Wired Norms

Inscription, resistance, and subversion in the governance of the Internet infrastructure

Niels ten Oever

Wired Norms:

Inscription, resistance, and subversion in the governance of the Internet infrastructure

ACADEMISCH PROEFSCHRIFT
ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus
prof. dr. ir. K.I.J. Maex
ten overstaan van een door het College voor Promoties ingestelde commissie,
in het openbaar te verdedigen in de Aula der Universiteit
op woensdag 28 oktober 2020, te 14.00 uur
door Niels ten Oever
geboren te Meppel

Promotiecommissie

Promotor:	Prof. Dr. M.E. Glasius Universiteit van Amsterdam
Copromotor:	Dr. S. Milan Universiteit van Amsterdam
Overige leden:	prof. dr. M. de Goede Universiteit van Amsterdam
	prof. dr. L.A. Bialasiewicz Universiteit van Amsterdam
	prof. dr. ir. C.T.A.M. de Laat Universiteit van Amsterdam
	dr. A. Freyberg-Inan Universiteit van Amsterdam
	prof. dr. L.E. DeNardis American University
	prof. dr. S. Braman Texas A&M University
	dr. F. Musiani CNRS, France

Faculteit der Geesteswetenschappen

This project has benefited from funding from the Ford Foundation (grant agreement 132156); the European Research Council under the European Union's Horizon 2020 research and innovation program (grant agreement 639379-DATACTIVE). Furthermore the RIPE Academic Cooperation Initiative covered my flight and accommodation during the RIPE78 meeting in Reykjavik, Iceland. The funders did not exert any influence on the design, topic, or conclusions of the research, data, or findings.

Summary

Wired Norms: Inscription, resistance, and subversion in the governance of the Internet infrastructure

The entanglement of the Internet with the daily practices of governments, companies, institutions, and individuals means that the processes that shape the Internet also shape society. In this dissertation, I study the norms that shape the Internet's underlying structure through its transnational governance. Norms are the 'widely-accepted and internalised [sic] principles or codes of conduct that indicate what is deemed to be permitted, prohibited, or required of agents within a specific community' (Erskine and Carr 2016, 87). Internet governance is the development, coordination, and implementation of policies, technologies, protocols, and standards. Internet governance produces a global and interoperable Internet functioning as a general-purpose communication network in transnational governance bodies. I examine four cases of norm conflict and evolution in three key Internet governance institutions: the Internet Engineering Taskforce (IETF); the Internet Corporation for Assigned Names and Numbers (ICANN); and the Réseaux IP Européens Network (RIPE).

I show how social and legal norms evolve and are introduced, subverted, and resisted by participants in Internet governance processes with distinct and dynamic values and interests, in order to develop policies, technologies, and standards to produce an interconnected Internet. I leverage notions and insights from science and technology studies and international relations to illuminate how a sociotechnical imaginary—the combination of visions, symbols, and futures that exist in groups and society—architectural principles, and an entrenched norm function as instruments of metagovernance in the Internet infrastructure. This way, I demonstrate how a sociotechnical imaginary, values, and norms facilitate, instruct, and evaluate the norm setting processes in Internet governance.

This dissertation is empirically grounded in the analysis of mailing lists; technical documents; policy documents; interviews and the extensive observation of governance meetings. I have operationalized this analysis using the following methods: quantitative descriptive analysis; network analysis; quantitative and qualitative discourse analysis, as well as in participant observation, including semi-structured interviews and ethnographic probes.

The aim of this dissertation is to show how Internet governance happening in multistakeholder bodies, what I call private Internet governance, solely functions to increase interconnection between independent networks. In this process, the introduction of social and legal norms—such as human rights principles and data protection regulations that might hamper increased interconnection—is resisted by significantly represented stakeholders in the process. Ultimately, I argue that while the sociotechnical imaginary and architectural principles serve to legitimize this governance ordering, the entrenched norm, what I call the infrastructural norm that transcends singular institutions, guides the distributed private governance regime.

Samenvatting

Ingesnoerde Normen: Inscriptie, weerstand en ondermijning in het bestuur van de Internet infrastructuur

Het Internet is verstrengeld met de dagelijkse praktijk van overheden, bedrijven, instellingen en individuen. Deze verstrengeling betekent dat de processen die het Internet vormgeven, ook de samenleving vormgeven. In dit proefschrift bestudeer ik de normen die de onderliggende structuur van het Internet vormen door middel van zijn transnationale bestuur. Normen zijn de 'breed geaccepteerde en geïnternaliseerde principes of gedragscodes die aangeven wat wordt geacht te zijn toegestaan, verboden of vereist van actoren binnen een specifieke gemeenschap' (Erskine en Carr 2016, 87). Het bestuur van het Internet, ook wel 'Internet governance' genoemd, is de ontwikkeling, coördinatie en implementatie van beleid, technologieën, protocollen en normen in internationale bestuursorganen. Het doel van Internet governance is het produceren van een wereldwijd en interoperabel Internet dat functioneert als een algemeen communicatienetwerk. Ik onderzoek vier casussen van normconflict en -ontwikkeling in drie belangrijke instituties voor Internet governance: de Internet Engineering Taskforce (IETF); de Internet Corporation for Assigned Names and Numbers (ICANN); en het Réseaux IP Européens Network (RIPE).

In dit proefschrift laat ik zien hoe sociale en juridische normen evolueren en worden geïntroduceerd, ondermijnd en weerstaan door verschillende groepen actoren in Internet governance in de ontwikkeling van beleid, technologieën en normen om een onderling verbonden Internet te produceren. Ik maak daarbij gebruik van begrippen en inzichten uit wetenschaps- en technologiestudies en internationale betrekkingen om te verduidelijken hoe architectonische principes, een verankerde norm en een sociotechnische verbeelding —dat wil zeggen, de combinatie van visies, symbolen en toekomsten die bestaan in groepen en de maatschappij— functioneren als instrumenten van meta-governance in de Internet infrastructuur. Op deze manier laat ik zien hoe een sociotechnische verbeelding, waarden en normen de normstellende processen in Internet governance faciliteren, instrueren en evalueren.

Dit proefschrift is empirisch onderbouwd met een analyse van mailinglijsten; technische documenten; beleidsdocumenten; interviews en de uitgebreide observatie van vergaderingen. Ik heb deze analyse vervolgens geoperationaliseerd met behulp

van de volgende methoden: kwantitatieve beschrijvende analyse; netwerkanalyse; kwantitatieve en kwalitatieve discours analyse, alsmede door participatieve observatie van deelnemers aan deze bestuursprocessen, inclusief semi-gestructureerde interviews en etnografisch sondes.

Het doel van dit proefschrift is om te laten zien hoe Internet governance in multistakeholder instituties, hetgeen ik 'privaat Internet governance' noem, uitsluitend functioneert om de interconnectie tussen autonome netwerken te vermeerderen. In dit proces wordt de invoering van sociale en juridische normen – zoals mensenrechten en regels voor gegevensbescherming, die de toename van interconnectie zouden kunnen belemmeren – tegengewerkt door sterk vertegenwoordigde belanghebbenden in Internet governance. Deze verankerde norm van vrijwillige interconnectie, die de toename van interconnectie voorschrijft, noem ik een infrastructurele norm. Deze infrastructurele norm overstijgt de aparte instituties van het private Internet governance regime. Uiteindelijk betoog ik dat, terwijl de sociotechnische verbeelding en architecturale principes dienen om de bestuursvorm van private Internet governance te legitimeren, terwijl het regime gestuurd wordt door de infrastructurele norm.

De infrastructurele norm van vrijwillige interconnectie speelt een instructieve en evaluerende rol in normontwikkeling en -evolutie in het private Internet governance regime. De infrastructurele norm is ingebed in de institutionele configuratie, technologische materialiteit, economische prikkels en het supranationaal belang dat het private Internet governance regime samenbindt. Tot slot constateer ik dat het private Internet governance regime is ontworpen en geoptimaliseerd voor de enge en beperkte rol van immer toenemende interconnectie tussen onafhankelijke netwerken. Als gevolg daarvan verzet het governance regime zich tegen het op één lijn brengen van de Internet infrastructuur met sociale of juridische normen die de toename van de interconnectie zouden kunnen beperken of belemmeren.

In controversies about technology and society, there is no idea more provocative than the notion that technical things have political qualities.

— Langdon Winner (1980)

Science and technology lie at the heart of social asymmetry. Thus technology both creates systems which close off other options and generate novel, unpredictable and indeed previously unthinkable, options. The game of technology is never finished, and its ramifications are endless

— Michel Callon (1990)

The Internet isn't value-neutral, and neither is the IETF.

— Mission Statement of the IETF (Alvestrand 2004)

Table of Contents

Acknowledgments

Our lives and societies are complex, entangled, and messy. In order to make sense of them we make abstractions to identify forces, eras, categories, and discontinuities. But when one looks closer, everything is often held together by duct tape, elastic bands, and people. This thesis has been the product of a long engagement with technology and social justice, in many different environments, in many different localities, but everywhere it were people holdings this together. I cannot blame anyone but myself for this work, but I have been strongly and positively influenced by the following people that have helped me pull this thesis together, ordered in several categories:

First and foremost all research participants and interviewees that I encountered in Internet governance bodies, who have been so graceful and forthcoming to share their insights, knowledge, and experiences. My promotor Prof. Dr. Marlies Glasius and my supervisor Dr. Stefania Milan, who challenged me to write and think better, and inspired me to actually do so by their careful reviews, endless patience, and useful comments.

Institutional

The University of Amsterdam, and especially the Amsterdam School for Cultural Analysis, where Eloe Kingma, Hotze Mulder, Rang Rademaker-Cortes, Swaan Janssen, and Wendy Bron ensure that anything is possible, and for providing me with the PhD Finishing Fellowship. The Amsterdam Institute for Social Science Research for providing excellent courses on research design and advanced social science theory, and funding to go to the International Studies Association meeting!

My institutional home during my PhD, the DATACTIVE research group, where Stefania Milan, Becky Kazansky, Frederike Kaltheuner, Kersti Wissenbach, Guillen Torres, Jeroen de Vos, Davide Beraldo, Lonneke van der Velden, Zhen Ye, Theresa Villeseñor, Jonathan Gray, Sander van Haperen and Fabien Cante introduced me to many new texts, methods, and memes. They gave color to the whole process of thesis writing and gave meaning to what it means to be a (data)activist researcher.

Many knowledgeable and committed civil society organizations and activists, such as my colleagues at ARTICLE19, Corinne Cath-Speth, Mehwish Ansari, Vidushi Marda, Amelia Andersdotter,

Mallory Knodel, Barbora Bukovska and Quinn McKew, with whom I started to explore the vast land of human rights and standard setting organizations. They taught me so much about collaboration and connection, getting stuff done, and kindly helped me explore and interrogate my own presumptions and biases. I was very fortunate to collaborate with many other people and organizations working on digital rights, such as Claudio Ruiz, Gisela Perez de Acha, and Maria Paz Canales at Derecho Digitales, Joana Varon Ferraz and Renata Avila at Coding Rights, Valeria Milanes, Leandro Ucciferri, and Jeanette Torrez at Asociación por los Derechos Civiles, Rebecca McKinnon and Lisa Gutermuth at Ranking Digital Rights, Charles Bradley, Sheetal Kumar, and Donja Ghobadi at Global Partners Digital, and Leon Willems and Bethel Tsegaye at Free Press Unlimited.

During my engagement with Internet governance bodies I came across many people who have helped me find my way, educated me about complex and legacy technologies, arcane processes and procedures, as well as institutional quirks and negotiations, and who made spending time at these long meetings and much more enjoyable. There would be too many people to mention, but I want to specifically mention dkg, Shane Kerr, Wes Hardeker, Gurshabad Grover, Stephen Farrell, Mark Nottingham, Martin Thomson, Lars Eggert, Adrian Farrel, Brian Trammell, Joe Hall, Andrew Sullivan, Shivan Sahib, Stéphane Bortzmeyer, Konstantinos Komaitis, Vesna Manojlovic, Mirjam Kuehne, Alexandra Kulikova, Farzaneh Badiei, Milton Mueller, Bill Drake, Tatiana Tropina, Ellen Strickland, Jordan Carter, and Jan Aart Scholte.

Then there are many academic fellow travelers who made helped me theorize and who provide a tremendous amount of inspiration. Again, there are many, but I wanted to specifically mention Chiara Poletti, Fenwick McKelvey, Corinne Cath-Speth (again), Fieke Jansen, Elinor Carmi, Leonie Tanczer, Louise Marie Hurel, Roya Ensafi, Svitlana Matviyenko, Jeroen van der Ham, Julia Rone, Biella Coleman, Pranesh Prakash, Beatrice Martini, Seda Guerses, Joris van Hoboken, Madeline Carr, Ben Wagner, Leonie Tanczer, Luca Belli, Sebastian Benthal, Nick Doty, Blayne Haggart, Natasha Tusikov, Stéphane Couture, Sophie Toupin, Ashwin Mathew, Sally Wyatt, Linnet Taylor, Thomas Poell, Marianne Franklin, and Christian Katzenbach.

Financial

Every kind of work is intrinsically linked to funding sources. In civil society and academia finding funding can be tough, but

I have been very fortunate to work with excellent donors whom have not only provided funding for the work I have been doing over the years, but also helped me to reflect, stop, and continue. They taught me that funding is not just a transaction, but also a relation, as well as joint problem solving. Thanks for that to Laura Cunningham, Michael Brennan, Dan Meredith, Eric Sears, Wei Fan, Max Steele, Lisa Vermeer, and Dan O'Maley.

Technological

When I was about six or seven years old, my brother sat me down behind my fathers Bull Micral BM-30, I stared at the flickering DOS prompt, which seemed to ask me: 'you don't know what you're doing, do you?'. Ever-since I have wanted to know how computers really work. It's now about 30 years later, and I still often have no idea. But I got a bit better at getting lost in a terminal and asking longer questions. Often the way of asking questions on a computer is by using software (and sometimes a soldering iron). I want to thank the contributors to free and open source software that make my explorations possible. First and foremost Sebastian Benthall and Nick Doty with whom I had the pleasure to work on Big Bang, and from whom I learned a lot about quantitative analysis. Other tools that I keep on returning to, and whose contributors I am therefore highly indebted: Debian GNU/Linux, the Gnome Project, LibreOffice, Zotero, Brave, Zsh, Grep, Python, R, Mutt, notmuch, offlineimap, and Nextcloud.

Personal

I am eternally grateful for my smart older brother Albert, who is the real computer scientist, and with whom I am still soldering antique computers together. I hope our joint explorations will never end. My partner Dorrit for being so close, but always giving me space. They, together with my sister-in-law Anneke and nephew Jonathan, are my compact but happy family. My friend Ernst van den Hemel, for his loyalty, his banter, his berimbolo attempts, and his wit. Niels de Groot for Culturée Revolté and folding nomads into monads (and vice versa). Matthijs Ponte for the books, the beers, and the bikes. And Guido, Grimm, Wessel and Frake for never turning off the light.

Physical

In life it is important to collaborate, but it is also important to know how to fight. I learned to fight in three places: Van der Vathorst, Bensy Gym, and R-Grip from senseis Rik van der Vathorst, Jacques van Eijsden, late Ome Jan van de Vathorst, Nourdin Bensellam, Roemer Trompert, Marloes Coenen, Leroy

La Rose, Cedric Cameron, Andreas Ewart, and Aram Clements. I also want to thank all my training and sparring partners, especially the ones that have been in my corner: Mohamed Schultz, Charles Kocuvie-Tay, Adil Bougzir, Boyd Emmen, and Ernst van den Hemel (again).

Previously published parts of the dissertation

Chapter 1, 'Coding and encoding rights in internet infrastructure', has been previously published, after peer review, as: Milan, Stefania, and Niels ten Oever. 2017. "Coding and Encoding Rights in Internet Infrastructure." Internet Policy Review 6 (1). This article was co-authored with Dr. Stefania Milan. The paper built on findings from participant observation and quantitative analysis during my research in ICANN. These findings were corroborated through Dr. Stefania Milan's engagement with ICANN. Though we collaborated throughout all aspects of this article, dr. Milan mainly developed the literature review and theoretical framework, whereas I focused on data collection, analysis and conclusions. The chapter was adapted for re-publication in this thesis by changing the hyperlinks from the original paper into footnotes, the adding of the header 'introduction', the removal of acknowledgments and keywords, and an update to the reference style to make it consistent with the style of the thesis.

Chapter 2, 'Productive Contestation, Civil Society, and Global Governance: Human Rights as a Boundary Object in ICANN' has been previously published, after peer review, as: ten Oever, Niels. 2018. "Productive Contestation, Civil Society, and Global Governance: Human Rights as a Boundary Object in ICANN." Policy & Internet, 11, as part of a special issue titled 'Internet Architecture and Human Rights'. I am the sole author of this paper. For the republication of this article in this thesis the following changes were made: the footnote and figure numbering were updated, the reference style was made consistent with the rest of the thesis. Keyword were removed, as well as the numbering of the subheadings.

Chapter 3, *'This is not how we imagined it'*: Technological affordances, economic drivers and the Internet architecture imaginary, has been accepted, after peer review, to be published in New Media & Society as: ten Oever, Niels. Forthcoming. "'This Is Not How We Imagined It' - Technological Affordances, Economic Drivers and the Internet Architecture Imaginary." New Media & Society, in a special issue titled '"We are on a mission". Exploring the role of future imaginaries in the making and governing of digital technology' (Chun 2007; 2008). I am the sole author of this paper. To publish it in this thesis, the following changes have been

made: the keywords have been removed, and the reference style and footnote number have been updated.

Chapter 4, ‘Norm conflict in the governance of transnational and distributed infrastructures: the case of Internet routing’ has been offered for peer review and publication to Globalizations. I am the sole author of this paper. To publish it in this thesis the following changes have been made: the footnote and figure number has been adapted, the reference style has been updated, and the keywords have been removed.

Abbreviations

3GPP	Third Generation Project Partnership
AC	Advisory Committee
AS	Autonomous System
ASN	Autonomous System Number
ASO	Address Supporting Organization
AUP	Acceptable Use Policy
BBN	Bolt, Beranek and Newman Inc
BGP	Border Gateway Protocol
DNS	Domain Name System
CoE	Council of Europe
ccNSO	Country Code Names Supporting Organization
CCWG	Cross Community Working Group
CCWP HR	Cross Community Working Party on ICANNs Corporate and Social Responsibility to Respect Human Rights
GAC	Governmental Advisory Committee
GAC WG HRIL	Governmental Advisory Committee Working Group on Human Rights and International Law
GDPR	General Data Protection Regulation
GNSO	Generic Names Supporting Organization
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IEEE	Institute for Electrical and Electronics Engineers
IETF	Internet Engineering Taskforce
IGF	Internet Governance Forum
IP	Internet Protocol
IR	International relations
M3AAWG	Messaging Malware Mobile Anti-Abuse Working Group
NCDNHC	NonCommercial Domain Name Holders Constituency
NCUC	Non-Commercial Users Constituency
NCSG	Noncommercial Stakeholder Group
NGO	Non-Governmental Organization
NPOC	Not-for-Profit Operational Concerns
NSF	National Science Foundation

NTIA	National Telecommunications and Information Administration
OSI	Open Systems Interconnection
RIPE	Réseaux IP Européens
RIR	Regional Internet Registries
RFC	Request for Comments
STS	Science and technology studies
UN	United Nations
UNGP	United Nations Guiding Principles on Business and Human Rights
U.S.	United States
WS1	Workstream 1
WS2	Workstream 2

List of Figures

Introduction

The Internet infrastructure is a distributed network of roughly 70.000 independent networks. There is no central authority that sets rules for the Internet. To agree on expected behavior for the network, representatives of industry, governments, academia, not-for-profit organizations, and individual advocates and activists jointly develop norms in a process that is called Internet governance. Through its technical properties and characteristics, the Internet enables and invokes visions of possible futures, it influences what we think is possible and what is not, and it enables certain behaviors and inhibits others. The Internet infrastructure has thus become an instrument of direct and indirect control. What this direct or indirect control looks like is in part determined by the design of the Internet. The design of the Internet can make censorship harder or private communications easier; it can provide opportunities for governmental control or resist centralized decision-making; moreover, it can create markets and opportunities that benefit all users, or just a particular group of actors. This means that the norms and values embedded in the technical infrastructure at the root of the Internet impact the ability of the people that use the Internet to exercise their human rights (Lessig 1999; Raymond 2019; DeNardis 2014).

The Internet infrastructure consists of cables that connect routers and computers, electromagnetic spectrum that allows for the transmission of signals between satellites, radio towers and mobile phones, but also data centers that allow for data storage. These devices and media do not merely work by themselves. Rather, the Internet infrastructure also includes the people that design and maintain them, the institutions through which these experts collaborate, and the bodies of knowledge they rely on. Therefore, the Internet infrastructure should be understood as inherently relational. Overall, the Internet infrastructure is continuously being produced in a complex interplay between and among engineers, users, companies, governments, technology, and institutions. Aside from *producing* a normative technical infrastructure, this infrastructure is also *produced* through norms of expected behavior.

Internet governance entails the standardization, implementation, and coordination of complex networking technologies that are to be deployed in different jurisdictions around the globe, developed, produced and implemented by competing corporations, which are scrutinized by governments, academics, advocates and other stakeholders with diverse values and interests. The governance of the Internet happens largely through what is

commonly referred to as multistakeholder governance (Hofmann, Katzenbach, and Gollatz 2017) in which primary stakeholders such as industry, civil society advocates, governments, research institutions and non-governmental organizations (NGO) cooperate in governance bodies that are not controlled by states. This is what I will call private Internet governance. Others describe this process as bottom-up industry self-regulation (Sowell 2012). This has led some researchers to state that Internet governance itself is a governance innovation (Verhulst et al. 2014). Some studies touch upon the topic of norms in Internet governance (Christou and Simpson 2007; Mueller, Mathiason, and Klein 2007; Malcolm 2008; DeNardis 2014). However, there has been limited research so far into how values and norms are encoded in the Internet infrastructure. This is an oversight, because Internet infrastructure currently has the power to shape society. To address this gap I analyze the governance of the Internet infrastructure to answer the following question: what role do norms and values play in the governance of the Internet infrastructure?

In this dissertation, drawing from detailed case studies in three different Internet governance bodies, I combine quantitative and qualitative analysis to disentangle the complexity of distributed Internet governance. This allows me to contribute to theory building on how social and technical norms are intertwined, and how they influence and inform institutional design, technological materiality, and participants in these governance processes. Moreover, it allows me to examine how these norms function as tools of 'meta-governance' (Jessop 1997)—tools for exercising control in distributed decision-making processes (Kooiman and Jentoft 2009). My objects of analysis thus include deeply embedded norms with sociotechnical imaginaries—the combination of visions, symbols, and futures that exist in groups and society that guide the co-creation of knowledge, technology, policies and institutions (Jasanoff and Kim 2015). I do this by building on frameworks and concepts from science and technology studies, as well international relations, and employ methodologies from anthropology and sociology. The combination of these concepts and methods allow me to analyze and theorize the shaping processes of technology, the design of governance institutions and regimes, and the role of norms in instructing and evaluating behavior.

In this introduction, I will first offer a high-level overview of the field of Internet governance, the different institutions and their remits. After that, I will introduce the fields of science and technology studies and international relations in which I ground this dis-

sertation. Subsequently, I will introduce main notions in this thesis and position them in relation to the object of study. Subsequently, I outline the research questions and the data and methods through which I seek to answer said research questions. Finally, I discuss the dissertations' contributions and highlight some of the main findings.

Setting the scene: Internet governance and its institutions

In contrast to earlier global communication networks like the telephone and the telegraph, the Internet infrastructure is not exclusively regulated by nation-states, nor is its international interoperation organized by the United Nations (UN). The setting of 'the rules of the road' (Wu et al. 2007) for the Internet is called Internet governance. It is performed by a variety of actors—corporations, states, researchers, and advocates—all engaged in a range of self-regulatory practices. These practices, which take place across a plethora of bodies, meetings, and events, set the norms that define the workings of the Internet infrastructure. In these ways, the technical, policy, and institutional norms that enable the world's largest information infrastructure are developed through extensive negotiations. Despite their profound influence on the lives of many, Internet governance institutions and practices are relatively unknown to many users of the Internet. Even within many governments, Internet governance is not a priority area. This also holds true for those that participate in particular Internet governance bodies: they might not oversee the whole field because of its distributed nature and complexity and variety of topics. Rather, the production and ownership of the Internet infrastructure is for the overwhelming part beholden to companies, who do not only own the infrastructure, but also hold the knowledge and expertise to operate it (Abbate 1999; Frischmann 2001; Van Schewick 2012; DeNardis 2009). This, in turn, puts smaller entities, institutions, and individuals with fewer resources, knowledge, exposure, and experience at a disadvantage in these discussions.

In this section, I will provide an overview of the main bodies for Internet governance and their respective functions. I will start off with the body that defines the processes and procedures for interconnecting all different networks and devices that make up the Internet. In order for computers and networks to be able to communicate, standard and non-obligatory ways of communication are defined. These manners of communication are called proto-

cols and standards. There is a dedicated body for the development of these protocols and standards: the Internet Engineering Taskforce. Next to agreed protocols, all networks that are interconnected through the Internet need a unique number. This is the purview of the Internet Corporation for Assigned Names and Numbers (ICANN), which assigns blocks of network and device numbers to different regions, and Regional Internet Registries (RIRs) (independent institutions of which there are five in the world), that delegate these numbers to independent networks, such as those operated by Internet service providers, transit networks, transnational corporations, and research institutions. ICANN also helps to coordinate the implementation of the Domain Name System (DNS), which functions as the telephone book of the Internet. The DNS links domain names (such as example.com) to numbering addresses, which are often called Internet Protocol (IP) addresses (such as 93.184.216.34). Altogether, the IETF, ICANN, and the RIRs have grown and developed in conjunction with the Internet and are fully dedicated to its coordination and operation. Because these bodies provide the bare minimum of technical preconditions for the Internet to function, these bodies are often understood as the core Internet governance bodies. This is why I will look at these bodies in-depth for this dissertation, starting by introducing other bodies that make up the field of Internet governance.

Other bodies set norms for the Internet, but are not exclusively dedicated to the governance and design of the Internet infrastructure, such as the Institute for Electric and Electronic Engineers (IEEE). The IEEE develops a wide variety of industry standards: ranging from power and electricity to biomedical and healthcare. The IEEE is relevant for Internet governance because it develops the specifications for most common standards for wired and wireless Internet access: WiFi and ethernet. There are also governance bodies that address subsections of the Internet, such as the World Wide Web Consortium (W3C), which sets standards for the web. There are also bodies that focus on particular subtopics, such as the Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG), which focuses on the protection against spam, malware, and viruses. Another kind of body is the Internet Governance Forum (IGF)—an annual meeting organized by the United Nations in collaboration with participants for the private sector, and civil society organizations (Malcolm 2008). The IGF is mandated to provide a platform to address Internet-related public policy issues, but it is not allowed to develop norms (Kummer 2007). There are also bodies that impact access to the Internet for many users, such as the 3rd Generation Project Partnership (3GPP),

which sets standards for mobile communications. In addition, there is the United Nations International Telecommunications Union (ITU), which sets standards for the international use of the radio spectrum and telecommunications.

In this dissertation, I will be focusing on the following bodies: ICANN, the IETF, and the Regional Internet Registry (RIR) that services Europe, West Asia, and the Middle-East, which is called Réseaux IP Européens (RIPE). A more elaborate discussion on the selection of the cases will then follow below in a separate section. In short, I focus on specifically these three types of bodies because they jointly perform the necessary technical preconditions for the Internet to function, and also because they fully focus on Internet governance. Looking at these three central and paradigmatic Internet governance bodies enables me to draw insights that apply to the whole field of private transnational Internet governance. However, before I elaborate on case selection, I will first outline what sets Internet governance bodies apart from other standards and governance bodies, and the role values and norms play in Internet governance.

Literature and intersections: science and technology studies, international relations, and Internet governance

To study the transnational communication network that is the Internet, I leverage theories and insights from science and technology studies and international relations. Whereas science and technology studies foregrounds the role of values, expertise, and collaboration in the shaping and development of infrastructure. International relations helps illuminate and theorize the role of norms, states, industry, and other actors in global governance. Jointly they help me to theorize the role of norms in the governance of a global infrastructure. Below I will introduce these two fields, the concepts that I will use in my analysis, and my contributions to the fields.

Science and technology studies and Internet governance

To critically examine values in the norm-settings processes in the infrastructure through its transnational governance, I build

on science and technology studies through concepts of 'ordering' (Jasanoff 2004), 'sociotechnical imaginaries' (Jasanoff and Kim 2015), and 'affordances' (Hutchby 2001). Science and technology studies provides the framework to understand internet governance 'as a normative "system of systems"' by examining 'the micro practices of governance as mechanisms of distributed, semi-formal or reflexive coordination, private ordering, and use of internet resources' (Epstein, Katzenbach, and Musiani 2016). These micro practices provide what science and technology scholars call 'ordering': a way of re-configuring society through the production of knowledge, institutions, and technology (Jasanoff 2004).

In my analysis, I build on the understanding of infrastructure that emerges from infrastructure studies and science and technology. Science and technology studies (STS) examines the interrelation between society, politics, culture, science and technological innovation. Infrastructure studies uses this science and technology notion to address the 'technical, social, and organisational [sic] aspects of the development, usage and maintenance of infrastructure in local communities as well as global arenas' (Bowker et al. 2009, 97). This helps researchers analyze how infrastructure is inherently entangled with practices—embedded in a social and political context, inherently processual, and relational. From this standpoint, the Internet infrastructure is the 'pervasive enabling resource in network form' (Bowker et al. 2009, 98) that makes the Internet work. Infrastructures are not simply erected or declared; they become infrastructural because people integrate them in their routines and come to rely on them. Infrastructures are thus in a permanent state of becoming because their ontology includes their own design and maintenance practices, as well as unintended use and demise. In other words, infrastructures ultimately are shaped 'in relation to organized practices' (Star and Ruhleder 1994, 256). Therefore, infrastructures in general, and specifically the Internet infrastructure, should be understood as relational, dynamic, and co-constituted through a wide range of practices. The relational perspective of the dialectic construction of the infrastructure overcomes the dichotomy between structure and agency in a process that Giddens calls structuration (Giddens 1984). This notion serves to explain how structure and agency take shape together in a process of infrastructuring (Pipek and Wulf 2009). This can be observed in the Internet infrastructure as well as in the interplay between institutions, materiality, economy, and the work of engineers and other experts. However, Giddens himself does not refer to infrastructure, but to institutions in gen-

eral. Therefore, what differentiates the institutions from infrastructure, is that infrastructure tends to become invisible and blend into the woodwork of society, instead of being reified as, for instance, the state.

The Internet infrastructure is not just the physical space of data centers, cables, routers, and wireless spectrum. It is also an archipelago of independent networks interconnected through numbering schemes that assign a unique number to every network and computer connected to the Internet, and a set of open protocols that connect the networks and devices together. The Internet infrastructure is also not solely of technical or material nature; trust relations between network operators that allow for interconnection and quick troubleshooting between networks (Mathew 2014) are also an inherent part of the Internet infrastructure. The institutions that facilitate coordination and the communication methods that are used to coordinate, such as mailinglists and virtual meeting tools, are also part of the Internet infrastructure. This means that all the choices, devices, configurations, relations, and characteristics that continuously shape the Internet infrastructure—and allow the Internet infrastructure to shape the lives of those who work on and with it—are inherently part of the Internet infrastructure.

These reconfigurations of society are often guided by sociotechnical imaginaries—collective visions of the future that help to construct group identities, narratives, policies, and institutions. Sociotechnical imaginaries help us comprehend how technologists are 'constantly trying to understand the present by borrowing from a cautiously imagined emergent future, filled with volatility, and uncertainty, but in which faith in practices of technoscience become even more complexly and interestingly constructed' (Marcus 1995, 2:4). Sociotechnical imaginaries guide the processes in which people co-create knowledge, technology, and order: a process that Jasanoff (2004) calls co-production because it emphasizes the collaboration among heterogeneous groups. In this process of co-production, the sociotechnical imaginary thus provides a particular ordering to society. This is in part through 'the work of innovators [which] is that of 'inscribing' this vision of (or prediction about) the world in the technical content of the new object' (Akrich 1992, 208).

The field of science and technology studies enables scholars to account for the material and non-material, alongside the human and non-human, that shape interactions, power, and society. It provides ways of studying large infrastructures, without losing

sight of the micro-practices that shape it (Star 1999; Bowker et al. 2009). Science and technology studies in general, and infrastructure studies in particular, allow scholars to understand how heterogeneous groups work together while having competing interests, and wildly varying specializations (Star 1990; 2010). Aside from understanding how things work, science and technology also provides insight into contestations and breakdowns (Sovacool, Lovell, and Ting 2018). This set of tools and theories thus allows me to engage with the complex mesh of collaboration that is the Internet infrastructure—that reportedly has the specific aim to prevent centralization power and control—exactly because it is an architecture of power and control (DeNardis 2014). While the governance of the Internet is distributed over different institutions, there are nonetheless 'chokepoints' (Tusikov 2016). This dissertation therefore questions how, in the governance of the Internet infrastructure, these points of control get shaped. To answer this question, I seek to open the 'black boxes' of complex, layered, and distributed networking technologies. That is, I look at the design, negotiation, implementation, and maintenance processes through which Internet governance is shaped. Even more so, I examine the role norms play in this process. By looking at the combination of institutions, practices, and processes, I shed light on this larger governance infrastructure of power and control as these are disseminated, facilitated, and shaped through the global communications infrastructure that is the Internet.

This dissertation contributes to the field of science and technology studies by enriching it with quantitative methodologies, and cross-body case studies that allow me to recognize and theorize emerging patterns, that might not have been obvious from looking at micro-practices in isolation. However, science and technology studies has also been criticized for its preference for and reliance on descriptions,and its refusal to take into account attributes of complex social relations. This thus means that science and technology research does not account for concepts like economic pressures, community norms, and institutional values. By using such a flat ontology, processes of sense-making and meaning-making risk being overlooked (Couldry and Hepp 2018). Complex power dynamics also might not be clearly delineated by the blurry borders of individuals, groups, institutions, and technologies (Callon 1990). However, by bringing science and technology studies in dialogue with quantitative methodologies from computational sociology and theoretical frameworks from international relations, I further the empirical analysis of macro-structures of power in science and technology studies. This contribution could

increase the field's relevance by informing policy and societal debates on the development and role of governance of technology in society.

International relations and Internet governance

International relation scholars have generally focused on the role of the state in the governance of the infrastructure (Chadwick 2006; Deibert 2008); the use and leveraging of the Internet infrastructure by the state to reach policy goals (Musiani et al. 2016; Arpagian 2016) and its use as a tool for repression (Gohdes forthcoming) by authoritarian states (Glasius and Michaelsen 2018). I start with the understanding that infrastructural power (Mann 1984) emanates from the state and subsequently 'diffuse[s] outwards from the particular power organizations that invented them' (Mann 1984, 194). Without a centralized means of control, infrastructural power still provides the ability to exert power. International relations has theorized different means of governance influence by the state, even in the case where the state is not the sole governing body. The discussion of these forms of private governance have taken a flight in international relations, in part because global governance is under pressure (Dingwerth et al. 2019), and some even argue that global governance is in crisis (Coen and Pegram 2018). Since the early 2000s, it has been recognized that private distributed governance bodies are a component of modern governance structures (Flinders 2004).

