wet ooreen, en benodig nie enige verdere verheldering nie.

Subartikel (2)(c) stem grootliks met die huidige artikel 71(2)(c) van

[186] Afd 6.4.4.2.3.

die EKT-wet ooreen, maar die woord "gespesifiseerde" is in die plek van die woord "voldoende" geplaas. Die rede hiervoor is dat die vereistes soos gespesifiseer in die gedragskode van die verteenwoordigende liggaam nagegaan moet word, en bepaal word of daaraan voldoen is. Dit is 'n feitevraag, en verskaf heelwat meer regsekerheid as die onsekere term "voldoende", wat huidig in die EKT-wet gebruik word.

Subartikel (2)(d) stem in wese met die huidige artikel 71(2)(d) van die EKT-wet ooreen, en benodig nie enige verdere verheldering nie.

Die uiteindelike gevolg van die voorgenome wetswysiging is dat heelwat meer Internet-rolspelers op die nie-aanspreeklikheidsbepalings van hoofstuk XI van die EKT-wet sal kan steun, en daar word aangevoer dat dit uiteindelik die doel van die wet was.

8.3.3.1.2 Vereiste van 'n Agent

In die studie is daar aangetoon dat die vereiste dat 'n agent aangestel moet word om afhaalkennisgewings te ontvang, 'n oorblyfsel uit die DMCA van die VSA is, en dat dit in die moderne era nie veel sin maak nie.[187] Daarom word daar aanbeveel dat die verwysing na 'n agent in die volgende gevalle geskrap word.

Artikel 75(2) behoort só te lees:

> (2) Die beperkings op aanspreeklikheid by hierdie artikel ingestel, is nie van toepassing op 'n diensverskaffer nie tensy hy of sy in staat is om kennisgewings van skendings te ontvang en ook op sy of haar webwerwe op plekke wat vir die publiek toeganklik is, die naam, adres, telefoonnommer en e-posadres waar kennisgewings afgelewer kan word, voorsien het.

Artikel 77(1) behoort só gewysig te word:

> (1) By die toepassing van hierdie Hoofstuk moet 'n kennisgewing van onwettige bedrywigheid op skrif wees, moet dit deur die klaer aan die diensverskaffer gerig wees, en moet dit insluit- ...

[187] Die EKT-wet maak op verskeie ander plekke, soos artikel 20, melding van 'n agent. Daar word nie aanbeveel dat hierdie verwysings na 'n agent verwyder word nie, aangesien die gebruik daarvan nie in hierdie studie bespreek is nie. Daar word slegs aanbeveel dat die verwysing na 'n agent in die artikels wat spesifiek genoem word, verwyder word.

Die gevolg van hierdie wetswysigings is nie ingrypend nie, maar dit verbeter tóg die algehele werking van die wet deurdat dit spesifiseer dat die ISP self die afhaalkennisgewing hanteer sonder die gebruikmaking van ’n onnodige tussenganger.

8.3.3.1.3 Suiwer Netwerkbeginsels

Vry-vloeiende data op ’n staat-intranet en op die groter Internet is ’n voorvereiste vir vooruitgang van enige staat. Dit is daarom baie belangrik om wetgewing in plek te stel om te verseker dat suiwer netwerkbeginsels gebruik word wanneer netwerke ontwikkel word. Die skrywer is van mening dat dit wenslik sou wees om afsonderlike wetgewing in hierdie verband te formuleer, aangesien dit die beste resultaat sal lewer om die gewenste uitwerking te bewerkstellig. Daar kan egter in die *interim* voorstelle gemaak word wat van nut behoort te wees totdat omvattende netwerkstruktuurwetgewing in plek gestel is. Dit sal die vorm aanneem van voorgestelde artikels wat by die EKT-wet gevoeg kan word. Daar word aanbeveel dat hierdie artikels by “Deel 2” van hoofstuk II van die wet gevoeg word as ’n nuwe artikel 10B.

10B Netwerk Neutraliteit

(1) Diensverskaffers wat openbare elektroniese kommunikasienetwerke bedryf, en diensverskaffers wat universele toegang tot Internetdienste lewer, moet toesien dat alle netwerke binne die republiek aan suiwer netwerkbeginsels voldoen, en mag nie enige gespesialiseerde apparate of programme in nodes van die netwerk in werking stel nie, behalwe waar dit gedoen word om aan subartikel 3 te voldoen.

(2) Die inhoud van data-pakkette wat deur nodes in enige netwerk vloei, mag nie ontleed word deur gebruikmaking van enige tegnologie wat tussen protokolle onderskei nie, behalwe waar dit gedoen word om aan subartikel 3 te voldoen.

(3) Diensverskaffers wat openbare elektroniese kommunikasienetwerke bedryf, en diensverskaffers wat universele toegang tot Internetdienste lewer, mag nie enige diens, program, of apparaat wat aan verbruikers gelewer word, verhinder, vertraag of blokkeer nie, en moet toesien dat gelyke verkeer gelyk behandel word, met dien verstande dat verhindering, vertraging en blokkering in die volgende gevalle gemagtig word:

> (a) Waar die fisiese integriteit en veiligheid van die netwerk bedreig word deur enige netwerkgebruik of aanhegting van ’n verbruiker, of
>
> (b) Waar opeenhoping op die netwerk voorkom, en slegs in die mate waarin dit nodig is om die opeenhoping te verlig: met dien verstande dat die verhindering, vertraging of blokkering gestaak sal word sodra die opeenhoping van die netwerk verlig is.
>
> (c) Ter uitvoering van ’n statutêre bepaling of hofbevel.
>
> (4) Indien die bedreiging van die fisiese integriteit en veiligheid van die netwerk, of die opeenhoping op die netwerk, te wyte is aan die gedrag van ’n verbruiker, sal, nadat die stappe geneem is om die netwerk te herstel, die verbruiker in kennis gestel word van die rede vir die verhindering, vertraging of smoring wat op die verbruiker se diens aangebring is, en sal die gebruiker die geleentheid gegun word om die gedrag wat die bedreiging of opeenhoping veroorsaak het, te staak.
>
> (5) ’n diensverskaffer wat ’n bepaling van hierdie artikel oortree of versuim om daaraan te voldoen, is skuldig aan ’n misdryf.

Subartikel 1 bevat die “end-to-end”-beginsel, en word gerig teen twee rolspelers, te wete (a) netwerkeienaars en administrateurs wat ruggraat-Internetdienste verskaf, en (b) ISP’s wat hierdie dienste van die ruggraat-netwerkeienaars huur en dit aan verbruikers beskikbaar stel. In beide gevalle word die installasie van gespesialiseerde harde- en sagteware op nodes verbied, wat die gevolg het dat die netwerk en internetwerk sonder steurnisse sal funksioneer.

Subartikel 2 verbied die praktyk van diep-pakket-inspeksie. Dit word nie by die naam genoem nie, maar enige soortgelyke tegnologie wat ontwikkel mag word, en wat dieselfde gevolg het, word eweneens verbied. Daar word wel uitsonderings toegelaat, omdat dit onmoontlik vir ’n ISP is om aan subartikel 3 (wat direk hieronder bespreek word), te voldoen indien daar nie een of ander moniteringsisteem in die netwerk ingebou is nie.

Subartikel 3 is die kern van hierdie reeks voorgenome artikels, en vervat die beginsel van netwerk neutraliteit. In die voorgenome subartikel word enige optrede van netwerkbestuurders om hulle netwerke só te manipuleer dat dit tot nadeel van die verbruiker strek, verbied. Die doel is om ’n netwerk daar te stel wat die vrye vloei van data verseker. Die gedrag wat verbied

word, is verhindering, vertraging of blokkering van data. Daar bestaan drie belangrike uitsonderings op hierdie algemene verbod. Die eerste is vervat in subartikel (3)(a), en behels dat verhindering, vertraging en blokkering van data toegelaat word om die fisiese integriteit van die netwerk te verseker. Hierdie subartikel sal in werking tree wanneer die netwerk om een of ander rede wanfunksioneer, en dit van die Internet ontkoppel sou word indien die regstellende maatreëls nie geneem word nie. In wese is daar twee wyses waarop 'n verbruiker die fisiese integriteit van die netwerk kan beïnvloed: die eerste is deur oormatige netwerkgebruik, en die tweede is die koppeling van 'n apparaat wat nie deur netwerk-administrateurs gemagtig is nie. In enige van hierdie gevalle kan die netwerk-administrateurs die nodige stappe neem om die integriteit van die netwerk te handhaaf.

Subartikel (3)(b) magtig die gebruik van verhindering, vertraging of smoring in gevalle waar opeenhoping op die netwerk voorkom. Dit gebeur gewoonlik gedurende spitstye op die netwerk, of in gevalle waar netwerkbestuur ontoereikend is aangesien té veel verbruikers op een netwerk geplaas word. (Laasgenoemde het te doen met groter profyte vir ISP's.) Wanneer so 'n opeenhoping voorkom, kan verhindering, vertraging of blokkering gebruik word om die probleem op te los en die netwerk weer na normale funksionering te neem. Sodra die netwerk egter weer korrek funksioneer, moet die beperkende meganismes wat geneem is om die netwerk te stabiliseer, beëindig word.

Subartikel (3)(c) magtig verhindering, vertraging of blokkering in gevalle waar 'n statuut of hofbevel sulke gedrag beveel. Dit is onwaarskynlik dat so 'n hofbevel gemaak sal word, maar dit is nie onmoontlik nie, byvoorbeeld waar 'n hof 'n ISP sal aansê om 'n verbruiker se diens te blokkeer aangesien dit met misdadigheid te doen het.

Dit is belangrik om daarop te let dat al die uitsonderings te doen het met behoorlike netwerkbestuur, en laat nie netwerkmanipulasie met die uitsluitlike doel van groter profyte toe nie. Dit is uiteindelik tot voordeel van die eindgebruiker, asook die integriteit van die netwerk.

Subartikel 4 bepaal dat 'n ISP die verbruiker in kennis moet stel indien sy gedrag die netwerk se integriteit beïnvloed het. Dit hoef slegs *ex post facto* gedoen te word, wat die ISP die geleentheid bied om *eers* die netwerk te stabiliseer, wat uiteraard tot alle netwerkgebruikers se voordeel is. Die gebruiker word dan die geleentheid gegee om sy gedrag te verander, maar indien dit nie gebeur nie, beskik die ISP oor die bevoegdheid om die diens op te skort.

Subartikel 5 word aanbeveel, nie met die hoofdoel om nóg 'n misdryf te skep nie, maar eerder om te verseker dat netwerk-eienaars en ISP's aan die wet voldoen. Indien daar nie 'n strafsanksie aan nie-voldoening gekoppel word nie, sal die voorgenome artikels nie die gewenste uitwerking hê nie.

Daar word aangevoer dat die voorgestelde wetswysigings tot 'n meer effektiewe EKT-wet sal lei. Dit is egter nie die enigste wetswysiging wat aanbeveel word nie, en vervolgens word daar oorbeweeg na die RICA-wet.

8.3.3.2 Die RICA-wet

Hierdie studie het aangedui watter ingrypende magte aan die intelligensiedienste verskaf word deur die totstandkoming van onderskeppingsentrums onder die RICA-wet.[188] Daar is ook verduidelik dat daar in Suid-Afrika vier oorsigmeganismes bestaan wat die intelligensiedienste in bedwang moet hou. Die gevolgtrekking is reeds gemaak dat hierdie vier oorsigmeganismes totaal ontoereikend is, en dat magsvergrype maklik kan voorkom. Daarom word daar aanbeveel dat Suid-Afrika dringend 'n oudit van die intelligensiedienste moet hou, asook nuwe oorsigstrukture in plek stel om effektiewe oorsig te bewerkstellig. In hierdie konteks word daar aanbeveel dat 'n kommissie wat soortgelyk aan die Church-kommissie is, gestig word, en dat daardie kommissie die nodige ondersoeke van stapel stuur.[189] Daar word verder aanbeveel dat die kommissie wat voorgestel word, 'n onafhanklike bestaan voer, en nie in enige opsig deur politieke partye bedryf word nie.

188 70 van 2002.

189 Afd 6.4.1.5.1.

So ’n kommissie sal ’n uitvoerige ondersoek moet doen en tot gedetailleerde bevindings kom. Daar word voorsien dat die uitslag van so ’n kommissie tot nuwe, omvattende wetgewing sal lei. Dit sal dus nie enige doel by hierdie studie se aanbevelings dien om spesifieke wetgewing aan te beveel nie. Die belangrikste aanbeveling bly egter dat aangesien die totstandkoming van onderskeppingsentrums so ’n ingrypende inbreuk op die reg op privaatheid vir alle Suid-Afrikaners meebring, die oorsig van intelligensiedienste ingrypend gewysig sal moet word.

Die totstandkoming van ’n afsonderlike hof wat spesifiek aangeleenthede van die nasionale intelligensiedienste beheer, soos die “Foreign Intelligence Surveillance Court” (FISC) in die VSA, is ’n baie goeie voorstel, aangesien dit by die dag-tot-dag bedrywighede van die intelligensiedienste betrokke is, en behoorlike oorsig kan verrig. Daar is egter in die studie aangedui dat die FISC in die VSA tóg ernstige tekortkomings het, maar daar word aan die hand gedoen dat hierdie tekortkomings beredder kan word deur die sisteem van verslagdoening en statistiekontleding wat aan ’n owerheid soos die Gesamentlike Staande Komitee oor Intelligensie[190] gedoen word. Indien die statistiek van ’n hof wat soortgelyk aan die FISC is, aantoon dat die hof bykans alle aansoeke op monitering toestaan, sal dit baie vinnig aan die Gesamentlike Staande Komitee oor Intelligensie toon dat effektiewe oorsig gebrekkig is. So ’n sisteem sal ongetwyfeld meer effektief wees as dit wat huidig in Suid-Afrika bestaan.

8.3.4 Aanbevelings ten aansien van Opleiding

Een van die ingrypendste aspekte van die Internet is dat die onderliggende argitektuur daarvan verander kan word. Benkler het treffend aangetoon dat wanneer die argitektuur van die Internet gewysig word, dit die regulerings-ingrepe op “hoër” vlakke so kan beïnvloed dat dit ongedaan gemaak kan word. Op dieselfde wyse het die *Yahoo v Licra*-hofbeslissings aangedui dat

[190] Afd 6.4.4.3.2.

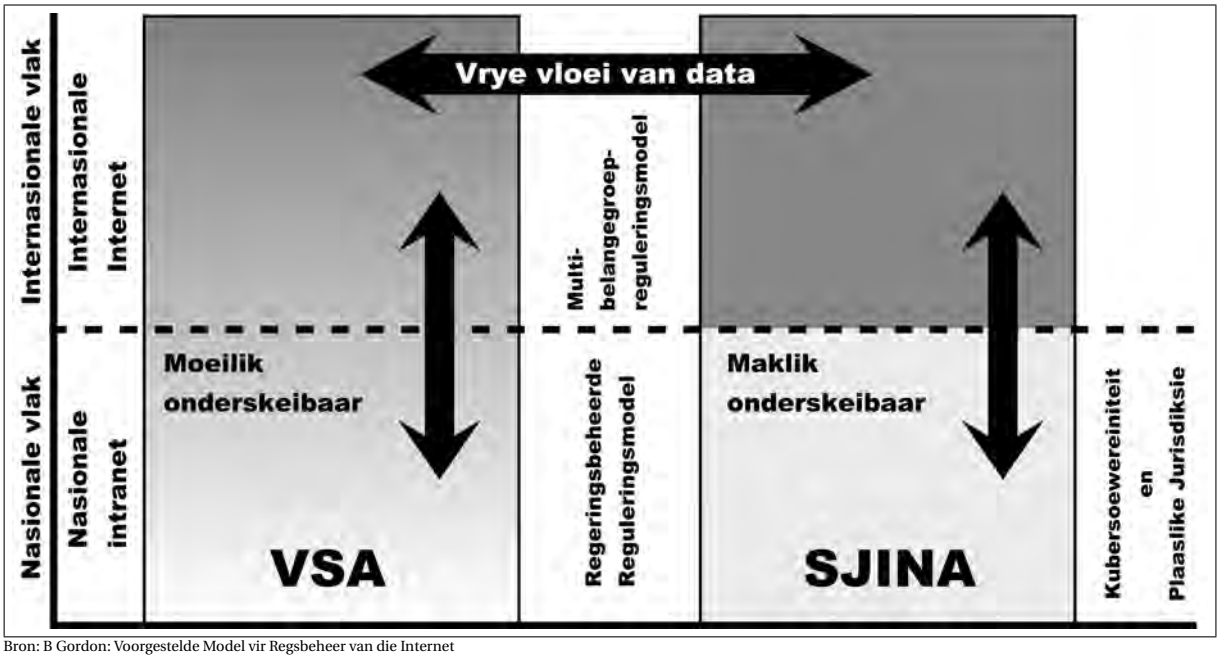
manipulering van netwerk argitektuur van die Internet baie effektief kan wees. Wanneer regulatoriese ingrepe op die argitektuur van die Internet toegepas word, moet reguleerders besef dat: (a) dit hoër vlakke se regulasies ongedaan sal maak, en (b) dat dit slegs op staat-intranetvlak ingestel moet word, en (c) dat daar baie versigtig te werk gegaan moet word om nie die argitektuur van die groter Internet daardeur skade te berokken nie. Hierdie is alles redelik eenvoudige konsepte, maar is iets wat nie noodwendig voor-die-hand-liggend is nie. Dit is daarom belangrik dat die Suid-Afrikaanse wetgewer, die howe, en regsgeleerdes wat met reguleringskwessies van die Internet te doen het, deeglik van hierdie beginsels ingelig word. Daarom word daar aanbeveel dat opleiding ten aansien hiervan aan die genoemde partye gelewer word.