Where some observe that '[i]nstitutional reform processes have halted, new processes have a hard time gaining traction' (Albright and Gambari 2015, 7), Internet governance is still a dynamically evolving practice. Internet governance is a form of private rule-making but is by no means decoupled from public authority (Porter and Ronit 2006). Governments do have influence, not solely by setting norms through state-informed and state-embedded institutions at the national level that subsequently permeate to the international arena (Weiss 2018), but rather through direct participation and interfacing with Internet governance institutions. One can, however, debate whether the impact of governments in the current configurations of transnational Internet governance is significant. Early analysis of the interrelation between the state, digital infrastructures, and power emphasized the relationship between the legal and the technological materiality, most famously captured in the adage 'code is law' (Lessig 2006). The systemic analysis of the interrelation between the state, technological infrastructure, law, and public values led to the analysis

of how this changed all parts involved (Braman 2009). There is thus a continuous debate on whether digital technologies change the structure and role of government (Easterling 2014; Susskind 2018), or whether the Internet infrastructure has been a tool of, mostly Northwestern, governments to assert power and control (Turner 2006; Carr 2015).

The Internet infrastructure is designed, standardized, developed, and regulated in distributed bodies that together form the Internet governance regime (Mueller, Mathiason, and Klein 2007; Bradshaw et al. 2015). A regime produces 'sets of implicit or explicit principles, norms, rules and decision-making procedures around which actors' expectations converge in a given area of international relations' (Krasner 1982, 186). Because of the distributed nature of the Internet governance ecosystem, Dutton and Peltu call it an Internet governance mosaic (2007, 63), Nye refers to it as a 'regime complex' (2014), while Radu terms it a 'multi-institutional Internet governance bricolage' (2019, 156), Scholte calls it a case of 'polycentric governance' (Scholte 2017b, 166). Instead of one particular institution demarcating the boundaries of the field and delineating the unit of analysis, it is the locus of governance that thus far has defined the scope of the regime. Within the transnational Internet governance regime complex, one can differentiate between private Internet governance bodies, sometimes also called 'multistakeholder Internet governance bodies' and 'multilateral Internet governance bodies'.

In this dissertation, I have chosen to focus on private and open Internet governance bodies—what I call the 'private Internet governance regime'. These bodies contrast with closed Internet governance bodies, or Internet governance bodies in which only states have a formal say, which make up the multilateral Internet governance regime. However, in the conclusion I will functionally delineate these two regimes that make up the transnational Internet governance regime complex by providing a functional description based on the infrastructural norms that characterize these regimes.

Whilst many of the bodies in Internet governance are open for participation—often called 'multistakeholderism' (Raymond and Denardis 2015) or the 'multi-stakeholder model' (Hill 2014, 16; Hofmann 2016)—the distributed feature presents some challenges for participation. That is, it takes serious investments in terms of time, expertise, financial resources, and accumulated social capital to participate in the norm development processes in

these institutions—let alone organizing representation and coordination among the whole breadth of the ecosystem. This has caused scholars such as Carr to argue that 'rather than disperse power to a wide range of actors, multistakeholderism reinforces existing power dynamics that have been 'baked in' to the model from the beginning' (Carr 2015, 658), favoring the private sector and particular states. What is described by Internet governance practitioners as bottom-up industry self-regulation (Sowell 2012), Scholte describes in a particular case as a 'complex hegemony' of a capitalist market ordering, a global governance elite, and the United States Government (Scholte 2017a). This regime, according to Scholte, is legitimated through discourses around technical resiliency, multistakeholder participation, market efficiency, and human rights (ibid.).

Recent steps towards increasing globalization of the Internet governance regime—such as the relinquishing by the United States of its stewardship over ICANN (discussed in Chapter Two)—can be interpreted as a case of orchestration, which is also understood as the governance through intermediaries (Abbott et al. 2015). But transnational Internet governance does not seem to be a consistently reliable instrument for representing the interests of specific states nor function like a stable policy instrument: not even for the United States (Rogers and Eden 2017) or the European Union (Perrin 2018). Therefore, it is not obvious to describe the transnational governance regime as a clear case of orchestration, or a governance instrument in the shadow of hierarchy (Scharpf 1994; Héritier and Lehmkuhl 2008; Nederhand, Bekkers, and Voorberg 2016). This is in part due to the complex international entanglements and interests as well as the strong institutional and regime identities that have developed since the privatization and the commercialization of the Internet in the early 1990s (Frischmann 2001). This was facilitated by the relative independence the Internet has had from direct governmental influence, which has been an inherent part of the identity of the private Internet governance regime since the rejection of government oversight over Internet standards (Abbate 1999; Russell 2006; DeNardis 2009). Overall, transnational private Internet governance is too structured and proceduralized to compare it to governance architectures that are described using the lens of open methods of coordination (Regent 2003; Szyszczak 2006): Internet governance participants are regularly found to be adamant about following existing practices and procedures, and not expanding scopes or methods.

Recent studies have examined the Internet infrastructure as an instrument for the reproduction of asymmetries in terms of both power and information (Rosa 2019), as well as a tool for extraterritorial projections of state power (Deibert and Pauly 2019). These questions of power and control have become more pertinent because of the growth of the influence of the Internet governance regime complex on other regimes, which some have even called the 'metastization of the global cyber regime complex' (Raymond 2019), taking place because of the penetration of 'the Internet in everything' (DeNardis 2020). This leads to overlapping regimes between, for instance, consumer protection, national security, intellectual property, and Internet governance. Ultimately, because there are no clear accountability structures and little to no inter-jurisdictional rules for complex trans-border data streams, the standards that undergird the data streams and their foundational infrastructure have the potential to impact and shape regimes beyond the transnational Internet governance regime complex.

I build on the field and frameworks of international relations by analyzing the distributed regime of Internet governance through the lens of global governance and I bring it in conversation with science and technology studies, to carefully analyze the micro-practices and cross-institutional design that makes Internet governance a governance innovation (Verhulst et al. 2014). Based on the analysis in this dissertation, I make two contributions to the field of international relations. Firstly, I showcase how norms shape distributed infrastructure governance and tie it together. With this, I contribute to the significant body of norm theory in constructivist international relations by showing how it applies to a different empirical field, and the role technology and institutional design play (Kelley 2008; Gilardi 2012). I build on the classic work by Finnemore and Sikkink (1998) that describes the process of norm emergence, norm cascade and norm internationalization, and combine it with theories on norm conflict and norm competition (Kelley 2008). Norm theory in international relations still largely focuses on the role of states and intergovernmental bodies; therefore, a detailed application of norm theory to a case of private regulation in a distributed governance model of a distributed transnational infrastructure, as seen in Chapter Four, could help with extending its applicability, and contribute to norm theory in Internet governance (Mueller, Mathiason, and Klein 2007). Secondly, I apply the framework of metagovernance. Metagovernance is the control that is being exercised in distributed or decentralized decision-making processes through the use of

norms, values, and standards (Kooiman and Jentoft 2009). Scholars also describe metagovernance as 'regulated self-regulation' (Torfing 2016, 527). Metagovernance is a concept that stems from international relations, first applied to Internet governance by Sandra Braman (2020). Metagovernance allows me to showcase how the combination of governance through norms and institutional design can be understood as sources and tools of metagovernance or 'regulated self-regulation' (Torfing 2016, 527). Norms, institutional design, and the 'mobilization of bias' (Schattschneider 1975, 71) are all examples of tools that can be used in the practice of metagovernance (Sørensen and Torfing 2009). Metagovernance can be exercised by public or private actors that can, but do not have to be part of the regime or arena that they seek to metagovern (Torfing 2016).

I use the lens of metagovernance (Jessop 1997) to frame emerging gover-nance practices that supersede particular Internet governance bodies and tie the different case studies together. This notion helps guide the examination of norms, hierarchies, and relations, in and among different governance regimes that jointly form the Internet governance regime complex. In the conclusion of this thesis, I will thus use the lens of metagovernance to functionally identify and differentiate between the private and multilateral Internet governance regime, based on their respective infrastructural norms. To approach the global Internet governance regime complex, I will use the following definition: transnational Internet governance is the development, coordination, and implementation of policies, technologies, protocols, and standards, aimed at producing a global and interoperable Internet, functioning as a general-purpose communication network, in transnational governance bodies such as ICANN, the IETF, and RIRs.

Metagovernance allows us to analyze, and functionally differentiate the private and multilateral Internet governance regimes that jointly make up the transnational Internet governance regime complex. Furthermore, it allows for the accommodation and theorization of the interrelation of the Internet governance regime complex with different regimes in the case of the metastization of the Internet. This is where Internet governance, due to the permeation of the Internet with society, touches upon different regimes such as consumer safety, national security, and human rights. Metagovernance thus promises to be a fruitful lens for the current analysis of the use of norms to exercise power and control in the distributed governance of the Internet. This includes future analysis of the interrelation of the Internet governance regime with other regimes:

ranging from security regimes– as can be observed in the many cybersecurity discussions—to the human rights regime (Kulesza and Balleste 2015).

Bringing together science and technology studies and international relations literature through their focus on Internet governance reveals their shared focus on the role of imaginaries, values and norms in Internet governance. The distributed governance structure of the Internet reflects a particular visions of the design of the physical Internet infrastructure. Its design process reflects particular values and is steered by norms about how to enact these visions and values. This requires a discussion of the current literature on sociotechnical imaginaries, values and norms in which I draw together thus far unconnected insights from science and technology studies and international relations to showcase their joint role in the global governance of the Internet infrastructure.

Sociotechnical imaginaries, values, and norms in Internet governance

A significant part of the work done in Internet governance processes is the development of technical norms that define the shape and characteristics of data streams that interconnect independent networks. The process through which these norms are developed is facilitated through norms that take the shape of rules and procedures, and values that reflect ideas about how the Internet infrastructure *should* work. Jointly, they produce a vision of a future, a sociotechnical imaginary of the Internet infrastructure, that allows different groups to work together on the continuous reconfiguration of the Internet architecture. In the following sections I will further elaborate on these three concepts and their interconnection.

Sociotechnical imaginaries

Sociotechnical imaginaries help create understanding regarding how experts and policymakers from different fields work together and spend time and resources to make a shared vision a reality. After all, the Internet would not have been possible without enormous public investments. What started as a Cold-War military project by the United States in response to the launch of Sputnik satellite by the Soviet Union (Abbate 1999), was in the 1990s advertised as the technological revolution of the informa-

tion superhighway by vice-president Al Gore, while in practice it was mostly used by the scientific community for interaction and cooperation (Flichy 2007). Sociotechnical imaginaries, however, are not only visions— they bring together the 'social' and the 'technological' and are 'descriptive of attainable futures and prescriptive of the kinds of futures that ought to be attained' (Jasanoff, Kim, and Sperling 2007, 1).

To produce the Internet, a lot of different groups, with widely different backgrounds, knowledge, and interests need to work together. Their collaboration is facilitated by a joint vision for the future: a sociotechnical imaginary for the Internet. While the development of the sociotechnical imaginary of the Internet has been studied and documented in detail (Turner 2006; Flichy 2007), there has been less attention for the sociotechnical imaginary of the governance of the Internet infrastructure.

The Internet infrastructure governance sociotechnical imaginary revolves around doing things that are 'for the good of the Internet' (Mathew 2014, 160), where what is good for the Internet is often understood as sustaining a 'generative' (Zittrain 2008, 6), multi-purpose network, with a global reach (Internet Society 2012). The production of this global communication network should happen through a paradigm of openness (Internet Society 2013) that is intertwined with the 'ideology of open standards' (Russell 2014, 21). In this dissertation, the Internet governance sociotechnical imaginary consists of the visions of the future Internet infrastructure that is anchored the in norms and values that facilitate Internet governance processes by enabling different stakeholder groups to work together.

Norms

There is no central authority in the private Internet governance regime, and the standards that are produced are largely voluntary. Therefore, Internet governance is a norm-setting regime rather than an authoritative rule-setting one. The norms that are produced in Internet governance are (by and large) not legally binding. Even if they are, their enforceability is often a challenge. This is in part due to the transnational nature of the Internet that encompasses many jurisdictions. Therefore, in order to theorize the relationship between norms and values, I build on theories of norm conflict from international relations (Finnemore and Sikkink 1998; Thomas 2001; Hurrell 2002).

Norms are 'widely-accepted and internalised [sic] principles or codes of conduct that indicate what is deemed to be permitted, prohibited, or required of agents within a specific community' (Erskine and Carr 2016, 87). Norms regulate dynamic and transnational systems such as the Internet by creating expectations without prescribing specific behavior. The application of general norms in particular concrete situations is delegated to individual agents (Okuyama, Bordini, and da Rocha Costa 2011). This therefore makes norms useful for governing a distributed infrastructure. According to Marini (2000), a norm is an evaluative description of acceptable behavior. It defines what one ought to be or do, or not to be or do. In order to study how specific norms are accepted, subverted, and resisted in the governance of the Internet infrastructure, I build on the notion of 'norm conflict' using the definition provided by Hilpinen (1987, 37): 'norm conflict occurs when the person is subject (by the normative system) to several requirements which cannot be simultaneously satisfied'.

Values

Values share similarities and distinctions with norms. Like norms, values are group-level phenomena based on shared agreement. Values, however, do not describe what is allowed or not allowed and thus do not provide an evaluative description of desirable behavior, but rather what *is* desirable. In the words of Hitlin and Piliavin,'norms capture an "ought" sense; values capture a personal or cultural ideal. People acting in accordance with values do not feel pushed as they do when acting under normative pressure.' (Hitlin and Piliavin 2004, 361). Applied to Internet infrastructure and its governance, this means that technical artifacts can reflect social values (Winner 1980; Friedman and Hendry 2019). This is also true for technical norms, such as Internet standards. Ergo, technical norms can reflect specific values (van Wynsberghe and Moura 2013). Simultaneously, through their enabling or containing characteristics, technical norms can also reflect social or legal norms, such as human rights (Brown, Clark, and Trossen 2010).

What sets Internet governance bodies apart from other traditional standards and governance bodies is that they allow for open participation and decision making, meaning that a wide range of actors can participate. Whereas in the governance of previous global communication networks—such as the telegraph and the telephone—only governments had an official say through

the ITU, one of the oldest bodies of the UN. At several moments in the history of the Internet, intergovernmental governance bodies such as the International Standards Organization (ISO) and the ITU have sought to gain more influence over the Internet infrastructure (Abbate 1999; Russell 2006; Shackelford et al. 2015), in a similar way to how governments have governed and shaped previous communication infrastructures. These attempts have been resisted (DeNardis 2009; Russell 2006) by other parts of the so-called 'Internet governance regime complex' (Nye 2014). These standoffs instilled and strengthened a strong sense of identity and values among participants in Internet governance bodies. Many of these values revolve around the perception of a lack of centralized control and the liberty to deploy new technologies. Whereas governments used to have the final say in the standardization of previous communication networks, the Internet is built upon voluntary standards that are developed through bottom-up industry self-regulation (Sowell 2012), a process also regularly called 'multistakeholder Internet governance' (Raymond and Denardis 2015). This is an important starting point for the investigation into norms and values in the governance of the Internet infrastructure, because values such as openness, permissionless innovation, and the lack of centralized authority are often mentioned as main characteristics of both the Internet as well as its governance. For example, such values enable the ability to develop and deploy one's own protocols without having to ask a network operator or equipment vendor for permission. They also give individuals the ability to freely participate in Internet governance processes, without having to be a representative of a state or company, nor a member of a specific club. This tendency can even be recognized in the distributed architecture of the Internet and its governance regime, which seeks to prevent centralized decision making and control. The IETF makes this clear through its mission statement:

> *The Internet isn't value-neutral, and neither is the IETF. We want the Internet to be useful for communities that share our commitment to openness and fairness. We embrace technical concepts such as decentralized control, edge-user empowerment and sharing of resources, because those concepts resonate with the core values of the IETF community. These concepts have little to do with the technology that's possible, and much to do with the technology that we choose to create.*
> (Alvestrand 2004)

At first glance, the private Internet governance regime seems quite value-laden. One could even argue that these shared values are what enable these experts from different backgrounds, such as governments, industry, academics, and civil society organizations, to work together on the design and evolution of the Internet infrastructure. However, at the same time, the Internet infrastructure and its governance processes are also used to enable censorship and surveillance (Musiani et al. 2016; Rogers and Eden 2017), for instance through the standardization of protocols with inadequate encryption methods. Whereas this would seem to be at odds with the values of openness, fairness, and sharing of resources. To explore this apparent contradiction, I now provide an overview of current debates about particular Internet governance norms, such as human rights.

Human rights and freedoms

Considerations about the political and policy impact of the Internet infrastructure have been part and parcel of its development since its early beginnings (Braman 2011), demonstrating that 'politics are not external to technical architecture' (DeNardis 2009, 10). This, however, is not widely recognized or structurally addressed within the private Internet governance regime, even though calls to consider that '[s]eemingly narrow technical choices can have a broad and lasting impact on public policy and individual rights' (Davidson, Morris, and Courtney 2002, 1) have been made since the early 2000s. These calls have included proposals for structural 'policy impact assessments' (Morris and Davidson 2003, 1). Since then, calls have been made—by influential Internet engineers, among others—for the Internet infrastructure to 'accommodate the tussles of society while continuing to achieve its traditional goals of scalability, reliability, and evolvability' (Clark et al. 2005, 348). This reiterates that 'the debate over network protocols illustrates how standards can be politics by other means' (Abbate 1999, 179). A report by the Council of Europe states it even more clearly by saying that 'ICANN's policies and procedures can have an impact on a broad range of internationally recognized human rights' (Zalnieriute and Schneider 2014, 50). A common response from actors that participate in the transnational Internet governance regime is that Internet governance bodies should stick to their limited technical remit (Jørgensen, Veiberg, and ten Oever 2019; Cath 2019). This has led to scholars arguing that 'some key, universal values—of which the UDHR [Universal Declaration

of Human Rights] is the most legitimate expression—should be baked into the architecture at design time' (Brown, Clark, and Trossen 2010, 3), or call for 'technical engineers that act as custodians for human rights' (Cath and Floridi 2017, 465). However, human rights are not the only norms that are discussed in the literature, nor were they the first. Ethnographic work by Mathew (2014) locates political power in the Internet infrastructure in the trust relations between network operators, that 'run across corporate and state boundaries' (Mathew 2014, 2) who jointly work with 'the social values of "freedom' and 'democracy" […] in mind, 'for the good of the Internet"(Mathew 2014, 3). Others emphasize the influence of economics on the governance of the information infrastructure. Meier-Hahn argues that the 'economics of convention' (Meier-Hahn 2014) in Internet governance enables competitors to work together. Others emphasize the shaping factor of market forces on the Internet infrastructure (Lessig 2006; Mueller, Kuerbis, and Asghari 2013). Moreover, others point to the importance of the technological materiality of the Internet infrastructure when seeking to explain the uptake of norms (Dourish 2018).

In short, a wide variety of scholars from anthropology, sociology, science and technology studies, and international relations, have studied the impact of the governance of the Internet infrastructure on rights and freedoms (Lessig 2006; DeNardis 2009; 2014). There has thus been ample discussion around the values of early Internet developers (Hafner and Lyon 1998; Abbate 1999; Levy 1996; Turner 2006; Flichy 2007), and the way the Internet infrastructure is leveraged to achieve governance aims (Musiani et al. 2016). Because of this, and the increasing influence of the Internet infrastructure on society, scholars have asked whether social norms and values should be inscribed by means of Internet governance (Clark et al. 2005; Cath 2019), and if so, how this should be done (Cath 2015; Cath and Floridi 2017; Brown, Clark, and Trossen 2010). However, so far there have been limited systematic studies into how social and legal norms and values get inscribed in the Internet infrastructure by means of transnational Internet governance.

Research Design

In the following section I will introduce the research design of this dissertation by introducing the research questions, case selection, my positioning, and the methods I used to operationalize the research.

Research Questions

In this dissertation, I seek to answer: what is the role that norms play in the process of the distributed private governance of the transnational Internet infrastructure? In order to answer this question, I ask four different subquestions that each are answered in a separate chapter of this dissertation.

In Chapter One, I seek to answer the first subquestion: how do norms in Internet governance evolve? To answer this question I, together with my co-author, investigate the evolving sociotechnical imaginaries of a particular group of actors engaged with Internet governance in ICANN from 2002 up to 2016 through a combination of quantitative mailinglist analysis, participant observation, and qualitative discourse analysis (Milan and ten Oever 2017). The chapter shows, by adopting a science and technology lens, how new ideas emerge through political opportunities and the influx of new participants in the groups, which iteratively results in changing discourses, frames, agendas, and norms. This, in turn, led to different approaches of this group in the institutional design of ICANN and the Internet infrastructure. This chapter helps to develop understanding how political opportunity and changes in participation help to evolve norms among those engaging in Internet governance.

In Chapter Two, I seek to answer the second subquestion: how are norms inscribed in Internet governance? In order to answer this question, I build on the conclusions of the previous subquestion, by analyzing the same group of Internet governance participants as they engage with other groups in ICANN to inscribe human rights in the organization's bylaws. I did this by engaging in participant observation, quantitative mailinglist analysis, and discourse analysis. This chapter shows how a political opportunity brought by different groups engaging together in a consensus-building process fueled by different interests and experiences—but bound together by a joint concept and objective—can lead to the acceptance of a new norm and the institutional re-design of ICANN in the form of a new bylaw.

In Chapter Three, I seek to answer the third subquestion: how are norms subverted in Internet governance? In order to answer this subquestion, I engaged in the analysis of widely shared norms and values in the IETF through participant observation, quantitative mailinglist analysis, discourse analysis, and semi-structured interviews. This foregrounded the importance of a specific set of architectural norms that jointly anchored an sociotechnical imag-

inary that facilitates norm-setting in this standards body. While investigating this set of norms by closely examining their role in the development of new norms in the IETF, it turned out that the professed sociotechnical imaginary, and the norms in which it is anchored, was side-lined in a process of contestation between network operators and equipment vendors on the one-hand, and providers of content and services on the other. While the professed sociotechnical imaginary provided legitimacy to the regime and its institutional design, it was actually being subverted in the process of the development and standardization of new technical norms.

In Chapter Four, I seek to answer the fourth subquestion: how is the introduction of norms resisted in Internet governance? This final subquestion builds on the findings from the previous chapters and seeks to increase the applicability of the findings that emerge from them through an experiment. To answer this question I engaged in an exploratory experiment in which I proposed the introduction of a legal and social norm in the Internet infrastructure, by means of its governance in RIPE. The experiment took the form of an ethnographic probe, which allowed me to capture the responses to the introduction of the probe by the RIPE community, which largely consists of network operators, by mailinglists analysis, participant observation, document and discourse analysis, as well as semi-structured interviews. This helped further the findings of the earlier chapters to contribute to a theory of normative governance and the use of norm conflict to reject the introduction of norms that are at odds with entrenched prevalent norms.

Through engaging in case studies in a range of different governance bodies that are central to and paradigmatic for the Internet governance regime, I answered these subquestions in order to then answer my main research question. The chapters both focus on the different roles that norms play in Internet governance, but they also iteratively build on the insights gained from the previous chapters. Together they form the foundation for a theory of norm-setting in Internet governance. All chapters compare the role of norms in the different governance bodies. Moreover, the consistent findings across Internet governance bodies allow me to build a theory of norm-setting in Internet governance, whilst findings in singular bodies provide venues for the development of new hypotheses and further theorization. The chapters thus ultimately show the role of norms in facilitating and providing legitimacy to Internet governance's regime, their role in facilitating collaboration among participants, and their role in subverting, resisting and rejecting norms that might endanger prevalent and entrenched norms.

Every chapter has been previously published or submitted as an academic article to an international peer-reviewed journal. The first chapter is co-authored with Dr. Stefania Milan and appeared as 'Coding and Encoding Rights in Internet Infrastructure' in *Internet Policy Review* (Milan and ten Oever 2017). The second chapter appeared as 'Productive Contestation, Civil Society, and Global Governance: Human Rights as a Boundary Object in ICANN' in *Policy and Internet* (ten Oever 2018). The third chapter has been accepted for publication as "This is not how we imagined it'—Technological Affordances, Economic Drivers and the Internet Architecture Imaginary' and will be published in 2020 by *New Media & Society* (ten Oever 2020). The final chapter, called 'Norm conflict in the governance of transnational and distributed infrastructures: the case of Internet routing' is currently under peer-review with the academic journal Globalization. All accepted and published articles have passed peer-review by internationally acclaimed academic journals.

Case Selection

To answer my research questions and to be able to make a contribution to the understanding of the field of Internet governance, my case study research covers three different Internet governance bodies: ICANN; the IETF; and the RIR for Europe, West Asia, and the former USSR, called RIPE. I selected these bodies because they are typical cases of Internet governance bodies, and can be understood as typical and representative cases for Internet governance bodies (Gerring 2007; Seawright and Gerring 2008). As described earlier, there are other bodies, and categories of bodies, that contribute to Internet governance. However, the development of the protocols, and the coordination and delegation of naming and numbering together provide the necessary technical preconditions for the Internet to function, and these functions are performed by IETF, ICANN, and the RIRs. Whilst other bodies also perform important functions, especially concerning interfaces to the network, the roles of the aforementioned bodies is the coordination of the essential technical preconditions for the Internet to function. In other words, the functioning of the Internet as we know it today would be significantly impaired without these bodies and the functions they perform. I argue that the role of standard-setting, the coordination of unique names and numbering resources, and the distribution of these numbers to independents networks are the core functions of the Internet governance regime, and these are performed by the IETF, ICANN, and the RIRs. In order to be able to make a generalization about the

Internet governance regime, one thus needs to examine these different bodies and functions.

From the five RIRs that currently exist, I selected RIPE because it is the oldest institution among the RIRs, and the RIR with the most active community measured by the amount of email traffic on their mailinglists over time, which is an indicator for the amount of deliberation on norm-setting and norm-conflict. ICANN, IETF, and RIPE are similar in the sense that they allow for open participation, which is not true for many other bodies as they either require a membership or are limited to specific stakeholders. However, the most important bodies in the private Internet governance regime do allow for open participation. Thus, I have focused on ICANN, the IETF, and RIRs as they allow for participant observation during their meetings and on their mailinglists. Moreover, they also provide access to ongoing discussions, archives, and outcome documents.

Internet governance does not solely take place in governance institutions. Rather, there are also other policy development and reflexive coordination practices outside of governance bodies (Hofmann, Katzenbach, and Gollatz 2017):, for instance, through national or private regulation, or one-off meetings such NetMundial. However, the advantage of studying Internet governance bodies over singular meetings or events and private regulation, is that the study of Internet governance bodies allows researchers to have a stronger sense of the evolution of the participants involved in these bodies, as well as their norms, positions, and interactions. This is not only because of their open character, but also because of the open and often standardized nature of their archives. While not all Internet governance practices take place in Internet governance bodies, the effects of Internet governance practices are often felt, discussed, and responded to through Internet governance bodies.

Even though the study of the governance of the Internet infrastructure is an inherently interdisciplinary field (Hofmann, Katzenbach, and Gollatz 2017), scholars often choose in their analysis to either focus mainly on the affordances—the 'constraining, as well as enabling, materiality of artifacts' (Hutchby 2001, 441)— of the institutional ordering, the technological materiality of infrastructure, its political economy, legal regulation, the analysis of imaginaries and discourses, or on case studies of particular practices. In my study, I aim to contribute to an interdisciplinary research agenda by connecting and building on theoretical lenses from

science and technology studies alongside international relations, and methodologies that have their roots in anthropology, and digital and computational sociology. With this, I seek to contribute to theory-building that takes into account different kinds of orderings and contributes to both academic and policy debates.

Positioning

To explain why I operationalized a combination of specific methods, I will first explain my position in the field, because my own knowledge and meaning-making is the result of my embeddedness in the field (Haraway 1988). By working with free and open-source software as an activist-hacker, I got introduced to the documents that for a long time I considered as the 'Bible of networking': namely the documents produced by the Internet Engineering Taskforce, called Request For Comments (RFCs). When I started working as Head of Digital for the international freedom of expression organization ARTICLE19, which lasted from 2014 to 2018, one of my first assignments were to further investigate the processes through which RFCs and the Internet infrastructure were produced. The initial steps of this investigation were easier than I expected, because I was able to join the mailinglists and meetings of the body that produced these documents.

Openness and transparency are often professed characteristics of transnational Internet governance, and reports and transcripts of meetings are carefully archived going back to the late 1960s. Similarly conversations that are largely conducted through mailinglists have been publicly archived. Next to that, the overwhelming majority of transnational Internet governance meetings are publicly accessible, both for participants and observers. It was therefore these mailinglists and meetings formed the entry point for my participation. It took, however, at least a year before I was able to orient myself within these tight-knit communities that communicate with a very high acronym density following many written and unwritten rules and procedures, which are also often the subject of debate. These acronyms, the tight-knit community, and dynamic rules and procedures allow epistemic communities from different backgrounds to work together, but at the same time, can form quite a hurdle for new participants. It thus took me several more years to understand the complex relations between different stakeholders and interest groups in an environment that some have described as 'a flying circus', due to the many meetings that take place in hotels and conference venues around the globe (Drake 2011).

Methods

The work and data gathering for this dissertation started as with my professional engagement with the field, which later transformed into participant observation. In this period, which started in March 2014 and ended in December 2019, I participated in 11 IETF meetings, 11 ICANN meetings, 4 IGF meetings, and 2 RIPE meetings, each of them lasting for roughly a week. Next to that, I participated in over 100 hours of videoconferencing sessions and many email list discussions. During this period, I also took up active roles in the field of Internet governance, that went beyond the role of participant. The reasoning for doing so is twofold: on the one hand it provided me with more access and deeper understanding of the community; on the other hand, it allowed me to give back to the communities I was researching. In these years I served as; the co-chair for the Human Rights Protocol Consideration Research Group; member of the Internet Research Steering Group; editor of 'the Tao of the IETF' (ten Oever and Moriarty 2018);, member of the Education, Mentoring and Outreach Directorate of the IETF; and rapporteur for the Cross Community Work Group on Enhancing ICANN's Accountability Subgroup on Human Rights during Work Stream 2. Fulfilling these roles provided me with access to conversations and corresponding insights that I otherwise, as a mere participant, would not have acquired. I have therefore significantly benefited in terms of access and understanding, both in and of the field, that years of professional engagement with the field have provided me. I thus designed my research in a way so I could foreground, reflect, and address possible prejudices in my gathering and analysis of data. Ultimately, through sequentially combining a variety of methods, I have sought to validate my intuition, data, and analysis.

I engaged in participant observation and semi-structured interviews, which I have subsequently transcribed and thematically coded (Guest, MacQueen, and Namey 2012). I also engaged in the thematic coding of technical and policy documents. Aside from qualitative methods, I also engaged in the quantitative analysis of technical and policy documents, as well as mailinglist conversations by operationalizing statistical, network, and discourse analysis to foreground the prevalence and evolution of norms, using the programming languages Python and R, and the BigBang toolkit[1]. In my analysis of mailinglists I solely used data from publicly archived mailinglists that exist for the explicit purpose of policy making, and are hosted by the Internet governance bodies. This way I made sure that the people that had engaged on these mailinglist had agreed with the policies of these lists for Internet

1 https://datactive.github.io/bigbang/ accessed on October 31st 2019

policy making, that clear privacy policies were in place, and that the participants had a reasonable expectation of their levels of privacy. I, however, chose not to cite names or email-addresses obtained from these lists.

In my final chapter I made use of an ethnographic probe to foreground existing habits and practices of participants in an Internet governance body. When I introduced the ethnographic probe, and during my participant observation, I made sure that I clearly communicated my role as an academic researcher and made it explicit that the probe and my participation was an inherent part of my research. When I engaged in individual semi-structured interviews, participants received an information sheet and signed a consent form. Both these documents have been reviewed by the ethics board of the DATACTIVE research group at the University of Amsterdam. To protect the identity of the participants, the names of the interviewees are not listed. Every interviewee has been assigned a code that can be found with every quote in this dissertation. I also maintained a physical log of all interviewees and their corresponding code that is, together with the transcripts, in the possession of my supervisor. This log with corresponding codes, however, will be destroyed on December 1st, 2021, in conformity with the General Data Protection Regulation.

I will provide an example on how I combined the different methodologies in my analysis. My analysis in Chapter One was based on my observation that American veterans of Internet governance emphasized the importance of freedom of speech and privacy, whereas advocates working for international not-for profit organizations tended to focus on corporate accountability, which expanded the topics of focus to include cultural rights and the right to association. In my quantitative analysis of the mailinglists of one group of activists in ICANN, I was able to analyze the same evolution in discourse. The qualitative analysis of the mailinglists, made it possible for me to attribute this to the influx of new cohorts of international actors, that diversified the initially mostly American group. Finally, I was able to link the influx of new participants with political opportunities presented by ICANN. Thus, I could combine quantitative and qualitative analyses to pursue my initial intuitions then systematize the findings. In addition, I have also discussed my findings at length with both academics and practitioners in the field, and where possible have used public sources, documented my methods, and made my analytical tools available. This furthers both approaches in digital sociology and the sociology of the digital by providing qualitative ways to analyze the quantitative and

vice versa. This approach facilitated the triangulation of my findings as well as theory building on emerging and possible future knowledge and governance frameworks (Marres 2017).

Outline of chapters

My first chapter and case study focuses on norm evolution. In particular, it examines the evolution of the norms and sociotechnical imaginary of a particular group of participants in the Internet governance body ICANN, namely the Non-Commercial User Constituency. I have been part of this group and thus my data gathering started during my professional engagement with this community, which provided some initial research intuitions about the different norms that existed within this group. To create some distance between my intuitions and the data gathering process, I developed a hypothesis, namely: three different cohorts of civil society spurred the iterative evolution and emergence of explicit values which they sought to wire into the infrastructure and institution of ICANN. Subsequently I developed a quantitative method to verify this proposition. Through the use and further development of the mailinglist analysis tool BigBang, I was able to confirm a relationship between changes in discourse with an influx of new participants. Qualitative analysis of the mailinglists and documents provided further support for this proposition and allowed for a more detailed explanation, because it showed that the new participants in new cohorts formed their own categories, which aligned with the language evolution that they brought about. Further document analysis then allowed me to correlate the topics that were discussed with changes in ICANN, which explained the reason for the influx of the new cohorts.