In hoofstuk 6 is daar aangedui watter rolspelers by Internetregulering geteiken kan word om regulering te bewerkstellig — ook buite die streek waar die regeringsrolspelers jurisdiksie het. Wanneer opleiding oor die gevolge van argitektuursveranderinge op die Internet ontwikkel word, word daar aanbeveel dat opleiding aangaande verskillende rolspelers op die Internet ook onder oorweging geneem word.

8.4 Voorgestelde Model vir Regsbeheer van die Internet

Soos in die titel van hierdie studie aangedui, is verskeie aspekte van regsbeheer in die konteks van die Internet bespreek, en aanbevelings is gemaak. Vervolgens word hierdie aanbevelings gebruik om ’n nuwe model van regsbeheer op die Internet voor te stel.

Die Internet van vandag bestaan uit twee vlakke. Die eerste vlak is die nasionale vlak, en die tweede vlak is die internasionale vlak. Die skeiding in twee vlakke het plaasgevind omdat die Internet sedert die jaar 2000 gefragmenteerd geword het. Elkeen van hierdie vlakke vertoon sy eie



Bron: B Gordon: Voorgestelde Model vir Regsbeheer van die Internet

Figuur 8.1: Nasionale- en Internasionale Vlakke van Regsbeheer op die Internet.

eienskappe. Die vlakke is egter nie absoluut geskei nie, maar oorvleuel in ’n klein mate. By sekere state is die vlakke maklik identifiseerbaar, soos by Sjina, maar by ander state, soos die VSA, is dit bykans ononderskeibaar. Die tendens van Internet-fragmentasie is steeds aan die gang, en daar word aan die hand gedoen dat hierdie tendens nie sal eindig voordat staat-intranette min of meer nasionale grense en ideologieë verteenwoordig nie. Soos wat die tyd verder verloop sal staat-intranette makliker onderskeibaar word. Sien figuur 8.1 vir ’n grafiese voorstelling hiervan.

Nasionale Vlak

Op nasionale vlak bestaan daar die staat-intranet. Dit bestaan uit netwerke wat aanmekaar geskakel word om internetwerke te vorm. Dit is die fisiese argitektuur van rekenaars, bedieners, roeteerders, kabels, selfoontorings en alle apparate wat daaraan geskakel is. Ál hierdie apparate val onder die jurisdiksie van die betrokke staat, en is vatbaar vir regulering. Dit vorm deel van kubersoewereiniteit. State kan dus regte, verpligtinge en bevoegdhede

ten aansien van alle toerusting op die staat-intranet uitoefen.

Alle data wat op die staat-intranet voorkom, kan weens die werking van soewereiniteit en jurisdiksie, deur die regering gereguleer word. Dit is nie iets nuuts nie, en gebeur daagliks in alle state van die wêreld, soos byvoorbeeld waar die Wet op Elektroniese Kommunikasies en Transaksies op netwerke in Suid-Afrika aanwending vind. Alle inhoudelike aangeleenthede (inhoud wat op netwerke aangetref word), val onder hierdie reguleringsproses, byvoorbeeld waar die EKT-wet gebruik word om ISP's se aanspreeklikheid oor data (inhoud) wat op hulle netwerke te vinde is, te reguleer. Wat wél nuut is, is dat die grense van plaaslike wetgewing duideliker sigbaar gaan word soos wat staat-intranette duideliker afgesper en beperk word. In hierdie konteks sal data-lokalisering veral belangrik word, aangesien sensitiewe data al hoe meer binne die staat se grense gehou word. Data (inligting) wat op staat-intranette voorkom, word deur die betrokke staat deur die werking van jurisdiksie en kubersoewereiniteit gereguleer.

Die staat het die bevoegdheid om sy staat-intranet na goeddunke te struktureer, maar daar word aan die hand gedoen dat aangesien Suid-Afrika 'n demokrasie is, die beste vorm van staat-intranet-ontwikkeling sal wees om 'n basiese netwerkstruktuur deur wetgewing te ontwikkel (koppeling van netwerke en internetwerke), maar dat *regulering* van die staat-intranet gedoen word deur van selfregulering gebruik te maak. Burgers van die land selfreguleer dus in 'n groot mate. Hierdie konstruksie is eweneens nie vreemd nie, want die Suid-Afrikaanse regering meng gelukkig nie in 'n groot mate met burgers se gebruik van plaaslike netwerke en die groter Internet in nie.

Die grootste verantwoordelikheid wat 'n staat ten aansien van sy eie staat-intranet het, is om dit goed te struktureer en te beskerm. Goeie strukturering het 'n vinnige en veilige staat-intranet tot gevolg. Beskerming van die staat-intranet geskied deur veral ISP's en netwerk-eienaars aan bande te lê deur goeie beginsels van netwerk neutraliteit en die "end-to-

end"-beginsel in staat-intranette gestalte te gee.

Die regeringsbeheerde reguleringsmodel, met sy drie vlakke van verantwoordelikhede, sal goed by staat-intranette gebruik kan word. Hiermee word bedoel dat die regering, die privaat sektor, en die burgerlike samelewing die drie vlakke vorm wat regulering meebring. Elkeen van hierdie vlakke het 'n rol te speel, soos deur die WSIS-I-proses uiteengesit.[191]

Internasionale Vlak

Die internasionale vlak van die Internet bestaan uit inligting wat op die "oop" Internet vloei. Hierdie data vloei vryelik tussen verskillende state se geografiese grense. Die gevolg is dat dit potensieël onderworpe is aan monitering deur enige staat, soos wat die VSA en vennote gedoen het toe dit deur die Snowden-spioenasieskandaal onthul is. Dit is raadsaam vir 'n staat om nie enige sensitiewe data op die internasionale vlak te laat vloei nie.

Jurisdiksievestiging van data op die internasionale vlak van die Internet word volgens die *Lotus*-beslissing hanteer. Dit beteken dat 'n staat ekstra-territoriale jurisdiksie ten aansien van die internasionale vlak kan vestig, en aangesien die *Lotus*-beslissing gewys het dat meeste state van die wêreld geneig is om ekstra-territoriale jurisdiksie ten aansien van strafsake te vestig, sal dit waarskynlik wees dat state jurisdiksie ten aansien van strafsake op die oop Internet sal vestig. Dit vorm nie 'n probleem nie, aangesien dit bloot die *status quo* van die Internet van vandag bevestig.

Daar word in hierdie model voorgestel dat die vryheid van die internasionale Internet verseker word deur die onderhandeling van 'n multilaterale ooreenkoms. Daar word aan die hand gedoen dat die totstandkoming van so 'n verdrag nie moeilik sal wees indien state daarvan bewus is dat staat-intranette geheel en al deur hulle gestruktureer sal word nie. Inhoudelike aangeleenthede wat in 'n verdrag op die internasionale

191 Afd 4.2.4.3.

Internet ingesluit behoort te word, is beginsels van ’n vrye netwerk soos netwerk neutraliteit, die beginsel van ’n “dom netwerk” volgens die “end-to-end”-beginsel, ’n verbod op diep-pakket-inspeksie en handhawing van menseregte. ’n Algehele verbod op monitering, soos die metadata-program wat die VSA bedryf het, behoort ook by so ’n verdrag ingesluit te word. Spioenasiebedrywighede van een staat op ’n ander staat se intranet behoort eweneens geheel en al verbied te word, aangesien sulke bedrywighede eenvoudig ’n handeling van “hacking”, of ongemagtigde toegang, sal wees. Om voldoening aan die verdrag te verseker, kan die strafmaatreëls van sanksies ingestel word om state tot gehoorsaamheid te dwing. Met die tegnologieë wat vandag beskikbaar is, is dit moontlik om sulke “elektroniese sanksies” ’n werklikheid te maak.

Die regeringsmodel wat op die internasionale Internet gebruik kan word, is die multi-belangegroepreguleringsmodel. Daar is reeds hierbo verduidelik dat data wat met inhoud te doen het — en wat gewoonlik kontroversieël tussen verskillende ideologieë is — op nasionale vlak hanteer word. In hoofstuk 5 is daar verduidelik hoe tegniese regulering grotendeels sonder veel konflik deurgevoer word, en die multi-belangegroepreguleringsmodel werk tans baie goed op hierdie vlak. Dit behoort net so gelaat te word.

Wat die struktuur van ICANN betref, is dit duidelik dat dit binne die Internasionale vlak geplaas behoort te word. Dit is tans ’n totale vreemdheid in die internasionale sfeer, en is nie bestaanbaar ingevolge die Internasionale reg nie. Daar word voorgestel dat dit volgens hierdie model as ’n internasionale organisasie ingevolge ’n multilaterale ooreenkoms (verdrag) vervorm word, en dat daar aan die vereistes soos wat die Internasionale Regskommissie neergelê het, voldoen word. Die hoofkantoor behoort nie in die VSA te wees nie, maar in ’n neutrale jurisdiksie vir internasionale organisasies, soos Genéve, Switserland. Dit behoort egter *nie* onder die vaandel van die Verenigde Nasies of die ITU geplaas te word nie, aangesien meeste state van die wêreld nie tot so ’n strukturering sal toestem nie.

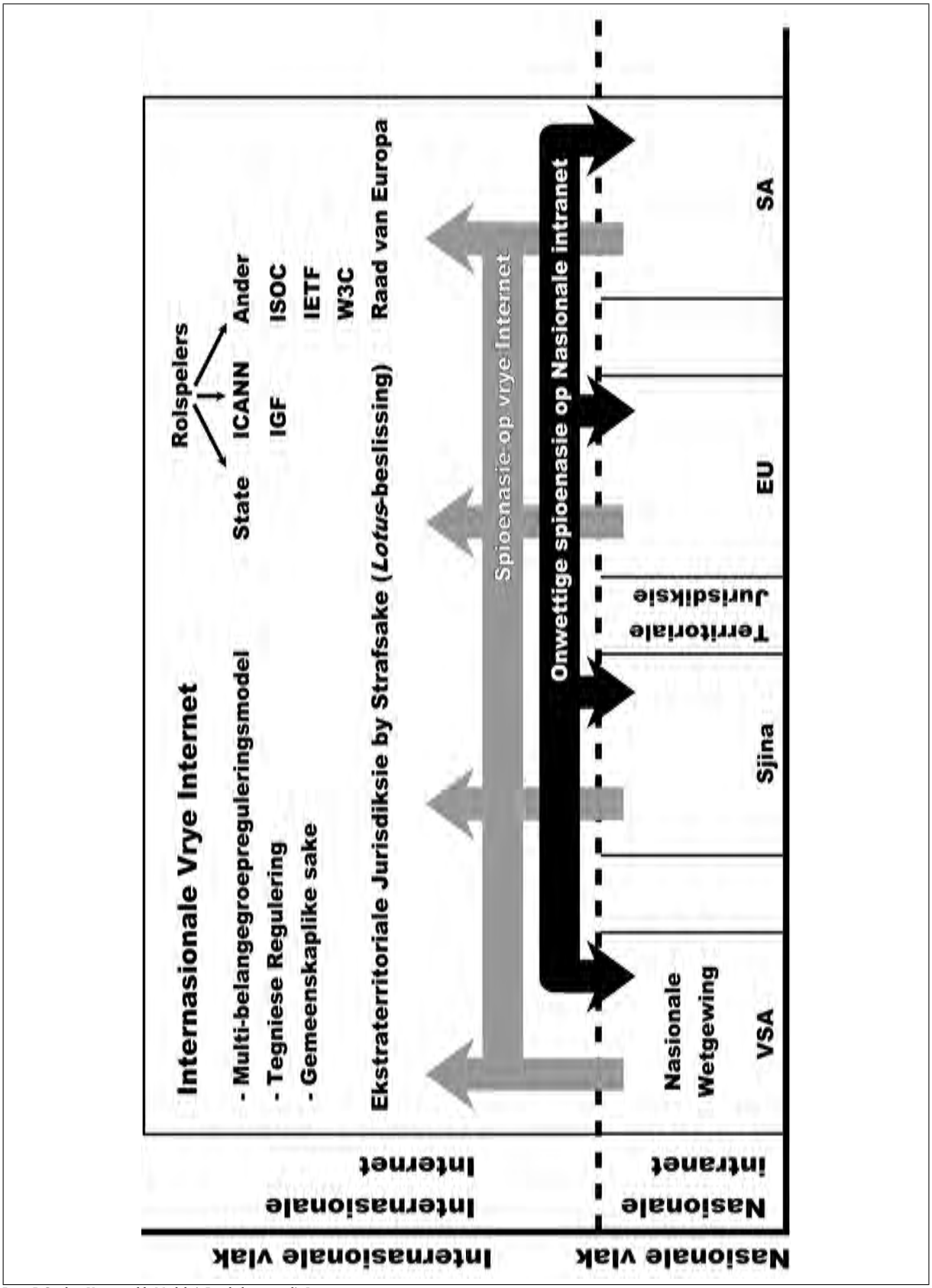
Wat ander internasionale organisasies betref, kan die IGF as gespreksforum onder ICANN se struktuur ingeskuif word. Die skrywer huldig die opinie dat hierdie organisasie se belang in die volgende dekade sal taan. Die Raad van Europa behoort aangemoedig te word om voort te gaan met die skepping van multilaterale verdrae wat menseregte op die Internet bevorder. Figuur 8.2 bevat 'n grafiese voorstelling van Regsbeheer van die Internet.

Vloei van Inligting

Vloei van inligting kan op verskillende wyses geskied. Data word op die nasionale vlak geskep. Indien dit van 'n sensitiewe aard is, word dit binne die staat deur gebruikmaking van data-lokalisering gehou. Indien dit nie van 'n sensitiewe aard is nie, kan data na die internasionale vlak vloei. Data op die Internasionale vlak vloei vryelik tussen verskillende state.

Inligtingspioenasie kan op twee wyses geskied. Enersyds is dit moontlik om data op die internasionale vlak te moniteer aangesien dit vry tussen state vloei. Andersyds is dit moontlik om deur die internasionale vlak te beweeg en data op ander state se intranette te verkry. Die eerste is bloot internasionale inligtingspioenasie, en die tweede is ongemagtigde toegang tot 'n staat-intranet. Beide vorme behoort in 'n internasionale verdrag verbied te word.

Nasionale Vlak	**Internasionale Vlak**
Staat-intranet	Globale Internet
Kubersoewereiniteit en jurisdiksie	Globale Vrye Internet
Netwerke en Internetwerke	Internasionale Internet
Data-lokalisering van sensitiewe inligting	Vrye inligting
Regering skep intranet-struktuur, maar gebruikers selfreguleer	Beheer deur verdrae; tegniese regulering deur ICANN, ISOC, IETF, W3C
Plaaslike ISOC-tak hanteer plaaslike aangeleenthede	Internasionale ISOC hanteer sake van gemeenskaplike belang
Regeringsbeheerde reguleringsmodel	Multi-belangegroepreguleringsmodel



Bron: B Gordon: Voorgestelde Model vir Regsbeheer van die Internet

Figuur 8.2: Voorgestelde Model vir Regsbeheer van die Internet.

8.5 Slot

In die begin van hierdie studie is daar verduidelik hoe die moderne wêreld in geografiese gebiede verdeel is, en hoe die beginsel van soewereiniteit dit alles onderlê. Die totstandkoming van die Internet het egter hierdie geografiese afbakenings verontagsaam, deurdat dit ’n internasionale netwerk gevorm het wat oor landsgrense heen beskikbaar was.

Aanvanklik was dit onduidelik hoe hierdie situasie aangespreek sal word, aangesien die Internet vele probleme vir reguleerders en regsgeleerdes, wat hul nasionale wetgewing moes uitvoer, geskep het. Dit het voorgekom asof die Internet ’n nuwe tydvak van ’n grenslose wêreld sou inlui, en dat die Internet die konsep van soewereiniteit, tot niet gemaak het.

Nadat hierdie studie verskeie *Aspekte van Regsbeheer in die Konteks van die Internet* bespreek het, blyk dit dat die teenoorgestelde júís waar is: *soewereiniteit* het die Internet onder *sý* beheer gebring.

*** * ***

Ek dank God.