My second chapter and case study focuses on norm inscription; in particular, the inscription of human rights norms in ICANN's bylaw. For this, I changed my field of focus from the Non-Commercial User Constituency in ICANN, to a process that had cross-community involvement, namely the Cross Community Working Group on Enhancing ICANN's Accountability during Work Stream 1, and several of its subgroups. I was an active participant in the process and thus knew the content of the discussions on the mailinglists and policy documents on this process intimately. I waited with my analysis until the process I would be analyzing was finished. I started off with a quantitative analysis of the mailinglists to understand the networks and role of actors within these discussions—focusing on word trends, but especially focusing

on how concepts travel between communities and the role of specific actors in that process. For this, I used descriptive analysis, network analysis, and quantitative discourse analysis. This foregrounded how actors functioned as translators of specific terms to their respective social worlds, and in return, translated the social worlds back into the process of productive contestation while shaping the norm. These findings were thus the basis for a close reading of the mailinglists, chat logs, and viewing of recordings of video calls, and thus added an extra layer of reflection on my own professional participation of this process that preceded my academic interest in it.

My third chapter and case study began with descriptive analysis and quantitative discourse analysis of IETF mailinglists and technical documents. This revealed a significant amount of language pertaining to norms and values, which was also confirmed in the literature. In my professional engagement with the field, which later transformed into participant observation in the IETF mailinglists and during IETF meetings, I recognized the language in the discourse, but this did not translate to the actual practices I observed. To gain more insight into this, I engaged in 25 semi-structured interviews with IETF leadership, experienced IETF community members, and RFC authors. I transcribed and coded the interviews using qualitative methods informed by the thematic analysis, which allowed me to cross-identify themes in the interviews. To summarize, the process tracing started from intuitions that emerged from my professional engagement that led to a quantitative analysis of mailinglists and technical documents. Subsequently, participant observation and speculative and iterative analysis of technical documents and mailinglist conversations allowed me to develop initial findings and intuitions, which I subsequently was able to cross-validate through the thematic analysis of 25 semi-structured interviews.

My fourth chapter took the shape of a case study in which I engaged in an explorative experiment. I started off with the descriptive and quantitative discourse analysis of RIPE's technical documents and mailinglists to find data that indicated norm evolution or norm conflict. Based on my initial findings, I designed an ethnographic probe to better understand norm conflict in RIPE. The ethnographic probe was a piece of code that was then added to the Internet Routing Registry, which allowed network operators to indicate whether their network respects data protection or human rights norms, and with that adds functionality to the network to route Internet traffic preferentially or exclusively based

on such preference. The ethnographic probe was thus released in three ways: on RIPE mailinglists; during a presentation at a RIPE meeting; and during semi-structured interviews, which were then transcribed and analyzed using thematic analysis. This allowed me to capture the responses to the ethnographic probe in a variety of ways, which also allowed me to cross-validate the findings.

Contribution

In this dissertation, I theorize the relationship between norms, values and the governance of the Internet infrastructure, and specifically how values get inscribed in the Internet infrastructure through the evolution, introduction, subversion, and resistance of norms in the norm-setting process that takes place in transnational Internet governance. I engage in case study research in three different bodies, looking at norm-evolution, norm-setting, the subversion of norms, and norm-conflict. Each chapter thus focuses on one of these aspects and contribute to theory building on the role of norms in the governance of the Internet infrastructure. This contribution is relevant for the following reasons:

- First, there are very limited systemic studies of the role that norms play in Internet governance beyond case studies. Several studies have touched upon parts of the norm-setting process in Internet governance (Christou and Simpson 2007; Mueller, Mathiason, and Klein 2007; DeNardis 2009; 2014), and its impact on society and users of the Internet (Lessig 2006; Bygrave and Bing 2009; Goldsmith and Wu 2008; Brown, Clark, and Trossen 2010; Rogers and Eden 2017), but none has sought to formulate an overall theory on the role of norms in Internet governance. The relevance of an examination of the role of norms in Internet governance seems obvious since the Internet infrastructure and its governance has become both a flash-point for geopolitical tensions, as well as a backbone for information societies.
- Second, Internet governance is regularly described as a governance innovation (Verhulst et al. 2014; Assche et al. 2015) and suggested as a role model for governance in other fields. In order to substantiate, refute, or qualify such a claim, a critical examination of Internet governance is needed.
- Third, one can observe an increase in the development of rules and norms, in the shape of laws, policies, and regu-

lations, by nation-states and intergovernmental bodies, and thus outside the private transnational Internet governance regime. This potentially puts a significant strain on this private governance regime, might limit its functions, spark a discussion about its relevance of application, or might trigger a debate on institutional re-design.

These three reasons jointly and independently significantly benefit from an increased understanding of the role of norms, as their evolution, inscription, subversion, and resistance, in Internet governance.

Main findings

In this thesis, I foreground the forces that shape Internet governance. By looking at different parts of a distributed and decentralized infrastructure governance ecosystem, I show recurring patterns that reveal a system of normative metagovernance. This system of normative metagovernance, on the one hand, instructs and evaluates the development and introduction of new norms. On the other hand, the system of metagovernance provides legitimacy to the institutional ordering of the Internet governance regime.

The sociotechnical imaginary in Internet governance allows different stakeholder groups to work together, while an embedded guiding norm instructs participants in the private Internet governance regime to increase interconnection. While it seems that private Internet governance is an encompassing system, actually the strength of this system of metagovernance is the narrow remit of the norm regime, which allows it to reject the introduction of social and legal norms, such as human rights and data protection, that hamper the increase of interconnection between networks and devices. The guiding norm of voluntary interconnection provides a very clear evaluation grid for the introduction of new norms. It allows for the inscription of the social norms of human rights in the Internet infrastructure, but only as far as it results in more interconnection. This means that the introduction of social and legal norms that hamper the increase of interconnection will be resisted, and that existing norms that hamper the increase of interconnection will be subverted. At the same time, the sociotechnical Internet architecture imaginary legitimizes the private Internet governance regime, and facilitates cooperation within it.

1

Coding and encoding rights in internet infrastructure

Abstract[2]

This article explores bottom-up grassroots ordering in internet governance, investigating the efforts by a group of civil society actors to inscribe human rights in internet infrastructure, lobbying the Internet Corporation for Assigned Names and Numbers. Adopting a Science and Technology Studies (STS) perspective, we approach this struggle as a site of contestation, and expose the sociotechnical imaginaries animating policy advocacy. Combining quantitative mailing-list analysis, participant observation and qualitative discourse analysis, the article observes civil society in action as it contributes to shape policy in the realm of institutional and infrastructure design.

2 This chapter has been previously published, after peer review, as: Milan, Stefania, and Niels ten Oever. 2017. "Coding and Encoding Rights in Internet Infrastructure." Internet Policy Review 6 (1).

Introduction

Does ICANN violate human rights?', asked a 2014 report[3] by the Council of Europe (CoE), questioning whether the policies and operations of the Internet Corporation for Assigned Names and Numbers (ICANN)[4] unintentionally infringe users' right to privacy, freedom of association, and freedom of expression. ICANN is a nonprofit corporation in charge of the coordination of a public resource, the internet's underlying address book or Domain Name System (DNS). The CoE report was the first exogenous attempt to gauge ICANN's policymaking in light of human rights, fundamental freedoms and democratic standards (Zalnieriute and Schneider 2014). Two years down the road, human rights are not only being encoded in the organisational structure by means of inclusion in the bylaws (Appelman 2016); they also permeate much of the policy development within ICANN. This ongoing multistakeholder process has been driven, among others, by a small group of civil society actors, who set up to inscribe human rights into names and numbers, protocols and standards, both within ICANN and the Internet Engineering Task Force (Cath 2015).

3 https://rm.coe.int/16806fc29c accessed on May 20, 2020

4 https://www.icann.org/ accessed on May 20, 2020

Internet governance embraces the global coordination of the DNS and internet addresses, but also various other 'environments with low formalization, heterogeneous organizational forms, large numbers of actors and massively distributed authority and decision-making power' (Eeten and Mueller 2013, 730). Here, we approach it as a 'politically contested process of meaning making in which past and future technological projects are framed in a particular light' (McCarthy 2011, 90). This article explores the

5 For an overview of STS in internet governance research see the Internet Policy Review special issue 'Doing Internet Governance: practices, controversies, infrastructures, and institutions', available at: https://policyreview.info/articles/analysis/doing-internet-governance-practices-controversies-infrastructures-and-0

meaning-making and discursive role of the organised civil society in institutional and infrastructure design, focusing on the management within ICANN of the DNS, an inherent part of internet infrastructure, and its relation to human rights values. We investigate civil society engagement with the organisation, in particular following the transition of the stewardship over ICANN from the US Congress to the global multistakeholder community announced in early 2014, and map the distinct articulations of the human rights discourse that emerged in relation to internet infrastructure and the organisation itself. In doing so, we adopt the disciplinary lenses of Science and Technology Studies, for STS allows us to address technology as a site of contestation, focusing on its unremitting interplay with the social and on the controversies that might emerge. STS allows us to understand internet governance 'as a normative "system of systems"', unpacking 'the micro practices of governance as mechanisms of distributed, semi-formal or reflexive coordination, private ordering, and use of internet resources' (Epstein, Katzenbach, and Musiani 2016). It empowers us to move away from a 'focus on institutions as agents' towards investigating 'the agency of technology designers, policy-makers, and users as those interact in a distributed fashion, with technologies, rules, and regulations, leading to unintended consequences with systemic effects' (Ibid.; see also (Musiani 2015)[5].

We see this civil society-led struggle to inscribe human rights in internet infrastructure as an instance of bottom-up design, defined as the process of enshrining 'radical' (Milan 2014a) or unconventional policy preferences - which sprung out of technological practice and cultures such as the hacker subculture[6] - into governance fora and institutions.[7] Our definition owes to the STS notions of social shaping of technology (e.g., MacKenzie and Wajcman 1999) and co-production (e.g., (Jasanoff 2004), which stress the role of users in technology innovation and in the diffusion of new ideas. It is also inspired by the disciplines of critical design (e.g., Dunne and Raby 2001) and critical technology practice, especially where these focus on culturally embedded discursive practices (e.g., Agre 1997; Dourish 2001).

Bottom-up design seeks to intervene in the organisational process that some STS scholars have termed 'ordering', which entails the negotiation of plurality and alternatives within a given context (Mol 2002).[8] Organisations like ICANN can thus be seen as materially heterogeneous institutions in charge of ordering and arranging difference (Law 1994; Woolgar and Neyland 2013). Fol-

6 See also Law (1994)

7 'Bottom-up' here is intended to evoke also the bottom-up process of ICANN itself, as we shall see in what follows. Although it does not equal grassroots participation and there is still limited civil society involvement in ICANN, we observe a slow increase in the participation of grassroots organisations from different backgrounds - as testified by the expanding organisational membership in the Noncommercial Users Constituency (NCUC) and in the number of advocates with grassroots activism or hacker backgrounds - a trend observed also in other internet governance venues (Milan 2014b)

8 Illustrating the evolution and uses of the notion of ordering goes beyond the scope of this article. For an overview see Flyverbom (2011; 2016) Hofmann, Katzenbach, & Gollatz (Hofmann, Katzenbach, and Gollatz 2017)

lowing Jasanoff, regulations like ICANN bylaws are to be understood as 'devices that order and reorder society' (Jasanoff 2004, 14). Looking at these ordering practices allows us to capture 'the normative effect of mundane practices and daily routines' that characterise internet governance as a series of 'hybrid configurations constantly reshaping their purposes and procedures in order to connect and mobilise objects, subjects and other elements, constituted and positioned relationally, around particular issues' (Epstein, Katzenbach, and Musiani 2016). Thus, bottom-up design can be seen as a way of 'making institutions' while/by 'making discourses', that is to say 'producing new languages or modifying old ones so as to find words for novel phenomena' (Jasanoff 2004, 39-41). In the context of this article, objects of ordering are internet infrastructure and the associated values as they bear on decision-making and infrastructure/organisation design.

Practitioners of bottom-up design typically operate as critical communities who 'seek acceptance of a new conceptualization of a problem', and try to shape the way people think about it (Rochon 1998, 22). An important source of legitimacy for such critical communities is expertise, including technical practice (Ibid.). At the core of bottom-up design is a (variably explicit) connection with technology-oriented movements like the open-source software community (Hess 2005), and with critical tech communities engaging with alternative technologies and technical practices (Hintz and Milan 2009; Tréguer, Panayotis, and Söderberg 2016). These take autonomous technologies as alternative institutions: not just as 'objects of governance, but also as a set of *tools for* governance' (Musiani 2016, 85 original italics). As such, they represent the source of the cultural and ideological references of an important portion of civil society advocates within ICANN.

Following the STS tradition, we approach the struggle for coding and encoding rights within ICANN as an instance of 'solving a problem of disorder within established cultures' (Jasanoff 2004, 6), where the disorder is a mismatch between a time-honored organisational culture, ICANN's, and the values of part of its community. We take ICANN, and the human rights debate within it, as a site of multi-level contestation (McCarthy 2011) characterised by 'disagreement, negotiation, and the potential for breakdown' (Akrich 1992, 207), and seek to capture the visions and internal diversity of the civil society contingent. We engage in a partial 'sociography' of this process, describing the relationships behind it (Ibid.) and the related 'ordering narratives' (Doolin 2003), con-

9 See lists.ncuc.org/cgi-bin/mailman/listinfo/ncuc-discuss. The e-mail list, which built on the pre-existing NCDNHC list later renamed, is the main venue for NCUC members to exchange views and strategise. Open to members only but publicly archived, members are subscribed by default upon joining NCUC. Ncuc-discuss archives include also e-mails from the period immediately before NCUC was formally established, including e-mails from ncdnhc-discuss for 2002-2003.

stantly moving between the 'technical' (of both technical infrastructure and organisational mechanisms) and the 'social' (of civil society mobilising) (cf. Bijker and Law 1992).

Original data for this article was collected analysing, by means of the Python toolkit BigBang (Benthall 2015), [NCUC-discuss], the principal mailing list of the NonCommercial Users Constituency (NCUC), the main home for civil society organisations and individuals within ICANN.[9] Mailing list analysis was selected for three reasons: first, even though ICANN holds regular face-to-face and teleconference meetings, mailing lists remain a key channel for deliberation and decision-making within the ICANN community; second, participation in the online discussion make differences and conflicts visible; third, language reflects the 'cultural and symbolic understandings surrounding the internet' (McCarthy 2011, 90). In addition to the quantitative analysis, we engaged in qualitative discourse analysis of selected e-mails as well as extensive participant observation (2013-present).[10]

10 Both authors are active within the ICANN civil society sector. Milan represents noncommercial users in the Council of the Generic Names Supporting Organization (GNSO), thus contributing to policy development in the generic domains space; ten Oever is the chair of the Cross Community Working Party on ICANNs Corporate and Social Responsibility to Respect Human Rights (CCWP HR). As such he played a key role in advancing the human rights discourse.

In what follows, we reflect on civil society's engagement in internet governance and introduce the notion of sociotechnical imaginaries, useful to capture the advocates' visions and values. Next, we present ICANN as an organisation in evolution particularly susceptible to organisational reform. The third section delves into the empirical analysis, and shows how the progressive inclusion of new civil society advocates in the process caused an expansion of the human rights agenda. We conclude linking these concerted efforts to the recent turn to infrastructure in internet governance (Musiani et al. 2016).

Civil Society and Internet Governance: Emerging Socio-Technical Imaginaries

Civil society[11] emerged as a significant player in the global internet governance debate at the United Nations' World Summit on the Information Society (WSIS, 2003-2005), when it was invited to the negotiation table 'on equal footing' (Hintz 2009). Ever since, the composite civil society rubric, constituted by individuals and nonprofit organisations, has made its voice heard at the yearly Internet Governance Forum, a WSIS spin-off for a multistakeholder dialogue on internet-related public policy issues (Mueller 2010).

11 'Civil society' indicates the realm of human activity outside the remit of the state and the market (see Cardoso 2004)

Rather than a uniform monolithic entity, civil society is a multifaceted field of action and beliefs where distinct approaches, worldviews and visions of what the internet is and should look like co-exist, not without conflicts. These collective visions or imaginaires link 'intentions and projects as well as utopias and ideologies' (Flichy 2007, 4). They are collective because they tend to be shared by groups and individuals across the world and regardless of national cultures. They can be seen as 'ways of thinking about what infrastructures are, where they are located, who controls them, and what they do' (Parks 2015, 355). These imaginaries, knitting together the 'technological' and the 'social' to say it with STS scholars, emerge from, among other, 'the imaginative faculties, cultural preferences and economic or political resources' of internet users (Jasanoff 2004, 16), and evolve in interaction with the actions and preferences of other actors including governments and industry (see also Bijker 1995). They originate in users' mundane practices as these shape governance discourses.8 They mirror subtending ideologies, but are also influenced by broader geopolitics such as foreign policy (cf. McCarthy 2011; see also Turner 2006).

Sociotechnical imaginaries embody a normative, prefigurative dimension. They can be seen as 'a means of relating the local and the present to broader developments and structures of the past or the future' (Hofmann, Katzenbach, and Gollatz 2017). They are at once 'descriptive of attainable futures and prescriptive of the kinds of futures that ought to be attained' (Jasanoff, Kim, and Sperling 2007, 1). Most importantly, they are instruments of co-production that 'have the power to shape technological design' (Ibid.). As we shall see, ICANN policy-making is shaped in 'bottom-up, consensus-driven, multi-stakeholder' policy development processes where discursive change is functional to issue naming and recognition as well as agenda setting (cf. Stone 1988; Dery 2000). Thus, there is a direct line between the visions enshrined in the sociotechnical imaginaries of the various actors, on the one hand, and the concrete outcomes of institutional and infrastructural formation, on the other.

Focusing on sociotechnical imaginaries allows us to observe civil society in action as it contributes to shape policy in infrastructural and institutional design. As the process is ongoing, this article tracks two moments of co-production, namely the emergence of new ideas and the ensuing contestation phase (Jasanoff 2004).

ICANN and the Struggle for Human Rights

ICANN is a nonprofit organisation incorporated in California whose mission is to 'ensure the stable and secure operation of the internet's unique identifier systems' (ICANN 2016). ICANN is in fact in charge of the management, operation and technical maintenance of a number of databases concerning both 'names' (e.g., root name servers, the DNS) and 'numbers' (e.g., Internet Protocol address spaces such as IPv4/6, the regional registries). Set up in 1998 to manage the Internet Assigned Numbers Authority (IANA) on behalf of the US Department of Commerce (Mueller 2002), ICANN is at a historical turning point. At its 55th meeting, in Marrakesh, Morocco (March 2016), the ICANN community voted in support of transitioning the stewardship over the IANA function from the US National Telecommunication and Information Agency (NTIA) to the global multistakeholder community.

ICANN consists of two parts: the corporation that implements policies and procedures to run the infrastructure, and the so-called 'community' that, supported by ICANN staff, develops in a multistakeholder fashion the policies that are implemented by the corporation. Since its inception, ICANN stimulated bottom-up policy development, although the industry still plays a leading role with civil society merely in tow, and the organisation has not been exempt from criticism (Bygrave 2015; Raymond and Denardis 2015). Civil society involvement dates back to the establishment of the NonCommercial Domain Name Holders Constituency (NCDNHC) in 1999, relabeled NCUC in 2003. NCUC membership, which is free of charge, includes both organisations and individuals, the latter ranging from technical experts and academics to professional advocates and users, with backgrounds as diverse as engineering, law, and development activism. At the time of writing, it counted 118 organisation and 415 individual members from 157 countries.[12] NCUC has a policymaking function, and contributes to elect six members in the Council of the Generic Names Supporting Organization, in charge of the policies for Generic Top Level Domains (e.g., .net, .com, .hotel, .لاثم).

Notwithstanding the early engagement of civil society in the organisation, human rights remained long at the margins of ICANN, in contrast to governance fora like WSIS and IGF

12 Together with the Not-for-Profit Operational Concerns Constituency (NPOC), NCUC constitutes the Non Commercial Stakeholder Group (NCSG). NCSG elects the six GNSO councilors representing civil society. A third entity, the At-Large Advisory Committee (ALAC), represents users' interests. NPOC and ALAC are not considered here for they have not been particularly vocal in the human rights debate.

Jørgensen 2006). The wind changed direction as a new group of advocates joined ICANN in 2014, following a combination of events such as the leaks by security contractor Edward Snowden of classified documents proving blanket surveillance of internet users by national security agencies (June 2013 onwards); the CoE report on ICANN's responsibility to respect human rights; and most importantly the announcement, on March 2014, that the United States would release control over the IANA function. Since early 2014, in an unprecedented experiment of 'polycentric governance' (Scholte 2016b), the ICANN community engaged in a major redesign endeavour. It launched, among others, the Cross Community Working Group on Enhancing ICANN Accountability (CCWG Accountability), tasked with 'develop[ing] a plan to transition the US government stewardship role with regard to the IANA functions and related root zone management'. The IANA transition, and CCWG Accountability in particular, worked as a 'policy window', or an occasion for political participation by civil society advocates (Kingdon 1995). This policy window represented an opportunity to connect the 'policy niche' of human rights (Milan 2009), until then largely ignored by the community at large, to a broader process at the core of the organisation's future.

The CoE report was presented at the 50th ICANN meeting, in London (June 2014). The ICANN 51 (Los Angeles, October 2014) agenda included a session on human rights co-organised by the CoE and the ICANN Government Advisory Committee (GAC). Two new entities were formed: the GAC Working Group on Human Rights and International Law (GAC WG HRIL) and the multistakeholder Cross Community Working Party on ICANNs Corporate and Social Responsibility to Respect Human Rights (CCWP HR),[13] established as a sub-entity of the NCSG and chaired by the freedom of expression non-governmental organisation ARTICLE 19 (recently affiliated to the NCUC). The two operate independently but coordinate their work through joint public meetings. At ICANN 52 in Singapore (February 2015), ARTICLE 19 launched the report ICANN's Corporate Responsibility to Respect Human Rights.

13 CCWPs are ad hoc, informal single-issue groups with no official policy development or advisory power.

At ICANN 53 (Buenos Aires, June 2015) and ICANN 54 (Dublin, October 2015), CCWP HR held both working and outreach sessions with other ICANN constituencies, representing the interests of other communities, e.g. the Intellectual Property (IP) Constituency. Meanwhile, the CCWG Accountability recommended a concrete commitment to human rights in the ICANN post-transition

bylaws, but parts of the community pushed back, concerned that a commitment to human rights would broaden ICANN's scope and mission. Eventually, the final report by CCWG Accountability, made public on February 2016, recommended that ICANN should commit to respect human rights within its narrow scope and mission; that it should not be forced to actively protect human rights or force external parties to do so; that such commitment is to be included in the ICANN bylaws, but that the specific bylaw would only be enacted pending the development of an adequate framework of interpretation.

The ICANN community vote in support of the IANA stewardship transition proposal, in March 2016, paved the way for the proposed regulations to be reworked into the organisation's bylaws. The bylaws revision concluded phase 1 (or Workstream 1) of the transition. Bylaw (viii), adopted in May 2016 and included in Article 1 Mission, Commitment and Core Values, Section 1.2(b) reads:

> *(viii) Subject to the limitations set forth in Section 27.2,11[14] within the scope of its Mission and other Core Values, respecting internationally recognized human rights as required by applicable law. This Core Value does not create, and shall not be interpreted to create, any obligation on ICANN outside its Mission, or beyond obligations found in applicable law. This Core Value does not obligate ICANN to enforce its human rights obligations, or the human rights obligations of other parties, against other parties.*

14 Section 27.2 sets some procedural limitations for the human rights bylaw, including their coming into force pending the development of a framework of interpretation.

This concluded the contestation phase concerning the inclusion of human rights into the bylaws (Jasanoff 2004). The NTIA announced in June 2016 its acceptance of the proposal put forward by the global internet multistakeholder community; the actual IANA stewardship transition was completed on 1 October 2016 when the ICANN contract with the US government officially came to an end. As far as human rights are concerned, the ongoing Workstream 2 of the IANA transition requires the development of the framework of interpretation for bylaw (viii), and of a human rights impact assessment instrument for ICANN policies and operations. Figure 1 shows how human rights relate to ICANN's themes and policies/processes.

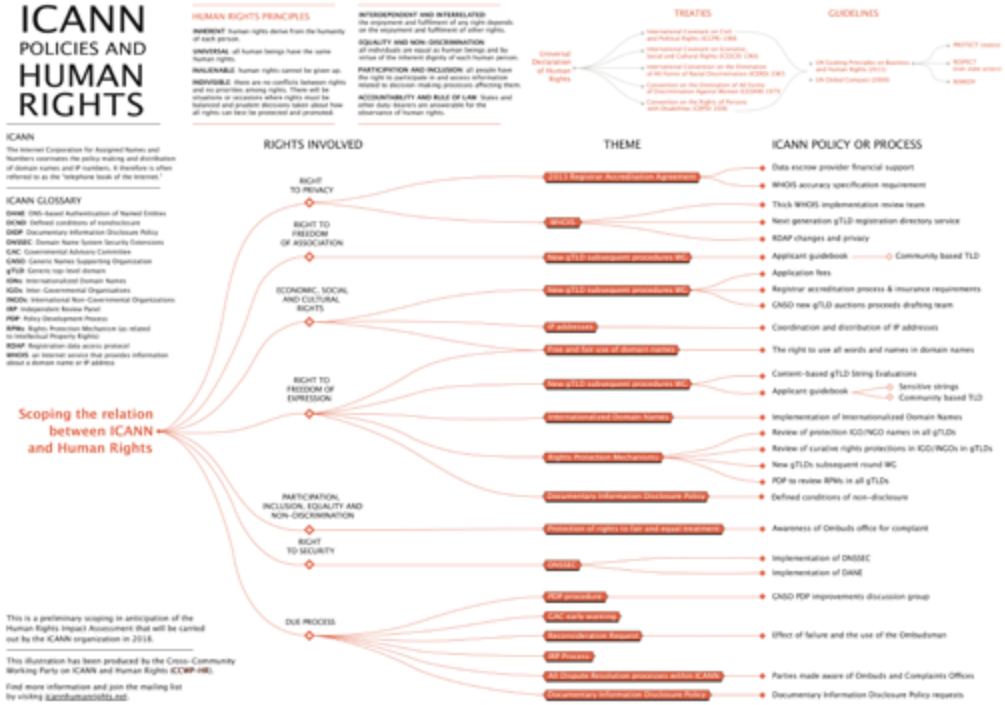

Figure 1: An overview of the relation between human rights, themes and policies/processes in ICANN, prepared by CCWP HR.

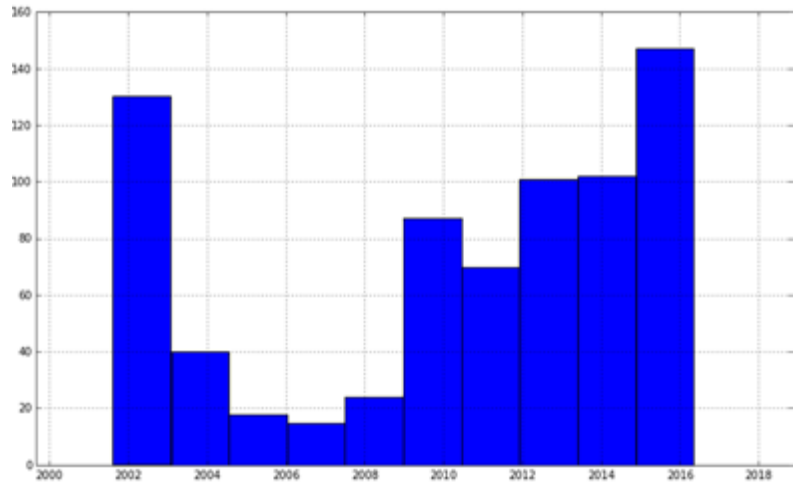

Figure 2: Growth of the NCUC community as reflected in NCUC-discuss (unit of analysis: e-mails from members who made their first post to ncuc-discuss).

NCUC: A Community in Expansion

Mailing lists constitute the main meeting point and organisation and discussion ground for ICANN constituencies and their membership. Examining the evolution of participation is key to understand civil society dynamics around ICANN.[15] By analysing traffic volume on NCUC-discuss, we identified two peaks of traffic, corresponding respectively to the NCUC inception and to the period 2014-present (figure 2). We link the recent growth in NCUC membership to the political opportunities (Tarrow 1998) brought about by the CoE report, the Global Multistakeholder Meeting on the Future of Internet Governance (NetMundial, São Paulo, Brazil, 2014), the Snowden revelations, and especially the IANA transition - which attracted the attention of civil society advocates who had to date kept ICANN at a distance, notwithstanding their commitment to digital rights. The increase in membership corresponded to a growing diversification in geographical origin, with a new cluster of NCUC active members from the Asia Pacific region.

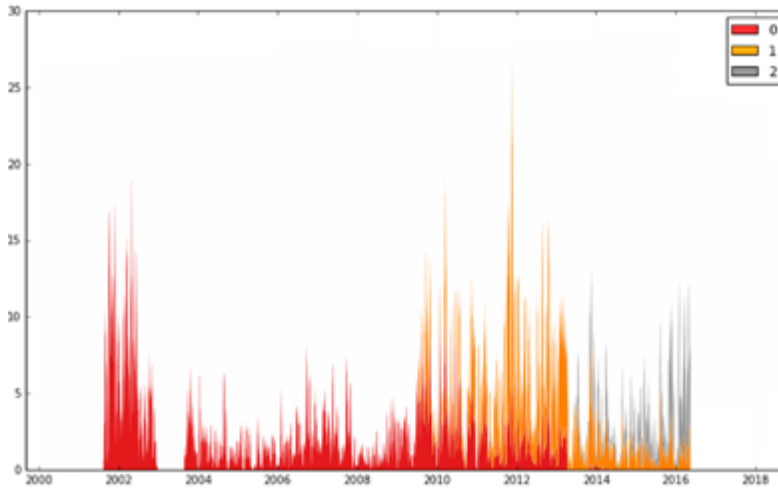

Figure 3: Relation between different groups of participants to NCUC-discuss. E-mails were divided into three cohorts based on when members sent their first e-mail to the list.

15 NCUC recent membership includes digital rights organisations like the Electronic Frontier Foundation and Access Now, freedom of expression organisations like ARTICLE 19 and Free Press, but also the American Civil Liberties Union, the Centre for Internet and Society (Bangalore, India), and the Washington-based Center for Democracy & Technology. A close reading of organisational membership over time would nicely complement our automated analysis of mailing list traffic, but it is outside the scope of this article.

Further analysis, linking individual participants' first e-mail to the list with their further participation to the online discussion, allows us to identify three groups of members (figure 3). Group 0 (in red) corresponds to the early days of the NCUC foundation; some members are still active today. Group 1 (in orange) relates to a second phase in the NCUC evolution, with membership from the Global South increasing and new issues entering the agenda, concerning e.g. the new round of allocation of generic Top Level Domain Names (gTLDs) that kicked off in 2010-12. Group 3, including yet another round of new participants (in grey), parallels the IANA transition and the other recent political opportunities described above.

We interpret these groups as three cohorts of civil society advocates in ICANN, which, as we shall see next, correspond to the progressive broadening of the advocacy agenda. Cohorts 2 and 3 could build on the institution-building and advocacy activities of the previous one(s), enjoying the expertise, structures and resources available over time thanks to internal lobbying (e.g., travel support for civil society advocates, infrastructure for remote participation and conference calls, translation services, and the list goes on).

These findings can be interpreted in light of earlier analyses pointing to a recent adjustment in membership for the civil society engaged in internet governance. Traditional internet governance venues are increasingly subject to the attention of digital rights activists and hackers. The Snowden revelations, but also processes like NetMundial, have determined a shift in the agendas and strategies of civil society actors, to the point of partially reconfiguring traditional equilibriums (Milan 2014a; 2014b). This represents an innovation with respect to the post-WSIS phase, characterised by a marginalisation of grassroots internet activists, who privileged a hands-on approach that prioritised technology design over policy design (Milan and Hintz 2013).

The Evolution of Socio-Technical Imaginaries

Mailing lists serve as a critical communication and deliberation infrastructure for ICANN constituencies and their membership, representing a crucial venue to investigate discursive change, albeit not the only channel of conversation.[16] We postulate a relation between the participation of new members to the discussion

16 By focusing on one constituency-based mailing list, this study fails to capture the contentious process of negotiation across constituencies, and this represents the main limitation of this approach. However, by concentrating on that main civil society avenue within ICANN that also happens to drive the bottom-up design efforts described here, the article offers a snapshot into the behind-the-scenes of the ongoing process of discursive change that has human rights at its core.

and the evolution of human rights discourse. In other words, the change of pace that affected the way human rights were framed and presented to the broader ICANN community, is a function of the inclusion of new members within NCUC - and by extension, of the novel policy windows that became available over time. We argue that the three cohorts of advocates we identified correspond roughly to three distinct sociotechnical imaginaries, which we now move to describe with the support of discourse analysis. These are to be seen as simplified ideal-types useful to depict the trajectory of human rights at ICANN, but there are no shift interruptions between the three. Rather, the civil society agenda is cumulative: visions and political preferences do not replace each other but co-exist and dialogue. For the sake of brevity, we highlight only a small selection of representative issues amongst the many advocates fought for over time.

2002-2009. Freedom of expression as a barrier to expansive IP rights.

The early civil society advocacy agenda focused on the fight against the strategy of IP protection enacted by ICANN to the detriment of noncommercial interests. It was indeed the observation that 'Trademark claims were limiting legitimate uses of words and concepts in the domain name space' (Mueller, 2012), that prompted freedom of speech advocates to create a space for civil society within ICANN - what is now the NCUC. To be safeguarded were the (then) three million .org domain name holders, plus users and potential registrants. The advocacy agenda included freedom of expression, consumer protection, 'trademark maximalism' (Mueller, 2012), ICANN's mission creep (in particular with respect to content regulation), transparency, and the power unbalance between commercial and noncommercial players. Qualitative analysis of the list reveals that activists mostly reacted to upcoming and potential threats at the level of policy-making and institutional design, resisting incumbent regulations by means of discursive tactics oriented to 'reorder' narratives and trying to secure a voice for noncommercial players in an organisation that was still designing itself.

With its emphasis on boundless freedom of expression and individual rights, the sociotechnical imaginary of this first cohort evoked libertarianism and the US First Amendment. Civil liberties, rather than human rights, were the main frame of reference, infused with the idea of the internet as enabler of individual rights and free expression. Privacy came in as a function of the latter,

in turn rooted in a fierce distrust for governments. This version of cyberlibertarianism resonates with the early cypherpunks (Greenberg, 2013) and with the tech movements of the 1960/70s (Flichy, 2007). The discourse, however, appears more complex if we separate rhetoric from content. While the rhetoric was indeed libertarian, and emphasised negative freedoms such as the protection of users against powerful institutions (both state and commercial players), the narrative was permeated by positive freedoms: advocates supported progressive ideas like user participation within a libertarian strategy - in a novel configuration similar to what, in a different context, Fuchs (2014) has termed 'social cyberlibertarianism'.

2009-2014. Beyond freedom of expression: privacy, due process, social and economic rights.

The second cohort of civil society advocates contributed to consolidate the voice and the standing of the constituency. Membership and diversity increased as new professionals joined, including technical experts but also organisations and individual activists with a hacker or human rights background. The liberal rights discourse expanded towards a broader definition of freedom of expression, which came to include neighbouring issues like privacy, due process, and social and economic rights. The strategy remained largely defensive as far as human rights were concerned, with advocates trying to offset threats and expand the discourse to include, for example, development issues. Sadly, the bulk of the ICANN community did not seem to take user rights seriously, as this reflection on the gTLDs auction procedure illustrates: 'Deep pockets win / communities lose / but no one in power at ICANN cares about communities / and if there had been applicants from developing countries they would also lose / and no one in power at ICANN cares about developing economies'. The concerns about the gTLDs programme by large nonprofits like the International Red Cross, and the subsequent creation of NPOC, added complexity to the game, with competing views on, among others, privacy. Due process within ICANN itself was of concerns to advocates, too, as this account relays: 'ICANN is insufficiently accountable to relevant noncommercial interests. [They] are not given the appropriate representation (…) There is a real worry that ICANN is an "industry organization"'. Overall, advocates expressed concern about 'The broader fit between ICANN's actions/policies and the sort of public interest values we're all here to champion'. The prevailing sociotechnical imaginary expanded

from a libertarian to a 'classical' human rights agenda, although rights were typically mobilised independently from each other and without a reference to the overall human rights programme, which was seldom explicitly invoked and largely upon initiative of single individuals. The notion of human rights of this period approximates the International Covenant on Economic, Social and Cultural Rights.

2014-present. Waving the digital rights banner: human rights at the forefront.

This 'third cohort' took a significant leap forward in the struggle to inscribe human rights into infrastructure and institutional design at ICANN. Exploiting novel policy windows and opportunities for engagement, larger non-profit organisations with a digital rights agenda joined NCUC, including the Center for Democracy & Technology, the Centre of Internet and Society, the Electronic Frontiers Foundation andAccess Now. The increased organisational membership - able to mobilise resources, thus ensuring continuity of engagement - was coupled by a growing participation of vocal individuals from the global South. These advocates built on the longstanding members' expertise, but their limited familiarity with unwritten community norms prompted them to occasionally bypass established practices to advance their goals. Strategy-wise, they reacted to threats but especially actively sought opportunities and created the conditions for advancing their cause. They connected human rights with the notion of corporate social responsibility; bridged over to other policy fora, and 'reordered' the narrative by other means (e.g. amovie) and through strategic alliances (e.g., cross-community engagement with CoE, GAC and other constituencies, participation in academic conferences). Human rights permeated institutional design also with a push for an ICANN privacy policy.

This third cohort includes human rights supporters who do not hesitate to evoke human rights by their name. They also have a much broader human rights agenda inspired to recent notions of digital rights as well as the International Covenant on Civil and Political Rights, foregrounding for instance cultural rights, such as linguistic diversity. These ideas are grounded in a profound understanding of the materiality of the infrastructure, and of its surveillance and control affordances. The human rights agenda is not embraced by the entire NCUC, and there exists criticism concerning the value and potential limitations of a human rights approach (e.g. Mueller, 2016). In fact, views by government representatives

coexist with hacker hands-on attitudes and 'social cyberlibertarian' perspectives, in a combination that sets aside dogmatism in favour of a pragmatic preference for flexible, ad hoc alliances and informal collaborations across constituencies.

Conclusions

Focusing on the emergence and contestation of new ideas, this article offered a snapshot into the concerted efforts of a group of advocates to wire human rights into the policies (the infrastructure) and procedures (the institution) of ICANN, seen as a site 'for the testing and reaffirmation of political culture' (Jasanoff 2004, 40). Embracing bottom-up design as a form of policy advocacy rooted on and inspired to technical practice, NCUC human rights advocates operated as a critical community advancing discursive tactics entrenched in sociotechnical imaginaries. Using novel 'ordering narratives' able to (re)structure relations strategically organised (Law 1990), they partially managed to subvert mainstream organisational narratives that had thus far been 'recursively told, embodied, and performed' (Law 1994, 259) by the ICANN community. Paraphrasing Jasanoff, advocates tried to make the organisation by making discourses. Further research could comprise, for instance, a cross-constituency analysis of the evolution over time of the human rights discourse, and a detailed discourse and social-network analysis of ICANN policy development processes as they related to specific human rights and portions of the ICANN infrastructure (e.g. the WHOIS database and its privacy implications).

Echoing Epstein et al. (2016), we believe STS has much to offer in the understanding of the complex ecosystem of internet governance. To name just one of the many promising venues, the STS perspective on ordering as a key organisational mechanism adopted in this article, encouraged us to approach both infrastructure and organisation as sites of contestation and co-production. It allowed us to illuminate some of the micro practices of governance by civil society actors within ICANN, tracking their meaning-making and discursive role as they unfolded in the NCUC mailinglist. Triangulating participant observation with quantitative and qualitative analysis of the main NCUC mailinglist, where organisation and deliberation unfold, we identified three ideal-type generations of civil society advocates corresponding to distinct but cumulative ideal-type human rights imaginaries, with

their respective agendas and tactics. We showed how the combination of emerging political opportunities and the progressive inclusion of new, diverse members brought about new issues, or new ways of framing certain issues, altering and empowering the emerging 'ordering narratives' from the bottom up.

We like to think of this struggle as an attempt to explicitly wire the politics of internet architecture into the politics of institutions (see DeNardis 2012). It can also be seen as an instance of the recent 'turn to infrastructure' in internet governance (Musiani et al. 2016), whereby private actors seek to expand the remit (and the features) of the infrastructure (i.e., the DNS) to positively permeate institutional design (i.e., ICANN). It remains to be seen how the ongoing human rights struggle will evolve over time, and how the stabilisation phase (Jasanoff 2004) will affect the agenda setting capability of civil society and its role within the ICANN community.

2

Productive Contestation, Civil Society, and Global Governance: Human Rights as a Boundary Object in ICANN

Abstract[17]

Human rights have long been discussed in relation to global governance processes, but there has been disagreement about whether (and how) a consideration for human rights should be incorporated into the workings of the Internet Corporation for Assigned Names and Numbers (ICANN), one of the main bodies of Internet governance. Internet governance is generally regarded as a site of innovation in global governance; one in which civil society can, in theory, contribute equally with government and industry. This article uses the lens of boundary object theory to examine how civil society actors succeeded in inscribing human rights as a Core Value in ICANN's bylaws. As a "boundary object" in the negotiations, the concept of human rights provided enough interpretive flexibility to translate to the social realities of the various stakeholder groups, including government and industry. This consensus-building process was bound by the organizing structure of the boundary object (human rights), and its ability to accommodate the interests of the different parties. The presence of civil society at the negotiating table demanded a shift in strategy from the usual "outsider" tactics of issue framing and agenda setting, to a more complex and iterative process of "productive contestation," a consensus-building process fueled by the differences of experience and interests of parties, bound together by the organizing structure of the boundary object. This article describes how this process ultimately resulted in the successful adoption of human rights in ICANN's bylaws.

17 This chapter has been previously published, after peer review, as: ten Oever, Niels. 2018. "Productive Contestation, Civil Society, and Global Governance: Human Rights as a Boundary Object in ICANN." *Policy & Internet*, 11.

New Roles, New Process?

The early development of the Internet was characterized by permissionless innovation, informal arrangements, and an unregulated "freedom to create"—but with the rising importance of the network, the need for organization, regulation, and governance increased. Calls of this kind (such as proposals for the regulation of encryption) were met with concern, however, by Internet users, nongovernmental organizations (NGOs), hackers and academics alike, because this meant that the unprecedented freedom of expression, access to information, and enjoyment of other human rights online (thus far taken for granted), might be at stake.

The governance of the Internet is distributed over different bodies in a mode of participation described as a "multistake-

holder model"—meaning that different stakeholders, such as governments, the private sector, technical operators, and civil society, make decisions jointly. Internet governance is thus distributed over a range of bodies in which the configuration and level of formalization of the multistakeholder model varies. The multistakeholder model represents an innovation in governance, because it allows for joint decision making by different stakeholders, and openness of participation by individuals and organizations alike. While multistakeholder governance is by no means a unique feature of the Internet governance field, there is no other area in which this model has been so widely embraced.

Equal access to negotiation and decision-making processes by all stakeholders (including by civil society) is formalized in the multistakeholder model, whereas in many other arenas civil society cannot engage on an equal footing. This changes the structure of the conversation and negotiations, meaning that civil society cannot simply rely on well-proven "outsider" tactics such as framing and agenda-setting, and is therefore challenged to adopt other approaches. To study these new approaches, this article examines a case in which civil society achieved its objectives and analyzes how this was achieved. Internet governance is not the only example of a global governance process in which civil society has a seat at the negotiating table, but it is arguably one of the most formalized and influential.

So far, the literature has treated civil society engagement in Internet governance discussions as either monolithic (Lentz 2011) or divided (Milan 2014a). Civil society managed to inscribe human rights in the foundational and regulatory documents of an Internet governance body for the first time in 2016, representing something of a historical achievement. In this article I argue that civil society succeeded in inscribing human rights in the legally binding bylaw of the Internet Corporation for Assigned Names and Numbers (ICANN)[18] because human rights functioned as a boundary object (Star and Griesemer 1989), that is to say an arrangement which allows people to achieve some form of coordination without necessarily requiring consensus. Because human rights functioned as a boundary object it could be the translated and adapted to the social worlds within and between different stakeholder groups in ICANN. I will show how diverging views between individuals and organizations within civil society actually contributed to a dialectical process and a positive outcome, a process that I call "productive contestation."

18 ICANN plays a central role in the coordination of the distribution of domain names and Internet addresses, which is crucial for the functioning of the Internet. It coordinates the assignment of Internet Protocol (IP) numbers and Autonomous System (AS) numbers, and the management of the Domain Name System (DNS) Root Zone and Protocol Assignments.

Internet Governance, Civil Society, and Boundary Object Theory

Global governance is changing fast (Bevir 2012; Nye 2011). Indeed, beside the state, the private sector (Weissbrodt and Kruger 2003) and civil society (Glasius 2002; Keck and Sikkink 1998; R. Price 1998; Raymond and Denardis 2015; Scholte 2016a) are making their way into governance fora and to the negotiation table. However, technological changes are out-pacing "the ability of institutions of governance to respond, as well as our thinking about governance" (Nye 2014, 6). Not only is the rate of change increasing, but also the importance of digital technologies in general and the Internet in particular (Benkler 2006; Castells 2009). This has led to a situation in which the Internet is itself mediating political and economic conflict (Bradshaw et al. 2015; DeNardis and Musiani 2016).

Developments in global governance, and advances in the technology, have combined with the increasing importance of the Internet in our lives and societies to drive discussions on Internet governance and regulation (Lessig 2008; Mueller 2010; Nye 2014). By being distributed over different fora and organizations (DeNardis 2014; Mueller 2010; Musiani et al. 2016) and being conducted in a multistakeholder manner involving a variety of actors on an "equal footing" (Mueller, Pagé, and Kuerbis 2004; Raboy and Padovani 2010), Internet governance is set apart from, for example, the governance of international telecommunications, which is governed instead in a multilateral manner (Drake and Wilson 2008; Keohane 2001) in which only governments have a final say. The processes of Internet governance are generally open for participation by different parties, such governments, the private sector, technical operators, and civil society alike, and decisions are jointly made, based on consensus (Hofmann 2016).

The diverse set of stakeholders and Internet governance bodies and fora gives rise to a rich institutional ecology (Abbott, Green, and Keohane 2016; Star and Griesemer 1989), which is itself the product of relatively recent governance innovation (Assche et al. 2015). Playing quite a new role in this process is civil society—the combination of individuals, organizations, and movements that belong neither to the state nor to the private sector (Cardoso 2004). Civil society has played an increasing part in international negotiations in the last few decades (Glasius 2002; Hajnal 2002;

Van Rooy 2004), but in the field of Internet governance it was never limited to lobbying, providing expertise, awareness raising, or street action (Glasius 2002), becoming instead an inherent part of the policy and decision-making process (Bond 2006; Frangonikolopoulos 2012; Milan and Hintz 2013; Mueller, Pagé, and Kuerbis 2004).

Civil society plays a uniquely important role in the Internet governance ecology because its motivations are different from those of other stakeholders. Its involvement is based on "ethical aspirations to better mankind" (Van Rooy 2004, 8), and to provide alternative channels of communication for voices that are not otherwise heard (Keck and Sikkink 1998, x). In the context of Internet governance, civil society advocates for a wide range of issues. Some of the most recurring important principles and frames include human rights, privacy, security, freedom of expression, connectivity, access, capacity, security, governance, equity, and diversity (DeNardis 2009; Franklin 2013; Isin and Ruppert 2015; Rogers and Eden 2017). Even though the right to privacy, the right to freedom of expression, and the right to security are human rights, they are not always used or understood within this frame, but rather as individual (and sometimes absolute) rights and freedoms in themselves. Human rights here are understood as "the norms and institutions of international human rights, as protected under customary international law and human rights treaties" (Land 2009, 7). Thus far, the literature has treated civil society engaged in Internet governance either as a rather monolithic group with similar issues, opinions, and concerns (Lentz 2011), or as fractured and compartmentalized (Milan 2014a). Civil society can instead be considered to consist of players who engage in strategic action, as individuals or as teams, and who pursue multiple goals within different arenas, in a complex system of dynamic interactions (Jasper and Duyvendak 2015).

This article examines the complex articulation of alliances and negotiation, both within civil society (among individuals and organizations) as well between civil society and other actors. In order to unpick the complexity of these processes, I propose to look at how human rights functioned as a boundary object during the discussions on adding a commitment to respect human rights to ICANN's bylaws. It will show how the structure of the process, that is, the translation and adaptation of human rights to the social worlds within and between different stakeholder groups, led to this final achievement.

I use boundary object theory (Burnett and Jaeger 2009; Gal, Yoo, and Boland 2005; Star 1990; Star and Griesemer 1989) as a lens to show how human rights were translated into the social worlds of the different stakeholders in ICANN governance without losing its effectiveness. In the scene-setting article by Star and Griesemer (1989), boundary objects were defined as having three components: (i) interpretive flexibility—they have different meanings and interpretations for various groups; (ii) they have the ability to accommodate different informational and work arrangements—the structure of the object can be used in both individual and group settings and collaborations; and (iii) they exhibit a dynamic between ill-structured and more tailored uses of the objects—that is, the tension between general abstract use and specific uses in different social worlds facilitates the process of standardization of the object (Star 2010). Boundary object theory provides us with a tool to analyze negotiations between stakeholders in multistakeholder governance. This theory seems particularly relevant for Internet governance because it aims to study the process that leads up to standardization, "the back-and-forth between ill structured and well structured; the architecture of the infrastructures involved" (Star 2010, 614). This captures the dynamics of Internet governance, in which groups with different backgrounds, discourses, and objectives aim to make the Internet "work" for them, and to embed their vision in the Internet infrastructure (Sandvig 2013). Analyzing human rights as a boundary object in the case of ICANN helps to illuminate the way in which multistakeholder negotiations are structured. Boundary objects are objects that cross the boundaries between multiple social worlds (in this case, the social worlds of stakeholder groups), that are used within them and adapted to many of them simultaneously (Star and Griesemer 1989, 408), and which "'sit in the middle' of a group of actors with divergent viewpoints" (Star 1990, 46). They "adapt to local needs" in a social world, yet are "robust enough to maintain a common identity across sites" (Star 1990, 46). Concretely, "boundary objects are a sort of arrangement that allow different groups to work together without consensus" (Star 2010, 602), which is of course a crucial aspect of multistakeholder negotiations and collaboration. This process could be also explained through a Habermasian framework of communicative action (Habermas 1984; Risse 2000), in which actors develop a shared rationality based on a process of dialogue. However, the problem with this position from a Science and Technologies Studies perspective is that the process of communicative action needs to assume a shared rationality to be developed against the background of a shared lifeworld. I will show that this idealistic

position does not fit with this specific case because of the different interests, interpretations, and embedded knowledge present in the different social worlds of the ICANN stakeholders. Boundary object theory, on the other hand, recognizes that there is room for disagreement and different localized practices, which are accommodated by the boundary object; it conversely represents a more adequate perspective to frame this and, possibly, other analogous processes.

Civil society brings normative visions to an area that might otherwise be interpreted only through technical or commercial lenses. It brings this normative vision through the use of the power of norms and ideas (Keck and Sikkink 1998), the ability to influence based on a normative framework. This power of norms and ideas can be leveraged in governance negotiations and discussions (Barnett and Duvall 2005; Finnemore and Sikkink 1998; Pavan 2012) by providing and supporting a specific frame (Benford and Snow 2000) as part of the process of constructing meaning for participants and opponents (Snow and Benford 1988). Framing processes can provide powerful categories that can shift debates; a category like "weapons of mass destruction" (Litwak 2002) can impact negotiations in a way that stabilizes meaning and thus shapes policy (Barnett and Duvall 2005). Framing has helped civil society to set agendas and influence negotiations by "rendering events or occurrences meaningful and thereby function[ing] to organize experience and guide action" (Benford and Snow 2000, 614). This action repertoire (Tarrow 2005; Tilly 1989)—the set of various tools and actions available to a group—has functioned to influence those in power while actors have been absent from the negotiating table. Now that civil society has become a part of the negotiation process—at least as far as Internet governance is concerned—it is faced with coming to terms with this new reality (Carr 2015) and developing new action repertoires to go along with it.

Recognizing human rights as a boundary object helps show how civil society leveraged its power of ideas beyond mere framing and agenda setting, managing instead to effectuate an inscription of human rights in ICANN's bylaw and thus progress on the road to make respect for human rights an inherent part of ICANN's processes. Using boundary object theory as an analytical lens increases our understanding of the tactics of civil society and the structure of negotiations in new global governance settings, without reducing the complexity of this player to the fictional ideal of a unified actor.

The process by which human rights functioned and got shaped as a boundary object I will call productive contestation; this describes the speculative development of the boundary object in and between the social worlds of the different stakeholder groups. This process is a phase that precedes standardization. In this period the understanding and meaning of a concept and its translations both within and across social worlds are developed and new working definitions are tested and contested. Nonproductive contestation occurs when translations of the boundary object occur that are incongruent with other social worlds.

This article seeks to contribute to the governance studies literature by using concepts from Science and Technology Studies. While it does not expand on the theory of the boundary object per se, I try to show its usefulness in understanding the specific empirical case of multistakeholder Internet governance.

Methods

One way to understand civil society engagement in global governance is to consider a specific case in order to generate a hypothesis (Yin 2009). Case studies are "an intensive study of a single case with an aim to generalize across a larger set of cases" (Gerring 2007, 25). Internet governance represents a field of experimentation for global governance, in that it is relatively new and brings states and nonstate actors together in the coordination of a global resource (Broeders 2016; Mueller 2010; Nye 2014). Studying the field of Internet governance can thus help us understand trends and possible future developments in the field of global governance more generally. Within the field of Internet governance, ICANN is seen as an influential case (Seawright and Gerring 2008), and landmark evolution (Mueller 2010).

I became involved in ICANN during my role as Head of Digital for ARTICLE 19, an international not-for-profit freedom of expression organization. The work on this article and theory building started as an ethnographic memoir while engaged in ICANN between March 2014 and July 2017. ICANN meetings are held three times per year for an average of 5 days. In addition, negotiation, discussion, and coordination takes place on mailinglists, in chat groups, and via video conferences. I was involved as a civil society actor within the Non-Commercial User Constituency (NCUC), the Non-Commercial Stakeholder Group (NCSG), the Cross Community Working Group on Enhancing ICANN Accountability (CCWG) and its Human Rights Subgroup during Work Stream 1 (WS1; the period

ahead of the ICANN transition away from unilateral control from the U.S. government in 2016), and as rapporteur for the Human Rights Subgroup during Work Stream 2 (WS2 the period after the transition in which plans made during WS1 needed to be further defined and implemented, which started in 2016 and is expect to run until June 2018). This experience provided me with a first-hand account of these multistakeholder governance practices, as well as access that an external observer might not otherwise have. On the other hand, my direct involvement might also have introduced some biases vis-à-vis ICANN and its stakeholders. To counter this potential bias, I reflected on my own role in the process, I interrogated my biases by discussing parts of the argument presented here with different members of the ICANN and academic community, and I rely solely on publicly available sources for every claim made in the analysis part of this article, with explicit references to excerpts of meeting transcripts and mailinglists.

In order to gain a more comprehensive overview of the processes, I carried out a document analysis of public ICANN mailing lists, meeting transcripts, working group reports, and working group draft reports. I obtained these documents from the ICANN website, where these documents were publicly available up to the time of writing of this article. I studied the mailing lists of the NCSG, NCUC, CCWG, and the CCWG Human Rights Subgroups during WS1 and WS2, as well as the transcripts of the calls of these groups. Furthermore, I undertook a quantitative mailing list analysis using the Python-based tool BigBang,[19] to gain a deeper insight into trends and interactions. This led to an informed analysis of civil society participation in WS2 human rights processes.

19 http://datactive.github.io/bigbang/ accessed September 15, 2017.

Human Rights in a Time of Infrastructure Oversight Transition

This section analyzes the discussion around the addition to ICANN's bylaws of a Core Value to respect human rights. The analysis is divided in three parts. The first part describes the context in which the discussion took place; the second part describes the actors in this multistakeholder environment; and the third part describes the actual discussion. The negotiations took place during the development of a proposal for the transition of oversight and control over ICANN from the U.S. government to the international Internet community. This brought together a wide range of stakeholders with different interests, experience, and expertise who, at the end of a period of intense negotiations, agreed to the addition

of a Core Value to respect human rights to ICANN's bylaws which will impact ICANN's policies and operations. The transition of the oversight function from the U.S. government to the international Internet community took place on October 1, 2016.

The Context: The Internet Assigned Numbers Authority Stewardship Transition

ICANN coordinates the assignment of Internet Protocol (IP) numbers and Autonomous System (AS) numbers, the management of the Domain Name System (DNS) Root Zone and Protocol Assignments, and with that it fulfills the role of the Internet Assigned Numbers Authority (IANA), which is the main coordination authority of Internet protocols and namespaces. While the architecture of the Internet is largely distributed and nonhierarchical, the root zone of the DNS is structured as an authoritative, centralized hierarchy, managed by ICANN (Froomkin 2000). ICANN was contracted to do so by the U.S. Department of Commerce National Telecommunications and Information Administration (NTIA) after its role was fulfilled by the Internet engineer Jon Postel for many years. The growth in the importance of the network led the U.S. government to institutionalize this role, which led to the establishment of ICANN. This remarkable construction came under increasing international scrutiny when the Internet gained global importance in the 1990s and 2000s. Policymaking in ICANN is done through one of the most formalized instances of the multistakeholder model. Policies are developed by three Supporting Organizations (SOs; covering generic and country codes, and Internet addressing), which suggest policies to the Board of Directors. There are also four Advisory Committees (ACs) advise the board and the community on specific issues.

In 2014 the NTIA released a press release titled: "NTIA Announces Intent to Transition Key Internet Domain Name Functions" (United States Government, Department of Commerce 2014). The press release called on ICANN to bring together global stakeholders to develop a proposal for a transition of the stewardship of IANA (the function which is currently fulfilled by ICANN) from the U.S. government to the "global Internet community." The proposal needed to:

1. Support and enhance the multistakeholder model;

2. Maintain the security, stability, and resiliency of the Internet DNS;

3. Meet the needs and expectations of the global customers and partners of the IANA services; and

4. Maintain the openness of the Internet.

The announcement also noted that it would not accept a proposal that "replaces the NTIA role with a government-led or inter-governmental organization solution," which made clear that the NTIA was not willing to hand over ICANN oversight to the United Nations (UN) in general or to the International Telecommunications Union specifically. There was much international interest in the stewardship transition because it does not often occur that a sovereign state voluntarily hands over control of a unique and valuable resource to an entity that thus far was not defined: "the international Internet community." The NTIA announcement jumpstarted two interdependent processes of cross-community work in which all constituencies played a role. One of these processes was aimed at creating a technical proposal for how ICANN would perform the IANA functions after the transitioning away from U.S. stewardship, and the second process aimed to enhance ICANN's accountability mechanisms. The process aimed at enhancing ICANN's accountability was the aforementioned CCWG. The CCWG separated its work into two terms: WS1, which "focused on mechanisms enhancing ICANN accountability that must be in place or committed to within the time frame of the IANA Stewardship Transition";4 and WS2, which would address the full development and implementation of these solutions after the IANA Stewardship Transition had taken place in October 2016, when the contract between ICANN and the NTIA was envisaged to end. The CCWG WS1 work was organized largely through mailing lists and regular video calls, in which members (official representatives from the SOs and ACs) and participants discussed the issues at hand.

The Actors: The ICANN Stakeholders

Governments, the private sector, the technical community, and civil society actors all take part in the multistakeholder process in ICANN. These actors generally do not make policy jointly in ICANN, because (as mentioned above) the policy development processes take place in three different SOs: the Generic Names Supporting Organization (GNSO), the Country Code Names Supporting Organization (ccNSO), and the Addressing Supporting Organization (ASO). ACs (like the Governmental Advisory Committee, GAC) advise ICANN's Board of Directors on the policies

made by the SOs. When there are issues that supersede the policy areas of generic Top-Level Domains (gTLDs), country code top-level domains, or Internet addressing, these issues are addressed by Cross Community Working Groups in which the SOs and ACs come together.

The "technical community" (as distinct from civil society) is not a stakeholder group one would necessarily encounter in other global governance bodies. The technical community often has a strong say in policy discussion because they describe "how things work," or how the materiality of the Internet is ordered. Whereas other stakeholder groups can find "creative solutions," the technical community often functions as "reality principle," even though these organizations also have specific interests. The technical community comprises organizations with a narrow technical remit; for example, the ccNSO is made up of Internet registries that manage country code top-level domains. In some cases, these registries are not-for-profit foundations or companies, and sometimes even parts of the government, since they provide an important technical function on which the DNS relies, they are grouped this way. This is equally true of the ASO which is made up of Regional Internet Registries (RIRs), which are all technical not-for-profit organizations that distribute blocks of IP addresses. Just like Country Code Top-Level Domain (ccTLD) registries, RIRs have not-for-profit objectives, but are not counted as civil society, but rather as part of the technical community, who de facto set policies and procedures for themselves, because their position is often perceived to be neutral, or in the interest of the Internet at-large.

The private sector in ICANN is largely found within the GNSO where there are registries (those maintaining top-level domains), registrars (those selling domains), Internet Service Providers, the Intellectual Property Constituency, which protects the interests of owners of intellectual property, and a Business Constituency, which advocates for the general interests of businesses. While these are all private enterprises, they have widely different interests and views. The GAC is made up of governments and International Governmental Organizations. The preconditions for the distribution of communities across the SOs and ACs is laid out in ICANN's bylaws (Figure 4).

Civil society in ICANN can be found in the NCSG, which consists of the NCUC and the Not-for-Profit Operational Concerns Constituency (NPOC), and in the At-Large Advisory Committee.

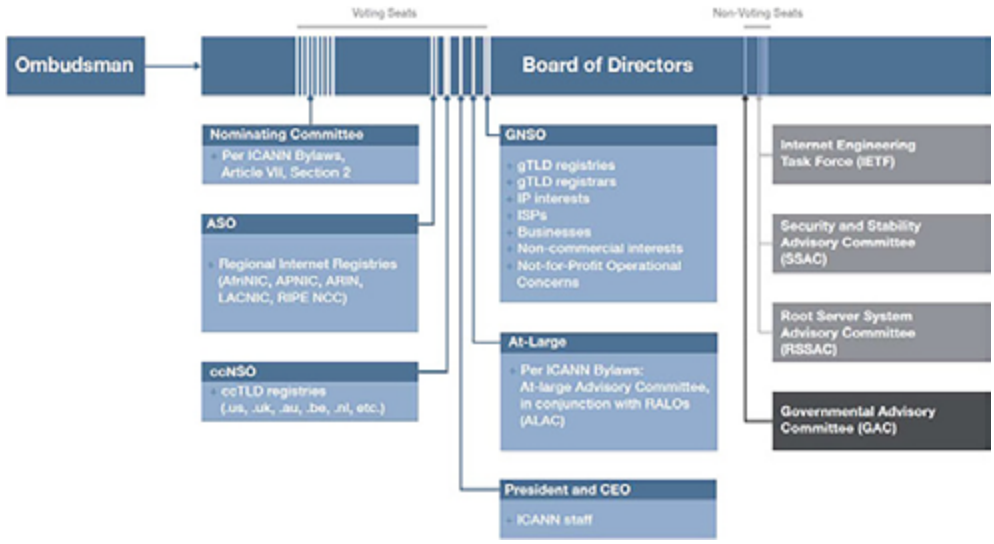

Figure 4: ICANN Organizational Chart. Source: ICANN.

The NCUC is the only place where individuals and organizations alike can become a member and engage in policymaking (albeit limited to gTLDs). This has probably contributed to the situation where the NCUC has 538 members,[20] while NPOC has 60 organizations as members,[21] and the At-Large Advisory Committee has 228.[22]

The Process: Negotiating a Human Rights Bylaw

In this section I will provide an analysis of the negotiations on the addition of an obligation to respect human rights to the Core Value section of ICANN's bylaws, which are intended to "guide the decisions and actions of ICANN."[23] We will follow the translation and accommodation of human rights as a boundary object to different social worlds through a process of productive contestation. This section presents: first, the process of translation of human rights between different parts of civil society; second, the accommodation of human rights to the needs and understandings of the private sector and the technical community, the translation between civil society and the intellectual property advocates; and finally, the accommodation of the ICANN board to the community consensus (see Figure 5).

20 https://www.ncuc.org/about/membership/ (accessed August 31, 2017).

21 https://www.npoc.org/about/members/ (accessed August 31, 2017).

22 https://atlarge.icann.org/alses (accessed August 31, 2017).

23 https://www.icann.org/resources/pages/governance/bylaws-en/#article1 (accessed March 12, 2017).

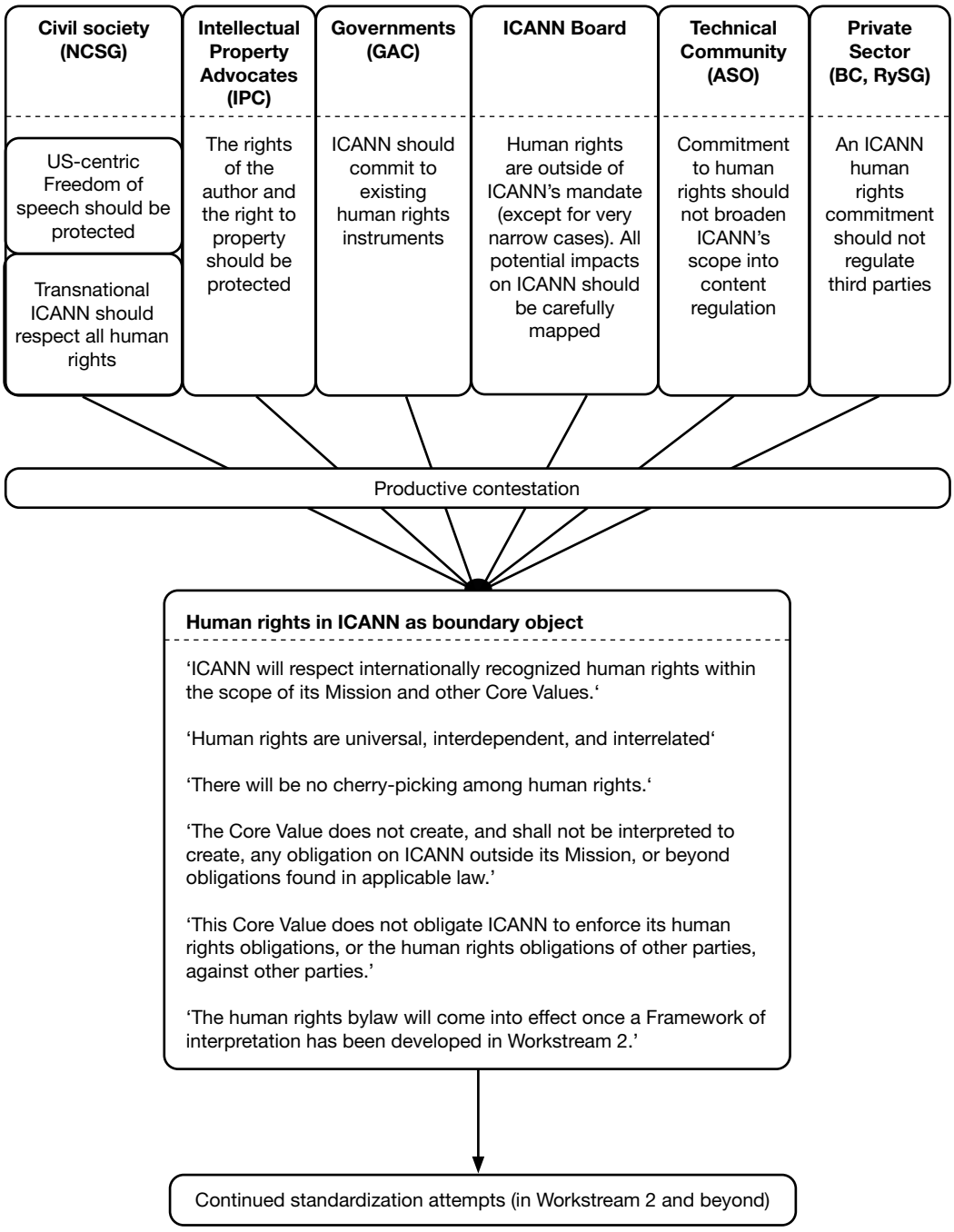

Figure 5: A Schematic Overview of the Process of Productive Contestation That Accommodated the Positions of Different Stakeholder Groups in the Human Rights Discussion During the IANA Stewardship Transition Preparations

Civil Society: Adapting to Different Needs

Previous research and analysis has shown that human rights as a frame has not always formed part of civil society's advocacy agenda in ICANN (Milan and ten Oever 2017). The earliest cohorts of civil society advocates in the NCUC were individuals lobbying for individual rights such as freedom of speech, privacy, and fair use. These are all legal concepts originating in the U.S. tradition, which also played central roles in the early U.S. Internet community (Greenberg 2013; Levy 1996; Turner 2006).

Only with the arrival of new cohorts of NGOs and participants from the Global South, did a more explicit overarching human rights discourse become increasingly prevalent (Milan and ten Oever 2017). NGOs brought with them international legal experience, an agenda for economic, social, and cultural rights, as well as experience with advocacy in multilateral bodies; but for their engagement in this complex structure they were dependent on the longstanding members' expertise and the space carved out by the earlier civil society cohorts. This does not mean that the human rights discourse in the NCUC was not contested. During the CCWG process several prominent members spoke out against pursuing a human rights approach. One of the co-founders of the NCUC, whose involvement with ICANN dates back to the late 1990s, wrote in a blog post about the adoption of the UN Guiding Principles on Business and Human Rights (UNGP) that "the HR effort will at best have no impact on ICANN's policies and at worst could make ICANN into an even more controlling and intrusive regulatory force than it already is."[24] One NCUC member who also served as civil society representative on the GNSO council said during a GNSO council meeting that human rights were not sufficiently defined and that considering that even North Korea invoked human rights, it was not clear what human rights exactly are. He ended by stating that there should be First Amendment protections, as granted by the U.S. Constitution, which made him proud to be an American.[25] This clearly illustrated the view of a cohort in civil society that viewed the U.S. Constitution as the best protection, especially for freedom of speech.