Bibliografie

Boeke

Abeyratne R *Aviation Security Law* (2010)

Albitz P en Liu C *DNS and BIND* (2001)

Ali K D *Maritime Security Cooperation in the Gulf of Guinea* (2015)

Alonso G *Web Services: Concepts, Architectures and Applications* (2004)

Amerasinghe C F *Principles of the Institutional Law of International Organizations* (2005)

American Bar Association *China Law Deskbook: A Legal Guide for Foreign-invested Enterprises* (2005)

Anderson J J *Wikipedia: The Company and Its Founders* (2011)

Andrews L *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy* (2012)

Archer C *International Organizations* (2014)

Arditti R en Brennan P *Science and Liberation* (1980)

Association for Information Management *Managing Information* (1995)

Bahga A en Madisetti V *Internet of Things: A Hands-On Approach* (2014)

Balleste R *Internet Governance: Origins, Current Issues and Future Possibilities* (2015)

Banerjee I *The Internet and Governance in Asia: A Critical Reader* (2007)

Bank D *Breaking Windows: How Bill Gates Fumbled the Future of Microsoft* (2001)

Barnes M *An Infinite Number of Monkeys: A Guide to Effective Business Communications* (2013)

Barry D K *Web Services, Service-Oriented Architectures, and Cloud Computing: The Savvy Manager's Guide* (2012)

Bayuk J, Healey J en Rohmeyer P *Cyber Security Policy Guidebook* (2012)

Benedek W, Bauer V en Kettemann M C (red) *Internet Governance and the Information Society: Global Perspectives and European Dimensions* (2008)

Benoît-Rohmer F en Klebes H *Council of Europe Law: Towards a Pan-European Legal Area* (2005)

Berners-Lee T *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web* (2000)

Bertin E, Crespi N en Magedanz T *Evolution of Telecommunication Services: The Convergence of Telecom and Internet: Technologies and Ecosystems* (2013)

Bidgoli H *The Internet Encyclopedia, Volume 3* (2003)

Bing B *3D and HD Broadband Video Networking (2010)*

Blane J V *Cybercrime and Cyberterrorism: Current Issues* (2003)

Boele-Woelki K *Internet — Which Court Decides? Which Law Applies?* (1998)

Boucadair M *Handbook of Research on Redesigning the Future of Internet Architectures* (2015)

Brousseau E, Marzouki M en Méadel C *Governance, Regulation and Powers on the Internet* (2012)

Brownlie I en Crawford J *Brownlie's Principles of Public International Law* (2012)

Brölmann C en Radi Y *Research Handbook on the Theory and Practice of International Lawmaking* (2016)

Buzacott A *Advanced Network Technology* (1993)

Byers M en Nolte G *United States Hegemony and the Foundations of International Law* (2003)

Bygrave L A en Bing J *Internet Governance: Infrastructure and Institutions* (2009)

Campbell J *1995: The Year the Future Began* (2015)

Casson L *Ships and Seamanship in the Ancient World* (2014)

Chair's Summary *8th Meeting of the Internet Governance Forum*

Chair's Summary *IGF 2014: Connecting Continents for Enhanced Multi-stakeholder Internet Governance* (2014)

Chair's Summary *Sixth Meeting of the Internet Governance Forum* (2011)

Chair's Summary *The 10th Internet Governance Forum* (2015)

Chairman's Summary *Fifth Meeting of the Internet Governance Forum (Final Version)* (2010)

Chairman's Summary *Fourth Meeting of the Internet Governance Forum* (2009)

Chairman's Summary *Second Meeting of the Internet Governance Forum* (2007)

Chairman's Summary *Third Meeting of the Internet Governance Forum* (2008)

Chatillon G *Internet International Law* (2005)

Choucri N, Mistree D en Haghseta F *et al Mapping Sustainability: Knowledge e-Networking and the Value Chain* (2007)

Ciment J *Social Issues in America: An Encyclopedia* (2015)

Claessen H J M en Oosten J G *Ideology and the Formation of Early States* (1996)

Coble H *Internet Domain Name Trademark Protection* (2000)

Collins English Dictionary (2003)

Collins R *Three Myths of Internet Governance — Making sense of Networks, Governance and Regulation* (2009)

Cooper M N (red) *Open Architecture v Communications Policy: Preserving Internet Freedom in the Broadband Era* (2004)

Copeland B J *Colossus: The Secrets of Bletchley Park's Codebreaking Computers* (2006)

Council of the European Union *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* (2016)

Cox M, Dunne T en Booth K (red) *Empires, Systems and States: Great Transformations in International Politics* (2001)

Craig P en De Búrca G *EU law: Text, Cases, and Materials* (2011)

Cranor L F *Communications Policy and Information Technology: Promises, Problems, Prospects* (2002)

Crawford J *Brownlie's Principles of Public International Law* (2012)

Creswell JW *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (2008)

De Busser E *Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters Between Judicial and Law Enforcement Authorities* (2009)

De Saint-Exupéry A *Vision and Challenges for Realising the Internet of Things* (2010)

Deacon J *Global Securitisation and CDOs* (2004)

Dean T *Network+ Guide to Networks* (2012)

Delener N *Strategic Planning and Multinational Trading Blocs* (1999)

DeNardis L *Protocol Politics: The Globalization of Internet Governance* (2009)

DiBona C en Ockman S *Open Sources: Voices from the Open Source Revolution* (1999)

Diederiks-Verschoor I H P en Butler M A *An Introduction to Air Law* (2006)

Dittrich D, Mirkovic J *et al Internet Denial of Service: Attack and Defense Mechanisms* (2004)

Dixon P *Surveillance in America: An Encyclopedia of History, Politics, and the Law* (2016)

Domanski R J *Who Governs the Internet?: A Political Architecture* (2015)

Dong J *Network Dictionary* (2007)

Drake W J *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance* (2005)

Dromgoole S *Underwater Cultural Heritage and International Law* (2013)

Dugard J *International Law – A South African Perspective* (2011)

Dulaney E *Linux All-in-One For Dummies* (2010)

Dunham B W *Introduction to Law* (2008)

Dwivedi Y K *Adoption, Usage, and Global Impact of Broadband Technologies: Diffusion, Practice and Policy* (2010)

Eagle L, Dahl S en Czarnecka B *et al Marketing Communications* (2014) 202

Ebrey P B *The Cambridge Illustrated History of China* (2010)

Editors of the American Heritage Dictionaries (red) *High Definition: An A to Z Guide to Personal Technology* (2006)

Ellis K en Kent M *Disability and New Media* (2011)

Essinger J *Jacquard's Web: How a Hand-Loom Led to the Birth of the Information Age* (2007)

Farer T J (red) *Beyond Sovereignty: Collectively Defending Democracy in the Americas* (1996)

Farivar C *The Internet of Elsewhere: The Emergent Effects of a Wired World* (2011)

Federal Communications Commission *FCC Adopts Strong, Sustainable Rules to Protect the Open Internet* (2015)

Federal Trade Commission *Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues: A Federal Trade Commission Staff Workshop Report* (2005)

Felt D E *Mechanical Arithmetic, or The History of the Counting Machine* (1916)

Firmino R J *ICTs for Mobile and Ubiquitous Urban Infrastructures: Surveillance, Locative Media and Global Networks* (2010)

Folsom R, Lake R B en Nanda V P *European Union Law After Maastricht: Practical Guide for Lawyers Outside the Common Market* (1996)

Foltea M *International Organizations in WTO Dispute Settlement: How Much Institutional Sensitivity?* (2012)

Forsyth C F *Private International Law: The Modern Roman Dutch Law Including the Jurisdiction of the High Courts* (2003)

Fowler M R en Bunck J M *Law, Power, and the Sovereign State: The Evolution and Application of the Concept of Sovereignty* (1995)

Franda M F *Governing the Internet: The Emergence of an International Regime* (2001)

Franklin M I *Digital Dilemmas: Power, Resistance, and the Internet* (2013)

Frye C *Privacy-enhanced Business: Adapting to the Online Environment* (2001)

Gadsby A (red) *Longman Dictionary of Contemporary English* (1995)

Gelbstein E en Kurbalija J *Internet Governance Issues, Actor and Divides* (2005)

Gentile C, Alsindi N en Raulefs R *et al Geolocation Techniques: Principles and Applications* (2012)

Gibson J L en Gouws A *Overcoming Intolerance in South Africa: Experiments in Democratic Persuasion* (2005)

Giemulla E M (red) *International and EU Aviation Law: Selected Issues* (2011)

Godwin M *Cyber Rights: Defending Free Speech in the Digital Age* (2003)

Golbeck J *Analyzing the Social Web* (2013)

Goldsmith J en Wu T *Who Controls the Internet? lllusions of a Borderless World* (2006)

Gosling W *Radio Spectrum Conservation* (2000)

Green P *Computer Network Architectures and Protocols* (2012)

Grewlich K *Governance in "Cyberspace": Access and Public Interest in Global Communications* (1999)

Guadamuz A *Networks, Complexity and Internet Regulation* (2011)

Guan S Y *China's Telecommunications Reforms: From Monopoly Towards Competition* (2003)

Hacid M, Ras Z W en Zighed A *et al Foundations of Intelligent Systems* (2003)

Hagen S *IPv6 Essentials* (2014)

Hagestad W *21st Century Chinese Cyberwarfare* (2012)

Hajiyev Y *Seventh Meeting of the Internet Governance Forum* (2012)

Handl G, Zekoll J en Zumbansen P *Beyond Territoriality: Transnational Legal Authority in an Age of Globalization* (2012)

Harris E E en Yunker J A (red) *Toward Genuine Global Governance: Critical Reactions to "Our Global Neighborhood"* (1999)

Heckmann O M *The Competitive Internet Service Provider: Network Architecture, Interconnection, Traffic Engineering and Network Design* (2007)

Henderson H *Encyclopedia of Computer Science and Technology* (2009)

Hess F M en Horn M B *Private Enterprise and Public Education* (2013)

Hey A J G en Pápay G *The Computing Universe: A Journey through a Revolution* (2014)

Hill R *The New International Telecommunication Regulations and the Internet: A Commentary and Legislative History* (2014)

Hiraoka L S *Underwriting the Internet: How Technical Advances, Financial Engineering, and Entrepreneurial Genius Are Building the Information Highway* (2005)

Hofmann M *Content Networking: Architecture, Protocols, and Practice* (2005)

Hogan A *Reasoning Techniques for the Web of Data* (2014)

Holt T J en Schell B H *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (2010)

Honick R *Software Piracy Exposed* (2005)

Hornle J en Zammit B *Cross-border Online Gambling Law and Policy* (2010)

Hua J *Toward A More Balanced Approach: Rethinking and Readjusting Copyright Systems in the Digital Network Era* (2014)

Human Rights Watch *Race to the Bottom: Corporate Complicity in Chinese Internet Censorship* (2006)

Humphreys C J *The Mystery of the Last Supper: Reconstructing the Final Days of Jesus* (2011)

Hyman A *Charles Babbage: Pioneer of the Computer* (1985)

Hörnle J *Cross-border Internet Dispute Resolution* (2009)

IBP.Inc *Macao Information Strategy, Internet and E-Commerce Development Handbook - Strategic Information, Programs, Regulations* (2015)

Ibrahim Y *Global Governance and the Local Internet* (2007)

Ifrah G *The Universal History of Computing: From the Abacus to the Quantum Computer* (2001)

IGF Secretariat *The Internet Governance Forum on the Desirability of the Continuation of the Forum* (2009)

Information Gatekeepers Inc *Repeatered Submarine Fiber Optics Systems* (1998)

Information Gatekeepers Inc *Telecom Standards Monthly Newsletter October 2010* (2010)

International Business Publications *China Telecom Industry Business Opportunities Handbook Volume 3 Strategic Information, Developments, Regulations* (2007)

International Business Publications USA *China E-commerce Business and Investment Opportunities Handbook* (2007)

International Telecommunications Union *Final Acts of the World Conference on International Telecommunications* (2012)

International Telecommunications Union *Collection of the Basic Texts of the International Telecommunication Union Adopted by the Plenipotentiary Conference: Edition 2011* (2011)

International Telecommunications Union *Final Acts of the Plenipotentiary Conference (Minneapolis, 1998)* (1998)

Internet Corporation for Assigned Names and Numbers *IANA Stewardship Transition Proposal and Enhancing ICANN Accountability Recommendations* (2016)

Irvine C en Armstrong H *Security Education and Critical Infrastructures* (2003)

Ivory J D *Virtual Lives: A Reference Handbook* (2012)

Jackson J *Introducing Language and Intercultural Communication* (2014)

Jin H, Yang L T en Tsai J P *Ubiquitous Intelligence and Computing* (2006)

Johnson D M *The Historical Foundations of World Order: The Tower and the Arena* (2008)

Johnson D R en Post D G "And How Shall the Net Be Governed?" in Kahin B (red) *Coordinating the Internet* (1997)

Jones K B *Search Engine Optimization: Your Visual Blueprint for Effective Internet Marketing* (2013)

Jones S (red) *Encyclopedia of New Media: An Essential Reference to Communication and Technology* (2002)

Karaganis J *Media Piracy in Emerging Economies* (2011)

Katz L S *Publishing and the Law: Current Legal Issues* (2013)

Kelly S en Cook S (red) *Freedom on the Net 2011* (2011)

Kelly S en Truong M (red) *Freedom on the Net 2013* (2013)

Kelly S en Truong M (red) *Freedom on the Net 2014* (2014)

Kelly S, Cook S en Truong M (red) *Freedom on the Net* 2015 (2015)

Kelly S, Cook S en Truong M (red) *Freedom on the Net 2012* (2012)

Kleinman D L en Moore K *Routledge Handbook of Science, Technology, and Society* (2014)

Kleinwächter W (red) *The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment* (2007)

Kleyn D en Viljoen F *Beginnersgids vir Regstudente* (2010)

Knake R K *Internet Governance in an Age of Cyber Insecurity* (2010)

Kozierok C M *The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference* (2005)

Krasner S D *Sovereignty: Organized Hypocrisy* (1999)

Kruger L G *Internet Governance and the Domain Name System: Issues for Congress* (2014)

Kruger L *Internet Governance and the Domain Name System: Issues for Congress* (2014)

Kurbalija J *An Introduction to Internet Governance* (2012)

Lauterpacht H *International Law: Volume 1, The General Works: Being the Collected Papers of Hersch Lauterpacht* (1970)

Lederer M en Muller P *Criticizing Global Governance* (2005)

Leonard B *Basic Facts about the United Nations* (1999)

Lessig L *Code 2.0* (2006)

Lessig L *The Future of Ideas: The Fate of the Commons in a Connected World* (2002)

Li X *Internet Newspapers: The Making of a Mainstream Medium* (2006)

Lindsay D *International Domain Name Law:* ICANN *and the UDRP* (2007)

Lindsay J R, Cheung T M en Reveron D S *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (2015)

Lloyd I J *Information Technology Law* (2000)

Lodder H W K en Kaspersen A R *e-Directives: Guide to European Union Law on e-Commerce: Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection* (2002)

Loshin P *IPv6 Clearly Explained* (1999)

Lueg C en Fisher D *From Usenet to CoWebs: Interacting With Social Information Spaces* (2003)

MacKenzie D *ICAO: A History of the International Civil Aviation Organization* (2010)

Maclean D F (red) *Internet Governance: A Grand Collaboration* (2004)

Malcolm J *Multi-Stakeholder Governance and the Internet Governance Forum* (2008)

Marckini F *Search Engine Positioning* (2001)

Marsden C T (red) *Regulating the Global Information Society* (2005)

Marsden C T *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (2011)

Marsden C T *Net Neutrality: Towards a Co-regulatory Solution* (2010)

Martens K *NGOs and the United Nations: Institutionalization, Professionalization and Adaptation* (2005)

Martinez J P *Net Neutrality: Contributions to the Debate* (2011)

Mason R *Globalising Education: Trends and Applications* (2005)

Massachusetts Institute of Technology Computer Science and AI Lab *New Arch: Future Generation Internet Architecture* (2004)

Mathiason J *Internet Governance: The New Frontier of Global Institutions* (2009)

McPhail T L *Global Communication: Theories, Stakeholders, and Trends* (2011)

Medhi D *Network Routing: Algorithms, Protocols, and Architectures* (2010)

Mehdi K P *Dictionary of Information Science and Technology, Volume 1* (2006)

Michals D B *International Privileges and Immunities: A Case for a Universal Statute* (2012)

Micheuz P *20 Years of Computers and Informatics in Austria's Secondary Academic Schools* (2005)

Miller P *TCP/IP: The Ultimate Protocol Guide* (2009)

Mohapatra S *E-Commerce Strategy: Text and Cases* (2012)

Moore J A en Pubantz J *The New United Nations: International Organization in the Twenty-First Century* (2015)

Mouton J en Marais HC *Basic Concepts: The Methodology of the Social Sciences (HSRC Studies in Research Methodology)* (1990)

Mueller M L *Ruling the Root: Internet Governance and the Taming of Cyberspace* (2002)

Mueller M *Networks and States: The Global Politics of Internet Governance* (2010)

Murray A D *The Regulation of Cyberspace* (2006)

Murray A D *The Regulation of Cyberspace: Control in the Online Environment* (2007)

Mwenda K K *Legal Aspects of Financial Services Regulation and the Concept of a Unified Regulator* (2006)

National Research Council *Signposts in Cyberspace: The Domain Name System and Internet Navigation* (2005)

Newman M *Networks: An Introduction* (2010)

Nguyen N *Essential 120000 English-Afrikaans Words Dictionary* (2014)

Nolon J R *Well Grounded: Using Local Land Use Authority to Achieve Smart Growth* (2001)

Nsour M F *Rethinking the World Trade Order: Towards a Better Legal Understanding of the Role of Regionalism in the Multilateral Trade Regime* (2010)

O'Farrell M J *et al Mobile Internet for Dummies* (2008)

Odendal F F en Gouws R H *Verklarende handwoordeboek van die Afrikaanse Taal* (2005)

Oestreich J E *International Organizations as Self-directed Actors: A Framework for Analysis* (2012)

Orakhelashvili A *Research Handbook on the Theory and History of International Law* (2011)

Øren J S T *International Jurisdiction and Consumer Contracts* (2004)

Oxford Economics *Economic Consequences of Movie Piracy: Japan* (2011)

Padovani C en Pavan E *Diversity Reconsidered in a Global Multi-stakeholder Environment: Insights From the Online World"* in Kleinwächter *The Power of Ideas* (2007)

Ploug T *Ethics in Cyberspace: How Cyberspace May Influence Interpersonal Interaction* (2009)

Pohlmann N, Reimer H en Schneidemeld W *ISSE/SECURE 2007 Securing Electronic Business Processes: Highlights of the Information Security* (2007)

Pohlmann N, Reimer H en Schneidemeld W *ISSE/SECURE 2007 Securing Electronic Business Processes: Highlights of the Information Security* (2007)

Poole W *The Internet: Biographies* (2005)

Porter J *Designing for the Social Web* (2008)

Post D G *In Search of Jefferson's Moose: Notes on the State of Cyberspace* (2009)

Potter P *China's Legal System* (2013)

Privacy and Civil Liberties Oversight Board *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* (2014)

Qin Z *Introduction to E-commerce* (2010)

Quelch J en Jocz K E *Google in China* (2010)

Rabban D M in Simmons R C (red) *The United States Constitution: The First 200 Years* (1989)

Radu R, Chenou J en Weber R (red) *The Evolution of Global Internet Governance: Principles and Policies in the Making* (2014)

Rawlings R, Leyland P en Young A *Sovereignty and the Law: Domestic, European and International Perspectives* (2013)

Reddie J *Inquiries in International Law, Public and Private* (1851)

Reed C *Internet Law: Text and Materials* (2004)

Reinold T *Sovereignty and the Responsibility to Protect: The Power of Norms and the Norms of the Powerful* (2013)

Reporters Without Borders *Internet Enemies Report 2012* (2012)

Riggs C *Network Perimeter Security: Building Defense In-Depth* (2003)

Ritchie C *Operating Systems Incorporating UNIX and Windows* (2003)

Roos A "Freedom of Expression" in Van der Merwe D, Roos A *et al Information and Communications Technology Law* (2008)

Royer A *The Council of Europe* (2010)

Rust S, Monani S en Cubitt S *Ecomedia: Key Issues* (2015)

Rustad M *Global Internet Law* (2013)

Rutenbeck J *Tech Terms: What Every Telecommunications and Digital Media Professional Should Know* (2012)

Sadiku M N O en Ilyas M *Simulation of Local Area Networks* (1994)

Savin A en Trzaskowski J *Research Handbook on EU Internet Law* (2014)

Saxena A N *Invention of Integrated Circuits: Untold Important Facts* (2009)

Schell B H *The Internet and Society: A Reference Handbook* (2007)

Schermers H G en Blokker N M *International Institutional Law: Unity Within Diversity* (2011)

Schiavone G *International Organizations* (2015)

Schultz D A *Encyclopedia of the United States Constitution* (2010)

Schwabach A *Intellectual Property: A Reference Handbook* (2007)

Sears A en Jacko J *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies and Emerging Applications* (2002)

Segal A *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (2016)

Shelly G B en Frydenberg M *Web 2.0: Concepts and Applications* (2010)

Shinder D L *Scene of the Cybercrime: Computer Forensics Handbook* (2002)

Simon L D *Netpolicy.com: Public Agenda for a Digital World* (2000)

Simpson G (red) *The Nature of International Law* (2001)

Skeet I *Opec: Twenty-Five Years of Prices and Politics* (1991)

Sloane S *Digital Fictions: Storytelling in a Material World* (2000)

Slomanson W *Fundamental Perspectives on International Law* (2011)

Smeby L C, Chapple M en Seidl D *Cyberwarfare* (2014)

Smith D E *History of Mathematics* (1958)

Smith G J H *Internet Law and Regulation* (2007)

So S en Westland J *Red Wired: China's Internet Revolution* (2010)

Sofroniou A *Surfing the Internet, Then, Now, Later* (2014)

Spang-Hanssen H *Cyberspace Jurisdiction in the US* (2001)

Stair R *Principles of Information Systems* (2013)

Sternberg P *Broadband Internet's Value for Rural America* (2010)

Stevens G *Privacy Protections for Personal Information Online* (2011)

Stevenson A *Oxford Dictionary of English* (2010)

Steward J M, Chapple M en Gibson *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide* (2015)

Svantesson D J B *Private International Law and the Internet* (2012)

Swedin E G *Science in the Contemporary World: An Encyclopedia* (2006)

Teague J C *DHTML and CSS for the World Wide Web* (2001)

Teehan K *Wikis: The Educator's Power Tool* (2010)

Tella A *Library and Information Science in Developing Countries: Contemporary Issues* (2011)

Tetlow P *Understanding Information and Computation: From Einstein to Web Science* (2016)

Thierer A D en Crews C W *Who Rules the Net?: Internet Governance and Jurisdiction* (2003)

Thirlway H *The Sources of International Law* (2014)

Toexcell Inc *Hypertext Transfer Protocol HTTP 1.0 Specifications* (1999)

Topley K *Java Web Services in a Nutshell* (2003)

Traynor P, McDaniel P en La Porta T *Security for Telecommunications Networks* (2008)

Tsagourias N en Buchan R *Research Handbook on International Law and Cyberspace* (2015)

Uckelmann D, Harrison M en Michahelles F *Architecting the Internet of Things* (2011)

United Nations Publications *International Geneva Yearbook: Organization and Activities of International Institutions in Geneva, Volume 16; Volumes 2002-2003* (2002)

United Nations *Implementing WSIS Outcomes: A Ten-year Review* (2015)

US Department of Commerce *Addressing the Challenges of International Bribery and Fair Competition 2001* (2001)

Van der Merwe D P en Roos A *et al Information and Communications Technology Law* (2016)

Van Dijk J *The Culture of Connectivity: A Critical History of Social Media* (2013)

Van Hoose D *e-Commerce Economics* (2011)

Viljoen F *International Human Rights Law in Africa* (2012)

Wacks R *Privacy: A Very Short Introduction* (2015)

Waldock H (red) *Brierly's The Law of Nations* (1963)

Walker S *In Defense of American Liberties: A History of the ACLU* (1999)

Wang F F *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China* (2010)

Wardrip-Fruin N en Montfort N (red) *The New Media Reader* (2003)

Watney M "The Use of Electronic Surveillance in Conducting Criminal Investigations on the Internet" in Jahankhani H (red) *Handbook of Electronic Security and Digital Forensics* (2010)

Weber R H en Burri M *Classification of Services in the Digital Economy* (2012)

Weber R H *Shaping Internet Governance: Regulatory Challenges* (2010)

Weeramantry C G *Universalising International Law* (2004)

Wheaton H *Elements of International Law: With a Sketch of the History of the Science* (1836)

Winter J en Ono R *The Future Internet: Alternative Visions* (2016)

Wolf M J P (red) *Encyclopedia of Video Games: The Culture, Technology, and Art of Gaming* (2012)

Wolfrum R en Röben V *Legitimacy in International Law* (2008)

Wrońska I *Fundamental Rights Protection in the Council of Europe: The Role of the European Court of Human Rights* (2011)

Yang G *The Power of the Internet in China: Citizen Activism Online* (2013)

Zelkowitz M V *Distributed Information Resources* (1999)

Zhao J *Corporate Social Responsibility in Contemporary China* (2014)

Ziccardi G *Resistance, Liberation Technology and Human Rights in the Digital Age* (2012)

Zimmermann O, Tomlinson M en Peuser S *Perspectives on Web Services: Applying SOAP, WSDL and UDDI to Real-World Projects* (2012)

Zittrain J *The Future of the Internet — And How to Stop It* (2008)

Artikels

Abbot K W en Snidal D "Hard and Soft Law in International Governance" 2000 *International Organization* 421

Anderson L "Demystifying the Arab Spring" 2011 *Foreign Affairs* 2

Ardia D S "Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity under Section 230 of the Communications Decency Act" 2010 *Loyola of Los Angeles Law Review* 373

August R "International Cyber-Jurisdiction: A Comparative Analysis" 2002 *American Business Law Journal* 531

Aupperle E M "Merit—Who, What, and Why" 1998 *Library Hi Tech* 15

Badgley R A "Improving ICANN in Ten Easy Steps: Ten Suggestions for ICANN to Improve its Anti-Cybersquatting Arbitration System." 2001 *Journal of Law, Technology and Policy at the University of Illinois* 109

Baistrocchi P A "Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce" 2002 *Santa Clara High Technology Law Journal* 111

Balkin J M "Old School/New School Speech Regulation" 2014 *Harvard Law Review* 2296

Balkin J M "The Future of Free Expression in a Digital Age" 2009 *Pepperdine Law Review* 427

Band J en Schruers M "Safe Harbors Against the Liability Hurricane: The Communications Decency Act and the Digital Millennium Copyright Act" 2002 *Cardozo Arts and Entertainment Law Journal* 295

Banks K "Summitry and Strategies" 2005 *Index on Censorship* 85

Bendrath R en Mueller M "The End of the Net as We Know It? Deep Packet Inspection and Internet Governance" 2011 *New Media and Society* 1142

Benkler Y "From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access" 1999 *Federal Communication Law Journal* 561

Benmamoun M, Kalliny M en Cropf R A "The Arab Spring, MNEs, and Virtual Public Spheres" 2012 *Multinational Business Review* 26

Bergen P, Sterman *et al* "Do NSA's Bulk Surveillance Programs Stop Terrorists?" 2014 *New America Foundation* 1

Berners-Lee T, Hendler J en Lassila O "The Semantic Web" 2001 *Scientific American* 28

Bingham J "Multicarrier Modulation for Data Transmission: An Idea Whose Time Has Come" 1990 *IEEE Communications Magazine* 5

Bitso C, Fourie I en Bothma T "Trends in Transition From Classical Censorship to Internet Censorship: Selected Country Overviews" 2012 *FAIFE Spotlight* 182

Black P, Delaney H en Fitzgerald B "Legal Issues for Wikis: The Challenge of User-generated and Peer-produced Knowledge, Content and Culture" 2007 *Murdoch University Electronic Journal of Law* 246

Bretan J "Harboring Doubts About the Efficacy of § 512 Immunity Under the DMCA" 2003 *Berkeley Technology Law Journal* 43

Carr N "Is *Google* Making Us Stupid?" 2008 *Yearbook of the National Society for the Study of Education* 89

Chang L "The Red Flag Test for Apparent Knowledge Under the DMCA § 512(c) Safe Harbor" 2010 *Cardozo Arts and Entertainment Law Journal* 195

Chinkin C M "The Challenge of Soft Law: Development and Change in International Law" 1989 *International and Comparative Law Quarterly* 850

Chueng A S Y en Zhao Y "An Overview of Internet Regulation in China" 2013 *University of Hong Kong Faculty of Law Research Paper* 1

Chueng A S Y "The Business of Governance: China's Legislation on Content Regulation in Cyberspace" 2006 *International Law and Politics* 1

Clapper J R "DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" 2013 *Office of the Director of National Intelligence* 1

Codding G "The International Telecommunications Union: 130 Years of Telecommunications Regulation" 1994 *Denver Journal of International Law and Policy* 501

Colonna L "*PRISM* and the European Union's Data Protection Directive" 2013 *Journal of Information Technology and Privacy Law* 227

Condry I "Cultures of Music Piracy: An Ethnographic Comparison of the US and Japan" 2004 *International Journal of Cultural Studies* 343

Conradi M, Baker en McKenzie "ISP Liability — UK: Liability of an ISP for Allowing Access to File Sharing Networks" 2003 *Computer Law and Security Review* 289

Cui D en Wu F "Moral Goodness and Social Orderliness: An Analysis of the Official Media Discourse about Internet Governance in China" 2015 *Telecommunications Policy* 265

Czas J "Note: Business, Law and Project *PRISM*" 2014 *The Georgetown Journal of Law and Public Policy* 897

De Beer J en Clemmer C D "Global Trends in Online Copyright Enforcement: A Non-neutral Role for Network Intermediaries?" 2009 *Jurimetrics* 375

Deeks A "An International Legal Framework for Surveillance" 2015 *Virginia Journal of International Law* 291

Defense Advanced Research Projects Agency "Bridging the Gap: Powered by Ideas" 2005 *Defence Advanced Research Projects Agency* 1

Determann L "Case Update: German *Compuserve* Director Acquitted on Appeal" 1999 *Hastings International and Comparative Law Review* 109

Dibbell J "A Rape in Cyberspace or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database Into a Society" 1994 *Annual Survey of American Law* 471

Dickerson N P "What Makes the Internet so Special? And Why, Where, How, and by Whom Should its Content be Regulated? 2009 *Houston Law Review* 61

Dixon P *Surveillance in America: An Encyclopedia of History, Politics, and the Law* (2016) 171

Doney L "NSA Surveillance, Smith and Section 215: Practical Limitations to the Third-Party Doctrine in the Digital Age" 2015 *National Security Law Journal* 462

Dong F "Controlling the Internet in China: The Real Story" 2012 *Convergence* 403

Donohue L K "Bulk Metadata Collection: Statutory and Constitutional Considerations" 2014 *Harvard Journal of Law and Public Policy* 757

Donohue LK "The Dawn of Social Intelligence (SOCINT)" 2015 *Drake Law Review* 1061

Ehrlich P "Communications Decency Act § 230" 2002 *Berkeley Technology Law Journal* 401

Eriksson J en Giacomello G "Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State" 2009 *International Studies Review* 205

Farrel J en Weiser P J "Modularity, Vertical Integration, and Open Access Policies: Towards A Convergence of Antitrust and Regulation in the Internet Age" 2003 *Harvard Journal of Law & Technology* 86

Farrell H en Finnemore M "The End of Hypocrisy: American Foreign Policy in the Age of Leaks" 2013 *Foreign Aff* airs 22

Fidler D P "Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations" 2013 *Insights* 1

Flaming H "The Rules of Cyberspace: Informal Law in a New Jurisdiction" 1997 *Illinois Bar Journal* 174

Forsyth B "Banning Bulk: Passage of the *USA FREEDOM* Act and Ending Bulk Collection" 2015 *Washington and Lee Law Review* 1307

Frieden R "Internet Packet Sniffing and Its Impact on the Network Neutrality Debate and the Balance of Power Between Intellectual Property Creators and Consumers" 2008 *Fordham Intellectual Property, Media and Entertainment Law Journal* 633

Garon J M "Tidying Up the Internet: Takedown of Unauthorized Content Under Copyright, Trademark, and Defamation Law" 2013 *Capital University Law Review* 513

Geist M A "Is There a 'There' There — Toward Greater Certainty for Internet Jurisdiction" 2001 *Berkeley Technology Law Journal* 1345

Gigante A "Blackhole in Cyberspace: The Legal Void in the Internet" 1997 *John Marshall Journal of Computer and Information Law* 413

Goldsmith J L "Against Cyberanarchy" 1998 *University of Chicago Law Review* 1199

Goldsmith T J "What's Wrong with this Picture? When the Lanham Act Clashes with Artistic Expression" 1997 *Fordham Intellectual Property, Media and Entertainment Law Journal* 821

Gong J *et al* "Defining and Addressing Virtual Property in International Treaties" 2011 *Boston University Journal of Science and Technology Law* 101

Grabosky PN en Smith R G "Telecommunications and Crime: Regulatory Dilemmas" 1997 *Law and Policy* 317

Greenberg M H "A Return to Lilliput: The *Licra v Yahoo* Case and the Regulation of Online Content in the World Market" 2003 *Berkeley Technology Law Journal* 1191

Greenway C "Outcome of the 2013 World Telecommunications and Information and Communication Technology Forum" 2013 *Australian Journal of Telecommunications and the Digital Economy* 14.1

Grimmelmann J "Sealand, *HavenCo*, and the Rule of Law" 2012 *University of Illinois Law Review* 405

Hamrick K B "The History of the Hand-Held Electronic Calculator" 1996 *The American Mathematical Monthly* 633

Hill J F "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for US Policymakers and Industry Leaders" 2014 *The Lawfare Institute, Lawfare Research Paper Series* 1

Hill R "The Internet, its Governance, and the Multi-stakeholder Model" 2014 *Info* 16

Hong J "Discourse Behind the Forbidden Realm: Internet Surveillance and its Implications on China's Blogosphere" 2009 *Telematics and Informatics* 67

Howard P N en Hussain M M "The Role of Digital Media" 2011 *Journal of Democracy* 35

Hua J J "Establishing Certainty of Internet Service Provider Liability and Safe Harbor Regulation" 2014 *National Taiwan University Law Review* 1

Hunter D "ICANN and the Concept of Democratic Deficit" 2002 *Loyola of Los Angeles Law Review* 1149

Hunter M "Interview with Jerry Yang from Liberation (16-6-00) Article by Launet Edouard" in "Business e-Ethics: *Yahoo* on Trial (B)" 2001 *INSEAD* 4956

Ibrahim Y "Global Governance and the Local Internet" 2007 *Linguistic and Cultural Online Communication Issues in the Global Age* 177

Inkster N "China in Cyberspace" 2010 *Survival* 55

International Business Publications *China Telecom Industry Business Opportunities Handbook Volume 3 Strategic Information, Developments, Regulations* (2007) 146

Jakobsen S S "Mobile Commerce and ISP Liability in the EU" 2010 19 *International Journal of Law and Information Technology* 29