The dependence hitherto on the U.S. Constitution for the protection of freedom of expression in ICANN was not sufficient when making for a plan for a new context that should support protection of expression without the oversight of or reliance on the U.S. government. That is where the texts of human rights declaration and treaties provided a solution, since they could

24 http://www.internetgovernance.org/2016/10/26/missing-the-target-the-human-rights-push-in-icann-goes-off-the-rails/ (accessed August 31, 2017).

25 https://meetings.icann.org/en/marrakech55/schedule/tue-ncsg/transcript-ncsg-08mar16-en.pdf pp. 39–40 (accessed May 10, 2017).

facilitate standardization of the protection of these rights on the global Internet, beyond the reliance on U.S. law. At the same time, they also catered to the needs and frames of the early civil society cohorts because the protection of freedom of speech is codified as the protection of the right to freedom of expression in human rights treaties, as well as the protection of the right to privacy.

This was the first time that human rights functioned as a boundary object, between the U.S. Constitution, the U.S.-originating practice of protection of speech through the DNS, and practices and traditions of protection of freedom of expression outside of the United States. This was possible because human rights fulfilled the three criteria that were initially defined for it (Star and Griesemer 1989). It provided:

1. Interpretive flexibility: human rights accommodated the U.S. Constitutional protection for speech as well as protecting freedom of expression in other parts of the world, and could be translated to also do so in the DNS—that is, to ensure the DNS would not be leveraged as a means to stifle expression;

2. The structure of information and work process needs and arrangements: the Universal Declaration for Human Rights[26] and human rights conventions, as well as the literature based on it and experiences advocating for human rights and implementing human rights in political and legal environments, provided sufficient experience, language, and contexts to facilitate abstract and specific uses as well as collaborations;

3. The dynamic between ill-structured and more tailored uses of the objects: only states are bound by customary international law and human rights treaties, but recent developments such as the UN Global Compact and the UNGPs, which provide guidance for nonstate actors to respect human rights, provided voluntary frameworks and implementation experience which functioned as example, inspiration and reference point in both a positive sense (in relation to human rights impact assessments)[27] and a more contentious sense (in relation to chain-responsibility).[28]

Human rights catered to different cohorts in civil society because it encompassed the frames of the respective groups. We will see in the next section how civil society contributed to its translation to different social worlds and how this coincided with productive contestation—the process by which consensus and

26 The Universal Declaration is an aspirational document adopted by the UN General Assembly in 1948, which would form the foundation of international human rights law.

27 http://schd.ws/hosted_files/icann572016/16/Transcript%20NCUC%20Hyderabad%2006%20Nov%202016.pdf accessed November 30, 2017

28 http://www.internetgovernance.org/2016/10/26/missing-the-target-the-human-rights-push-in-icann-goes-off-the-rails accessed August 31, 2017

workable definitions are built through testing new definitions that cater to different interests, or by chiseling away the parts that do not fit.

Beyond Civil Society: Limited Definition

In the process of working toward standardizing and operationalizing respect for human rights in ICANN, civil society pushed forward on the work on human rights, and human rights helped to structure the discussion between different parts of civil society, thus resulting in a process I term "productive contestation"—a consensus-building process that benefits from the tension built by the differences of experience, knowledge, and interests of the parties involved. Civil society representatives would, during the whole CCWG process, be the people who put human rights on the agenda and push to keep it on the agenda whenever it was removed or declared to be "out of scope." The inclusion of human rights as part of the IANA transition even became an issue, in the words of one participant, "to die in a ditch over."[29]

Government representatives who were more familiar with the language of human rights urged the community to not (re-)define human rights, but to make a high-level commitment to them, given they were already laid out in international law.[30] Members of the private sector responded that there might be significant risks in committing to international human rights and that the potential consequences should be studied in detail and mapped before making any commitment.[31] A former ICANN CEO, who was now part of the private sector, added that all potential impacts of human rights on ICANN should be mapped out first before committing to them,[32] whereas civil society was arguing for assessing ICANN's impacts on human rights. A solution was found by converging on a limited definition (Star, Bowker, and Neuman 2003), in which it was made explicit that a commitment to human rights would and should not expand ICANN's mission.

Among Stakeholder Groups: Translations

A similar arc could be observed in other stakeholder groups, where initially the relation between human rights and ICANN was not clear. For instance, the chair of the ICANN Board and Internet veteran Steve Crocker, who observed during ICANNN51 in Los Angeles, that "Human rights is sort of even stronger than motherhood and apple pie," but that he did not see any connection between human rights and ICANN.[33] Steve Crocker and

29 https://community.icann.org/x/K6vRAw accessed May 9, 2017

30 https://mm.icann.org/pipermail/wp4/2015-August/000001.html accessed August 31, 2017

31 https://mm.icann.org/pipermail/wp4/2015-August/000025.html accessed August 31, 2017

32 https://mm.icann.org/pipermail/wp4/2015-August/000052.html accessed August 31, 2017

33 https://la51.icann.org/en/schedule/tue-board-ncsg/transcript-board-ncsg-14oct14-en.pdf p. 5. accessed May 10, 2017

others made the argument several times that ICANN had a purely technical function, and that it therefore did not impact on human rights. It was no surprise that civil society put human rights on the agenda in one of the CCWG subgroups, Working Party 2 (WP2), which also dealt with defining the new ICANN mission and bylaws during WS1. Nonetheless, human rights was moved from the WP2 work plan by the group's rapporteur, working for one of the largest gTLD registries, who informed the CCWG plenary mailing list in March 2015 that: "Various suggestions about giving ICANN a human rights mission was [sic] not included: ICANN is not in the business of content and giving ICANN a promotion of human rights was problematic."[34]

34 https://mm.icann.org/pipermail/accountability-cross-community/2015-March/001550.html accessed May 9, 2017

This opposition changed when civil society participants started translating human rights concepts to the ICANN context. One example was the translation of human rights principles such as the right to due process to ICANN's Independent Review Process and other dispute resolution instruments. Similarly, the right to freedom of expression related to rules in the Applicant Guide Book for the auction of gTLDs, and ICANN's activities as an employer related to the International Labor Association's Declaration on Fundamental Principles and Rights. This translation—or "the task of reconciling meanings" (Star and Griesemer 1989, 388) of a concept across social worlds—ensured that people could "work together" (Star and Griesemer 1989, 389). This position was galvanized by the agreement reached and confirmed toward the end of 2015 that ICANN would not enforce human rights obligations on third parties, but solely focus on respecting human rights in its own policy development processes and operations.[35]

35 https://community.icann.org/download/attachments/56132135/ICANN%20Commitment%20to%20Human%20Rights-210817658-v2.pdf?version=1&modificationDate=1446762030000&api=v2 accessed March 12, 2018

When it was clear ICANN would respect human rights within its own scope and mission, the discussion shifted to individual human rights, and the balancing of the interests of different groups. This tested the ability of human rights as a boundary object to be "both plastic enough to adapt to local needs and constraints of the several parties employing them, yet robust enough to maintain a common identity across sites" (Star and Griesemer 1989, 393). The Right to Property was regularly mentioned as a concept of contention. This is because there is an inherent tension between the Intellectual Property Constituency on the one hand and parts of civil society that have strong views on freedom of expression on the other. While intellectual property advocates wanted to protect trademarks and potential violations of trademark and copyright, both in terms of content and domain names, through DNS freedom of expression advocates aligned with the technical commu-

nity, and the existing ICANN bylaws, on the idea that ICANN has a technical function and does not engage in content regulation. This coincided with the discussion on the potential inclusion of a reference in the new bylaw to one particular human right (such as freedom of expression or the right to property), to several human rights, or to all of them. Here the civil society participants advocated that human rights are "universal, interrelated and inter-dependent,"[36] and that there should be no "cherry-picking"[37] among different human rights; a position subsequently also embraced by representatives of the Intellectual Property Constituency. This led to some contention in both the Intellectual Property Constituency as well as in the NCSG, where people argued that the right to property, the right of the author, and freedom of expression should be singled out. In this situation, human rights accommodated both groups and bridged the concerns by functioning as a boundary object that allowed "social worlds which share the same space but different perspectives" (Star and Griesemer 1989, 412) to translate each other perspectives, because the full set of human rights make the boundary object recognizable from both social worlds, therefore allowing both to progress.

36 http://mm.icann.org/pipermail/wp4/2015-November/000265.html accessed September 1, 2017

37 http://mm.icann.org/pipermail/wp4/2015-October/000184.html accessed September 1, 2017

The Last Steps: Tacking Back and Forth Between the Ill-Structured and the Well-Structured

With the translation to different social worlds and the accommodation of the boundary object, respect for human rights came closer to being standardized in ICANN's procedures. However, this section shows how a boundary object can also resist standardization and demand a higher level of interpretative flexibility, forming part of the process of productive contestation. One of the final topics of contestation during WS1 was the discussion on which human rights document should be explicitly mentioned in the new bylaw. The deadline for finalizing the work before the contract between ICANN and the NTIA ran out in October 2016 was fast approaching, so there was a palpable sense of urgency. Governmental representatives, and the civil society representative on the Board of Directors (who nevertheless worked his career in the Swiss government), preferred a sole reference to the Universal Declaration of Human Rights (UDHR), whereas several other individual civil society participants preferred a reference to the UDHR, the Internet Covenant on Civil and Political Rights (ICCPR), and the International Covenant on Economic, Social and Cultural Rights (ICESCR),[38] with some civil society participants also wanting to include a reference to the UNGPs. This was countered by

38 The UDHR, ICCPR, and ICESCR are together called the "International Bill of Human Rights." The UDHR is an aspirational document, whereas the ICCPR and the ICESCR contain binding commitments.

many participants in the CCWG, because it was unclear what a commitment to binding documents like the ICCPR and ICESCR would entail for ICANN, and there were severe concerns about the possibility for chain responsibility that might come with adopting the UNGPs. Civil society representatives countered that the UDHR was merely an aspirational document, and therefore quite weak. This standoff signals the resistance to detailed standardization at this point in time, or "the process of tacking back-and-forth between the ill-structured and well-structured aspects of the arrangements" (Star 2010, 601). The conflict was resolved by not mentioning a specific declaration, covenant, or instrument, but by instead using the phrase "internationally recognized human rights," without defining in WS1 which documents would be applicable. It was also agreed that the bylaw would receive a "Framework of Interpretation" (FOI), to be developed in WS2; allowing for even more detailed translations of the boundary object, and working toward standardization. Until this FOI was developed, the Human Rights bylaw would not come into force. This appeased both the civil society representatives who wanted human rights to be part of WS1 and the bylaws, as well as the other participants who were of the opinion that it needed further elaboration before it came into force. This was the proposal that gained consensus in the CCWG and was approved by the ICANN community, and thereafter by the ICANN board and the NTIA, which led the U.S. government to voluntarily rescind direct control over ICANN and handing stewardship over to the "international Internet community."

Productive Contestation at Work

This article has shown how human rights functioned as a boundary object in the negotiations that took place during the IANA stewardship transition, both within civil society and between civil society and other stakeholder groups.

Human rights functioned as a boundary object within civil society, translating between the social worlds of different cohorts of civil society advocates with different backgrounds and experience; this showed that civil society is not a monolith, but rather consists of different cohorts and factions. On the one hand, there were free speech advocates, often with a North American background, and on the other hand there were more recent participants in ICANN who had a broader conception of rights and more experience with the human rights framework (Milan and ten Oever 2017). Human

rights provided structure to the discussion, which allowed for the accommodation of both perspectives. I call this a process of "productive contestation," because despite disagreement and conflict between the parties, the interpretative flexibility of human rights as a boundary object allowed for a historical achievement. Whereas human rights in civil society could be translated to an overarching norm between the different groups, norms by themselves do not always have sufficient pull to structure consensus among actors outside of civil society. Human rights needed to be translatable to the respective social worlds of the stakeholders in the overall institutional ecology, in order to result in a productive outcome. This requires both active translators, as well as contestation from the different social worlds to make the boundary object "work."

Human rights, in the context of ICANN, was "worked on by local groups who maintain[ed] its vaguer identity as a common object, while making it more specific, more tailored to local use within a social world" (Star 2010, 604–5). Governments translated it to their own environments, in which they were already beholden to human rights as part of their treaty obligations; civil society understood it as development toward a standardization in the ICANN process of rights that are relevant to ICANN, such as the right to freedom of expression, the right to privacy, the right to freedom of association, and the right to due process;[39] intellectual property advocates felt reassured by the right to property and the right of the author; for the business sector it helped to fulfill the fourth criterion of the NTIA, which was "to maintain the openness of the Internet." Human rights as a boundary object allowed different stakeholders to have different interpretations, while having enough immutable content to maintain its integrity. This process clearly does not resemble the Habermasian ideal of an encounter based on dialogue in which agreement and understanding are produced based on a shared rationality. Rather, what we see is the accommodation of different social worlds with their own interpretations, interests, and embedded knowledge, which are made to work thanks to the structuring properties of human rights as boundary object.

39 https://community.icann.org/download/attachments/53772653/article19_ICANN_1706_reviewed.png?version=1&modificationDate=1466841961000&api=v2 accessed March 12, 2018

The process of negotiation was a standardization effort to create a practice of respecting human rights in ICANN procedures, as well as an effort to develop an understanding of what human rights in the context of Internet governance meant and entailed for the various stakeholder groups. When stakeholder groups developed interpretations that were incongruent with the interpretations of other stakeholder groups, contestation emerged. The structure

and functioning of the boundary object led to a productive contestation, because it allowed for the accommodation between different social worlds, and thus for the development and exploration of specialized identities of the boundary object, while keeping a common overarching and recognizable identity. Contestation comes into play when the common identity is threatened or when incongruent identities are developed in different social worlds. Productive contestation happens when the boundary object is further explored or developed toward standardization by providing the basis for a collaboration, while also accommodating dissent through a process of translations and interpretative flexibility. In this case, this happened both within the civil society stakeholder group (between different cohorts of civil society actors), as well as between stakeholder groups.

Human rights as a boundary object allowed for sufficient interpretative flexibility to: offer the assurance of the informational structure of the human rights treaties (such as the UDHR, ICCPR, and ICESCR); offer process guidance as is provided in the UNGPs; and allow for the customization of the process in WS2. This allowed civil society to start a process of standardization, and embed human rights in the regulatory documents of a central Internet governance body, an inherent part of the Internet infrastructure, while still tacking back-and-forth between the ill-structured and the well-structured aspects of this particular boundary object (Star 2010, 614).

While there is now a commitment to respect human rights in ICANN's bylaws, this does not necessarily mean a concrete policy change, because the bylaw will only get activated once a framework of interpretation is developed in WS2, which is expected to take from August 2016 until June 2018. Some critics might argue that this means that nothing concrete has been achieved, except for the prospect of more discussion after the IANA transition in October 2016. I argue that the development of a framework of interpretation paves the way for a process of further standardization. When the bylaw is implemented after the development of a framework of interpretation, the boundary object will become standardized; potentially leading to new practices (and communities of practice) that could also function in turn as boundary objects—such as the practice of undertaking human rights impact assessments of ICANN policies in the Policy Development Processes, or of engaging in human rights impact assessments of the operations of ICANN as an organization.

Conclusions

In this article I have shown that, during the discussions on the transition of the control over ICANN from the U.S. government to an entity called "the international Internet community" from June 2014 until October 2016, human rights functioned as a boundary object, meaning that it was sufficiently familiar and acceptable as a concept to all stakeholders, but at the same time meant something different for the different groups in their respective social worlds. This allowed for human rights to "both inhabit several intersecting social worlds (…) and satisfy the informational requirements of each of them" (Star and Griesemer 1989, 393), while also adapting to the structure of information and work process needs and arrangements, providing interpretive flexibility, and tacking back and forth between structured and more tailored uses of the concept of human rights (Star 2010; Star and Griesemer 1989).

Human rights formed a bridge between the information infrastructure in ICANN and international law, and allowed for local interpretations by different stakeholder groups, while keeping a recognizable conceptual integrity across social worlds in a process of productive contestation. The power of ideas helped civil society to put the topics on the agenda, but the functioning of human rights as a boundary object structured the multistakeholder negotiations, which would not have been possible without the translations made by civil society actors. The arrangement of the negotiations was built on the translation between the social worlds of respective stakeholders in these negotiations, and translations between existing legal and political texts, practices and experience of human rights, the ICANN context, and the NTIA criterion for the maintenance of an open Internet.

Boundary object theory offers a lens to analyze negotiations in a multistakeholder environment in which stakeholders with different backgrounds and perspectives govern a global resource. It has shown how civil society was able to leverage a long-discussed topic during a time of transition, and to engage in a cross-community process of productive contestation; the development, negotiation, and inscription that altered the infrastructure of a global governance institution.

Further research is needed to compare whether similar patterns can be observed in other multistakeholder Internet gover-

nance organizations in particular (such as the Internet Engineering Task Force and Institute of Electrical and Electronics Engineers), and within global governance in general. Another possible angle for further research is understanding whether the intentional choosing of concepts and topics that can function as boundary objects is a tried and tested action repertoire of civil society in global governance, or whether it is being developed as part of a new repertoire of strategic action. In order to understand the effectiveness of civil society's participation in negotiations in the multistakeholder model, and thus potentially some of its democratic affordances, it is crucial to build an understanding of whether civil society actually has a say and is able to influence the outcomes of discussions, while structurally having access to fewer resources than other stakeholder groups. A final angle for further research could be analysis of how the commitment to human rights actually impacts ICANN's operations and its policy development processes—especially where it comes to discussions touching on freedom of expression, copyright, privacy, and social, economic, and cultural rights.

3

'This is not how we imagined it': Technological affordances, economic drivers and the Internet architecture imaginary

Abstract[40]

The Internet architecture is widely perceived as engine for innovation by providing the equal opportunity to deploy new protocols and applications. This view reflects an imaginary that guides the co-production of policy and technology that can be traced back to the early days of the Internet, which is still prominent among the engineers in one of the main governance bodies of the Internet: the Internet Engineering Taskforce. After the privatization of the Internet architecture in the 1990s, the interplay between the architectural principles of end-to-end, permissionless innovation, and openness subverted equality among Internet users and hampered their ability to redesign the Internet. I draw on media studies, science and technology studies and international political economy, and use a combination of qualitative and quantitative methods to show how the Internet architecture's affordance structure got reconfigured, and how this facilitated the prioritization of corporate interests over the interests of end-users.

40 This chapter has been accepted, after peer review, to be published in New Media & Society as: ten Oever, Niels. Forthcoming. "'This Is Not How We Imagined It' - Technological Affordances, Economic Drivers and the Internet Architecture Imaginary."

Introduction

When in the early nineties the Internet was released from the labs and found its way to millions of users, it was widely perceived as an engine for innovation (Van Schewick 2012), an information highway (Flichy 2007) and a tool for democratization (Castells 2009). These expectations and aspirations accompanied the development of the Internet architecture and were operationalized through three main architectural principles: end-to-end, permissionless innovation, and openness. In this paper, I show how the interplay between these principles, after the privatization of the Internet in the early 1990s, undermined the equality of users and the ability of individuals, researchers, and small companies to redesign the Internet.

The Internet architecture is co-produced by corporations, state actors, researchers and advocates in a self-regulatory industry standards body called the Internet Engineering Taskforce (IETF).[41] Self-regulation has been the general paradigm for the governance of the Internet because it is assumed to be most suited to the transnational and quickly evolving nature of the Internet (Price and Verhulst 2000). The evolution of the architecture of the Internet is taking place through the development of open and voluntary standards that facilitate interoperability between the products of

41 The IETF is by no means the only standards body involving the Internet. For instance the World Wide Web Consortium (W3C) sets standards for the web. Other examples are the Third Generation Partnership Project (3GPP) and the Institute for Electrical and Electronics Engineers (IEEE) who set standards for wireless and wired communication.

network operators, equipment vendors, content and service providers, and software developers. Because of the nature of the standard setting process, it has been described as a 'wild mix of politics and economics' (Shapiro and Varian 1998) and 'politics by other means' (Abbate 1999). While the standards and protocols that are developed in the IETF are largely hidden from the larger public, they shape our behavior (Chadwick 2006), determine vectors of control over user data flows (Galloway 2006), how users access information (DeNardis 2014), how users can exercise their rights online (Lessig 2006).

To understand the standard setting process I use the terms 'sociotechnical imaginary', 'co-production', and 'technological affordance'. A sociotechnical imaginary is the combination of visions, symbols, and futures that exist in groups and society. It influences behavior, individual and collective identity as well as the development of narratives, policy, and institutions (Jasanoff and Kim 2015). A sociotechnical imaginary guides the process in which people co-create knowledge, technology, and order, a process that Jasanoff (2004) calls co-production. Technology, which is an inherent part of this co-production process, inhibits and stimulates human behavior. Hutchby (2001, 441) describes this 'constraining, as well as enabling, materiality of artifacts' as *technological affordances*. I leverage these terms to show how the Internet architecture's sociotechnical imaginary and its technological affordances got reconfigured and subverted during three decades of co-production following the commercialization and privatization of the Internet. This compounded theoretical lens allows me to simultaneously take into account the shaping of institutional configurations, technological orderings, economic drivers, and the collaboration among disparate groups and competitors facilitated by a joint vision. This approach enables me to analyze the Internet architecture as a site of contestation (ten Oever 2018), as an assemblage of power (DeNardis 2014), and 'as a normative "system of systems"', and to unpack 'the micro practices of governance as mechanisms of distributed, semi-formal or reflexive coordination, private ordering, and use of internet resources' (Epstein, Katzenbach, and Musiani 2016), without defaulting to a reductionist approach.

First, I will provide an overview of the relevant literature, subsequently I give an overview of the methods used in this research, and provide an analysis in which I will establish the Internet architecture imaginary and subsequently show how it got subverted. Finally, I will offer some thought about what this means

for self-regulatory Internet governance models and avenues for further research.

An imaginary space between a technological dream and an economic reality

Instead of looking at the content of data streams, which is like the 'juicy piece of meat carried by the burglar to distract the watchdog of the mind' (McLuhan 2013, 19), I argue we should rather look at the *preconditions, shapes, and characteristics* of data streams: the Internet architecture. Before elaborating this position, I will first describe the process through which the Internet architecture is co-produced and introduce the concept of the sociotechnical imaginaries as a lens to understand this process and give an overview of recent academic debates pertaining the Internet architecture. Contemporary debates in media studies, science and technology studies and governance studies that discuss the Internet architecture focus on: (1) the values, or lack thereof, that are enshrined in the internetworking protocols (Braman 2012b; Flanagin, Flanagin, and Flanagin 2009), (2) how the Internet infrastructure is used to exercise control (Eeten and Mueller 2013; Musiani et al. 2016), and (3) consolidation and market concentration in the Internet architecture (Mansell 2013; Easterling 2014; McKelvey 2018).

Technical standards, of which networking protocols are a subset, are rules, procedures and formats that facilitate communication between two or more parties. The Internet architecture consists of 'standards which make up the technical back-bone of an information infrastructure' (Hanseth and Monteiro 1997, 183) that, through its affordance structure, dynamically shapes our information societies. The Internet architecture is co-produced in governance bodies and Standards Developing Organizations such as the IETF. Whereas theoretically participation in the IETF is open for everyone, it is dominated by employees of transnational corporations. The most common affiliations of the authors of IETF output documents, the so-called RFC-series, are: Cisco, Huawei, Ericsson, Google, Juniper, IBM, Nokia, Microsoft, AT&T, and BBN.[42] The RFC-series (an abbreviation for Request for Comments) should not only be understood as a series of technical documents but also as policy documents (Braman 2013) which describe the values, processes and procedures for co-production

42 https://www.arkko.com/tools/allstats/companydistr.html accessed on November 17, 2018

and therefore are relevant for understanding the sociotechnical imaginary of the Internet architecture. Most RFCs, however, are written by authors with an affiliation in the private sector, there are also many RFCs that have been authored by researchers, and even some by members of civil society organizations.

The Internet architecture's sociotechnical imaginary revolves around doing things that are 'for the good of the Internet' (Mathew 2014, 160), sustaining a 'generative Internet' (Zittrain 2008, 6), and is underpinned by three specific engineering principles: end-to-end, permissionless innovation, and openness (Internet Society 2012). The Internet architecture's imaginary is rooted in the idea that the network is a general purpose 'common carrier network' (Davies et al. 1967, 3) where 'all hosts are equal' (Mogul et al. 1984, 1), meaning that they can function as general purpose end nodes (cf. Padlipsky 1982; Braden 1989; Carpenter 1996), and that everyone has the freedom to shape their own traffic by deploying new protocols between end nodes, and thus redesigning the Internet. The ability to freely deploy protocols fits very well with the 'ideology of open standards' (Russell 2014, 21) and the voluntary nature of the Internet standards developed in the IETF. In this paper I interrogate this sociotechnical imaginary because '[m]yths are important for what they reveal (including a genuine desire for community and democracy) and for what they conceal (including the growing concentration of communication power in a handful of transnational media businesses)' (Mosco 2005, 19).

DeNardis (2009) explores the complex process of the co-production of the Internet architecture by describing how the mere transition from one protocol to another caused a significant amount of contestation because of its geopolitical interests and impacts. This process of contestation is described by Clark et al (2005), who argue that there are different adverse interests at work in defining the Internet architecture, that this 'tussle' should be accommodated because 'it is crucial to the evolution of the network's technical architecture' (Clark et al. 2005, 462), and that rigid designs which do not accommodate this tussle will not survive the passage of time and will be broken. Braman (2011) convincingly shows that social policy issues such as rights and freedoms have always been part of the Internet standards deliberations. Braman (ibid), however, did not address how or whether these discussions actually resulted in changes in the technical materiality of the network. Davidson, Morris, and Courtney foresaw Braman's findings but argue that while 'many technologists within the leading standards bodies are public-minded, few have explicit expertise

in policy-making or at interpreting the public interest. Standards organizations have always (appropriately) emphasized technical goals over societal ones' (Davidson, Morris, and Courtney 2002, 4). Since the call of Davidson et al to assess the impact of protocols in the IETF there have been several efforts to better understand the relationship between values and networks (Orwat and Bless 2016), develop guidelines to integrate human rights considerations in protocol design (ten Oever and Cath 2017), and calls for the IETF to 'enable the actualisation of human rights through the protocols and standards it designs by implementing a responsibility-by-design approach to engineering' (Cath and Floridi 2017, 449).

The IETF has not operationalized any structural assessment of the impacts of their standards and protocols. The lack of integration of impact assessments in the standards process and the intentional undermining of technical standards has led to a discussion about the legitimacy and adequacy of the self-governing technical standards bodies to deliver a trustworthy Internet architecture (Rogers and Eden 2017). Internet shutdowns during political events, such as elections, foregrounded how the Internet architecture is used as a domain of control and showed how infrastructure is used by governments to realize their objectives. Research has established a trend of the enactment of governance objectives through and by private parties rather than governments (Arpagian 2016; DeNardis and Musiani 2016). Levinson and Cogburn (2016, 219) remark that this process is tightly connected with the privatization of the governance of the Internet architecture. While the privatization of the Internet architecture was supposed to lead to competition and innovation (Cowhey, Aronson, and Richards 2009; Van Schewick 2012), this paper argues that actually led to the subversion of equality between hosts and the freedom to deploy new protocols.

As described above the Internet architecture has been an object of research in different fields, but analyses that take into account the combination of the guiding sociotechnical Internet architecture imaginary, the materiality of the technology, and economic drivers, are still quite rare, but are gaining traction (eg. DeNardis 2014; Mathew 2014; McKelvey 2018). Analyses generally take into account institutional and technical aspects, such as Dourish (2018) has done in his analysis of IPv6; or rather, it takes economic and institutional aspects into account, such as Van Schewick (2012), Russell (2014) and Smyrnaios (2018) have done. Arguably, both approaches undervalue the dynamic interplay

between technological materiality, institutional configurations, and economic drivers. I argue that it is exactly this interplay that creates new orderings and affordances. My theoretical contribution is to reveal how economic drivers prompted an interplay among architectural principles which led to a reconfiguration and subversion of technological affordances and the Internet architecture's sociotechnical imaginary. This seeks to overcome an economic, legal, or technological reductionist approach in the analysis of the Internet architecture.

Methods

My research into the IETF started with a long-standing fascination for RFCs: their language, particular formatting, and authoritative standing for everyone interested in computer networking. The institutions, people, and processes behind the production of the RFCs, their infrastructure so to say, only became apparent when I started participating in the IETF and its surrounding environs. This participation is the basis for my ethnographic memoir, which developed into participant observation when I formalized my research plans. The research period spanned between March 2014 and July 2018, during which I participated in 11 tri-annual IETF meetings and actively participated on mailinglists. I participated in several Working Groups, and served in several leadership positions. This experience provided me with a first-hand account of the practices in the most prominent Internet standards body, as well as access that an external observer might not otherwise have. In qualitative research, the researcher is an inherent part of the creation of meaning (Denzin, Lincoln, and Giardina 2006), part of a critical ethnographic practice is therefore 'an ongoing commitment to re-thinking and re-doing one's work as ethnographer and activist' (Lave 2011, 2). Part of this process was to address my particular situatedness in the fieldsite (Haraway 1988), namely as an activist-engineer-researcher. In order to gather and seek to understand different points of views, I employed a mixed method approach, to triangulate and validate my findings, and in that process to create an opportunity for reflection on research context, the relationships with the community I researched and was situated in, and the power dynamics in the process of knowledge production (Haraway 1991).

In order to analyze the evolution and emergence of explicit values in the large body of data on transnational governance of the Internet infrastructure, I engaged in the quantitative analysis of

IETF mailinglists and the IETF's technical documents published in the so-called RFC-series. In my analysis I focused on prevalence and development over time of language related to society, ethics and rights, as well as trends in the professional affiliation of document authors, guided by intuitions that arose from participant observation. I obtained these documents from the IETF website, after which I undertook a quantitative document analysis of the RFC-series using the JavaScript-based tool rfc-analysis[43], and engaged in quantitative mailing list analysis using the Python-based tool BigBang[44], to gain a deeper insight into cases, trends and interactions. The outcome of these quantitative analyses informed the creation of the questionnaire I developed for the interviews, and helped me focus on architectural principles and specific protocols. I engaged in 25 semi-structured interviews with IETF leadership and RFC authors through a purposive sample of seasoned and visible members of the Internet protocol community. The audio was transcribed and analyzed using qualitative methods informed by thematic analysis, with which themes were identified and coded across interviews. Through the identification of themes, concepts, practices, and activities, I analyzed the interview data to understand the ways in which the Internet architecture fundamentally changed from the early 1990s up to now, and how that affected the equality of users and their ability to design and deploy new protocols. The last step of triangulation and validation was to see how my findings on the Internet architecture compared to the description of the Internet architecture in the RFC-series. Therefore I engaged in the qualitative analysis of a specific subset of RFCs. I made a purposive sample of 20 RFCs that mention 'architecture' and made a chain sample of 20 RFCs that are referred to in the aforementioned 20 RFCs to add background understanding for the architectural issues that are being referred to and that they are responding to. Finally, I analyzed 5 RFCs that specifically got mentioned during the interviews.

43 https://github.com/npdoty/rfc-analysis access on October 11, 2018

44 http://datactive.github.io/bigbang/ accessed on August 25, 2018

Analysis - On the idea of smart endpoints and the dumb pipes

I will first describe the Internet architecture imaginary, then I will describe the challenges in the form of the rise of the middlebox and the accompanying reconfiguration of the affordances of the architecture, and the subsequent iterative responses to overcome the obstacles presented by this new ordering.

The Internet architecture imaginary

The sociotechnical Internet architecture imaginary emerged during the early phases of the development of the Internet while it was still a research network. I focus on the stabilization of this imaginary that started with the privatization of the Internet in the early nineties when the US government ceded direct control over the Internet. This gave way to an increased amount of self-regulation through private governance bodies such as the IETF. When asking engineers in the IETF about the central architectural values or principles of the Internet protocol community, their answers have a significant amount of overlap. I will describe the imaginary as a category, or ideal type, based on the research data, which in reality can appear less monolithic and will have fuzzy edges. Nonetheless in the interviews, documents, and observations, the imaginary turned out to be remarkably consistent. The end-to-end principle (Saltzer, Reed, and Clark 1984), permissionless innovation, and openness (Russell 2014) get mentioned time and again in interviews as well as in technical and policy documents (Internet Society 2012). These three architectural principles shaped a sociotechnical imaginary which is rooted in the equality of 'internet host computers' (Mogul et al. 1984; Deering 1989), the ability to design and deploy new protocols between these computers, and to increase and grow the Internet with more computers and more users (Braman 2012a). The architectural principles have both sociotechnical and sociopolitical conceptions which play important roles in the co-production of the Internet. I will discuss the three architectural principles in depth, because they played a central role in the demise of the Internet architecture's imaginary.

The first architectural principle, the end-to-end principle, appeared as a central pillar of the values and principles of the architecture in nearly every interview, RFC3724 even calls it: 'the core architectural guideline of the Internet' (Internet Architecture Board 2004). The principle describes where to put functionality in the network, namely at the edges (Internet Architecture Board 1996), and let the network be 'dumb pipes'[45] that solely transports data. The end-to-end principle allowed for a 'tremendous amount of agency in individuals and anyone who could put a server anywhere. Anybody could make arrangements to have a prototype protocol pair that you could talk to with each other from anywhere to anywhere.'[46] This principle was infrastructurally a revolution because it contrasted so strongly with the communication networks that preceded the Internet. Endpoints that are controlled

45 N1418 (For reasons of anonymity the names of the interviewees are not listed here. Each interviewee was coded and is distinguished from other interviewees by a number)

46 N0218

by their owners can be altered quickly, and thus allow for freedom and flexibility. Changes in the infrastructure are far more cumbersome, or in the words of a former telecommunications engineer turned Internet engineer: 'we have the end-to-end principle because so you can do things really quickly on the infrastructure, but [..] if you have to change the infrastructure, that takes a long time'.[47] This captures the importance of the end-to-end principle for innovation, but it has further implications as a sociopolitical conceptualization, one engineer mentioned that:

> *There are other folks who take that principle to be more than an engineering principle, but rather an ethical or values driven principle which says that the role of the network is to enable parties to communicate with each other, and not to enable the network itself as a form of control, centralized control. I take both views.*[48]

48 N0618

The end-to-end principle provides users with the freedom to shape and create their own networking experience. This had a tremendously empowering effect on engineers: there was 'a desire to go your own way, um, and a kind of idea that we can invent our own rules and we don't need too many rules, but the ones that we want, we can invent'[49].