Jean-Kenix L "Blogs as Alternative" 2009 *Journal of Computer-Mediated Communication* 790

Jensen E T "Cyber Sovereignty: The Way Ahead" 2015 *Texas International Law Journal* 273

Johnson D R en Post D "Law and Borders — The Rise of Law in Cyberspace" 1996 *Stanford Law Review* 1367

Karjala D S, Brown J E en O'Connor S D "International Convergence on the Need for Third Parties to Become Internet Copyright Police (But Why?)" 2013 *Richmond Journal of Global Law and Business* 189

Karjala D S "Liability of Internet Service Providers Under United States Law" 2006 *Jurisprudencia* 9

King I "Internationalising Internet Governance: Does ICANN Have a Role to Play?" 2004 *Information and Communications Technology Law* 243

Kissel T K "Licence to Blog: Internet Regulation in the People's Republic of China" 2007 *Indiana International and Comparative Law Review* 229

Kleinrock L "An Early History of the Internet" 2010 *IEEE Communications Magazine* 26

Kohl U "The Rise and Rise of Online Intermediaries in the Governance of the Internet and Beyond — Connectivity Intermediaries" 2012 *International Review of Law, Computers and Technology* 185

Koppell J G S "Pathologies of Accountability: ICANN and the Challenge of 'Multiple Accountabilities Disorder'" 2005 *Public Administration Review* 94

Kryczka K "Ready to Join the EU Information Society — Implementation of E-Commerce Directive 2000/31/EC in the EU Acceding Countries — The Example of Poland" 2004 *International Journal of Law and Information Technology* 55

Kumar A "Internet Intermediary (ISP) Liability for Contributory Copyright Infringement in USA and India: Lack of Uniformity as a Trade Barrier" 2014 *Journal of Intellectual Property Rights* 272

Land M "Toward an International Law of the Internet" 2013 *Harvard International Law Journal* 423

Landau S "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations" 2013 *IEEE Security and Privacy* 54

Lee J A en Liu C Y "Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China" 2012 *Minnesota Journal of Law, Science, and Technology* 125

Leistner M "Structural Aspects of Secondary (Provider) Liability in Europe" 2014 *Journal of Intellectual Property Law and Practice* 75

Leitner J "A Legal and Cultural Comparison of File-sharing Disputes in Japan and the Republic of Korea and Implications for Future Cyber-regulation" 2008 *Columbia Journal of Asian Law* 3

Lessig L "The Internet Under Siege" 2001 *Foreign Policy* 56

Lessig L "The Law of the Horse: What Cyberlaw Might Teach" 1999 *Harvard Law Review* 501

Lessig L "The New Chicago School" 1998 *Journal of Legal Studies* 661

Levinson D J "Collective Sanctions" 2003 *Stanford Law Review* 345

Liang B em Lu H "Internet Development, Censorship, and Cyber Crimes in China" 2010 *Journal of Contemporary Criminal Justice* 103

Lidi W "The Spread of English in China and its Implications" 2011 *Australian Review of Applied Linguistics* 32.1

Litt R S "US Intelligence Community Surveillance One Year After President Obama's Address" 2015 *National Security Law Journal* 210

Lodder A R en Van der Meulen N S "Discussion of Dutch Pirate Bay Case Law and Introducing Principles on Directness, Effectiveness, Costs, Relevance, and Time" 2012 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 130

MacKinnon R "China's Networked Authoritarianism" 2011 *Journal of Democracy* 32

Margulies P "Defining Foreign Affairs in Section 702 of the FISA Amendments Act: The Virtues and Deficits of Post-Snowden Dialogue on US Surveillance Policy" 2015 *Washington and Lee Law Review* 1283

Marx F en O'Brien N "To Regulate or to Overregulate? Internet Service Provider Liability: The Industry Representative Body in Terms of the ECT Act and Regulations" 2011 *Obiter* 537

Marx F "Hate Speech on Social Network Sites: Perpetrator and Service Providers' Liability" 2011 *Obiter* 322

McGhee J E "Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy" 2013 *Journal of Law & Cyber Warfare* 64

Mehra S en Trimble M "Secondary Liability, ISP Immunity, and Incumbent Entrenchment" 2014 *American Journal of Comparative Law* 685

Mehra S "Keep America Exceptional! Against Adopting Japanese and European-Style Criminalization of Contributory Copyright Infringement" 2011 *Vanderbilt Journal of Entertainment and Technology Law* 811

Menthe D C "Jurisdiction in Cyberspace: A Theory of International Spaces" 1998 *Michigan Telecommunications Technology Law Review* 69

Milanovic M "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" 2015 *Harvard International Law Journal* 81

Mills A "The Private History of International Law" 2006 *International and Comparative Law Quarterly* 1

Moorefield T "Communications Decency Act of 1996" 1997 *Boston University Journal of Science and Technology Law* 281

Morrow G "Hypertext May Let PC Users Create Unique Structures for Data Organization" 1988 *Infoworld* 42

Mueller M L en Wagner B "Finding a Formula in Brazil: Representation and Legitimacy in Internet Governance" 2014 *Internet Policy Observatory* 8

Mueller M L en Asghari H "Deep Packet Inspection and Bandwidth Management: Battles Over BitTorrent in Canada and the United States" 2012 *Telecommunications Policy* 462

Myer K S "Wikimmunity: Fitting the Communications Decency Act to Wikipedia" 2006 *Harvard Journal of Law and Technology* 163

Negroponte, J D Palmisano S J en Segal A "Defending an Open, Global, Secure, and Resilient Internet" 2013 *Independent Task Force Report No 70* 13

Nel S S "Problematic Issues Surrounding Transborder Cybersmear" 2010 *South African Mercantile Law Journal* 360

Newman J "Keeping the Internet Neutral: Net Neutrality and it's Role in Protecting Political Expression on the Internet" 2008 *Hastings Communications and Entertainment Journal* 153

Noeth K "The Never-Ending Limits of § 230: Extending ISP Immunity to the Sexual Exploitation of Children" 2009 *Federal Communications Law Journal* 765

Ofek E en Richardson M "Dotcom Mania: The Rise and Fall of Internet Stock Prices" 2003 *The Journal of Finance* 1113

Ombres D "NSA Domestic Surveillance From the PATRIOT Act to the FREEDOM Act: The Underlying History, Constitutional Basis, and the Efforts at Reform" 2015 *Seton Hall Legislative Journal* 27

Overmeyer D L "From 'Feudal Superstition' to 'Popular Beliefs': New Directions in Mainland Chinese Studies of Chinese Popular Religion" 2001 *Cahiers d'Extrême-Asie* 103

Post D G "Against 'Against Cyberanarchy'" 2002 *Berkeley Technology Law Journal* 1365

Powell C D "The *eBay* Trademark Exception: Restructuring the Trademark Safe Harbor for Online Marketplaces" 2011 *Santa Clara High Technology Law Journal* 1

Qiu J L "Virtual Censorship in China: Keeping the Gate Between the Cyberspaces" 2000 *International Journal of Communications Law and Policy* 1

Rascoff S J "Presidential Intelligence" 2016 *Harvard Law Review* 633

Reese R A "The Relationship Between the ISP Safe Harbors and the Ordinary Rules of Copyright Liability" 2009 *Columbia Journal of Law and the Arts* 427

Rens A "*Tsichlas and Another v Touch Line Media (Pty) Ltd*" 2005 *South African Law Journal* 740

Robertson A "Connecting in Crisis: 'Old' and 'New' Media and the Arab Spring" 2013 *The International Journal of Press/Politics* 1

Roos A en Slabbert M "Defamation on *Facebook*: *Isparta v Richter* 2013 6 SA 529" 2014 *Potchefstroom Electronic Reserves* 2844

Ruger T W "Chief Justice Rehnquist's Appointments to the FISA Court: An Empirical Perspective" 2007 *Northwestern University Law Review* 239

Rustad M L en Koenig TH "Rebooting Cybertort Law" 2005 *Washington Law Review* 335

Saltzer J H, Reed D P en Clark D "End-to-End Arguments in System Design" 1984 *ACM Transactions on Computer Systems (TOCS)* 277

Sandoval C "Disclosure, Deception, and Deep-Packet Inspection: The Role of the Federal Trade Commission Act's Deceptive Conduct Prohibitions in the Net Neutrality Debate" 2009 *Fordham Law Rev*iew 641

Schultz T "Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface" 2008 *The European Journal of International Law* 799

Scott M D "Would a 'Right of Reply' Fix Section 230 of the Communications Decency Act?" 2012 *International Journal of Law and Information Technology* 73

Segura-Serrano A "Internet Regulation and the Role of International Law" 2006 *Max Planck Yearbook of United Nations Law* 191

Seltzer W "Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment" 2010 *Harvard Journal of Law and Technology* 171

Sideri K "Questioning the Neutrality of Procedural Law: Internet Regulation in Europe Through the Lenses of Bourdieu's Notion of Symbolic Capital" 2004 *European Law Journal* 61

Sivan Y (red) "Escaping the World: A Chinese Perspective on Virtual Worlds" 2012 *Journal of Virtual Worlds Research* 1

Sohmen P "Taming the Dragon: China's Efforts to Regulate the Internet" 2001 *Stanford Journal of East Asian Affairs* 17

Stevenson C "Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World" 2007 *Boston College International and Comparative Law Review* 531

Svantesson J B "Borders on, or Border Around — the Future of the Internet" 2006 *Albany Law Journal of Science and Technology* 343

Sylvain O "Internet Governance and Democratic Legitimacy" 2010 *Federal Communication Law Journal* 205

Tsui L "The Panopticon as the Antithesis of a Space of Freedom: Control and Regulation of the Internet in China" 2003 *China Information* 65

Van Eeten M J G en Mueller M "Where is the Governance in Internet Governance?" 2012 *New Media and Society* 720

Varshney U *et al* "Voice Over IP" 2002 *Communications of the ACM* 89

Wall D S "The Internet as a Conduit for Criminal Activity" 2005 *Information Technology and the Criminal Justice System* 78

Wallace M J en Singer D "Intergovernmental Organization in the Global System, 1815–1964" 1970 *International Organization* 239

Wang S S en Hong J "Discourse Behind the Forbidden Realm: Internet Surveillance and its Implications on China's Blogosphere" 2009 *Telematics and Informatics* 67

Watney M "Regulation of Internet Pornography in South Africa (1)" 2006 *Tydskrif vir die Hedendaagse Romeins Hollandse Reg* 227

Watney M "State Surveillance of the Internet: Human Rights Infringement or E-security Mechanism?" 2007 *International Journal of Electronic Security and Digital Forensics* 42

Watney M "The Evolution of Legal Regulation of the Internet to Address Terrorism and Other Crimes" 2007 *Tydskrif vir die Suid-Afrikaanse Reg* 494

Weber R H "Future Design of Cyberspace Law" 2012 *Journal of Politics and Law* 3

Wei R en Su J "The Statistics of English in China" 2012 *English Today* 10

Welch K "The PATRIOT-act and Crisis Legislation: The Unintended Consequences of Disaster Lawmaking" 2015 *Capital University Law Review* 481

Werbach K "Breaking the Ice: Rethinking Telecommunications Law for the Digital Age" 2005 *Journal on Telecommunications and High Technology Law* 59

Werbach K "The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart" 2008 *University of California Davis Law Review* 343

Williams J "Sites Go Straight to Video" 2000 *Editor and Publisher* 133

Wu T "Copyright's Communications Policy" 2004 *Michigan Law Review* 278

Wu T "Network Neutrality, Broadband Discrimination" 2003 *Journal on Telecommunications and High Technology Law* 141

Yang K C C "A Comparative Study of Internet Regulatory Policies in the Greater China Region: Emerging Regulatory Models and Issues in China, Hong-Kong SAR, and Taiwan" 2007 *Telematics and Informatics* 30

Yeo S "Book Review: Networks and States: The Global Politics of Internet Governance" (2011) *Journal of the American Society for Information Science and Technology* 1648

Yuen S "Becoming a Cyber Power: China's cybersecurity upgrade and its consequences" 2015 *China Perspectives* 53

Zekos G I "Demolishing State's Sole Power Over Sovereignty and Territory Via Electronic Technology and Cyberspace" *Journal Of Internet Law* 3

Zheng H "Regulating the Internet: China's Law and Practice" 2013 *Beijing Law Review* 37

Zhuo X, Wellman B en Yu J "Egypt: The First Internet Revolt?" 2011 *Peace Magazine* 6

Zook M "The Geographies of the Internet" 2006 *Annual Review of Information Science and Technology* 53

Wetgewing

Duitsland

Duitse Strafkode: Duitse Kode op die beskerming van Jeugdiges (Gesetz ueber die Verbreitung Jugendgefahrdender Schriften [GjS]) v 28.10.1998 (BGBI I S 3186)

Europese Unie

Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data

European Commission Joint Statement on the Final Adoption of the New EU rules for Personal Data Protection (14 April 2014) Statement/16/1403

Trade Marks Directive 95/2008

Frankryk

Franse Strafkode (Code Pénal) — Art R645-1

Japan

Chosakuken Hõ (Japanese wet op Kopiereg) 48 van 1970

Sjina

Administration of Engagement by Internet Sites in the Business of News Publication Tentative Provisions 2000

Administration of the Maintenance of Secrets in the International Networking of Computer Information Systems Provisions 2000

China Internet Domain Name Regulations 2006

Decision of the Standing Committee of the National People's Congress People's Congress Concerning Maintaining Internet Security 2000

Interim Procedures on the Regulation and Filing of Online Business Operation 2000

Interim Provisions on the Administration of Internet Publication 2002

Management Provisions on Electronic Bulletin Services in the Internet 2000

Measures for Security Protection Administration of the International Networking of Computer Information Networks 1997

Measures on Internet Information Services 2000

Measures on the Administration of Business Sites of Internet Access Services 2001

Provisions for the Administration of Internet News Information Services 2005

Provisions of the Supreme People's Court on Certain Issues Related to the Application of Law in the Trial of Civil Cases Involving Disputes Over Infringement of the Right to Network Dissemination of Information. Sien Hua J Toward A More Balanced Approach: Rethinking and Readjusting Copyright Systems in the Digital Network Era 2014

Regulation on Internet Information Service of the People's Republic of China 2000

Regulations on the Administration of Business Sites of Internet Access Services 2002

Security Management Procedures in Internet Accessing 1997

Telecommunications Regulations of the People's Republic of China 2000

Temporary Regulation for the Management of Computer Information Network International Connection 1996

Suid-Afrika

Consumer Protection Act 68 of 2008 (Slegs in Engels uitgevaardig)

Staatskoerant 29903 (18 Mei 2007)

Suid-Afrikaanse Polisiedienswet 68 van 1995

Wet op die Beskerming van Persoonlike Inligting 4 van 2013

Wet op die Reëling en Onderskepping van Kommunikasies en Verstrekking van Kommunikasie-Verwante Inligting 70 van 2002

Wet op Elektroniese Kommunikasies en Transaksies 25 van 2002

Wet op Elektroniese Kommunikasie 36 van 2005

Wet op Films en Publikasies 65 van 1996

Wet op Verbruikersbeskerming 68 van 2008

Verenigde Koninkryk

Computer Misuse Act of 1990

Defamation Act of 2013

VSA

15 USC § 1114(2)(B) en (C) (2006)

17 USC § 512 (2012)

18 USC § 1030 (2001)

Communications Act of 1934 48 Stat 1064

Communications Decency Act 47 USC § 230 (2006)

USA PATRIOT Act of 2001 Pub L No 107-56

Digital Millennium Copyright Act 17 USC § 512 (2012)

Foreign Intelligence Surveillance Act 50 USC Chapter 36 - Foreign Intelligence Surveillance

Freedom of Information Act 5 USC § 552

Intelligence Authorization Act for Fiscal Year 1995 Pub L No 103–359 § 302(c) 108 Stat 3423 3445 (1994) (gekodifiseer deur 50 USC §§ 1821–1829)

Intelligence Authorization Act for Fiscal Year 1999 Pub L No 105–272, § 601 112 Stat 2396 2404–2410 (1998) (gekodifiseer deur 50 USC §§ 1841–1846)

Lanham Act 15 USC § 1114(2)(B) en (C) (2006)

National Security Act of 1947

Scientific and Advanced-Technology Act of 1992

Unlawful Internet Gambling Enforcement Act of 2006 31 USC Chapter 53 Subparagraph IV

USA FREEDOM Act H R 2048 2015

Regspraak (Sake)

Europese Unie

Delfi *v Estonia* ECtHR 64659/09

Google *France SARL v Louis Vuitton Malletier SA* 2010 E C R I 2417 (2010)

Google *Inc v Agencia Española de Protección de Datos (AEPD)* ECLI:EU:C:2014:317

L'Oreal *v eBay* C-324/09

Frankryk

Uejf *et Licra v Yahoo Inc et Yahoo France* Tribunal De Grande Instance De Paris, N° RG: 00/05308 May 22 2000

Japan

Japan *v Kaneko* Kyõtõ Chihõ [Kyõtõ Dist Ct] Dec 13 2006 Hei 16 (wa) no 726 1229 (Japan)

Kanada

Equustek *Solutions Inc v Google Inc* 2014 BCCA 295

Equustek *Solutions Inc v Google Inc* 2015 BCCA 265

Suid-Afrika

Coin *Security Group (Pty) Ltd v Smit* 1991 2 SA 315 (T)

Commissioner *of Taxes, Federation of Rhodesia v McFarland* 1965 1 SA 470 (W)

R *v Pienaar* 1948 1 SA 925 (A)

Tsichlas *and Another v Touch Line Media (Pty) Ltd* 2004 (2) SA 112 (W)

Verenigde Koninkryk

Bunt *v Tilley* 2006 E W H C 407 (QB)

Byrne *v Deane* 1937 1 KB 818

Davison *v Habeeb and Others* 2011 E W H C 3031 (QB)

Regina *v Paddy Roy Bates and Michael Roy Bates* [1968] (UK-NA LO 2/1088)

Tamiz *v Google Inc* 2013 E W C A Civ 68 2012 E W H C 449 (2013)

VSA

American *Civil Liberties Union v Reno* 929 F Supp 824 (ED Pa 1996)

Automattic *Inc v Steiner* 82 F Supp 3d 1011 (N D Cal 2015)

Avdeef *v Google* No 4 14-CV-788-A (N D Tex Aug 26 2015)

BMG *Rights Management v Cox Communications* Civil No 1 14-cv-1611 (E D Va Dec 1 2015)

BWP *Media USA v Clarity Digital Group* Civil Action No 14-cv-00467-PAB-KMT (D Colo Mar 31 2015)

China *Central Television v Create New Technology (HK)* No CV 15-01869 MMM (MRWx) (C D Cal June 11 2015)

Clapper *v Amnesty International* 133 S Ct 1138 – Supreme Court 2013

Columbia *Pictures Industries v Fung* 710 F 3d 1020 – Court of Appeals 9th Circuit 2013 1040

Comcast *v FCC* US Court of Appeals for the DC circuit April 6 2010 440 US

Cubby *Inc v CompuServe Inc* 776 F Supp 135 — Dist Court SD New York 1991 op 140

Doe *v Bates* 2006 W L 3813758 (2006)

Doe *v MySpace Inc* 474 F Supp 2d 843 (W D Tex 2007)

Doe *v Sexsearch.com* 502 F Supp 2d 719 (N D Ohio 2007)

Ellison *v Robertson* 357 F 3d 1072 — Court of Appeals 9th Circuit 2004

FC *Online Marketing v Burke's Martial Arts* No 14-CV-3685 (SJF)(SIL) (E D N Y July 8 2015)

Google *v Hood* 96 F Supp 3d 584 (S D Miss 2015)

Hendrickson *v eBay* 165 F Supp 2d 1082 — Dist Court CD California 2001

Lenz *v Universal Music Corp* 801 F 3d 1126 — Court of Appeals 9th Circuit 2015 1130

Lightspeed *Media Corp v Smith* 761 F 3d 699 — Court of Appeals 7th Circuit 2014

Lunney *v Prodigy Services Co* 723 NE 2d 539 — NY Court of Appeals 1999

Milo *and Gabby v Amazon.com* No C13-1932RSM (W D Wash July 16 2015)

O'Brien *v Western Union Telegraph Co* 113 F 2d 539 (lst Cir 1940)

Perfect *10 Inc v Ccbill LLC* 488 F 3d 1102 — Court of Appeals 9th Circuit 2007

Religious *Tech Center v Netcom On-line Comm* 907 F Supp 1361 (N D Cal 1995)

Reno *v American Civil Liberties Union* 521 US 844 117 S Ct 2329 138 L Ed 2d 874 (1997)

Sarvis *v Polyvore* Civil Action No 12-12233-LTS (D Mass Mar 2 2015)

Square *Ring Inc v John Doe-1* Civil Action No 09-563 (GMS) (D Del Jan 23 2015)

Stratton *Oakmont Inc v Prodigy Services Co* 1995 WL 323710 (N Y Sup Ct May 24 1995)

TD *Bank v Hill* Civil No 12-7188 (RBK/JS) (D N Y July 27 2015)

Totallyher *Media v BWP Media USA* No 2 13-cv-08379-AB-PLAX (C D Cal Apr 7 2015)

Tuteur *v Crosley-Corcoran* 961 F Supp 2d 333 — Dist Court D Massachusetts 2013

UMG *Recordings v Escape Media Group* No 11 Civ 8407 (TPG) (S D N Y Apr 23 2015)

Verizon *v FCC* 740 F 3d 623 — Court of Appeals Dist of Columbia Circuit 2014

Viacom *International v YouTube* 676 F 3d 19 — Court of Appeals 2nd Circuit 2012

William *Business Services v Waterside Chiropractic* No 3 14-cv-05873-BHS (W D Wash Mar 18 2015)

Yahoo *Inc v La Ligue Contre Le Racisme Et* 145 F Supp 2d 1168

Zeran v *America Online* Inc 129 F 3d 327 330 (4th Cir 1997)

Internasionaal

Fr *v Turk* 1927 PCIJ (ser A) 10 (1927)

Lotus-saak (*Fr v Turk* 1927 PCIJ (ser A) 10 (1927))

Reparation *for Injuries Suffered in the Service of the United Nations* International Court of Justice Reports 1949 174

Diverse

124 Congress Records 34,845 (1978) – Ted Kennedy

Chueng A S Y en Zhao Y "An Overview of Internet Regulation in China" 2013 *University of Hong Kong Faculty of Law Research Paper* 1

Council of Europe *Parliamentary Assembly of the Council of Europe* 17 Oktober 1994 Doc 7178 1

Dischinger M *et al* "Detecting BitTorrent Blocking" *8th ACM SIGCOMM Conference on Internet Measurement ACM 2008*

European Commission *Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection* (14 April 2014) Statement/16/1403

European Parliament *Motion for a Resolution: To Wind up the Debate on Statements by the Council and the Commission Pursuant to Rule 110(2) of the Rules of Procedure on the Forthcoming World Conference on International Telecommunications (WCIT-12) of the International Telecommunication Union, and the Possible Expansion of the Scope of International Telecommunication Regulations* (2012/2881(RSP))

Federal Communications Commission *Protecting and Promoting the Open Internet* Federal Register Vol 80 No 70 April 13 2015

Field S G *Internet Piracy in Japan* (2010) (Thesis) 36

Great Britain Parliament House of Commons European Scrutiny Committee *HC 219-ix — House of Commons European Scrutiny Committee Ninth Report of Session 2014-15* (2014) 62 vn 37

Gurumurthy A *Statement by Anita Gurumurthy, Executive Director, IT for Change 1 at the Closing Ceremony of WSIS Plus 10 Review held by UNESCO from 25th to 27th February, 2013* (2013) 3

Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act Before the Senate Committee on the Judiciary 113th Congress 3 (2013) 8–9 (geskrewe getuienis van Edward W Felten, Professor by Princeton Universiteit)

IETF se *Requirements for Internet Hosts — Communication Layers* RFC:1122 1.1

International Telecommunications Union *Collection of the Basic Texts of the International Telecommunication Union Adopted by the Plenipotentiary Conference: Edition 2011* 38

Kreibich C *et al* "Netalyzr: Illuminating the Edge Network" *10th ACM SIGCOMM Conference on Internet Measurement ACM 2010*

Privacy and Civil Liberties Oversight Board *Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* (2014) 158

Recognition *of the Internet Service Provider's Association as an Industry Representative Body for Internet Service Provider* GN 588 in GG 32252 van 2009-05-22.

Report of the International Law Commission (2011) GAOR 66th Session, Supplement No 10 (A/66/10 en Addendum 1) Par 87

Russian Federation *Written Submission of the Russian Federation to the Draft Final Document of the UNGA High-level Meeting on the Implementation of WSIS Outcomes* (2015) 2

United Nations *General Assembly Resolution 56/183* (21 Desember 2001)

Wentworth S "Hearing: Fighting for Internet Freedom, Dubai and Beyond" 2013 *US House of Representatives Committee on Energy and Commerce's Subcommittee on Communications and Technology* 3

Internet

Anoniem "Administration White Paper: Bulk Collection of Telephony Metadata under Section 215 of the *USA PATRIOT* Act"
http://perma.cc/V7VM-5MAU
(besoek op 8 Maart 2016)

Anoniem "Charters of Freedom — A New World is at Hand"
http://www.archives.gov/exhibits/charters/bill_of_rights.html
(besoek op 3 Mei 2013)

Anoniem "Facts About W3C"
http://www.w3.org/Consortium/facts#history
(besoek op 3 Junie 2014)

Anoniem "IANA Report on the Redelegation of the .za Toplevel Domain"
https://www.IANA.org/reports/2005/za-report-05aug05.pdf
(besoek op 25 Augustus 2014)

Anoniem "In the Matter of Preserving the Open Internet"
https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf
(besoek op 20 Junie 2014)

Anoniem "Report of the Working Group on Internet Governance 2005" http://www.wgig.org/docs/WGIGREPORT.pdf (besoek op 11 September 2014) par 3

Anoniem "Telecom Decision CRTC 2008–108" http://www.crtc.gc.ca/eng/archive/2008/dt2008-108.htm#archived (besoek op 15 September 2014)

Anoniem "Text of the Scientific and Advanced-Technology Act of 1992" https://www.govtrack.us/congress/bills/102/s1146/text (besoek op 25 Februarie 2016)

Anoniem "World Telecommunication/ICT Policy Forum 2013: OPINION 5: Supporting Multi-stakeholderism in Internet Governance" http://www.itu.int/en/wtpf-13/Documents/WTPF-13-Opinion5.pdf. (besoek op 27 Mei 2014)

Barlow J P "A Declaration of the Independence of Cyberspace" https://projects.eff.org/~barlow/Declaration-Final.html (besoek op 4 Maart 2014)

Berners-Lee T "Information Management: A Proposal" http://www.w3.org/History/1989/proposal.html (besoek op 22 Augustus 2014)

Berners-Lee T "Ten Years Public Domain for the Original Web Software" http://tenyears-www.web.cern.ch/tenyears-www/ (besoek op 27 Julie 2012)

Berners-Lee T "WorldWideWeb: Summary" https://groups.*Google*.com/forum/?fromgroups=#!msg/alt.hypertext/eCTkkOoWTAY/bJGhZyooXzkJ (besoek op 2 September 2014)

Bigthink "The Long Arm Of China's Internet Police" http://bigthink.com/think-tank/how-to-censor-the-internet-in-china-2 (besoek op 31 Maart 2016)

British Broadcasting Corporation News "China Internet: Ren Zhiqiang's Account Blocked After Xi Criticism"

http://www.bbc.com/news/world-asia-china-35682030
(besoek op 28 Maart 2016)

British Broadcasting Corporation "Human Rights: What is China Accused Of?"
http://www.bbc.com/news/magazine-34592336
(besoek op 28 Maart 2016)

British Broadcasting Corporation "China Employs Two Million Microblog Monitors State Media Say"
http://www.bbc.com/news/world-asia-china-24396957
(besoek op 31 Maart 2016)

British Broadcasting Corporation "Google Attacks UN's Internet Treaty Conference"
http://www.bbc.com/news/technology-20429625
(besoek op 18 Mei 2016)

British Broadcasting Corporation "European Parliament Warns Against UN Internet Control"
http://www.bbc.com/news/technology-20445637
(besoek op 18 Mei 2016)

British Broadcasting Corporation "Victorian 'Supercomputer' is Reborn"
http://news.bbc.co.uk/2/hi/technology/7391593.stm
(besoek op 20 Augustus 2014)

British Broadcasting Corporation "China Employs Two Million Microblog Monitors State Media Say"
http://www.bbc.com/news/world-asia-china-24396957
(besoek op 31 Maart 2016)

British Broadcasting Corporation "Human Rights: What Is China Accused Of?"
http://www.bbc.com/news/magazine-34592336
(besoek op 28 Maart 2016)

British Broadcasting Corporation News "China Internet: Ren Zhiqiang's Account Blocked After Xi Criticism"
http://www.bbc.com/news/world-asia-china-35682030
(besoek op 28 Maart 2016).

Cable News Network "China Employs 2 Million to Police Internet"
http://edition.cnn.com/2013/10/07/world/asia/china-internet-monitors/
(besoek op 31 Maart 2016)

Cailliau R "A Little History of the World Wide Web"
http://www.w3.org/History.html
(besoek op 25 Augustus 2014)

Carsten P "China Calls for Internet Front to Fight Hacking, Cyber 'Arms Race'"
http://www.reuters.com/article/us-china-internet-idUSKBN0TZ09-920151216
(besoek op 26 Maart 2016)

Cerf V, Kahn B en Chapin L "Announcing the Internet Society"
http://www.Internetsociety.org/Internet/Internet-51/history-Internet/announcing-Internet-society
(besoek op 11 September 2014)

Cerf V "IETF and the Internet Society"
http://www.internetsociety.org/internet/what-internet/history-internet/ietf-and-internet-society
(besoek op 28 Mei 2014)

Cerf V "Re: Registration of .ZA Domain"
http://web.archive.org/web/20041012150242/http://www2.frd.ac.za/-uninet/history/zacleard.htm
(besoek op 2 September 2014)

China Internet Network Information Center "The Internet Timeline of China (2009)"
http://www1.cnnic.cn/IDR/hlwfzdsj/201209/t20120904_36020.htm
(besoek op 23 Maart 2016)

China Internet Network Information Center "The Internet Timeline of China (2007)"
http://www1.cnnic.cn/IDR/hlwfzdsj/201209/t20120904_36018.htm
(besoek op 23 Maart 2016)

China Internet Network Information Center "The Internet Timeline of China 2004–2006"
http://www1.cnnic.cn/IDR/hlwfzdsj/201209/t20120904_36017.htm
(besoek op 23 Maart 2016)

China Patent Agent "China Internet Domain Name Regulations (2006)"
http://www.cpahkltd.com/EN/static/20100315155837187932.html
(besoek op 23 Maart 2016)

ChinaItLaw "Administrative Provisions for Electronic Bulletin Services on the Internet"
http://www.china.org.cn/business/2010-01/20/content_19274960.htm
(besoek op 17 Maart 2016)

ChinaITLaw "Telecommunications Regulations of the People's Republic of China"
http://www.china.org.cn/business/laws_regulations/2010-01/20/content_19273945.htm
(besoek op 17 Maart 2016)

Cicconi J "AT&T Statement on the US Court of Appeals DC Circuit Open Internet Decision"
http://www.attpublicpolicy.com/fcc/att-statement-on-the-u-s-court-of-appeals-d-c-circuit-open-internet-decision/
(besoek op 6 Junie 2014)

City U "Measures for Managing Internet Information Services"
http://newmedia.cityu.edu.hk/cyberlaw/gp9/pdf/lr01.pdf
(besoek op 17 Maart 2016)

Cnet "Net Neutrality Rules Get Published — Let the Lawsuits Begin"
http://www.cnet.com/news/fccs-net-neutrality-rules-hit-federal-register-lawsuit-underway/
(besoek op 13 April 2016)

CNN Money "Global Wage Calculator"
http://money.cnn.com/interactive/news/economy/davos/global-wage-calculator/
(besoek op 15 Maart 2016)

Committee to Protect Journalists “Read and Delete: How *Weibo*’s Censors Tackle Dissent and Free Speech”
https://cpj.org/blog/2016/03/read-and-delete-how-weibos-censors-tackle-dissent-.php
(besoek op 28 Maart 2016)

Committee to Protect Journalists “Olympics: Jing Jing, Cha Cha, and Other Online Cops”
https://www.cpj.org/blog/2008/08/olympics-jing-jing-cha-cha-and-other-online-cops.php
(besoek op 31 Maart 2016)

Computer History Museum “The Babbage Engine”
http://www.computerhistory.org/babbage/
(besoek op 20 Augustus 2014)

Congressional Executive Commission on China “Provisions on the Administration of Internet News Information Services (Chinese Text and CECC Full Translation)”
http://www.cecc.gov/resources/legal-provisions/provisions-on-the-administration-of-internet-news-information-services
(besoek op 22 Maart 2016)

Corporation for Assigned Names and Numbers “IANA Stewardship Transition Proposal and Enhan- cing ICANN Accountability Recommendations”
https://www.ICANN.org/en/system/files/files/IANA-stewardship-transition-package-10mar16-en.pdf
(besoek op 19 Mei 2016)

Council of Europe “Chart of Signatures and Ratifications of Treaty 185”
http://www.coe.int/en/web/conventions/full-list/-/conventions/-treaty/185/signatures
(besoek op 22 Mei 2014)

Council of Europe “Convention on Cybercrime”
http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
(besoek op 22 Mei 2014)

Council of the European Communities “Treaty on European Union”
http://europa.eu/eu-law/decision-making/treaties/pdf/treaty_-

on_european_union/treaty_on_european_union_en.pdf
(besoek op 16 Februarie 2016)

Cunningham W "What is Wiki"
http://wiki.org/wiki.cgi?WhatIsWiki
(besoek op 22 Augustus 2014)

De Wet P "Namespace Moves Towards Controlling ZA Names"
http://www.itweb.co.za/index.php?option=com_content&view=article&id=93404
(besoek op 11 September 2014)

De Wet P "Govt Slammed Namespace 'By Mistake'"
http://www.hellkom.co.za/newsviewer/local/1862/Govt-slammed-Namespace-by-mistake-
(besoek op 11 September 2014)

De Wet P "The Tyranny of the Majority"
http://www.itweb.co.za/index.php?option=com_content&view=article&id=87538:the-tyranny-of-the-majority&catid=79:columnists
(besoek op 30 Oktober 2014)