49 N1518

The second principle, the principle of permissionless innovation, describes that there should be no barriers to the deployment of new protocols. In other words: 'you don't need to negotiate with any entity in the middle of the network to get your new thing deployed. [...] [Y]ou don't need to negotiate with any entity in the middle of the network in order to transport your packets.'[50] Negotiating is meant here in both technical as well as sociopolitical terms; permissionless innovation depends on the fact that there is no authority that can sanction what protocols can or should be used. '[A] typical example is the Web. Tim Berners-Lee did not ask permission from anyone, he invented something, went back, built it, and then it was downloaded and no one [...] had anythin to say about it.'[51] This sociotechnical conceptualization has clear sociopolitical implications: there should be no limitations on the ability to deploy new technologies on the network. With this principle participants in the IETF also limit their own authority and responsibility, summarized in an often repeated phrase among long time participants: 'we're not the protocol police'[52].

50 N0118

51 N1618

52 N0218

The third principle, the principle of openness, is described as the property 'that you can reach from any point of the Internet to

any other point of the Internet without your packets been hampered or they'd been stopped or so on'[53], it furthermore means that new computers can be added to the network.

53 N0918

The sociotechnical conception of openness is directly coupled with a conception of connectivity, access, as well as their explicit sociopolitical consequences. Except for the socio-technical conception of openness of the network, openness is also often associated with the socio-political consensus approach to standards development, which fits into an 'ideology of open standards' (Russell 2014, 21)that 'linked the open standards-making process with the ideals of participatory democracy, open markets, individual autonomy, and social progress' (Rogers and Eden 2017, 804). Similar to the end-to-end principle and permissionless innovation, openness is not only associated with a technical ability, in this case to add nodes to the network, but also with open communications, open standards, as well as with open governance (Internet Society 2013). The ideal of participatory democracy is also reflected in the IETF's unofficial motto: *'We reject: kings, presidents, and voting. We believe in: rough consensus and running code'* (Clark 1992, 543), a credo which was minted during the Internet-Open Systems Interconnection (OSI) standards war (Russell 2006; DeNardis 2009), when the governance model of the IETF was heavily tested and further refined. This process strengthened the organizational practice that individuals opinions should seriously be considered and discussed, and cannot simply be overruled by an authority or a majority (Resnick 2014). This shows the strong interrelation between the technology, the institutional organization of the IETF, and the community that co-produces the architecture. The make up of the community participating in the IETF, however, has changed over the years. In the early days of its work, the Internet architecture was produced largely by network researchers that were working at universities and as government contractors. Since the privatization of the Internet in the early nineties, there has been an exodus of researchers (Ding et al. 2013), whose ranks have been filled by contributors from the private sector who now dominate the IETF. This can, for instance, be observed in increasing preeminence of private sector affiliations among authors of RFCs.[54]

54 https://www.arkko.com/tools/allstats/companydistr.html accessed on November 19, 2018

55 https://www.ietf.org/about/participate/get-started/ accessed on November 19, 2018

56 https://www.srgresearch.com/articles/switch-router-revenues-set-new-record-cisco-market-share-still-over-50 accessed on March 5, 2019

While the IETF community makes explicit statements about values and principles, its website says: 'We try to avoid policy and business questions, as much as possible'[55]. This is quite a remarkable statement for self-regulatory body of a $44 billion networking-infrastructure market[56]. Interestingly, the architectural

principles that have strong sociotechnical and sociopolitical conceptions at the same time anchor the architectural imaginary and obfuscate the socioeconomic reality.

Cracks in the Imaginary I: Firewalls, NATs, and network management

The first threat to the end-to-end principle, the openness of the Internet, and permission innovation took the form of *middleboxes*. Middlebox is a shorthand for: 'intermediary device[s] performing functions other than the normal, standard functions of an IP router on the datagram path between a source host and destination host' (Carpenter and Brim 2002). Middleboxes can have many different functions, such as firewalls, Network Address Translation (NAT) routers, IP-tunnels (such as Virtual Private Networks), and network management devices. The introduction of middleboxes formed a paradigmatic shift in the functioning of the network (McKelvey 2018). Whereas the network was previously supposed to function as a 'dumb pipes'[57], as outlined by the end-to-end principle, functionality was added to the network. This happened because of three issues that resulted from the rapid growth of the network: (1) an increased need for security, (2) the depletion of Internet Protocol (IP) addresses, and (3) increasing business interests (Internet Architecture Board 2004). I will shortly describe the reactions tho these issues below.

57 N1018

To be able to connect to the network every device needs a unique number: an IP address. It was never envisaged that so many devices would be connected to the network, so when more devices were connected, IP addressed were running out and a new addressing scheme needed to be developed. This was especially pressing since adding new nodes to the network is an inherent part of the principles of openness, one of the Internet's architectural principles. However, there was no direct replacement addressing scheme ready, and there were projections that IP addresses would run out by 1994[58]. This led to the introduction of the 'temporary solution' of Network Address Translation (NAT), which allowed a network of computers to share one public IP address (Francis and Egevang 1994) from the pool of IP addresses. While this was an efficient short-term solution, this directly went against end-to-end principle according to which 'packets [should] flow unaltered through the network' (Carpenter 2000). NATs interrupted the packet flow because the IP address of the end-device is not known to the network or the recipient and needed to be added by

58 N0718

the middlebox, thus adding functionality to the network.

When the network grew beyond a group of researchers, there was the need to introduce firewalls 'which screens network traffic in some way, blocking traffic it believes to be inappropriate, dangerous, or both' (Freed 2000, 2). Firewalls were installed on end-devices, home routers, but also inside larger networks and thus not only found at the edges of the Internet. A regularly implemented functionality of firewalls is directionality. This means that a network, and the computers connected to it, are 'protected' from receiving connections from an outside computer that it did not request. This is a sound security measure on the one hand, but on the other hand, it creates a difference between servers and clients. If your computer is located behind a directional firewall (or NAT), the computer cannot function as a server because other clients cannot reach you, traffic can only be initiated from one end of the connection. While many smartphones currently have more processor capacity and storage space than early webservers, they cannot function as a server because the network is imposing a one-directional ordering. This is how NATs and firewalls create the difference between producers and consumers. Network operators, with the help of equipment vendors, inscribed boundaries into the Internet architecture and attempted 'thereby to configure the user such that s/he can only meaningfully encounter the technology on the company's terms' (Hutchby 2001, 451). This represents the first step in the creation of inequality between Internet hosts, and thus creation of a class of mere users.

Network management is used by network operators to optimize network performance. There are different ways for approaching network management, a contested approach is the differentiation and prioritization of specific services over others, or even the blocking of some services or providers for economic reasons. This discussion is more commonly known as the net neutrality debate (Crowcroft 2007). One probably would not notice if you would receive an email a few milliseconds later, but if there is a delay in the delivery of a videostream, this might cause irritating hiccups. It might seem efficient to prioritize video content over mail traffic, there is, however, a fine line between network management and discrimination between kinds of traffic. If one prioritizes a specific kind of traffic or traffic from a specific provider, this could pose a barrier for alternative streams and providers to grow and develop, since competitors would have a distinct advantage. Violations of network neutrality also interfere with the end-to-end principle and the idea that the network should just transport packets.

The introduction of middleboxes in the network solved some immediate problems such as security issues, delayed other problems, such as the shortage of IP addresses, and create some economic incentives, in the case of the prioritization of services. The response to the issues of security and the lack of IP addresses could also be understood as response to the architectural principle of openness because if these issues would not be addressed it would hamper the connectivity of existing and new nodes. The changes in network management could be interpreted as enactments of permissionless innovation, but all responses inherently violated the end-to-end principle.

Cracks in the Imaginary II: The Advent of Ossification and the failure of SCTP

While middleboxes improved performance of specific kinds of traffic, they also negatively impacted the ability to alter protocols through a process called ossification (Thaler 2011). Ossification is the decreasing flexibility of the network which results in the inability to deploy a new protocol or protocol extensions due to the unchangeable nature of infrastructure components that have come to rely on a particular feature of the current protocols (Clark 2018). NATs and firewalls ossify around specific protocol characteristics. If these middleboxes receive traffic with other, and thus unknown, characteristics they will reject the traffic. While middleboxes seek to optimize the network, they actually hamper the ability to deploy new protocols. Or in the words of a senior network operator:

> *So at the moment there's a whole industry of middleboxes that basically break […] end-to-end connections. [T]hey end up ossifying the internet itself [...] because these are boxes that are trying to operate transparently and sort of invisibly you don't know that they exist or where they exist. You can't point to them even. They don't have an address. You can't do anything. They are bumps in the wire*[59]

59 N2218

Actually, ossification by middleboxes sometimes turns out to be a lot more than a proverbial bump in the wire by actually obstructing the deployment of new protocols as the following example shows.

The Stream Control Transmission Protocol (SCTP) was developed as an evolution to transport more data in a faster way than

was possible up to then. Initially it was standardized for telephone networks in 2000 (Taylor et al. 2000) and was adapted to be a general purpose Internet protocol in 2004 and after that has received updates for over a decade. Nonetheless, SCTP never significantly worked on the Internet. SCTP worked perfectly in the lab and lived up to all of its design expectations, but it would not work *in the wild*, on the actual Internet, because middleboxes added inflexibility to the network, in other words: *ossification*. In the words of a former SCTP developer:

> *[Y]ou can run [SCTP] on your own network when you control all of the middleboxes, but if you try to run it across the public internet there's some non-trivial points that the traffic won't get through because there will be some boxes like: "SCTP, what's that?". NAT middleboxes are a classic example there. [...] [Y]ou can't really run SCTP across the public network. We tried that and there's too many things in the way.*[60]

60 N2318

Middlebox induced ossification changed the Internet from an environment where equal hosts could deploy their own protocols, to a network where to design for the future, protocols need to look like the past. Foundational architectural principles of the Internet imaginary cannibalized themselves: in order to safeguard openness, permissionless innovation in the network was leveraged. This undercut the end-to-end principle, which in turn undermined permissionless innovation.

The introduction of middleboxes reconfigured the affordances of the network, with pivoted the locus of control from the endpoints to the network operators (Minar and Hedlund 2001). The latter were enabled in this endeavor by networking equipment vendors. There were clear incentives for both the network operators and the equipment vendors: the network operators wanted more control over their networks, and offer better performance to their customers. Equipment vendors wanted to sell the network operators equipment. The way they did this was adding more intelligence to the network, which was a relatively low investment for the operators which yielded results on the short term, and benefited the network equipment vendors. An Internet pioneer who was on the forefront of connecting new countries and continents formulated it this way:

> *There seems to have been the development that there is now more, some would say, 'intelligence' in the net-*

> *work now. Well, this is a bunch of shit from a bunch of basket cases like Cisco with a willing set of co-conspirators called network operators because in the telephone world they were the center of the universe. […] The network folks looked at this [the Internet] and said, no, no, and they found a willing co-conspirator in Cisco and instead of having 15 line router that just switched packets, now they have something with 50,000,000 lines of code.*[61]

61 N0818

Freedom, agency, and control was taken from the endpoints by network operators, with devices that were provided by equipment vendors. As I have shown this had both technical and economic reasons, which jointly surmounted to a reordering of the affordances of the network. This reordering largely benefited network operators and equipment vendors, not so much the people that were operating services on the endpoints, because they were hampered in the deployment of new protocols, such as SCTP. Thus a response from the latter group was to be expected.

The return of the strong endpoints: The Rise of QUIC

The limitations introduced by middleboxes accrued quite some resentment in the Internet protocol community because it constricted the freedom to deploy new protocols in the network. The fact that middleboxes do not announce themselves, and thus make the troubleshooting issues harder, added to the frustration. For quite some time, protocol developers could not find a solution: SCTP developers had worked on it for almost a decade and did not solve it. For content providers it became increasingly important to have a protocol that would deliver content in a faster manner over the networks, because of the increasing demand in streaming video and media rich websites. This finally became possible with the development of the Quick UDP Internet Connections (QUIC) protocol: a connection based stream protocol which supports multiple streams. QUIC functioned in a way similar to SCTP, with some extra features. A quintessential difference between SCTP and QUIC however was that the latter was developed by Google. Google already had a fast global Content Distribution Network and developed the most-used browser in the world: Google Chrome. Thus Google held two important pieces of the puzzle but needed a protocol to connect the two pieces: ‘Google is very invested in this [QUIC] because they make a lot of money off of making sure that no one gets in the path between them and the

user, and they centralize all that power.'[62] QUIC would allow Google to serve their content faster, and ensure that user data would not be shared with other parties, such as network operators. Both have significant economic implications for a company that makes most of its money via targeted advertising. But except for motive, Google also had the network control and capacity to develop this. In the words of a long time protocol developer: 'the reason that QUIC [..] can do what it can do is because the two endpoints are controlled by the same people, so they [Google] can, they can do like dark releases and AB-testing and all that that we can't do'[63]. 62 N2118 63 N0218

Google started developing QUIC in 2012 and in January 2018 between 2.1% and 9.1% of all Internet traffic was using QUIC, which is dominated by Google that uses it for 42.1% of its traffic (Rüth et al. 2018). Google was able to gain much better results than SCTP because it could do testing between its network and its browsers, and because it had significant resources to invest. Network operators would also think twice about blocking Google's faster services because it would negatively impact many of their users:

> *Google's big enough that it's very hard to stop in the sense that when you think about blocking Google you're blocking access to search and peoples' email and all of the different services that they provide, a huge number of different services.*[64] 64 N2118

This was another large non-technical but rather economic difference between QUIC and SCTP: QUIC already had a large market share through its user-base: Google's users. Google did not keep QUIC for itself as a proprietary protocol, Google brought QUIC to the IETF for standardization, which would increase the chances of broader adoption of the protocol, and therefore further ensure that new and updated middleboxes would not block QUIC traffic.

The implementation of QUIC will lead to a reordering of the network. QUIC was built to penetrate middleboxes and provide as little control as possible for network operators to shape, filter, or access data streams. QUIC was built to reconfigure the affordances of the architecture: it will reinstate the end-to-end principle and re-enable permissionless innovation but only as long as the QUIC protocol is used, creating a new path dependency. The cause and the effect are clear for protocol developers: 'the incentive for QUIC was to try and prevent ossification in the network,

but I think the implication is that it's going to take power away from the network'[65]. The reasons for this are the limitation incurred by the ossified network and power imbalance: 'I do think that there's a massive power differential that exists between people who run the network and the end users'[66], and now 'the pendulum is swinging the opposite way'[67] back to the end users. While QUIC restores the end-to-end principle, it cannot overcome the differentiation between users and providers introduced through NAT directionality, and therefore it does not restore equality between all hosts.

65 N2218

66 N2218

67 N2218

This brings us back to the initial conception of the Internet architecture's imaginary, wherein all hosts were equal and one could freely deploy protocols, strutted by architectural principles like end-to-end, permissionless innovation, and openness. While the limitations of ossification have partially been overcome through QUIC, this has only been possible by a significantly resourced transnational corporation, that also controlled large parts of the network, and controlled the worlds most-used browser, and could hire the best engineers, some of whom previously extensively worked on SCTP.

In other words, a precondition to restore part of the Internet architecture imaginary, was a significant economic incentive and technical and economic concentration, which contributes to an even further consolidated technological and economic reality. The increasing dominance of socioeconomic considerations over sociopolitical considerations is illustrated a member of the senior IETF leadership who confirmed that: 'you need to play into some of the operators or vendors earning models in order to get something deployed'[68]. This reflects demographic changes in the IETF: whereas the IETF used to be dominated by researchers, the overwhelming majority of participants now is representing the private sector. Deploying new protocols is still possible on higher layers of the networking stack, but less so in the lower layers of the architecture, unless one can gather resources like the one Google could muster, as we have seen in the example of SCTP. One simply needs to abide by the rules set by transnational corporations. In the words of a long time participant in the Internet protocol community: '[t]he mantra of the Internet enterprise is simple: 'Get Big or Get Bought!"(Huston 2017, 5).

68 N0118

It is probably the same phenomenon we see in other industries. When it is brand new[..] you have more freedom to think exactly about how you want this thing to work and not worry about

how much money you're going to make, because you're you will just make a lot of money. Now, a lot of people have made a lot of money off the Internet, there is still more, gobs and gobs need to be made, but it is a little bit crowded. We are heading a bit into the 'winner-take-all'-phase.[69]

69 N0118

While this startling socioeconomic reality, with significant impact on the material affordances of the Internet architecture, is widely recognized in interviews, the official IETF position is 'to avoid policy and business questions, as much as possible'[70]. This new socioeconomic reality, which is in part produced by the networks affordances, has cannibalized the Internets architectural imaginary, that is still being professed. The hollowed out sociotechnical imaginary actually functions as a cover, or even an implicit justification, for this consolidation of communication power.

70 https://www.ietf.org/about/participate/get-started/ accessed on November 19, 2018

Conclusion

The Internet architecture is hailed as an architecture in which all hosts are equal and everyone has the freedom to deploy their own protocols. This sociotechnical imaginary is anchored in the principles of end-to-end, permissionless innovation, and openness, and was operationalized through a process of co-production in Internet governance institutions such as IETF. When the Internet architecture was privatized a tussle over control over datastreams ensued between networks operators, enabled by equipment vendors, and content providers. This tussle led to the reconfiguration of the technical affordances of the Internet architecture. In this reconfiguration the equality of hosts and the ability to deploy new protocols between hosts has been subverted.

The sociotechnical Internet architecture imaginary and its self-regulatory governance model have not been able to cement the equality of Internet hosts and the freedom of researchers, small companies or individuals to function deploy new protocols, especially on lower layers of the protocol stack. Previously central sociopolitical conceptions and considerations that were part and parcel of the architecture's sociotechnical imaginary effectively faded into the background, while socioeconomic considerations have acquired a far more prominent place in the shaping of the Internet's technological affordances. The Internet architecture imaginary, that is still professed in IETF, obscures the socioeconomic reality in which interoperation between transnational

corporations has overshadowed the practice and ethos of doing things for 'the good of the Internet' (Mathew 2014). This dynamic arguably has contributed to the relative absence of the Internet architecture in current academic and policy debates on government regulation of the Internet, whereas the much discussed platforms and search engines are only a part of the Internet power assemblage.

The preceding analysis has shown how economic drivers spurred iterative changed in the affordances and materiality of the Internet architecture as well as its sociotechnical imaginary, illustrating the dynamic interrelation between economic drivers and technological affordances. This analysis contributes to the debates in governance studies by concluding that the self-regulation of the Internet architecture undermined the very design goals of the Internet architecture, changed its sociotechnical imaginary, and facilitated the prioritization of corporate interests.

Future research could focus on how standards development and self-regulatory governance bodies can take explicit values, such as the equality and freedoms of users, structurally into account as a formalized part of their processes, and what internal or external incentive structures would be needed to achieve this.

4

Norm conflict in the governance of transnational and distributed infrastructures: the case of Internet routing

Abstract[71]

This paper explores how prevalent norms are used to exert power and control in the governance of distributed infrastructures, such as the Internet. Through the lens of norm conflict, I analyze the structural resistance against the introduction of new norms in the transnational governance of the Internet routing. In a mixed-methods case study, I examine through an experiment how a community of network operators resists the introduction of data protection and human rights norms in the Internet routing infrastructure. To explain the ways in which existing norms enable the structural resistance to the introduction of new ones, I develop the notion of 'infrastructural norms'. This concept explains why Internet infrastructure governance thus far has defied national and international democratic norms. The understanding of how transnational infrastructure governance is used to exercise power and disseminate control contributes to the fields of global governance, international relations, and Internet governance.

71 This chapter has been offered as article for peer review and publication to *Globalizations*

Routing, Power, and Control

Something unusual happened in the realm of Internet governance in 2017: a Regional Internet Registry (RIR), an institution responsible for the coordination of numbers and addresses on the Internet, made headlines. In response to increasing Internet shutdowns on the African continent, a policy proposal was submitted to the RIR responsible for Africa. The proposal argued that when a 'government ordered blocking access to the general internet'[72], resources that are a necessary precondition to be connected to the Internet should be seized from that government by the RIR. The aimed result would be to disconnect the censoring government from the Internet. While the proposal was rejected, and later retracted[73], it shows how technical actors, such as RIRs, can have a significant impact on how governments, organizations, and individuals are connected to the Internet.

72 https://www.afrinic.net/library/corporate-documents/2061-anti-shutdown-01 accessed on July 18 2019

73 https://lists.afrinic.net/pipermail/rpd/2017/007671.html accessed on July 18 2019

As the Internet gets ever further entrenched into our civilization, '[s]ome of the most radical changes to the globalising world are being written, not in the language of law and diplomacy, but in [...] infrastructural technologies' (Easterling 2014, 15). Infrastructures, such as the Internet, mediate and penetrate all parts of society, and thereby set the invisible 'rules governing the spaces of everyday life' (Easterling 2014, 11). A significant part of the norms and

rules for the Internet are produced through a range of self-regulatory practices in a 'mosaic' (Dutton and Peltu 2007) of institutions, which together make up the transnational Internet governance regime complex (Nye 2014), also described as the polycentric Internet governance network (Scholte 2017b), of which Internet routing is a significant part. In this paper I explore the question how power and control are exerted in Internet routing, by looking at one of the places where the transnational governance of Internet routing takes place: a Regional Internet Registry.

By facilitating the interconnection among roughly 70.000 separnaturalate and independent networks, commonly known as Autonomous Systems (ASes), Internet routing forms a foundational part of the Internet as we know it, even though it is unknown and invisible to most people. These interconnected independent networks are mostly Internet Service Providers, Network Transit Providers, and large institutions, such as transnational corporations or universities. The routing of data traffic between these independent networks is shaped by an epistemic community (Haas 1992) of network operators that are often competitors, but that collaborate nonetheless through an 'economic of convention' (Meier-Hahn 2014). This in turn is enabled through relationships of trust, guided by an ideal of collaboratively acting 'for the good of the Internet' (Mathew 2014). However, Internet routing is regularly used as a tool for surveillance and censorship.

The interconnection, or 'inter-networking', of independent networks functions in a distributed manner. Facilitated by protocols, networks 'negotiate' among each other how data streams get routed through different networks to reach their destination. Internet routing nevertheless relies on centralized institutional structures for specialized functions, such as Regional Internet Registries (Mathew 2014). These bodies ensure that networks have unique numbers and addresses allocated to them. Next to that, RIRs are also the vehicle for policy development processes for Internet routing.

For this paper, I embarked on a case study of the RIR for the European region, the Réseaux IP Européens (RIPE), to understand how in cases of norm conflict, a dominant norm remains uncontested, while the introduction of data protection and human rights norms gets resisted. To examine this process, I engaged in an exploratory experiment in the form of an ethnographic probe through which I sought to inscribe a legal and an ethical norm in the Internet routing system. This process helped me to under-

stand how norms are used to exercise power and control in such a distributed, complex, and transnational infrastructure. To explain this process I deploy the concept of 'infrastructural power' (Mann 1984). This concept was coined to describe the capacity of the state to exercise control over its territory by means of infrastructure. In order to apply this notion to a transnational infrastructure such as the Internet, I expand the concept of infrastructural power beyond the territoriality of the state. Therefore, I introduce the notion of 'infrastructural norms', based on theories of norm conflict in international relation (Finnemore and Sikkink 1998; Thomas 2001). This concept helps to explain how norms are used to control and regulate dynamic and transnational infrastructure like the Internet, because norms create specific expectations, without having to prescribe specific behavior, or anticipate all possible changes, challenges, and innovations.

I will start off by providing an overview of recent discussions in the field of international relations and internet governance in relation to norms, Internet infrastructure, and Internet routing. Subsequently I introduce the literature on infrastructural power and norm conflict, after which I will give an overview of the methods used in this research. I start my analysis with the description of the prevalent norm in Internet routing. After establishing the prevalent norm, I describe the experiment I undertook, the responses that the experiment evoked, and what taught me about the prevalent norm and norm conflict. Finally a number of conclusions and avenues for future research is presented.

Internet governance, infrastructural power, and norm conflict

I approach Internet governance from the understanding that '[a]rrangements of technical architecture are arrangements of power' (DeNardis 2014, 7). To uncover practices of Internet governance, is to locate 'the politics of this architecture' (Ibidem). One way of doing this is by looking at the turn to infrastructure in Internet governance to exercise control (Musiani et al. 2016), which is especially relevant when it comes to control over main 'chokepoints' (Tusikov 2016, 36). Governance bodies and standard-setting institutions, such as the Internet Corporation for Assigned Names and Numbers, the Internet Engineering Taskforce, as well as Regional Internet Registries are examples of such chokepoints, because they are persistent fields of convergence for coordination, collaboration, and policy development. However, not only the formal

processes that these bodies facilitate are important. The building of trust, reputation, and personal relations, which is an essential part of these coordination processes, happens for a significant part at the meetings that these institutions organize (Mathew 2014; Meier-Hahn 2014). While not all Internet governance practices unfold in governance and standard-setting institutions, these bodies are focus points for coordination, and a place where many of the actors that produce the Internet, and exercise infrastructural power, meet to engage in so-called industry self-regulation, or in the *parlance* of the field: bottom-up coordination (Sowell 2012).

Within the field of transnational Internet governance research, the Internet's routing infrastructure has received relatively little attention. This is quite astounding since the production of interconnection between different networks is an important part of what makes the Internet work. Studies focusing on routing governance are concentrated on security (Kuerbis and Mueller 2011; Mueller, Schmidt, and Kuerbis 2013) or the economics of the routing infrastructure (Mueller and Kuerbis 2013; Mueller, Kuerbis, and Asghari 2013; Winseck 2019). Since the Snowden revelations that unveiled global surveillance practices in June 2013, there has been an uptick in research focusing into surveillance practices that are enabled by Internet routing (Rosa 2019), and research into geographically limited routing as a countermeasure to data surveillance and manipulation (Obar and Clement 2013; Dönni et al. 2015; Baur-Ahrens 2017; Lambach 2019). Two notable exceptions transcend the categories of security, economics, and surveillance, namely the work of Ashwin Matthew and Uta Meier-Hahn. Both have engaged in extensive ethnographic research into the epistemic community of network operators to foreground the social, socio-technical and socioeconomic fabric that enables, often competing, companies to collaborate (Mathew 2014; Meier-Hahn 2014; 2015). In this paper, I build on this literature to understand how norms are maintained and resisted in the Regional Internet Registry for the European region, the Réseaux IP Européens (RIPE).

To conceptualize how power and control is exercised through infrastructure, I leverage the framework of 'infrastructural power' (Mann 1984). Mann describes infrastructural power as the ability to exert control over territory without a centralized means of control. Infrastructural power is the weaving of an infrastructure induced web of control, which 'will territorialise social relations.' (Mann 1984, 210). Mann mentions communications infrastructures as a prime example of the exertion of infrastructural power

that produces territoriality. For the exertion of these powers, an actor does not need to have a monopoly over these infrastructures. Mann even argues that 'infrastructural techniques diffuse outwards from the particular power organizations that invented them' (Mann 1984, 194). I argue that this conceptualization of power, control and territorialization becomes even more powerful when it is applied to the Internet, especially because the Internet has been designed as an international network of networks (Braman 2012). Some researchers even argue that 'the Internet is non-territorial' (Van Eeten and Mueller 2013, 248). Because geographical borders are not recognized by the Internet's protocols and networks, the Internet functions as a plane of power and control that seems to transcends territoriality.

To expand the notion of infrastructural power and increase its applicability to deterritorialized, transnational and distributed infrastructures, such as the Internet, I will build on theories of norm conflict in international relations (Finnemore and Sikkink 1998; Thomas 2001; Hurrell 2002). Norms are 'widely-accepted and internalised principles or codes of conduct that indicate what is deemed to be permitted, prohibited, or required of agents within a specific community' (Erskine and Carr 2016, 87). Norms are a very effective means of regulation of dynamic and transnational systems like the Internet, because they create specific expectations, without having to prescribe specific behavior. The application of general norms in particular concrete situations is delegated to individual agents (Okuyama, Bordini, and da Rocha Costa 2011). In order to study norm conflict, I use the following definition: 'norm conflict occurs when the person is subject (by the normative system) to several requirements which cannot be simultaneously satisfied' (Hilpinen 1987, 37).

I combine the concepts of infrastructural power and norms to create the compounded lens of infrastructural norms. I argue that infrastructural power is exercised in the transnational and distributed Internet routing infrastructure through an infrastructural norm. Subsequently, I show that in the case of norm conflict, four sources of resistance emerge from the analysis to support the prevalent norm: (1) institutional configuration, (2) technological materiality, (3) economical incentives, and (4) supranational interest. Developing the concept of infrastructural norms, and exploring how several sources of resistance get leveraged in cases of norm conflict, adds to the empirical usefulness of the concepts of both norms and infrastructural power, and their application in polycentric governance networks.

Methods

Internet routing is co-produced by network operators of independent (mostly commercial) networks in coordination bodies called Regional Internet Registries, enabled by packet switching technologies that are implemented through commercial networking equipment. To understand this complex assemblage, I engaged focused on one specific Regional Internet Registry, namely RIPE, the RIR that is responsible for the European region. I started off my analysis with the main archives of RIPE decision making processes: its mailinglists and technical documents. On these I operationalized statistical, network, and discourse analysis to foreground the prevalence and evolution of norms, using the programming languages Python and R, and the BigBang toolkit[74]. To further explore initial findings and intuitions, I deployed an ethnographic probe to invite reflections on existing norms, values, and practices that were present in the RIPE community. The ethnographic probe consisted of a proposal to make data protection and human rights norms and inherent part of decision-making in Internet routing. This probe was introduced in three ways: via working group mailinglists, which are the authoritative channels for working group decision making, in a presentation at the bi-annual RIPE meeting, and in conversations with members of the epistemic community of network operators. The responses to the probe were captured through semi-structured interviews, mailinglist analysis, and participant observation. The selection of interviewees was based on a quantitative analysis of contributors to the RIPE mailinglists, and was subsequently adjusted to diversify the group with regards to tenures and roles in the RIPE community. The interviews were analyzed through thematic analysis, which enabled the identification of themes, which were coded across interviews. Through the identification of themes, concepts, practices, and activities, I analyzed the interview data to understand norms and norm conflict.

74 https://datactive.github.io/bigbang/ accessed on October 31st 2019

My research is situated in a paradigmatic body for the governance of Internet routing, namely the Réseaux IP Européens (RIPE), and lasted from September 2018 until October 2019. In this period, I participated in meetings, engaged in discussions on mailinglists, and visited the organizations offices. This allowed me to bare witness, and participate in, a process of meaning making as a researcher (Denzin, Lincoln, and Giardina 2006). I was particularly privileged in my access to the fieldsite because I had been involved in Internet governance through previous professional engagements. This provided a heightened amount of

access to, and knowledge of, the community, the technology as well formal and informal processes and procedures, which might not be as ready-at-hand for other researchers. To address my situatedness in the fieldsite (Haraway 1988), I employed a mixed method approach, to triangulate and validate my findings. This created an opportunity for reflection on the research context, the relationships with the community I researched and was situated in, and the power dynamics that are always present in the process of knowledge production (Haraway 1991). In every step of my research process, I sought to combine qualitative and quantitative approaches: I started with quantitative analysis of mailinglists (ten Oever, Milan, and Beraldo 2020) and technical documents, which was followed by extensive qualitative document analysis. The insights and intuitions inferred from this informed the development of an ethnographic probe. I captured the responses to this probe through mailinglist analysis, participant observation, and semi-structured interviews. The participants of the interviews were selected through quantitative methods. Through this combination of methods I sought to critically examine my own assumptions, preferences, and preliminary findings, to open pathways to new perspectives and explanations.

The voluntary interconnection norm

The Reseaux IP Europeens (RIPE) was the first Regional Internet Registry. RIPE was informally established in 1989 to help coordinate the fast-growing interconnection between different networks in Europe. From its inception onwards its goal and mission were clear. As described in in RIPE's establishing document, called RIPE-1:

- 'The objective of RIPE is to ensure the necessary administrative and technical coordination to allow the operation and expansion of a pan-European IP network.'
- 'All parties operating wide area IP networks are encouraged to participate'
- 'RIPE promotes and coordinates interconnection of IP networks within Europe and to other continents.
- 'RIPE is not a network service provider. IP networks collaborating in RIPE remain under the executive authority of their respective organisations.'(Blokzijl et al. 1992)

The interconnection between independent networks, as described in this founding document, produces the Internet. RIPE

is an inherent part of this process, because it helps to ensure that all numbers that are used for the independent networks (Autonomous System Numbers (ASNs)) and numbers for devices that need to be reached over the Internet (IP addresses) are unique, and are used by the organization to whom they are delegated. However, RIPE has no formal power over these independent networks. This stems, in part, from the social setting that helped spawn the organization. One of the people who witnessed the establishment process described this as follows:

> *The original operators were kind of the techies that knew each other on one hand and that were operating all the layers of the network in their organization. They had total control about their network, and so they could decide both the routing policies and the security measures, and they could actually agree on both of that with their fellow operators in kind of a social setting. And then there was a lot of trust because it was a much smaller community, much smaller environment. Everybody knew each other, and they didn't believe in like the malicious actors, or they thought that they could fight the malicious actors, there was the technical settings then and the social pressures and the social contacts. And then the internet itself grew, and the community kind of both grew and split, because there were differentiations of roles with the companies, and the internet became more like a business requirement which also required better security, let's say more businesslike, more structured.*[75]

75 N3319

The informal power of RIPE lies in the coordination of groups with diverging interests. This happens through the *voluntary interconnection norm*, a norm that can already be recognized in the aforementioned founding document, and which also emerged from interviews with network operators and staff of the RIPE Network Coordination Center, and from the analysis of RIPE mailinglists and other RIPE documents. This voluntary interconnection norm is a guiding norm that shapes a complex set of behaviors between actors with competing interests, that underlie the transnational infrastructure of the Internet. In the words of a seasoned network operators:

> *The Internet is not one thing. It's a composition of networks. People want to have control over their network. So in routing, being completely independent, being*

> *able to make your own choices, that's always been very important. The other one is [...] cooperation. There's no such thing as the internet, it's all networks connected to each other. So you need a lot of cooperation between all the parties involved to make it work.*[76]

76 N2719

The undertone of this attitude is caught more shortly in the often repeated adage 'my network, my rules'[77]. A long time RIPE participant further elaborated how the collaborations take shape:

77 N2719, N2819, N3719, N3819, N4019

> *We always think: 'oh there is a leadership. There is a center. There's a control'. But internet is nothing more—I mean, the closest thing to internet that I can see if a flock of birds, right? They fly together. […] They only follow some simple rules. [...] There is no leader bird or anything. But the flock works. And that's exactly how the internet works with BGP and DNS. It's decentralized. There is no decision maker, and the consensus of the whole thing, which is based on their interest. Again, that's another part that people forget. Each ASN has their own interest, but at the end, the common one, the only common one is that this network should work.*[78]

78 N3119

The Internet works through the interconnection between the different networks, and is based on the premise that all networks interconnect to make the routing of information possible. The more networks are interconnected, the better the network is, because it contains more users and information. But it also means that when networks are better interconnected among each other, the better the whole network is, because it is more resilient, and more data can be transferred with less delay. This can be understood as a network ethic, or network effect: more interconnected networks, and interconnection among networks, produces an increase in value for all networks (Lemley 1997). Therefore, what is good for interconnection, is understood as working 'for the good of the Internet' (Mathew 2014). This results in a norm that values interconnection between networks over everything.

If one further analyzes the voluntary interconnection norms according to the properties that norms have according to Finnemore and Hollis (2016, 438–42), it becomes evident that the interconnection norm applies to network operators, who make decisions about network architecture and interconnection among networks. The behavior that the norm informs, is the creation of

more interconnection between and among networks, in order to create a resilient network with high bandwidths and low latency. The voluntary interconnection norm is anchored and propagated through an institutionalized culture of network self determination and voluntary interconnection, and a common goal of doing 'what is good for the Internet'[79]. Some interviewees express there is an overlap between 'what is good for the Internet' and 'what is good for society', but are quick to add that this is currently not an inherent part of deliberations within RIPE[80]. In the words of a member of RIPE leadership:

> *very little of the routing decisions are made deliberately for the public good. I think there's a lot of accidental public good there, like a lot of capitalism. Sometimes it is good for people, but it's not designed to be.*[81]

79 N3219

80 N3919

81 N4019

The collective behavior upheld by the interconnection norm is that network operators facilitate and engage in interconnection between networks. The agreements between the networks are propagated through the network through route announcements, and recorded in the RIPE database. Many agreements are made at RIPE meetings, where reputation and trust play an important factor in the ability to make more and better interconnection agreements. As described by an industry pundit:

> *RIPE meetings become very important because you can establish direct contacts with the key movers at the key internet exchanges, the key engineers who are at the major ISPs and at the content providers.*[82]

82 N3819

To safeguard the independence of networks and their operators in the policy making process in RIPE, there is a strong emphasis on procedural values such as 'bottom-up processes', 'openness', and 'transparency'[83]. They function to safeguard the voluntary nature of the interconnection norm. In the words of a long time participant:

> *We have the old values of bottom-up structure, openness, transparency. And the people that are still around from that era—I think I should include myself in that—are still making sure those values stay there.*[84]

83 N2619, N2719, N2819, N3119, N3219, N3319, N3519, N3619, N3719, N3819, N3919, N4019 N2619, N2719, N2819, N3119, N3219, N3319, N3519, N3619, N3719, N3819, N3919, N4019

84 N2719

The interconnection norm functions, like every durable norm, in a self-reinforcing manner: if more people follow the norm, the norm becomes stronger, and creates more value for those who

subscribe to the norm. This value creation is not necessarily, or exclusively, financial. Every single interviewee mentioned the role of 'the RIPE community or 'the Internet routing community'[85] as an essential part of the production of interconnection. The community started from a wide-felt need of problem solving, in the words of a long-time participant: 'we built a network which was built on people trusting each other and people being able to pick up the phone to somebody else or send them an email'[86]. This sense of community among network operators allows for quicker problem solving, and help to increase personal reputation[87] and build trust[88] relations. This sense of community and trust relations have become an inherent part of the interconnection process, in the words of the seasoned network operators: 'to be able to peer with others, you need to establish trust relations'[89]. Thus delivery on the collective expectation of respect for the inter-connectivity norm, creates an institutional normativity among network operators, that in turn motivates willing compliance and cooperation (Jackson 2018), which in turn is rewarded with trust and reputation.

85 N{26-42}19

86 N4019

87 N2518, N3219, N4219

88 N2619, N2719, N3119, N3319, N3719, N3919, N4019, N4219

89 Peering is the interconnection of networks without costs involved for any of the involved networks

The voluntary interconnection in RIPE started through the production of interconnection between academic networks. One of the people who was there at the times describes this as follows:

> *That's how the RIPE community started, the RIPE community basically was just a bunch of physicists and other scientists [who] got together, and they tried to use that new IP protocol*

When the Internet later grew in size and importance, commercial actors became part of it, which was when a global inter-networking market was created. This global inter-networking market enabled profit-making, adding to the reinforcement of the interconnection norm. It also enables the financial sustainability of routing institutions, such as RIPE, through the payment of fees for acquiring numbering resources. While there are thus several incentives to reproduce the voluntary interconnection norm, a network operator reiterates that 'the main value is global IP connectivity'[90], that is the sense that is being shared in the community. It is the main, leading, and common denominator.

90 N4219

In the previous part of the analysis, I have shown how the voluntary interconnection norms guides the production of the Internet. In the following part of the analysis, I will further explore how the voluntary interconnection norm does not only enable specific

behavior, but also inhibits other behavior and norms. I will showcase this through an experiment in which I sought to introduce two norms into the routing of independent networks.

Probing the norm

In this final part of the analysis I explore the workings of the voluntary interconnection norm in norm conflict, by analyzing how it informs responses to the introduction of other norms. I explored conflict between norms by introducing an ethnographic probe to foreground existing habits and practices of network operators, as guided by the voluntary interconnection norm. The ethnographic probe consisted of the introduction of two relatively simple objects to RIPE's Internet Routing Registry, commonly referred to as the RIPE database. The simple objects I introduce are called 'as-sets'. An as-set is generally used to declare a policy that applies to a number of Autonomous Systems (ASes). An as-set could for instance indicate that a group of ASes are customers of another AS that is providing them with connectivity. This generally makes handling a large number of ASes more readable, scalable, and maintainable (Schmitz et al. 1999). The two as-sets I introduced contained the setting 'mbrs-by-ref: ANY', which meant that any network operator could add their AS to this as-set. The two proposed objects I introduced can be observed in figure 1 and figure 2 below:

Figure 6: AS-GDPR, source: RIPE database

Figure 7: AS-UNGP, source: RIPE database

The two as-sets, AS-UNGP and AS-GDPR, allow network operators to express that their AS respects the General Data Protection Regulation, or the United Nations Guiding Principles on Business and Human Rights. I chose these two norms because both are well defined international frameworks, and have been discussed and implemented by members of the Internet community. The General Data Protection Regulation (GDPR) is the current binding legal framework for data protection for Europe and European citizens, which means that many of the ASes are already subject to this regulation. The United Nations Guiding Principles for Business and Human Rights (UNGPs) is a leading set of guidelines for both companies and states to prevent, access, and remedy human rights abuses (Ruggie 2011), which also has been widely adopted in the sector, for instance by Cisco, Google, Ericsson, Microsoft, and Orange[91]. If these ASes would use these as-sets, one could for instance route data traffic preferentially, or exclusively, through networks that declare that they respect the GDPR or UNGPs.

91 https://business-humanrights.org/en/find-companies accessed on November 17, 2019

The proposal to introduce these two as-sets to the RIPE database was met with resistance among network operators from the get go. My first step was to share the proposal with the chairs of the two relevant working groups in RIPE, in order to present the proposal to the network operators gathered in the working groups that meet during RIPE meetings. The two working groups were the routing working group and the database working group. The chairs of these working groups rejected the presentation with the argument that this was not a technical proposal, and should be presented to a larger forum, namely the plenary meeting, in order for the working groups to obtain guidance from the whole routing community. Subsequently, I submitted the proposal to the Programme Committee for the plenary. The Programme Committee rejected the presentation proposal, and suggested it should first be discussed at the working group level. When I tried to bring up this deadlock with the working group chairs, they did not respond. After this, I suggested the introduction of these two as-sets to the mailinglists of the two respective working groups that set the policies for routing and the RIPE database, which did not yield any response. When asking experienced members what could have been the reason for this, they responded: 'That's very unusual. You should be proud of this. [laughs]'[92]. Another experienced participant explained it as follows:

92 N2619

> *That's—the idea that's time has not come yet. It's too early to introduce such a thing. [...] Because the oper-*

ators that can understand part of your proposal don't care about the other part, and the people who care about the other part—which is ethics and values—they don't understand what's the first bit.[93]

93 N3319

The participant made it clear here that the members of the epistemic community of network operators, who understand how the routing database works, do not care for the introduction of ethics and values in the routing system. But yet I did not know why.

Four sources of resistance

In order to gain deeper understanding of the question *how* the interconnection norms resists the introduction of new norms, I went to the RIPE meeting in May 2019 in Reykjavik, Iceland to conduct more interviews. When I arrived in Iceland, on the first day of the meeting, I received a one-line email from one of the co-chairs of the routing working group, asking me whether I could give a five-minute presentation to the working group, followed by five-minutes for questions and answers. Naturally, I responded positively. After I delivered a short presentation outlining the choice for the data protection and human rights framework, and their operationalization, a senior network operator who works for one of the largest networks of Europe and who has been active in RIPE since its inception was the first to respond. In a quite agitated manner he said at the microphone: *As we are forwarding packets, we have no concepts in the processing that are related to the stuff you are interested in.*[94] Initially, I understood this as a *technical source* of resistance to the introduction of values into routing. This technical resistance can be understood in a material way, in the sense that current equipment and technology does not allow for the introduction of new norms, or even of non-technical norms. It can also be understood as an *institutional source* of resistance, in the sense that it does not fit the objectives and rationality of RIPE and the RIPE database. The engineer then continued: *[…] Would I actually invest in the mechanisms to deal with that?'*[95] Here an *economic source* of resistance was led to bare. There is no reason, no incentive structure, for network operators to actually invest in the introduction of these norms. Especially since the introduction of these norms might potentially be detrimental to the increase of interconnectivity, since it would allow for discrimination between networks. There is simply no incentive for network operators to spend money or time to facilitate other

94 https://ripe78.ripe.net/archives/video/111/ accessed on August 23, 2019

95 https://ripe78.ripe.net/archives/video/111/ accessed on August 23, 2019

norms than the interconnection norm. A large network operator mentioned that even if they were willing to implement it, networking equipment vendors 'have limited software engineering time [...]. And they make decisions on what [equipment functionality] they want to press. And if it's not making them money, or if it's not a case of their largest clients asking them for something, they just de-prioritize it.'[96], which means they could not even implement it in the running of their networks.

96 N4019

Another response from the audience followed suit, which undermined the technical source of resistance provided by the previous networking engineer by saying:

> *Yes, we are in the forwarding packet business, but how we forward packets, and how we send them, already takes into account non-technical criteria, money being the most obvious one […] the question is whether the RIPE database is the good place? I am not so sure. Can it be done with the RIPE database? I am not so sure either.*

This confirms that the initial resistance, which I first understood as technical, was rather institutional. The technical protocol actually does already take explicit economic values into account, not solely concepts from computer science. Rather than a technical issue, it was a matter of behavior and expectations. In interviews that followed, networks operators framed their resistance in an institutional manner by stating that the scope of the RIPE database should be kept limited. Because adding norms 'is not what the RIPE database was made for'[97] and integrating these norms would 'build more things onto a system which is already just about fit for purpose'[98], by any means it should be maintained that Regional Internet Registries are not 'the routing police'[99]. These statements show that the interconnection norm, and the routing practices that are guided by it, are not seen as *neutral*, but rather to be in support an all encompassing norm, as a clear objective. The norm is hardly hidden.

97 N2619

98 N4019

99 N2619, N2719, N3119, N3219, N3719, N3919, N4119

The last source of resistance was harder to identify, even though it was widespread. It resembled institutional resistance, in the sense that it referred to an objective that got hampered, but instead of limiting it to the (narrow) objective of the routing database, it referred to the objective of the Internet to be global. I will call this the *supranational source* of resistance.

In the words of an interviewee:

> *I have concerns over attempting to encode those values into routing. I'm concerned that it's trying to put too—it's trying to build more things onto a system which is already just about fit for purpose. When we suddenly start kind of going, "Okay, you're making your routing decisions based on local law or otherwise, or on GDPR," it starts to potentially make local what we want to make global.*[100]

100 N4019

In another interview an engineer entertained the idea that the proposed as-sets might be useful, but then quickly realized the risks it might bring to the inscription of national boundaries:

> *The question is how we would implement something that is sort of ideologically, politically, and ethically neutral. No, ethically not. Ideologically and politically neutral so that anybody can express anything they want, you know, that certain countries, for instance, could say, "Okay. Let's tag some routes as national if we want to."*[101]

101 N2819

The concern of involving national interests was echoed by the routing software developer:

> *[H]ow can it [RIPE] say, "Well, we're just gonna stick with Western European values?' Well, hang on a second. [RIPE] serves 76 different countries or 73 different countries. That actually doesn't wash. You've shot your value system in the foot by taking a position to start off with, so you need to steer clear of this.*[102]

102 N2819

These concerns are not solely referring to the proposal at hand, but also about what consequences the adoption of these as-sets might have. In the history of RIPE, there has been a lot of resistance to the influence of countries who could demand national or regional routing proposals. Proposals to facilitate routing based on national borders have always been received with a lukewarm response within RIPE, to say the least (Dönni et al. 2015).

The supranational source of resistance makes the concerns of the network operators become more clear. When network operators say they 'don't like politicizing identifiers'[103], this should

103 N3119

be understood as: do not introduce norms that potentially limit interconnection and thus interfere with the interconnection norm. Every norm that relies on the responsibility of nation states or intergovernmental bodies is per definition such a conflicting norm, because it introduces borders that are perceived as unnecessary thresholds in the view of network operators. They prefer to understand internetworking as a border-less market for data, a free trade zone. When adopting this viewpoint, it also helps to understand responses to the presentation on the introduction of the as-sets such as:

> *it is not an appropriate use of the RIPE database [...] the RIPE NCC should not be seen to make judgments about human rights, or anything else not related to sources and routing*[104]

104 https://ripe78.ripe.net/archives/video/111/ accessed on August 23, 2019

This is not because norms have nothing to do with routing. Previously I established that economic values and the interconnection norm are an inherent part of the routing practice. Rather, integrating norms that are *currently not expressed* in the practice routing, would hamper the interconnection norm and make implementing it harder. Or, as a long-time routing pundit said: '[I]t would add more complexity and not necessarily help the job of shifting bits around the network.'[105]

105 N3819

Through the exploratory experiment of introducing two as-sets as ethnographic probe I was able to show that the voluntary interconnection norm is deeply embedded in the epistemic community of network operators in RIPE. Furthermore, I was able to show that norms that compete or conflict with the interconnection norm are resisted.

By applying the lens of infrastructural norms to the data captured in response to the ethnographic probe, I conclude that norms that conflict with the interconnection norm are resisted. The sources for this resistance can be located in four different realms:

- economically, because norms that might limit interconnection would decrease, or limit the increase, of the value of the network. As a consequence, there would be no reason for networking equipment vendors to provide networking equipment that takes these values into account in routing decisions 'if it's not making them money'[106],
- institutionally, because the scope of the RIPE database is kept limited: adding norms 'is not what the RIPE database was made for'[107] and integrating these norms would 'build

106 N4019

107 N2619

more things onto a system which is already just about fit for purpose'[108], by any means it should be maintained that Regional Internet Registries are not 'the routing police'[109];

- technically, because the routing protocols and Internet routers do not allow to take other norms than economic value and efficiency into account in routing decisions, and add too much complexity[110];

- supranationally, because these norms would encourage the 'politicizing [of] identifiers'[111], which would be 'a slippery slope'[112]. This in turn could create thresholds and boundaries in internetworking, which would not work 'for the good of the network'[113].

108 N4019

109 N2619, N2719, N3119, N3219, N3719, N3919, N4119

110 N3819

111 N3119

112 N3019, N3819

113 N3219

These sources of resistance are leveraged when a new norm is being introduced that could impinge on the interconnection norm, that seeks to facilitate adding new networks and increasing interconnectivity between networks. New norms could create thresholds or boundaries making the exchange of traffic harder, while at the same time instituting specific properties. These properties could, for instance, be exclusive or preferential routing between networks that abide by the same legal norms. This would hamper the traffic to networks that do not (explicitly) abide by these norms.

Conclusion

Internet routing is a foundational enabler of the Internet, which in turn is a core infrastructure of modern information societies. Internet routing is made possible through the coordination that takes place in governance bodies, such as Regional Internet Registries. In this paper I have argued that the coordination and policy development that takes place in RIPE, the RIR for the European region, is guided by the infrastructural norm of interconnection. This norms instructs the epistemic community of networks operators in RIPE to create more interconnection between and among networks, and resist any norm or value that could hamper that. I have demonstrated the workings of the voluntary interconnection norm through an experiment that consisted of the introduction of data protection and a human rights norm into RIPE database, which facilitates Internet routing. The resistance against the introduction of these norms allowed me to identity four sources of resistance, namely: economical, institutional, technical, and supranational resistance.

The infrastructural norm of voluntary interconnection helps to explain why the proposal that was fielded in the RIR responsible for Africa, to repay Internet censoring governments in kind, was resisted and rejected: network operators, and their institutions, are expected to create more interconnection, not less. Even when other actors, such as governments, limit network interconnection, network operators believe that the Internet governance regime should not engage in any limitation of connections among networks. These sentiments can be traced back to official technical and policy documents, as well as commonly repeated adage that says that Regional Internet Registries are not 'the routing police'[114].

114 N2619, N2719, N3119, N3219, N3719, N3919, N4119

The theoretical lens of infrastructural norms allows for the extension of the concept of 'infrastructural power' (Mann 1984) beyond territoriality, and with that make it applicable to transnational infrastructures. This revitalized and increases the relevance of the concept for global governance and international relations in general, and Internet governance in specific. It provides an analytical framework for the understanding of the workings of power and control in distributed, complex, transnational infrastructures. Future research could seek to apply this lens to other internet governance bodies to validate its regained empirical usefulness, and to see whether the same sources of resistance can be identified. Such research could inform both policy making in, and the reconfiguration of, Internet governance bodies, as well as the development and implementation of regulation at the national and intergovernmental level.

Conclusion

The role of norms

In the practice of Internet governance, groups of heterogeneous epistemic communities with discrete and dynamic values and interests engage in processes of developing policies, technologies, protocols, and standards to produce a global and inter-operable general-purpose communication network. In this dissertation, I investigated the role that norms and values play in the governance of the Internet infrastructure, particularly in relation to the introduction of social and legal norms. To explore this topic, I created four case studies of three Internet governance bodies: the Internet Engineering Taskforce (IETF); the Internet Corporation for Assigned Names and Numbers (ICANN); and the Réseaux IP Européens (RIPE). These bodies are paradigmatic for the private Internet governance regime and make up a significant part of the population of Internet governance bodies. By investigating the role of norms and values in the introduction, evolution, subversion, and resistance of norms in these different bodies, I traced and compared the evolution, introduction, subversion, and resistance of norms across different bodies, to make a generalization about the role of norms and values for the field of Internet governance. I argue this is timely and important because the Internet infrastructure, and the norms encoded in it, have become entangled with the lives of billions of people. Because of the ever-increasing role of the Internet infrastructure, I focused particularly on the introduction of social and legal norms, and how they got translated and inscribed into the technical infrastructure of the Internet. Thus, in the first step of my analysis, I investigated how certain social and legal norms evolved in the groups of people that try to inscribe them.

Chapter One explored the evolution of the norms and values of a group of civil society activists engaged in Internet governance. In this chapter, my co-author and I followed the process of meaning-making and the development of discourse in a group of organized civil society actors in institutional and infrastructure design. We focused on the coordination of the Domain Name System—an inherent part of the Internet infrastructure in ICANN, as the main governance and coordination body of the DNS. The DNS is the telephone book of the Internet, connecting unique naming resources to unique numbering resources. Our analysis showed that the group's most recent effort—the encoding of a human rights commitment into ICANN's bylaw—has only been a recent objective of the group. The group of civil society actors began this work because an opportunity was presented to them

due to a change in ICANN's oversight and stewardship structure. This meant that the sociotechnical imaginary of the group—the combination of its norms and values that shape their vision of the future—altered with the influx of a new cohort of activists. On the one hand, this shows that civil society actors engaged in Internet governance are not a monolithic entity, and their collective norms and values (or imaginary) evolves when engaging with governance institutions and other stakeholders. On the other hand, it shows that changes in Internet governance are intrinsically linked with changes that originate from outside the Internet governance system. This group of civil society actors initially prioritized the norm of the protection of freedom of speech against other groups that prioritized the norm of the protection of intellectual property through the DNS. By then, the group largely consisted of advocates from the US. With this influx of a new group of more diverse actors, concerns about norms of privacy, due process, social and economic rights were added to the group's imaginary and the agenda. The influx of yet another cohort, which included international organizations, brought together the different concerns under the banner of human rights. This showed how a new sociotechnical imaginary—an encompassing human rights norm—emerged through contestation among a stakeholder group engaged in Internet governance. This imaginary emerged not only through contestation within the group, but in the practice of providing a grassroots ordering in Internet governance. This process was spurred by several opportunities, such as the establishment of ICANN, the process of delegating new Top Level Domains, and the transition of stewardship over ICANN, which led to the influx of new cohorts of activists. This in turn altered the joint norms, tactics, and agenda of the group. Overall, this chapter showed how, through exogenous interventions, 'human rights' became a central norm for civil society actors engaged in a process of political contestation with other groups of heterogeneous epistemic communities with discrete and dynamic values and interests.

While Chapter One analyzed the dynamics within a particular stakeholder group of actors engaged in Internet governance, in Chapter Two I focused on the dynamics amongst such groups that seek to wire their norms into the Internet infrastructure through governance processes. I continued to follow the group of civil society actors when they successfully engaged with other actors in Internet governance to inscribe a human rights norm into ICANN's bylaws. This way, I was able to observe what was needed for this norm to be introduced. The introduction of the human rights norm happened against the backdrop of a significant

change for ICANN: the possibility of moving away from the oversight regime by the US government. For this transition to happen, the different groups engaged in ICANN needed to jointly develop a plan for the stewardship transition which was to be approved by the US government. In a consensus-building process fueled by the differences of experience and interests of parties—a process I labeled 'productive contestation'—human rights functioned as a boundary object. In other words, the concept of human rights was plastic enough to be translated to the different social worlds of the respective groups that engaged in the negotiations. However, it maintained enough consistency across the groups to still be meaningful and allow for collaboration between lawyers, engineers, activists, government representatives, intellectual property advocates, and civil society activists. In this process of productive contestation, the concept of human rights did not just play a passive role—it was also actively shaped in the process of negotiation towards standardization and implementation. Within this lens, it was also useful to look back at Chapter One to see how human rights functioned both within civil society, as well as among civil society and other stakeholder groups, as a boundary object that allowed for the collaboration and aligning of interests. However, as the aligning of interests was made possible because of the political opportunity of the stewardship transition, which success was in the interest of all stakeholders, and a commitment to human rights would contribute to making this possible. This process required both active translations to different groups, as well as contestation about the translations by actors from different social worlds to make this early step toward making standardization happen. Interestingly, the instigation of this process, and its final adjudicator, was the United States government. Thus, similar to Chapter One, for existing norms to change or for new ones to be introduced, significant exogenous input was required.

In Chapter Three, I shifted from examining ICANN to taking a closer look at another Internet governance body, the IETF. The IETF is one of the oldest Internet governance bodies, and it focuses on the development of technical norms for the Internet. To study how new norms are introduced, I first examined the sociotechnical imaginary present in this body, and the prevalent norms and values that shape it. There was a surprisingly large overlap among the participants in the IETF about the norms and values that make up the Internet architecture's sociotechnical imaginary, and how these translated into instructive architectural norms. Aside from finding the same three architectural norms repeatedly and consistently mentioned, it also showed how these architectural norms

of openness, end-to-end, and permissionless innovation had strong sociopolitical connotations. These connotations were not only found in technical documents, but also on t-shirts that participants wore to IETF meetings and in my interviews with them. Some examples of the sociotechnical norms and process values that were widely shared included: transparency of processes; the ability for everyone to freely participate; the free availability of documents and archives; conceptions about the equality of all users; the ability for new users to deploy new protocols without having to ask for permission; and the ability to always add new computers to the network. However, when concrete technical issues emerged, the architectural principles were de-prioritized over the interests of significantly represented groups such as network operators, equipment vendors, and content providers. Whereas the Internet architecture's sociotechnical imaginary relies on the equality of all hosts and the ability of everyone to deploy their own protocols, the tussles for power and control between network operators—enabled by equipment vendors and content providers—have reconfigured the Internet infrastructure, which subverted the norms on which the sociotechnical imaginary rests. Based on this analysis, I concluded that the self-regulatory governance model in the IETF has not been able to uphold the sociotechnical imaginary that provides legitimacy to the institution.

In practice, many of the sociopolitical conceptions of the architectural norms have faded into the background, while socioeconomic considerations dominated the shaping of the Internet architecture and infrastructure. The combination of norms and values that are still being professed are actually obscuring this new socioeconomic reality. In this reality, the interests of the transnational corporations that sponsor the participation of the majority of IETF participants transcend architectural norms and the interests of individual Internet users, developers, and smaller infrastructure organizations. In this way, they inform the reconfiguration of Internet infrastructure. Ultimately, the professed sociotechnical imaginary—anchored in the norms and values that shape a vision of the Internet architecture—combined with the concealed nature of infrastructure, shrouds this reordering while legitimizing the institutional design of the IETF. The chapter demonstrates why it is no longer possible for individuals or researchers to easily deploy new protocols. This is especially true for the lower layers of the Internet infrastructure, where transnational corporations retain control over significant parts of the Internet infrastructure. In short, this means that in the IETF, the professed norms and values captured in its sociotechnical imaginary solely serve to legitimize the insti-

tution, while in reality they have actually been subverted by the interests of the significantly represented groups of transnational corporations in the IETF.

Chapter four built on the previous chapters and looked at yet another Internet governance body: RIPE. RIPE delegates numbering resources such as IP addresses to independent networks in Europe, the Middle East, and Western Asia. These numbering resources allow the networks, and the users of these networks, to be connected to the Internet. In this chapter, I used a quasi-experiment to validate some of the findings found in the earlier chapters on other Internet governance institutions, namely that explicit social norms and values only get inscribed and upheld in the Internet infrastructure if they are translatable to the social worlds of the significantly represented groups in the governance body, and if they serve the interest of these significantly represented stakeholders. This quasi-experiment took the shape of an ethnographic probe in which I sought to introduce two norms to the Internet infrastructure in RIPE: the social norm of the soft law instrument of the UN Guiding Principles for Business and Human Rights (UNGPs); and the legal norm of the Generic Data Protection Regulation (GDPR) of the European Commission. To introduce these norms, I translated them to the social worlds and environment of the significantly represented groups in this governance body, namely network operators. To do this I introduced two routing objects into the RIPE database through which networks could signal that they had adopted the UNGPs or the GDPR. Some of the companies that owned these networks had already signed up to the UNGPs or were subject to the GDPR. Nonetheless, the introduction of these norms was unequivocally rejected: not a single network signed up to these routing objects. The ethnographic probe subsequently allowed me to gather data to understand why no productive contestation ensued and what the reasons for the resistance were. Why did human rights and data protection regulation not function as a boundary object in this case?

The ethnographic probe enabled me to engage with the epistemic community of network operators and foreground the deep-rooted norms and beliefs captured in their sociotechnical imaginary. I found that there was an underlying norm that served to instruct and evaluate the introduction of new norms: the voluntary interconnection norm. This norm encompassed the architectural norms of end-to-end, permissionless innovation, and openness that I found in the IETF, as described in Chapter Three. Whereas the architectural norms that I found in the IETF were explicitly

communicated and documented, the sources of the norm of voluntary interconnection were embedded in different realms, such as the institutional configuration, the technological materiality, the political economy, and the supranational values of the epistemic community. To describe this type of norm embedded in different parts of this distributed governance regime, I coined the term 'infrastructural norm'. The infrastructural norm of voluntary interconnection instructs network operators and others engaged in RIPE to create more interconnection without assigning obligations to independent networks, without assigning obligations to independent networks. Norms that either limit the creation of more interconnection or assign obligations to independent networks are resisted by network operators. The two proposed norms that were part of the ethnographic probe might limit interconnection between networks because this might lead networks to not route data through a networks that have, or have not, adopted these human rights and data protection norms. Because of this, the proposed norms would not lead to an increase in interconnection, which is why no productive contestation ensued, and why the introduction of these norms was resisted by the community of network operators. This is a clear example of norm conflict, where a prevalent norm, the norms of voluntary interconnection, is used to prevent the introduction of new social and legal norms.

In these four chapters, I thus examined the process of the evolution, introduction, subversion, and resistance of norms in three different Internet governance bodies: ICANN, IETF, and RIPE. In the consecutive chapter I foregrounded how norms evolved, were introduced successfully, became subverted. Further, I found that a deeply embedded infrastructural norm instructed the resistance against the introduction of conflicting norms. In each chapter, distinct aspects of the role that norms play in private Internet governance were discussed. While this limits the generalizability of the results, I argue that the distinct features that emerge from these case studies do interrelate. Together, they create a coherent image that provides new insights into the workings of norm-setting in the transnational governance of Internet infrastructure.

Viewed as a whole, these chapters show the different roles that norms play in the governance of the Internet infrastructure, with a particular emphasis on social and legal norms. My analyses show that the practice of distributed Internet governance is guided by the Internet's sociotechnical imaginary. This imaginary shapes a vision of the Internet architecture, based on embedded architectural norms and values such as openness, end-to-end,

and permissionless innovation. This architectural sociotechnical imaginary, as examined throughout my dissertation (particularly Chapter Three), facilitates and informs norm development. This combination of norms and values is then reflected in every observed Internet governance institution in this dissertation. For instance, the sociopolitical conception of the norms of openness are reflected in the commitment of all the observed Internet governance institutions in the sense that they allow for open participation, maintain publicly available archives of meetings and conversation alongside freely-available standards and policy documents. The sociotechnical Internet architecture imaginary and its embedded norms and values serve to guide and facilitate the process of norm development, and legitimize the current institutional ordering, even if the norms are then concretely subverted in practice, as shown in Chapter Three. New norms are introduced and subsequently shaped in a process that I refer to as productive contestation, in which the new candidate norm is translated to the social worlds of the participating epistemic communities, and subsequently shaped to accommodate their understandings and interests in a process of negotiation, which I theorized in detail in Chapter Two.

Whereas all chapters examined the role of social and legal norms in Internet governance, the norms that have successfully evolved and been encoded in the Internet infrastructure are examined in Chapters One and Two, whereas Chapters Three and Four examine the social and technical norms that have been subverted and resisted. These findings have thus provided a sound basis as to speculate what the reason for these results might be. The first two chapters show how exogenous influences—namely the iterative influx of new communities in the constituency of civil society activists, alongside criteria set by the United States government during the ICANN stewardship transition—are important preconditions for the success of the evolution and introduction of social and legal norms, in this case human rights, in Internet governance. In Chapter Three, I demonstrated how the norms of equality of all nodes, end-to-end and permissionless innovation were subverted. Subsequently, in Chapter Four I examined how the introduction of social and legal norms of data protection (GDPR) and human rights (UNGP) in the Internet routing infrastructure were resisted. In the cases of Chapters Three and Four, there was no exogenous influences to uphold, integrate, or encode these norms. This was not due to the fact that these norms were alien to the community, as the architectural principles that were subverted are inherent aspects of the technical and policy documents of the IETF. More-

over, many of the networks that are represented in RIPE are subject to the GDPR, and some have even signed up to the UNGPs. Chapter Four thus provides the frame of the infrastructural norm to serve as the primary evaluation criterion of candidate norms, and whether these candidate norms will increase voluntary interconnection. Ultimately, I argue that the difference between the norms and values that make up the sociotechnical imaginary and the infrastructural norm is that the latter does not serve to legitimize a particular institutional or architectural ordering, but rather serves as a concrete and deeply embedded evaluation mechanism for new and existing norms.

Exogenous factors are an inherent part of the evolution and inscription of social and legal norms in Internet governance. However, this only happens when these norms do not hamper the growth of interconnection. The growth and internationalization of the non-commercial user constituency in ICANN as examined in Chapter One went hand-in-hand with the development of its discourse from a relatively narrow, US-centered, freedom of speech focus, to a more integrated human rights approach. This resulted in norms of due process as well as social, cultural, and economic rights, playing an important role, alongside freedom of expression and privacy norms. The growth and internationalization of this group was important, not only for its legitimacy, but also to allow this community to increase its relevance to non-commercial users around the world. Moreover, it also allows this community to enhance its communication with other stakeholders. All of these are clear cases of improved interconnection. In the second chapter, I examined how the prospect of the internationalization of the oversight over ICANN and the transition away from US government oversight was a strong factor for stakeholders with different interests to work together, because this would mean an increase in the legitimacy of ICANN in transnational Internet governance. Overall, I argued that the connection of human rights to one of the criteria set by the US government for the approval of this process thus spurred a process of productive contestation. In Chapter Three, I analyzed how architectural principles that are widely shared in the IETF community were deprioritized for other interests; arguably because there was no strong advocate, incentive, or process to uphold them, and because they did not necessarily created more voluntary interconnection. There was no exogenous factor that sought to uphold these architectural norms in concrete tussles between advocates with strong incentives. Moreover, there was also no endogenous process that could safeguard them. In Chapter Four, I showed how the network operators made it very clear

that the introduction of data protection and human rights norms would not increase interconnection, and therefore these norms should not be introduced. I concluded that the infrastructural norm of voluntary interconnection functions as a tool to evaluate candidate norms in the process of productive contestation. Since its inception, discussions on social and legal norms have been part of the Internet infrastructure, but this research suggests that lack of their prioritization, implementation, and survival is connected to a lack exogenous pressures and opportunities, and because they do not necessarily increase interconnection between independent networks. This has led me to conclude that without exogenous pressures, social and legal norms that do not increase interconnection are likely to be resisted or subverted.

The Internet architecture's sociotechnical imaginary consists of a vision of the Internet architecture that anchored in norms and values, which provides legitimacy to a complex and distributed transnational governance mosaic. In contrast, an infrastructural norm enables the Internet infrastructure's growth. Norms are an instrument of governance that are very fitting for a transnational and distributed governance environment because norms create specific expectations—without prescribing specific responses—or anticipate all possible changes, challenges, and innovations. The sociotechnical imaginary alongside the infrastructural norm should be understood as sources of metagovernance that tie the transnational distributed private Internet governance regime together, provide it with direction, and are a means to hold it on a specific course: namely one of producing more interconnection between almost 70.000 independent networks. The Internet architecture's sociotechnical imaginary and infrastructural norm thus jointly form an efficient instrument of metagovernance by enabling a wide variety of actors to collaborate on creating more interconnection. To be precise, the sociotechnical imaginary facilitates collaboration that allows for the introduction of sociotechnical norms that are evaluated, in a process of productive contestation, through the infrastructural norm. Consequently, the result is that sociotechnical norms, especially social and legal norms, that interfere with the increase in interconnection, are either or subverted or resisted upon introduction.

Overall, this dissertation does not provide any answers as to the intentionality of this normative metagovernance constellation, but it does show that exogenous factors, such as the transition of stewardship in the case of ICANN, facilitate the introduction and evolution of social and legal norms. Furthermore, where it comes

to existing legal and social norms that are inscribed in the Internet infrastructure, these are likely to be subverted in cases of norm conflict with the norm of voluntary interconnection.