Defenceweb "State Can Spy on Citizens — Report"
http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=30932:state-can-spy-on-citizens–report&catid=-90:science-a-defence-technology&Itemid=204
(besoek op 4 April 2016)

Department of Communication "Discussion Paper on Electronic Commerce Policy" http://www.polity.org.za/polity/govdocs/discuss/ecomm.html
(besoek op 11 September 2014)

Desai N "Report of the Working Group on Internet Governance"
http://www.wgig.org/docs/WGIGREPORT.pdf
(besoek op 2 Januarie 2014)

Dickinson S "WTPF-13 Day 3: Brazil's Draft Opinion, Informally Known as Opinion 7"
http://linguasynaptica.com/wtpf-13-part3/
(besoek op 7 September 2014)

Dubai L S "A Digital Cold War? The Economist 14 Dec 2012"
http://www.economist.com/blogs/babbage/2012/12/internet-regulation
(besoek op 26 Mei 2014)

EASSy "What is EASSy"
http://www.eassy.org/about.html
(besoek op 4 April 2016)

Electronic Freedom Foundation "Section 215 of the *USA PATRIOT* Act"
https://www.eff.org/foia/section-215-usa-patriot-act
(besoek op 8 Maart 2016)

Ermert M "5th World Telecom Policy Forum — Stepping Stone to Changes in the Internet Governance Arena?"
http://policyreview.info/articles/news/5th-world-telecom-policy-forum-%E2%80%93-stepping-stone-changes-internet-governance-arena/129
(besoek op 7 September 2014)

Ethnologue "China"
http://www.ethnologue.com/country/CN
(besoek op 15 Maart 2016)

European Union "The Schuman Declaration – 9 May 1950"
http://europa.eu/about-eu/basic-information/symbols/europe-day/schuman-declaration/index_en.htm
(besoek op 16 Februarie 2016)

Federal Communications Commission "Memorandum Opinion and Order"
https://apps.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf
(besoek op 4 September 2014)

FindLaw "China's Telecommunications Industry: The New Ministry of Information Industry (MII) and Foreign Investment Opportunities"
http://corporate.findlaw.com/law-library/china-s-telecommunications-industry-the-new-ministry-of.html
(besoek op 23 Maart 2016)

Forbes "Online Cigarette Sales? Shocking!"
http://www.forbes.com/2001/12/11/1211tobacco.html
(besoek op 30 Maart 2016)

Gelman B en Poitras L "US, British Intelligence Mining Data From Nine US Internet Companies in Broad Secret Program"
http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html
(besoek op 12 Mei 2014)

Global Web Index "90 Million VPN Users in China Have Accessed Restricted Social Networks"
http://www.globalwebindex.net/blog/vpn-in-china
(besoek op 24 Maart 2016)

Gomez J J "*Licra and UEJF v Yahoo Inc and Yahoo France*"
http://www.lapres.net/yahen11.html
(besoek op 11 November 2013)

Griffiths J "Chinese President Xi Jinping: Hands Off Our Internet"
http://edition.cnn.com/2015/12/15/asia/wuzhen-china-internet-xi-jinping
(besoek op 26 Maart 2016)

Gutterman B "IGF 2010 — Developing the Future Together: The Fifth Meeting of the Internet Governance Forum Vilnius Lithuania 14–17 September 2010"
http://www.intgovforum.org/cms/documents/publications/175-developing-the-future-together/file
(besoek op 11 September 2014)

Harrison L "Beijing Shakes Fist at 'Cults and Feudal Superstition' Online"
http://www.theregister.co.uk/2000/10/14/beijing_shakes_fist_at_cults/
(besoek op 15 Maart 2016)

Hovey R "The Organizations Involved in the IETF Standards Process"
http://tools.ietf.org/html/bcp11
(besoek op 22 Mei 2014)

Hu J en Hansen E "*Yahoo* Auction Case May Reveal Borders of Cyberspace" http://news.cnet.com/*Yahoo*-auction-case-may-reveal-borders-of-cyberspace/2100-1023_3-244365.html (besoek op 11 November 2013)

Huffpost Business "Fadi Chehadé: If We Fragment The Internet, 'It Will Not Be The Internet As We Know It'" http://www.huffingtonpost.com/2014/01/24/fadi-chehade-davos_n_4635949.html (besoek op 14 April 2016)

IC on the Record "Hearing of the Senate Judiciary Committee on Strengthening Privacy Rights and National Security: Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs" http://icontherecord.tumblr.com/post/57811913209/hearing-of-the-senate-judiciary-committee-on (besoek op 11 Maart 2016)

Intellectual Property Watch "NETmundial Internet Governance Meeting Closes With Less Than 'Rough Consensus'" http://www.ip-watch.org/2014/04/25/netmundial-internet-governance-meeting-closes-with-less-than-rough-consensus/ (besoek op 16 April 2016)

Intellectual Property Watch "ICANN Meeting In Marrakesh: More Hiccups On Way To IANA Transition" http://www.ip-watch.org/2016/03/08/ICANN-meeting-in-marrakesh-more-hiccups-on-way-to-IANA-transition/ (besoek op 8 Mei 2016)

International Communications Union "WTPF 2013: Final Opinions" http://www.itu.int/en/wtpf-13/Pages/opinions.aspx (besoek op 22 Mei 2014)

International Telecommunications Union "Brief Guide to ITU Conferences, Assemblies and Events" https://www.itu.int/en/history/Documents/GuideToConferencesAssembliesEvents.pdf (besoek op 3 September 2014)

International Telecommunications Union "Plenipotentiary 98 – A New Beginning for the ITU?"

http://www.itu.int/newsarchive/press/PP98/Documents/Backgrounder1_General.html
(besoek op 29 Oktober 2014)

International Telecommunications Union "Press Release: 80 Organizations Sign MoU to Restructure the Internet"
http://www.itu.int/newsarchive/press_releases/1997/itu-08.html
(besoek op 11 September 2014)

International Telecommunications Union "List of Member States"
https://www.itu.int/online/mm/scripts/gensel8
(besoek op 22 Mei 2014)

International Telecommunications Union "World Conference on International Telecommunications (WCIT-12)"
http://www.itu.int/en/wcit-12/Pages/default.aspx
(besoek op 17 Mei 2016)

Internet Assigned Numbers Authority http://www.IANA.org/reports/2005/za-report-05aug05.pdf
(besoek op 11 September 2014) 2

Internet Assigned Numbers Authority "IANA Report on the Redelegation of the .za Toplevel Domain"
https://www.IANA.org/reports/2005/za-report-05aug05.pdf
(besoek op 9 Mei 2016)

Internet Corporation for Assigned Names and Numbers "Beginner's Guide to Participating in ICANN"
http://www.ICANN.org/en/system/files/files/participating-08nov13-en.pdf
(besoek op 13 Mei 2014)

Internet Corporation for Assigned Names and Numbers "IANA Stewardship Transition Proposal and Enhancing ICANN Accountability Recommendations"
https://www.ICANN.org/en/system/files/files/IANA-stewardship-transition-package-10mar16-en.pdf
(besoek op 8 Mei 2016)

Internet Corporation for Assigned Names and Numbers “ICANN Board Meeting August 22 2013 FY14 Budget Approval”
http://www.ICANN.org/en/about/financials/adopted-opplan-budget-fy14-22aug13-en.pdf
(besoek op 13 Mei 2014)

Internet Corporation for Assigned Names and Numbers “ICANN Bylaws Provisions Relating to Nominating Committee”
http://archive.ICANN.org/en/committees/nom-comm/bylaws.htm
(besoek op 4 September 2014)

Internet Corporation for Assigned Names and Numbers “Montevideo Statement on the Future of Internet Cooperation”
https://www.ICANN.org/news/announcement-2013-10-07-en
(besoek op 8 Mei 2016)

Internet Corporation of Assigned Names and Numbers “Montevideo Statement on the Future of Internet Cooperation”
https://www.ICANN.org/news/announcement-2013-10-07-en
(besoek op 20 Junie 2014)

Internet Engineering Task Force “Past Meetings”
http://www.ietf.org/
meeting/past.html (besoek op 22 Mei 2014)

Internet Engineering Task Force “Requirements for Internet Hosts: Communication Layers”
http://tools.ietf.org/html/rfc1122
(besoek op 20 Augustus 2014)

Internet Governance Forum “Report of the Working Group on Internet Governance”
http://www.wgig.org/docs/WGIGREPORT.pdf
(besoek op 28 April 2016)

Internet Governance Forum “Internet Governance Forum Background Note Nairobi 27–30 September 2011”
http://www.intgovforum.org/cms/2011/press/Backgrounder_What_is_IGF_final.doc
(besoek op 3 September 2014)

Internet Governance Forum "The IGF 2009 Meeting"
http://www.intgovforum.org/cms/2009-igf-sharm-el-sheikh
(besoek op 17 Mei 2016)

Internet Governance Project "Alternate DNS Roots and the Abominable Snowman of Sovereignty"
http://www.internetgovernance.org/2016/04/07/alternate-dns-roots-and-the-abominable-snowman-of-sovereignty/
(besoek op 16 April 2016)

Internet Society "An Oral History of the Internet Society's Founding"
http://www.internetsociety.org/internet-society-founding
(besoek op 20 Junie 2014)

Internet Society "Formation of Internet Society Announced at INET '91 Copenhagen"
http://www.internetsociety.org/history-timeline/formation-internet-society-announced-inet-%E2%80%9991-copenhagen
(besoek op 20 Junie 2014)

Internet Society "Internet Society Mission"
http://www.internetsociety.org/who-we-are/mission
(besoek op 20 Junie 2014)

ISPA "Key Milestones and Victories for ISPA"
http://ispa.org.za/about-ispa/key-milestones/
(besoek op 15 Februarie 2016)

IT-Online "ISPA Gets Minister's Recognition"
http://it-online.co.za/2009/05/21/ispa-gets-ministers-recognition/
(besoek op 15 Februarie 2016)

ITWeb "State Can Spy On Citizens — Report"
http://www.itweb.co.za/index.php?option=com_content&view=article&id=65120
(besoek op 4 April 2016)

Knoch C "Uninet — The South African Academic and Research Network"
http://web.archive.org/web/20030419023522/http://www.idrc.ca/-acacia/outputs/op-unin.htm
(besoek op 2 Augustus 2014)

Kostecke S "UMN Gopher Released under the GPL"
https://groups.*Google*.com/forum/#!msg/comp.infosystems.gopher/4A-LS_A6qtA/nT89yWKzzsIJ
(besoek op 22 Augustus 2014)

Kozlowski L "The Future of the Web Looks a Lot Like You"
http://www.forbes.com/sites/lorikozlowski/2012/06/15/the-future-of-the-web-looks-a-lot-like-you/
(besoek op 25 Augustus 2014)

Kuo K *TEDxHonolulu Technology, Entertainment and Design Conference* 5 November 2009. *YouTube* "TEDxHonolulu - Kaiser Kuo - 11/05/09"
https://www.*YouTube*.com/watch?v=M-jqGmc6xKI
(besoek op 15 Maart 2016)

La Quadrature Du Net "Civil Society Calls on the ECHR's Grand Chamber to Overturn Delfi v Estonia Ruling"
https://www.laquadrature.net/en/civil-society-calls-on-the-echrs-grand-chamber-to-overturn-delfi-v-estonia-ruling
(besoek op 23 Februarie 2016)

Lapres D "*Licra and the Uejf v Yahoo Inc and Yahoo France*"
http://www.lapres.net/yahen11.html
(besoek op 11 November 2013)

Laurie B "An Expert's Apology"
http://www.apache-ssl.org/apology.html
(besoek op 25 Augustus 2014)

Law 360 "Telecom Cases To Watch In 2016"
http://www.law360.com/articles/737221/telecom-cases-to-watch-in-2016
(besoek op 13 April 2016)

LawInfoChina "Provisions on the Administration of Newspaper Publication"
http://www.lawinfochina.com/display.aspx?lib=law&id=4716&CGid=#
(besoek op 17 Maart 2016)

Lawrie M "The History of the Internet in South Africa"
http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf
(besoek op 25 Augustus 2014)

Laws of the People's Republic of China "Interim Provisions Governing the Management of Computer Information Network International Connection"
http://www.asianlii.org/cn/legis/cen/laws/ipgtmotcinitproccttin1488/
(besoek op 15 Maart 2016)

Legal Information Institute "15 USC § 1114 — Remedies; Infringement; Innocent Infringement by Printers and Publishers"
https://www.law.cornell.edu/uscode/text/15/1114#2_D
(besoek op 2 Maart 2016)

Legalbrief "Extent of State Spying on Individuals Revealed"
http://legalbrief.co.za/story/extent-of-state-spying-on-individuals-revealed/
(besoek op 4 April 2016)

Lehman, Lee en Xu "Measures for the Administration of the Publication of Audio-Visual Programs Through the Internet or Other Information Network 2004"
http://www.lehmanlaw.com/resource-centre/laws-and-regulations/information-technology/measures-for-the-administration-of-the-publication-of-audio-visual-programs-through-the-internet-or-other-information-network-2004.html
(besoek op 22 Maart 2016)

Li D "The Expanding Great Firewall of China: A New Rule Banning All Foreign Media from Publishing Online Goes Live Today"
http://www.usnews.com/news/best-countries/articles/2016-03-10/the-expanding-great-firewall-of-china
(besoek op 26 Maart 2016)

Licklider J C R "Memorandum for Members and Affiliates of the Intergalactic Computer Network"
http://www.kurzweilai.net/memorandum-for-members-and-affiliates-of-the-intergalactic-computer-network
(besoek op 20 Augustus 2014)

Mail and Guardian "Secret State: How the Government Spies on You"
http://mg.co.za/article/2011-10-14-secret-state/
(besoek op 4 April 2016)

Markoff J "An Internet Pioneer Ponders the Next Revolution"
http://web.archive.org/web/20080922095019/http://partners.nytimes.com/library/tech/99/12/biztech/articles/122099outlook-bobb.html
(besoek op 22 Augustus 2014)

Maroela Media "Taaltoffie: Miljarde, Biljoene, en Triljoene"
http://maroelamedia.co.za/afrikaans/taaltoffie/taaltoffie-miljarde-biljoene-en-triljoene/
(besoek op 15 Maart 2016)

Ministry of Foreign Affairs of the People's Republic of China "Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference"
http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml
(besoek op 15 April 2016)

Mirriam Webster "Spanish Central"
http://www.spanishcentral.com/translate/mundial
(besoek op 27 April 2016)

Mockapetris P "Domain Names — Concepts and Facilities"
http://tools.ietf.org/html/rfc882
(besoek op 22 Augustus 2014)

Mueller M "WTF? WTPF! Internet Governance Project — The Continuing Battle Over Internet Governance Principles"
http://www.internetgovernance.org/2013/04/23/wtf-wtpf-the-continuing-battle-over-internet-governance-principles/
(besoek op 27 Mei 2014)

Mybroadband "South African Movie, Music Piracy Labs Busted – Here They Are"
http://mybroadband.co.za/news/general/119234-south-african-movie-music-piracy-labs-busted-here-they-are.html
(besoek op 30 Maart 2016)

National Bureau of Statistics in China "National Data"
http://data.stats.gov.cn/english/
(besoek op 15 Maart 2016)

National Telecommunications and Information Administration "NTIA Announces Intent to Transition Key Internet Domain Name Functions"
https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions
(besoek op 3 Oktober 2014)

National Telecommunications and Information Administration "Statement of Policy on the Management of Internet Names and Addresses"
http://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses
(besoek op 11 September 2014)

National Telecommunications and Information Administration "An Update on the IANA Transition"
https://www.ntia.doc.gov/blog/2015/update-IANA-transition
(besoek op 28 April 2016)

National Telecommunications and Information Administration "NTIA Announces Intent to Transition Key Internet Domain Name Functions"
https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions
(besoek op 28 April 2016)

National Telecommunications and Information Administration United States Department of Commerce "Statement of Policy on the Management of Internet Names and Addresses"
http://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses
(besoek op 9 Mei 2014)

National Telecommunications and Information Administration "Reviewing the IANA Transition Proposal"
https://www.ntia.doc.gov/blog/2016/reviewing-IANA-transition-proposal
(besoek op 19 Mei 2016)

National Telecommunications and Information Administration "Moving Together Beyond Dubai"

https://www.ntia.doc.gov/blog/2013/moving-together-beyond-dubai
(besoek op 27 April 2016)

National Telecommunications and Information Administration "NTIA Announces Intent to Transition Key Internet Domain Name Functions"
http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions
(besoek op 8 Mei 2016)

NETmundial "Global Multistakeholder Meeting on the Future of Internet Governance"
http://netmundial.br/
(besoek op 27 April 2016)

NETmundial "NETmundial Multistakeholder Statement"
http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf
(besoek op 8 Mei 2016)

New York Times "Comcast and Netflix Reach Deal on Service"
http://www.nytimes.com/2014/02/24/business/media/comcast-and-netflix-reach-a-streaming-agreement.html?_r=0
(besoek op 12 April 2016)

New York Times "E-Commerce Report; Now that Credit Card Companies Won't Handle Online Tobacco Sales, Many Merchants are Calling it Quits"
http://query.nytimes.com/gst/fullpage.html?res=9800E3DD1E3FF9-37A35757C0A9639C8B63
(besoek op 30 Maart 2016)

New York Times "Keep the Internet Open"
http://www.nytimes.com/2012/05/25/opinion/keep-the-internet-open.html?_r=0
(besoek op 28 April 2016)

New York Times "Merkel Backs Plan to Keep European Data in Europe"
http://www.nytimes.com/2014/02/17/world/europe/merkel-backs-

plan-to-keep-european-data-in-europe.html?hp&_r=0
(besoek op 15 April 2016)

New York Times "Obama Asks F.C.C. to Adopt Tough Net Neutrality Rules"
http://www.nytimes.com/2014/11/11/technology/obama-net-neutrality-fcc.html
(besoek op 13 April 2016)

October A "Internet Users Relax — .za Domain is Safe"
http://www.iol.co.za/news/politics/Internet-users-relax-za-domain-is-safe-1.51648#.UIGMmFLNdNA
(besoek op 11 September 2014)

Office of the Attorney General "Attorneys General and ATF Join with Credit Card Companies to Prevent Illegal Internet Cigarette Sales"
http://www.ag.idaho.gov/media/newsReleases/2005/nr_0317200-5b.html
(besoek op 30 Maart 2016)

Oyama Y "Copyright Law of Japan"
http://www.cric.or.jp/english/clj/index.html
(besoek op 9 Desember 2014)

Pelkey J "Entrepreneurial Capitalism and Innovation: A History of Computer Communications 1968–1988"
http://www.historyofcomputercommunications.info/Book/6/6.3-CYCLADESNetworkLouisPouzin1–72.html
(besoek op 20 Augustus 2014)

Proch D "Plumb the Depths of Deep Packet Inspection"
http://electronicdesign.com/communications/plumb-depths-deep-packet-inspection
(besoek op 5 Junie 2014)

Quartz "Beijing is Banning All Foreign Media From Publishing Online in China"
http://qz.com/620076/beijing-is-banning-all-foreign-media-from-publishing-online-in-china/
(besoek op 26 Maart 2016)

Quartz "The Seven Tweets That Could Cost a Chinese Human Rights Lawyer Eight Years in Jail"
http://qz.com/569370/the-seven-tweets-that-could-cost-a-chinese-human-rights-lawyer-eight-years-in-jail/
(besoek op 28 Maart 2016)

Randi J "China and Superstitions"
http://archive.randi.org/site/index.php/swift-blog/2120-china-and-superstitions.html
(besoek op 15 Maart 2015)

Reuters "AT&T, US Telecom Groups Seek to Block New Internet Rules"
http://in.reuters.com/article/usa-internet-neutrality-idINKBN0NM4AH20150501
(besoek op 13 April 2016)

Russian Federation "World Conference on International Telecommunications (WCIT–12) Dubai, 3–14 December 2012: Proposals for the Work of the Conference"
http://www.soumu.go.jp/main_content/000188224.pdf
(besoek op 4 September 2014)

Salon "Choke Points Leave Us Vulnerable"
http://www.salon.com/2010/07/06/yes_technology_fails_sometimes/
(besoek op 4 April 2016)

Seacom "Seacom"
http://seacom.mu/network/
(besoek op 4 April 2016)

SFGate "China Censors Internet Users With Site Bans, Cartoon Cop Spies"
http://www.sfgate.com/opinion/article/China-censors-Internet-users-with-site-bans-2501596.php
(besoek op 31 Maart 2016)

Shackleford S J "Spotlight on Cyber V: Back to the Future of Internet Governance?" 2015 *Georgetown Journal of International Affairs (Cyber)*
http://journal.georgetown.edu/back-to-the-future-of-internet-governance/
(besoek op 16 April 2016)

Smith CS "Cell Phone Triangulation Accuracy Is All Over The Map" http://searchengineland.com/cell-phone-triangulation-accuracy-is-all-over-the-map-14790 (besoek op 4 Maart 2016)

Steward W "ARPANET — The First Internet" http://www.livingInternet.com/i/ii_arpanet.htm (besoek op 22 Augustus 2014)

Steward W "IMP — Interface Message Processor" http://www.livinginternet.com/i/ii_imp.htm (besoek op 22 Augustus 2014)

Stewart W "*Paul Baran Invents Packet Switching*" http://www.livinginternet.com/i/ii_rand.htm (besoek op 20 Augustus 2014)

Straziuso J "Associated Press, French Anti-Racist Group Sues *Yahoo*" http://www.apnewsarchive.com/2000/French-Anti-Racist-Group-Sues-*Yahoo*/id-1a0475ef8b88a12f717b6975f67a5043 (besoek op 2 Januarie 2013)

Telegeography "Submarine Cable Map" http://www.submarinecablemap.com/#/submarine-cable/africa-coast-to-europe-ace (besoek op 4 April 2016)

The Atlantic Monthly "As We May Think" http://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/303881/ (besoek op 20 April 2012)

The Diplomat "'Internet Plus' and the Salvation of China's Rural Economy" http://thediplomat.com/2015/07/internet-plus-and-the-salvation-of-chinas-rural-economy/ (besoek op 28 Maart 2016)

The Economist "A Digital Cold War?" http://www.economist.com/blogs/babbage/2012/12/internet-regulation (besoek op 14 April 2016)

The Globe and Mail "Supreme Court Grants *Google* Appeal in Case of Blocked Search Results"
http://www.theglobeandmail.com/technology/tech-news/supreme-court-to-hear-*Google*s-appeal-in-bc-search-injunction-case/article28794728/
(besoek op 30 Maart 2016)

The Guardian "Edward Snowden and the NSA Files — Timeline"
http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline
(besoek op 8 Mei 2016)

The Guardian "NSA Chief Claims 'Focused' Surveillance Disrupted More Than 50 Terror Plots"
http://www.theguardian.com/world/2013/jun/18/nsa-surveillance-limited-focused-hearing
(besoek op 11 Maart 2016)

The Guardian "NSA Chief Says Exposure of Surveillance Programs Has 'Irreversible' Impact"
http://www.theguardian.com/world/2013/jun/18/nsa-chief-house-hearing-surveillance-live
(besoek op 11 Maart 2016)

The Guardian "NSA Collecting Phone Records of Millions of *Verizon* Customers Daily"
http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
(besoek op 9 Maart 2016)

The Hill "House Approves Resolution to Keep Internet Control Out of UN Hands"
http://thehill.com/blogs/floor-action/house/271153-house-approves-resolution-to-keep-internet-control-out-of-un-hands
(besoek op 18 Mei 2016)

The Hill "Spy Chief: Snowden Killed 'Important' Spy Program in Afghanistan"
http://thehill.com/policy/national-security/253040-snowden-killed-important-spy-program-in-afghanistan-spy-chief-says
(besoek op 9 Maart 2016)

The Wall Street Journal “China Targets Human-Rights Lawyers in Crackdown”
http://www.wsj.com/articles/china-targets-human-rights-lawyers-in-crackdown-1436715268
(besoek op 28 Maart 2016)

United Nations Treaty Collection “Charter of the United Nations”
https://treaties.un.org/doc/publication/ctc/uncharter.pdf
(besoek op 17 Mei 2016)

United Nations “Member States of the United Nations”
http://www.un.org/en/members/index.shtml
(besoek op 15 September 2014)

United Nations “WSIS+10 United Nations General Assembly High Level Meeting”
https://publicadministration.un.org/WSIS10/
(besoek op 28 April 2016)

US Chamber Litigation Center “United States Telecom Association v FCC”
http://www.chamberlitigation.com/united-states-telecom-association-v-fcc-et-al
(besoek op 13 April 2016)

Veltman K “Challenges for a Semantic Web”
http://semanticweb2002.aifb.uni-karlsruhe.de/proceedings/Position/-veltmann.pdf
(besoek op 25 Augustus 2014)

W3C-SA “Contact W3C-SA”
http://www.w3c.org.za/officecontact.html
(besoek op 25 Augustus 2014)

W3C “Current Members”
https://www.w3.org/Consortium/Member/List
(besoek op 19 Mei 2016)

W3C “Facts about W3C”
https://www.w3.org/Consortium/facts
(besoek op 19 Mei 2016)

W3C "History of the Web"
http://www.w3c.it/education/2012/upra/documents/origins.pdf
(besoek op 25 Augustus 2014)

W3C "Semantic Web Road Map"
https://www.w3.org/DesignIssues/Semantic.html
(besoek op 25 Augustus 2014)

W3C "W3C Process Document"
https://www.w3.org/2005/10/Process-20051014/organization.html#AB
(besoek op 19 Mei 2016)

Wikipedia "CERN"
https://en.wikipedia.org/wiki/CERN
(besoek op 22 Augustus 2014)

Wikipedia "Commission on Global Governance"
https://en.wikipedia.org/wiki/Commission_on_Global_Governance
(besoek op 16 Mei 2016)

Wikipedia "Donald Davies"
http://en.wikipedia.org/wiki/Donald_Davies
(besoek op 20 Augustus 2014)

Wikipedia "European Union"
https://en.wikipedia.org/wiki/European_Union#Governance
(besoek op 16 Februarie 2016)

Wikipedia "Facebook"
https://en.wikipedia.org/wiki/Facebook
(besoek op 25 Augustus 2014)

Wikipedia "General Data Protection Regulation"
https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
(besoek op 16 April 2016)

Wikipedia "History of the African Union"
https://en.wikipedia.org/wiki/History_of_the_African_Union#Organisation_of_African_Unity
(besoek op 15 Mei 2016)

Wikipedia "Internasionale Reg"
https://af.wikipedia.org/wiki/Internasionale_reg
(besoek op 27 April 2016)

Wikipedia "International League against Racism and Anti-Semitism"
https://en.wikipedia.org/wiki/International_League_against_Racism_-and_Anti-Semitism
(besoek op 11 November 2013)

Wikipedia "International Telecommunication Union"
http://en.wikipedia.org/wiki/International_Telecommunication_-Union#Membership
(besoek op 22 Mei 2014)

Wikipedia "Internet Governance Forum"
http://en.wikipedia.org/wiki/Internet_Governance_Forum
(besoek op 11 September 2014)

Wikipedia "Internet in South Africa"
https://en.wikipedia.org/wiki/Internet_in_South_Africa
(besoek op 4 April 2016)

Wikipedia "IP Address"
http://en.wikipedia.org/wiki/IP_address
(besoek op 22 Augustus 2014)

Wikipedia "List of Countries and Dependencies by Population"
https://en.wikipedia.org/wiki/List_of_countries_and_dependencies_-by_population
(besoek op 15 Maart 2016)

Wikipedia "List of Sovereign States"
http://en.wikipedia.org/wiki/List_of_sovereign_states
(besoek op 15 September 2014)

Wikipedia "Root Name Server"
http://en.wikipedia.org/wiki/Root_name_server
(besoek op 3 Oktober 2014)

Wikipedia "SAT-2"
https://en.wikipedia.org/wiki/SAT-2
(besoek op 4 April 2016)

Wikipedia "Standard Chinese"
https://en.wikipedia.org/wiki/Standard_Chinese
(besoek op 15 Maart 2016)

Wikipedia "State Council of the People's Republic of China"
https://en.wikipedia.org/wiki/State_Council_of_the_People's_Republic_of_China
(besoek op 17 Maart 2016)

Wikipedia "The Star-Spangled Banner"
https://en.wikipedia.org/wiki/The_Star-Spangled_Banner
(besoek op 9 Maart 2016)

Wikipedia "WACS (Cable System)"
https://en.wikipedia.org/wiki/WACS_%28cable_system%29
(besoek op 4 April 2016)

Wikipedia "Root Name Server"
http://en.wikipedia.org/wiki/Root_name_server
(besoek op 3 Oktober 2014)

Wikisource "Consolidated Version of the Treaty on the Functioning of the European Union (2007)"
https://en.wikisource.org/wiki/Consolidated_version_of_the_Treaty_on_-the_Functioning_of_the_European_Union
(besoek op 16 Februarie 2016)

Wilson C "Chris Pinkham: Veteran of the Virtual"
http://www.techcentral.co.za/chris-pinkham-veteran-of-the-virtual/25403/
(besoek op 25 Augustus 2014)

Wilson C "Mike Lawrie: SA's Internet Pioneer"
http://www.techcentral.co.za/mike-lawrie-sas-Internet-pioneer/24774/
(besoek op 25 Augustus 2014)

Wilson C "The SA Internet Turns 20"
http://www.techcentral.co.za/the-sa-Internet-turns-20/27371/
(besoek op 2 September 2014)

Wired "CDA Struck Down"
http://archive.wired.com/politics/law/news/1997/06/4732
(besoek op 25 Augustus 2014)

Wolchok S, Yao R en Halderman J A "Analysis of the Green Dam Censorware System"
https://jhalderm.com/pub/gd/
(besoek op 31 Maart 2016)

Wolf G "The Curse of Xanadu"
http://www.wired.com/wired/archive/3.06/xanadu.html
(besoek op 22 Augustus 2014)

Wood M "Statute of the International Law Commission"
http://legal.un.org/avl/pdf/ha/silc/silc_e.pdf
(besoek op 3 September 2014)

World Intellectual Property Organization "China Internet Domain Name Regulations"
http://www.wipo.int/wipolex/en/text.jsp?file_id=182419
(besoek op 23 Maart 2016)

World Intellectual Property Organization "Measures for Security Protection Administration of the International Networking of Computer Information Networks"
http://www.wipo.int/edocs/lexdocs/laws/en/cn/cn115en.pdf
(besoek op 15 Maart 2016)

World Intellectual Property Organization "Measures for the Administrative Protection of Internet Copyright"
http://www.wipo.int/edocs/lexdocs/laws/en/cn/cn034en.pdf
(besoek op 23 Maart 2016)

World Internet Conference — Wuzhen Summit "An Interconnected World Shared and Governed by All"
http://www.wicwuzhen.cn/english/
(besoek op 26 Maart 2016)

World Summit on the Information Society "Tunis Agenda for the Information Society"
http://www.itu.int/WSIS/docs2/tunis/off/6rev1.html
(besoek op 7 September 2014)

World Summit on the Information Society “Implementing WSIS Outcomes: A Ten-year Review”
http://unctad.org/en/PublicationsLibrary/dtlstict2015d3_en.pdf
(besoek op 8 Mei 2016)

World Wide Web Consortium “About W3C”
https://www.w3.org/Consortium/
(besoek op 25 Augustus 2014)

Yeti DNS Project “A Live Root DNS Server System Testbed”
https://yeti-dns.org/
(besoek op 16 April 2016)

***

Student: B J Gordon

Studentenommer: 3923-337-5

Studieleier: Prof S S Nel

Afkortings

AOL	America Online
ARPA	Advanced Research Project Agency
ARPANET	Advanced Research Project Agency Network
CAIP	Canadian Association of Internet Providers
CDA	Communications Decency Act of 1996 [USA]
CERN	Conseil Européen pour la Recherche Nucléaire
CORE	International Council of Registrars
CRTC	Canadian Radio–Television and Telecommunications Commission
DMCA	Digital Millennium Copyright Act of 1998 [USA]
DNS	Domain Name System (domeinnaamstelsel)
DPI	Deep Packet Inspection
DVD	Digital Video Disc
EFF	Electronic Frontier Foundation
EU	European Union
FBI	Federal Bureau of Investigations

FCC	Federal Communications Committee
FISA	Foreign Intelligence Surveillance Act of 1978 [USA]
FISC	Foreign Intelligence Surveillance Court [USA]
FRD	Foundation for Research and Development
HTBC	High Tech Broadband Coalition
HTTP	Hyper Text Transfer Protocol
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICAO	International Civil Aviation Organization
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IMP	Interface Message Processor
INRIA	Institut National de Recherche en Informatique et en Automatique
IP-adress	Internet Protocol Address (Internet Protokol-adres)
IPv6	Internet Protocol version 6
IRTF	Internet Research Task Force
ISOC	Internet Society
ISP	Internet Service Provider

ISPA	Internet Service Providers Association
ITR	International Telecommunications Regulations
ITU	International Telecommunications Union
LAN	Local Area Network
MAPC	Measures for the Administrative Protection of Internet Copyright [China]
MCI	Temporary Regulation for the Management of Computer Information Network International Connection [China]
MIIS	Measures on Internet Information Services [China]
MIT	Massachusetts Institute of Technology
MUD	Multi-user Dungeon
NSA	National Security Agency
NSF	National Science Foundation
NSI	Network Solutions Inc
NTIA	National Telecommunications and Information Administration [USA]
OPEC	Organization of the Petroleum Exporting Countries
P2P	Peer-to-peer File Sharing
PANS	Measures on Internet Information Services [China]
PINN	Measures for Security Protection Administration of the International Networking of Computer Information Networks [China]
QoS	Quality of Service

SMP	Security Management Procedures in Internet Accessing [China]
SMTP	Send Mail Transfer Protocol
SRI	Stanford Research Institute
TCP/IP	Transmission Control Protocol / Internet Protocol
TRPC	Telecommunications Regulations of the People's Republic of China [China]
Uninet	University Network
VN	Verenigde Nasies
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WCIT-12	World Conference on International Telecommunications 2012
WGIG	Working Group on Internet Governance
WIPO	World Intellectual Property Organization
WNNR	Wetenskaplike en Nywerheidsnavorsingsraad
WSIS+10	World Summit on the Information Society Plus 10
WSIS-I	World Summit on the Information Society I 2003
WSIS-II	World Summit on the Information Society II 2005
WTPF	World Telecommunications Policy Forum
WWW	World Wide Web