Methodological innovation

Mailinglist analysis

Mailinglist archives are a precious and surprisingly under-explored source of data about discursive and norm change as well as stakeholder conflicts and alliances (ten Oever, Milan, and Beraldo 2020). A distinctive feature of Internet governance bodies such as the ICANN, the IETF, and RIPE, is their (relative) openness and the degree of meticulous documentation of their activities through public archives. Consequently, I concluded that only a mixed-methods approach that combined computational and interpretative tasks would be best able to exploit these data sources . There were no readily available quantitative analysis tools to effectively analyze word trends, networks, participation, and affiliation in the Internet governance mailinglist archives. Moreover, qualitative analysis of the raw mailinglist data would be very challenging because of the sheer amount of data available. I thus contributed to the development of the BigBang tool—which is freely available for the use of other researchers—and helped to make it applicable to Internet Governance. This approach resulted in three ways of approaching these mailinglist archives: descriptive statistics; network analysis; and qualitative/quantitative text analysis. Both the tool and the mailinglist archives of the respective organizations are available online, which adds to the overall robustness of the findings in this dissertation, and increases the validity of the results through the triangulation between multiple methods and sources.

Use of an exploratory experiment

The development of an ethnographic probe, two objects that invited responses and laid bare underlying values and norms (De Leon and Cohen 2005) in Chapter Four allowed me to translate the legal and ethical norms of data protection and human rights to the technical worlds of Internet routing engineers. This took the form of the proposed introduction of two so-called ‘as-sets’ in the Internet Routing Registry. This use of an ethnographic probe allowed me to uncover and foreground values, opinions, and responses that I would not have been able to capture otherwise. By translating, or trans-coding, social and legal norms into candi-

date technical norms, I reorientated the discussion from hypothetical or high-level abstractions into a concrete proposal that could be implemented. The probe thus allowed me to test and examine the opinions of network operators by making these norms directly applicable to their technical contexts. This helped me explore, and understand, not only how and when norms get inscribed, but also why they get resisted, which helped me to uncover the workings of the infrastructural norm. This was a methodological innovation for two reasons. Firstly, the usage of a quasi-experiment is uncommon in both science and technology studies as well as international relations. This allowed me to operationalize the findings from earlier chapters and to engage with the field of study using a more (inter)active approach than through a survey or participant observation. Secondly, it is uncommon for a researcher to actually propose new norms in norm-setting regimes and observe the response. Thus, this was both a methodological innovation as well as an approach to valorize research by increasing its societal relevance and impact.

Conceptual Innovation

Productive contestation

In Chapter Two, I developed the term 'productive contestation' to explain the process of negotiation, shaping, and consensus-building in the introduction of norms between heterogeneous groups of experts with different interests who ultimately share a sociotechnical imaginary. Productive contestation takes place when a concept becomes a bridge between the different groups and enables collaboration among them in the shaping disputation that is the norm development process. When a concept plays such a bridging role, it can be defined as a boundary object (Star 1990; 2010). This concept requires the need to be able to accommodate different understandings by differing groups, whilst also having sufficient plasticity to remain sufficiently consistent. The process of consensus-building that takes place thus needs to allow for the different stakeholder groups to align with the meaning of the boundary object with their interests and incentives. In this process of negotiation, groups define the concept in a way that limits the ability for other groups to accommodate the object to their interests and incentives. I thus developed the term productive contestation through my findings in Internet governance where I witnessed that this negotiation entails a careful shaping and sculpting of the meaning of the concept alongside loading it up with different meanings. While the translations and interpreta-

tions of the respective social worlds do not need to overlap, they should not exclude each other; and when they do, work needs to be done to make the translations converge. A back-and-forth between epistemic communities enables collaboration to move towards standardization and implementation in a diverse environment. The concept of productive contestation therefore helps to explain how negotiations take place in Internet governance, and thus how norms are shaped in their introductory phase. The concept also expands the applicability boundary object-theory to the field of global governance. The term of productive contestation helps expand the field boundary object theory in the sense that it accounts for how the accommodation to different social worlds shapes the boundary object in early stages of standardization.

Infrastructural norms

The concept of infrastructural norms builds on the concept of productive contestation. Where the process of productive contestation shows the shaping of norms in the consensus-building process, the infrastructural norm is the evaluation criterion in Internet governance for a norm to be accepted. In other words, I introduced the term of 'infrastructural norms' to explain why and how the introduction of certain norms is resisted. This concept helps explain how norms tie the distributed governance of a transnational infrastructure together by instructing and informing institutional design and epistemic communities in the production of technological materialities. This theoretical lens of infrastructural norms allows for the extension of the concept of 'infrastructural power' (Mann 1984; Weiss 2006) beyond the territoriality of the state, and makes it applicable to transnational infrastructures in general while being specifically applicable to Internet governance. By coining this concept, I have therefore contributed to the theory-building around tools of metagovernance. While norms are already recognized as tools for metagovernance, as is institutional design, infrastructural norms help theorize the reinforcement of a particularly ingrained norm through norm conflict, technological materialities, institutional configurations, economic drivers, and supranational ideals, and its legitimation through a sociotechnical imaginary. This therefore increases the applicability and empirical value of the concept of metagovernance in global governance within international relations in general, and Internet governance and the governance of other transnational infrastructures specifically.

Relevance

Perspectives for policy-making and Internet governance practice

The introduction of the Generic Data Protection Regulation of the European Commission (Kulesza 2018; Perrin 2018) and the Russian 'Sovereign Internet' regulation (Stadnik 2019) are new milestones in the governance of the Internet infrastructure. These initiatives could form the beginning of a trend in state-based rule-setting on Internet infrastructure, or even the emergence of a multilateral Internet governance regime, which is inherently different from the private Internet governance regime which has dominated the development and scaling of the Internet thus far. Increasingly, states are engaging in intergovernmental initiatives for norm-setting for the Internet. For instance, this can be seen in the 'United Nations Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security', the 'United Nations Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security', as well as the Digital Strategy of European Commission of the European Union that is grounded in the concept of 'Data Sovereignty'[115]. A reason for the emergence of this multilateral Internet governance regime could be the perceived inability or unwillingness of the private Internet governance regime to accommodate the needs of (groups of) governments because their proposals do not pass the evaluation of the infrastructural norm of interconnection. By engaging in these initiatives, the multilateral Internet governance regime creates exogenous pressures and incentives that the private Internet governance regime needs to take into account. On the one hand, this can be perceived as a threat to norm-setting in the private Internet governance regime, since it gives rise to other norm-developments in this field: even for norms that might not be voluntary, but are binding. On the other hand, this could also be seen as an attempt to keep geopolitical tensions between and among nation-states inside multilateral institutions and initiatives and outside of the private Internet governance regime, as to identify 'the Internet's core protocols as a neutral zone in which governments, pursuing their national interests, are prohibited from interfering' (Broeders 2016, 7). This would, however, leave the shaping of the Internet's infrastructure largely in the hands of transnational corporations, which perhaps are not as neutral as indicated by Broeders. As shown in this dissertation, the private Internet governance regime, in its current form, is not conducive for upholding, protecting, or encoding social or legal norms that do not increase interconnectivity, but

115 https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy accessed on July 19, 2020

rather, it subverts and resists them, unless there is exogenous opportunity or pressure. People active in policy-making could consider whether it would be possible to overcome this conundrum by creating an exogenous pressure on the private Internet governance regime, to integrate a structural consideration of the impact of existing and candidate norms on social and legal norms, and thus enhance the infrastructural norm. Conversely, the private Internet governance regime could continue to focus on its narrow mission to follow its infrastructural norm and increase interconnectivity. However, it would then need to expect an increase in norms set by the multilateral Internet governance regime that it will subsequently need to conform to. Overall, the multilateral Internet governance regime is currently still peripheral in the Internet governance regime complex compared to the private Internet governance regime. However, this may change, at least in part, due to the willingness and ability of the latter to accommodate the social and legal norms.

Advancing the academic debate on Internet governance

This dissertation addresses the gap in the global governance literature on the role of norms in the governance of the Internet infrastructure. It illustrates how an infrastructural norm is what effectively guides the private Internet governance regime. This analysis of the Internet private governance regime, as an instrument of creating more interconnection, shows the strengths of the distributed regime particularly to foster a global communication network that connects machines, people, states, companies, and research institutions. But it also shows its narrow remit. The metagovernance frame provides a lens for analysis for the shaping of the global and distributed Internet infrastructure by different actors with distinct interests and rationalities and the role institutional design and norms play in it. The private transnational multistakeholder Internet governance regime thus produces interconnection. This is reinforced through the infrastructural norm that is embedded in the institutional configuration, the technological materiality, the economic drivers, and in the epistemic communities that produce this infrastructure. The metagovernance lens also provides the ability to theorize the functional differences between, but also the interaction among, the different governance regimes. For instance, one could speculate about the interrelation between the private and the multilateral Internet governance regimes that jointly make up the Internet governance regime complex. Ultimately, while the private Internet governance

regime has a normative governance model to increase interconnection, it might be in the interest of the multilateral governance regime to clearly shape the network to delineate nation-states and ensure that the infrastructure accommodates their respective norms. This is where the lens of metagovernance has allowed me to theorize and functionally differentiate regimes within a regime complex, without separating these regimes into different sub-regimes based on their area of application, nature of the institution, or other formal criteria. Therefore, metagovernance allows for a more granular analysis that still builds on the abstractions that regime theory provides.

The discussion on how the governance of the Internet infrastructure impacts human rights and how human rights can provide a lens to analyze the governance of the Internet infrastructure from the perspective of rights holders is still in its infancy. Human rights have played a returning role in this dissertation. However, more as a proxy for social and legal norms rather than in an analysis of the engagement of the human rights regime with the private Internet governance regime. The reason for this is that the interrelation between the governance of the Internet infrastructure and human rights has not yet been widely explored neither inside academia nor outside of it (Scholte 2020). Except for one report by the UN special rapporteur on Freedom of Expression (Kaye 2016), there has been little engagement of the human rights regime with Internet infrastructure governance. While there is ample discussion regarding the impact of Internet applications and platforms on human rights, the underlying infrastructure and its governance that enables and shapes the platforms and applications is escaping critical assessment. When there is a focus on the Internet infrastructure, it is mostly in terms of the importance of proliferating access, and thus creating more interconnectivity. This is not dissimilar to the norms found among the first cohort in the ICANN constituency that were analyzed in Chapter One, as well as the architectural norms of end-to-end and openness and the infrastructural norm of interconnection. I argue that an understanding of human rights that goes beyond freedom of expression can turn this around and provide a productive lens to critically examine the impact of the governance of Internet infrastructure, because it forces researchers to anchor their analysis at the points where the infrastructure impacts the ability of groups and individual users to exercise their human rights, and from there navigate the expansive and complex assemblage of the Internet infrastructure and its governance.

Human rights could also prove to be a useful lens to exam-

ine the transnational Internet governance regime complex, consisting of the private and multilateral Internet governance regime, because human rights are applicable to both in a different manner. Human rights are a social norm when it comes to non-state actors and an international legal norm where it comes to states. In this sense, human rights provide a heuristic to critically question the norms-setting of both regimes. Whereas the human rights of freedom of expression might fit very well with the infrastructural norm of interconnection, the right to privacy limits the unlimited free flow of all information. This makes human rights a prism into the impact of sociotechnical norms that are prioritized. For instance, while freedom of expression is a human right that is extensively discussed in the private Internet governance regime, and to a lesser extent regarding privacy as well, the right to freedom of association, non-discrimination, political participation, or the right to science, are much less discussed. Therefore, I argue that human rights function as a productive, albeit not simple, lens to understand the choices made in the governance of the Internet infrastructure.

Future Research

In his interdisciplinary examination of the Internet routing infrastructure, Ashwin Mathew tells us that '[t]o make sense of the modern world—of the information society—we must pay attention to the details of the production of space through infrastructure' (Mathew 2014, 242). Yet, to do this, we need to take into account the infrastructure's embedded and relational nature. To increase the understanding of the infrastructural normative wiring of the information society that comes with deeper integration of the Internet infrastructure in our daily lives and our increasing dependency on it, one needs to understand not only the complex assemblage of the transnational Internet governance regime, but also how it works when it touches upon other governance regimes. This dissertation thus argues that metagovernance provides a lens into the dynamics both inside and among regimes. In regards to further research, there are a number of differing avenues that can be taken.

Firstly, future research could seek to increase support for the functional differentiation of infrastructural norm regimes within the transnational Internet governance regime complex; for instance, by replicating the approach used in this dissertation on the multilateral Internet governance regime. This would then allow schol-

ars to establish a relationship between the role of the multilateral Internet governance regime and the self-regulatory transnational private Internet governance regime.

Secondly, established scholars like Milton Mueller argue there is a structural misalignment between Internet governance and national sovereignty (Mueller 2017). Future research could therefore investigate, and perhaps challenge, Mueller's view that Internet governance produces one global Internet, while nation-states seek to apply rules based on their own limited geographical reach. Instead, it could depart from the hypothesis that the private Internet governance regime that produces interconnection, and the (inter)governmental regime that sets the limitations to interconnection through laws and regulations, actually form one metagovernance regime that shapes the global Internet with its own discrete functions and functionalities. Rather, such research could build a framework that, instead of focusing on a structural misalignment, explains the relation between the two complexes as mutually beneficial. While states may not need or want to focus on interconnection and innovation of technologies, transnational corporations do not need or want to develop their own policies and standards vis-à-vis social and legal norms. The crux of this research could thus be found in the interfacing between these regimes, and how they adapt and accommodate each other.

Thirdly, embedded scholars like Stephanie Perrin have shown the frictions between the multilateral Internet governance regime and the private Internet governance regime in the case of personally identifiable information in the DNS system. Perrin has showcased the inability, or unwillingness, of the epistemic communities in ICANN to accommodate the requests by data protection authorities and privacy advocates (Perrin 2018). The narrow remit set by the infrastructural norm for private Internet governance bodies, supplements the findings Perrin, but also the findings of by Musiani et al. who observe a turn to infrastructure by states to achieve their policy goals such as surveillance or censorship (Musiani et al. 2016). However, in the cases the authors describe, the nation-states do not engage with infrastructure governance bodies, but rather directly engage with infrastructure providers to achieve policy goals. Future research could therefore further investigate whether, or when, influence from the multilateral governance regime on the private Internet governance regime is direct, such as in the case of WHOIS and ICANN, or rather indirect, such as in the cases of government sanctioned censorship and filtering that are implemented through infrastructure provid-

ers, as described by Musiani et al. The study of the roles and interactions between different actors in the governance of the Internet infrastructure will provides insights into global power relations for years to come.

Wiring norms

The transnational sociotechnical norm development that happens in the private Internet governance regime is expected to gain influence for the foreseeable future. The norms that instruct and inform this process have shaped governance bodies, epistemic communities, protocols, standards, hardware, and software that is getting ever further integrated into the mesh of society. This norm induced growth has not been one-dimensional. Rather, these wired norms have set the invisible rules that run through the information society, and have helped spread the Internet throughout the world and deeply into our lives. It is here that the private Internet governance regime has attained tremendous power.

Over a thousand engineers participated in the 102nd meeting of the IETF, held in Montreal, Canada in July, 2018. The meeting agenda was filled with working groups that discussed complex technical topics, as well as several administrative and logistical issues. In the midst of the working group sessions, the power went off. In the dark room, the glow of hundreds of laptop screens lit up the faces of the engineers in the room. This is when the picture on the front on this dissertation was taken. Without any interruption, the working group continued its work, their eyes glued to their screens.

Their norms of behavior were less dictated by collective engagement in the room itself but rather by the norms and values that are embedded in their sociotechnical imaginary. Ironically, during the same IETF meeting, the decision was made to not hold any IETF meetings in India for the foreseeable future due to ‘infrastructure problems’. This may indicate the actual problems that lie within the wired norms that form an inherent part of the Internet infrastructure. Their rapt attention to technology should give us pause. Sociotechnical imaginaries are flawed and subject to unconscious biases and logical inconsistencies, like the failure to notice how the three architectural norms are being quietly subverted. However, in this dissertation, I have shown how exogenous incentives and the influx of new people can change a norm, and subsequently encode it into the Internet infrastructure.

This finding is perhaps hopeful, because it shows we might chart alternate routes to govern the Internet.

The question remains: can we take our eyes off the screen to recognize that the Internet infrastructure has a shaping power that benefits specific actors and hampers others? Future routes for the Internet architecture have not been programmed yet. The way the future Internet infrastructure will be shaped depends on public and political engagement with Internet governance.

References

Abbate, Janet. 1999. *Inventing the Internet*. Inside Technology. Cambridge, MA: The MIT Press.

Abbott, Kenneth W., Philipp Genschel, Duncan Snidal, and Bernhard Zangl. 2015. “Orchestrating Global Governance: From Empirical Findings to Theoretical Implications.” In *International Organizations as Orchestrators*, edited by Kenneth W. Abbott, Philipp Genschel, Duncan Snidal, and Bernhard Zangl, 349–79. Cambridge England ; New York: Cambridge University Press.

Abbott, Kenneth W., Jessica F. Green, and Robert O. Keohane. 2016. “Organizational Ecology and Institutional Change in Global Governance.” International Organization. April 2016. https://doi.org/10.1017/S0020818315000338.

Agre, Philip. 1997. *Computation and Human Experience*. Cambridge University Press.

Akrich, Madeleine. 1992. “The De-Scription of Technical Objects.” In *Shaping Technology/Building Society : Studies in Sociotechnical Change*, edited by Wiebe E. Bijker and John Law, 205–24.

Albright, Madeleine K., and Ibrahim A. Gambari. 2015. “The UN at 70: Confronting the Crisis of Global Governance.” *Global Policy* 6 (4): 510–16. https://doi.org/10.1111/1758-5899.12292.

Alvestrand, Harald Tveit. 2004. “RFC3935 - A Mission Statement for the IETF.” RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc3935.

Appelman, Daniel L. 2016. “Internet Governance and Human Rights: ICANN’s Transition Away from United States Control.” *The Clarion, a Journal of the American Bar Association’s International Human Rights Committee* 1 (1).

Arpagian, Nicolas. 2016. “The Delegation of Censorship to the Private Sector.” In *The Turn to Infrastructure in Internet Governance*, edited by Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, 155–65. Information Technology and Global Governance. New York: Palgrave Macmillan US. https://doi.org/10.1057/9781137483591_8.

Assche, Kristof Van, Raoul Beunen, Iulian Barba Lata, and Martijn Duineveld. 2015. “Innovation in Governance.” *SpringerLink*, 313–25. https://doi.org/10.1007/978-3-319-12274-8_21.

Barnett, Michael, and Raymond Duvall. 2005. “Power in International Politics.” *International Organization* 59 (1): 39–75. https://doi.org/10.1017/S0020818305050010.

Baur-Ahrens, Andreas. 2017. “The Power of Cyberspace Centralisation: Analysing the Example of Data Territorialisation.” *Security/Mobility: Politics of Movement*, 37–56.

Benford, Robert D., and David A. Snow. 2000. “Framing Processes and Social Movements: An Overview and Assessment.” *Annual Review of Sociology* 26 (1): 611–39. https://doi.org/10.1146/annurev.soc.26.1.611.

Benkler, Yochai. 2006. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven Conn.: Yale University Press.

Benthall, Sebastian. 2015. “Testing Generative Models of Online Collaboration with BigBang.” In , 182–89. https://conference.scipy.org/proceedings/scipy2015/sebastian_benthall.html.

Bevir, Mark. 2012. *Governance: A Very Short Introduction*. Oxford: OUP Oxford.

Bijker, Wiebe E. 1995. *Of Bicycles, Bakelites, and Bulbs. Toward a Theory of Sociotechnical Change*. Cambridge, MA and London, England: MIT Press.

Bijker, Wiebe E., and John Law, eds. 1992. *Shaping Technology/Building Society*. Cambridge, MA: MIT Press.

Blokzijl, Rob, Mats Brunel, Francois Fluckiger, Daniel Karrenberg, Olivier Martin, and Enzo Valente. 1992. “RIPE-001 RIPE Terms of Reference.” Amsterdam: RIPE. https://www.ripe.net/publications/docs/ripe-001.

Bond, Patrick. 2006. “Civil Society on Global Governance: Facing Up to Divergent Analysis, Strategy, and Tactics.” *Voluntas: International Journal of Voluntary and Nonprofit Organizations* 17 (4): 357–369. https://doi.org/10.1007/s11266-006-9024-2.

Bowker, Geoffrey C., Karen Baker, Florence Millerand, and David Ribes. 2009. “Toward Information Infrastructure Studies: Ways of Knowing in a Networked Environment.” In *International Handbook of Internet Research*, 97–117. Springer, Dordrecht. https://doi.org/10.1007/978-1-4020-9789-8_5.

Braden, R. 1989. “RFC1122 - Requirements for Internet Hosts - Communication Layers.” RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc1122.

Bradshaw, Samantha, Laura DeNardis, Fen Osler Hampson, Eric Jardine, and Mark Raymond. 2015. “The Emergence of Contention in Global Internet Governance.” Global Commission on Internet Governance Paper Series. Canada: Global Commission on Internet Governance.

Braman, Sandra. 2009. *Change of State: Information, Policy, and Power*. MIT Press.

———. 2011. “The Framing Years: Policy Fundamentals in the Internet Design Process, 1969–1979.” *The Information Society* 27 (5): 295–310. https://doi.org/10.1080/01972243.2011.607027.

———. 2012a. “Internationalization of the Internet by Design: The First Decade.” *Global Media and Communication* 8 (1): 27–45. https://doi.org/10.1177/1742766511434731.

———. 2012b. “Privacy by Design: Networked Computing, 1969–1979.” *New Media & Society* 14 (5): 798–814. https://doi.org/10.1177/1461444811426741.

———. 2013. “Laying the Path: Governance in Early Internet Design.” *Info* 15 (6): 63–83. https://doi.org/10.1108/info-07-2013-0043.

———. 2020. “The Irony of Internet Governance Research: Metagovernance as Contextpractices.” In *Research Methods in Internet Governance*, edited by Derrick L. Cogburn, Laura DeNardis, Nanette S. Levinson, and Francesca Musiani. Cambridge, MA: MIT Press.

Broeders, Dennis. 2016. *The Public Core of the Internet: An International Agenda for Internet Governance.* Amsterdam University Press.

Brown, Ian, David Clark, and Dirk Trossen. 2010. “Should Specific Values Be Embedded in the Internet Architecture?” In *Proceedings of the Re-Architecting the Internet Workshop*, 10:1–10:6. ReARCH ’10. New York, NY, USA: ACM. https://doi.org/10.1145/1921233.1921246.

Burnett, Gary, and Paul T. Jaeger. 2009. “Small Worlds, Lifeworlds, and Information: The Ramifications of the Information Behaviour of Social Groups in Public Policy and the Public Sphere.” *Information Research: An International Electronic Journal* 13 (2): er.

Bygrave, Lee A. 2015. *Internet Governance by Contract*. Oxford University Press Oxford.

Bygrave, Lee A., and Jon Bing. 2009. *Internet Governance: Infrastructure and Institutions*. Oxford University Press on Demand.

Callon, Michel. 1990. “Techno-Economic Networks and Irreversibility.” *The Sociological Review* 38 (S1): 132–61.

Cardoso, Fernando Henrique. 2004. “We the Peoples: Civil Society, the United Nations and Global Governance.” *Report of the Panel of Eminent Persons on United Nations-Civil Society Relations*.

Carpenter, Brian E. 2000. “RFC2775 - Internet Transparency.” RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc2775.

Carpenter, Brian E., and Scott W. Brim. 2002. “RFC3234 - Middleboxes: Taxonomy and Issues.” RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc3234.

Carr, Madeline. 2015. “Power Plays in Global Internet Governance.” *Millennium* 43 (2): 640–59. https://doi.org/10.1177/0305829814562655.

Castells, Manuel. 2009. *Communication Power*. Oxford, UK; New York: Oxford University Press. http://public.eblib.com/choice/publicfullrecord.aspx?p=472226.

Cath, Corinne. 2015. “A Case Study of Coding Rights: Should Freedom of Speech Be Instantiated in the Protocols and Standards Designed by the Internet Engineering Task Force?” MA dissertation, Oxford, UK: University of Oxford.

———. 2019. “Internet Governance and Human Rights: A Literature Review.” In *The 2018 Yearbook of the Digital Ethics Lab*, edited by Carl Öhman and David Watson, 105–32. Digital Ethics Lab Yearbook. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-17152-0_8.

Cath, Corinne, and Luciano Floridi. 2017. “The Design of the Internet’s Architecture by the Internet Engineering Task Force (IETF) and Human Rights.” *Science and Engineering Ethics* 23 (2): 449–468. https://doi.org/10.1007/s11948-016-9793-y.

Chadwick, Andrew. 2006. *Internet Politics: States, Citizens, and New Communication Technologies*. 1 edition. New York: Oxford University Press.

Christou, George, and Seamus Simpson. 2007. “Gaining a Stake in Global Internet Governance: The EU, ICANN and Strategic Norm Manipulation.” *European Journal of Communication* 22 (2): 147–164.

Chun, Wendy Hui Kyong. 2007. “Race and Software Wendy Hui Kyong Chun.” *Alien Encounters: Popular Culture in Asian America*, 305.

———. 2008. *Control and Freedom: Power and Paranoia in the Age of Fiber Optics*. mit Press.

Clark, David. 1992. “A Cloudy Crystal Ball - Visions of the Future.” In *Proceedings of the Twenty-Fourth Internet Engineering Task Force*, 539–43. http://www.ietf.org/proceedings/24.pdf.

———. 2018. *Designing an Internet.* 1 edition. Cambridge, MA: The MIT Press.

Clark, David, John Wroclawski, Karen R. Sollins, and Robert Braden. 2005. “Tussle in Cyberspace: Defining Tomorrow’s Internet.” *IEEE/ACM Transactions on Networking* 13 (3): 462–475. https://doi.org/10.1109/TNET.2005.850224.

Coen, David, and Tom Pegram. 2018. “Towards a Third Generation of Global Governance Scholarship.” *Global Policy* 9 (1): 107–113.

Couldry, Nick, and Andreas Hepp. 2018. *The Mediated Construction of Reality*. John Wiley & Sons.

Cowhey, Peter F., Jonathan D. Aronson, and John Richards. 2009. “Shaping the Architecture of the US Information and Communication Technology Architecture: A Political Economic Analysis.” *Review of Policy Research* 26 (1–2): 105–125.

Crowcroft, Jon. 2007. “Net Neutrality: The Technical Side of the Debate: A White Paper.” *SIGCOMM Comput. Commun. Rev.* 37 (1): 49–56. https://doi.org/10.1145/1198255.1198263.

Davidson, Alan, John Morris, and Rob Courtney. 2002. “Strangers in a Strange Land: Public Interest Advocacy and Internet Standards.” In *Proceedings of the 30th Research Conference on Communication, Information and Internet Policy (TPRC 2002)*. Arlington, Virginia.

Davies, D. W., K. A. Bartlett, R. A. Scantlebury, and P. T. Wilkinson. 1967. “A Digital Communication Network for Computers Giving Rapid Response at Remote Terminals.” In *Proceedings of the First ACM Symposium on Operating System Principles*, 2.1–2.17. SOSP ’67. New York, NY, USA: ACM. https://doi.org/10.1145/800001.811669.

De Leon, Jason Patrick, and Jeffrey H. Cohen. 2005. “Object and Walking Probes in Ethnographic Interviewing.” *Field Methods* 17 (2): 200–204. https://doi.org/10.1177/1525822X05274733.

Deering, S. E. 1989. “RFC1112 - Host Extensions for IP Multicasting.” RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc1112.

Deibert, Ronald J. 2008. “The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace.” In *Routledge Handbook of Internet Politics*, 339–352. Routledge.

Deibert, Ronald J., and Louis W. Pauly. 2019. “Mutual Entanglement and Complex Sovereignty in Cyberspace.” *Data Politics: Worlds, Subjects, Rights. Abingdon: Routledge*, 81–99.

DeNardis, Laura. 2009. *Protocol Politics: The Globalization of Internet Governance.* Cambridge, MA: MIT Press.

———. 2012. “Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance.” *Information, Communication & Society* 15 (5): 720–738.

———. 2014. *The Global War for Internet Governance*. New Haven: Yale University Press.

———. 2020. *The Internet in Everything: Freedom and Security in a World with No off Switch*. Yale University Press.

DeNardis, Laura, and Francesca Musiani. 2016. “Governance by Infrastructure.” In *The Turn to Infrastructure in Internet Governance*, edited by Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, 3–21. New York: Palgrave MacMillan.

Denzin, Norman K., Yvonna S. Lincoln, and Michael D. Giardina. 2006. “Disciplining Qualitative Research.” *International Journal of Qualitative Studies in Education* 19 (6): 769–82. https://doi.org/10.1080/09518390600975990.

Dery, David. 2000. “Agenda Setting and Problem Definition.” *Policy Studies* 21 (1): 37–47.

Ding, Aaron Yi, Jouni Korhonen, Teemu Savolainen, Markku Kojo, Joerg Ott, Sasu Tarkoma, and Jon Crowcroft. 2013. “Bridging the Gap between Internet Standardization and Networking Research.” *ACM SIGCOMM Computer Communication Review* 44 (1): 56–62. https://doi.org/10.1145/2567561.2567572.

Dingwerth, Klaus, Antonia Witt, Ina Lehmann, Ellen Reichel, and Tobias Weise, eds. 2019. *International Organizations under Pressure: Legitimating Global Governance in Challenging Times*. Oxford, New York: Oxford University Press.

Dönni, Daniel, Guilherme Sperb Machado, Christos Tsiaras, and Burkhard Stiller. 2015. “Schengen Routing: A Compliance Analysis.” In *Intelligent Mechanisms for Network Configuration and Security*, edited by Steven Latré, Marinos Charalambides, Jérôme François, Corinna Schmitt, and Burkhard Stiller, 100–112. Lecture Notes in Computer Science. Springer International Publishing.

Doolin, Bill. 2003. “Narratives of Change: Discourse, Technology and Organization.” *Organization* 10 (4): 751–770.

Dourish, Paul. 2001. *Where the Action Is: The Foundations of Embodied Interaction*. Cambridge, Massachusetts: MIT Press.

———. 2018. “The Once and Future Internet: Infrastructural Tragedy and Ambiguity in the Case of IPv6.” *Internet Histories* 2 (1–2): 55–74. https://doi.org/10.1080/24701475.2018.1455311.

Drake, William J. 2011. “Multistakeholderism: Internal Limitations and External Limits.” *Discussion Paper Series*, no. 1.

Drake, William J., and I. I. I. Wilson. 2008. *Governing Global Electronic Networks: International Perspectives on Policy and Power / Ed. by William J. Drake and Ernest J.*

Wilson, III. The Information Revolution and Global Politics. Cambridge, MA etc: MIT Press.

Dunne, Anthony, and Fiona Raby. 2001. *Design Noir: The Secret Life of Electronic Objects:* Basel: Birkhäuser.

Dutton, William H., and Malcolm Peltu. 2007. "The Emerging Internet Governance Mosaic: Connecting the Pieces." *Information Polity* 12 (1–2): 63–81. https://doi.org/10.3233/IP-2007-0113.

Easterling, Keller. 2014. *Extrastatecraft: The Power of Infrastructure Space*. Verso Books.

Eeten, Michel JG van, and Milton Mueller. 2013. "Where Is the Governance in Internet Governance?" *New Media & Society* 15 (5): 720–36. https://doi.org/10.1177/1461444812462850.

Epstein, Dmitry, Christian Katzenbach, and Francesca Musiani. 2016. "Doing Internet Governance: Practices, Controversies, Infrastructures, and Institutions." *Internet Policy Review*. http://dx.doi.org/10.14763/2016.3.435.

Erskine, Toni, and Madeline Carr. 2016. "Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace." *International Cyber Norms: Legal, Policy & Industry Perspectives*, NATO CCD COE Publications.

Finnemore, Martha, and Duncan B. Hollis. 2016. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110 (3): 425–479.

Finnemore, Martha, and Kathryn Sikkink. 1998. "International Norm Dynamics and Political Change." *International Organization* 52 (4): 887–917. https://doi.org/10.2307/2601361.

Flanagin, Andrew J., Craig Flanagin, and Jon Flanagin. 2009. "Technical Code and the Social Construction of the Internet:" *New Media & Society*, November. https://doi.org/10.1177/1461444809341391.

Flichy, Patrice. 2007. *The internet imaginaire*. Cambridge, Mass.: MIT Press.

Flinders, Matthew. 2004. "Distributed Public Governance in the European Union." *Journal of European Public Policy* 11 (3): 520–44. https://doi.org/10.1080/13501760410001694282.

Flyverbom, M. 2011. *The Power of Networks: Organizing the Global Politics of the Internet*. Cheltenham, UK: Edward Elgar.

Flyverbom, Mikkel. 2016. “Disclosing and Concealing: Internet Governance, Information Control and the Management of Visibility.” *Internet Policy Review* 5 (3).

Francis, P., and K. Egevang. 1994. “RFC1631 - The IP Network Address Translator (NAT).” RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc1631.

Frangonikolopoulos, Christos A. 2012. “Global Civil Society and Deliberation in the Digital Age.” *International Journal of Electronic Governance* 5 (1). https://doi.org/10.1504/IJEG.2012.047440.

Franklin, M. I. 2013. *Digital Dilemmas: Power, Resistance, and the Internet*. Oxford, New York: Oxford University Press.

Freed, Ned. 2000. “RFC2979 - Behavior of and Requirements for Internet Firewalls.” RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc2979.

Friedman, Batya, and David G. Hendry. 2019. *Value Sensitive Design: Shaping Technology with Moral Imagination*. Mit Press.

Frischmann, Brett. 2001. “Privatization and Commercialization of the Internet Infrastructure.” *Colum. Sci. & Tech. L. Rev.* 2: 1–25.

Froomkin, A. Michael. 2000. “Wrong Turn in Cyberspace: Using ICANN to Route around the APA and the Constitution.” *Duke Law Journal* 50 (1): 17–186. https://doi.org/10.2307/1373113.

Gal, Uri, Youngjin Yoo, and Richard Boland J. 2005. “The Dynamics of Boundary Objects, Social Infrastructures and Social Identities.” ResearchGate. 2005. https://www.researchgate.net/publication/221407571_The_Dynamics_of_Boundary_Objects_Social_Infrastructures_and_Social_Identities.

Galloway, Alexander R. 2006. *Protocol: How Control Exists After Decentralization*. New Ed edition. Cambridge, Mass.: MIT Press.

Gerring, John. 2007. *Case Study Research: Principles And Practices*. Cambridge: Cambridge University Press.

Giddens, Anthony. 1984. *The Constitution of Society: Outline of the Theory of Structuration*. Univ of California Press.

Gilardi, Fabrizio. 2012. “Transnational Diffusion: Norms, Ideas, and Policies.” In *Handbook of International Relations*, edited by Walter Carlsnaes, Thomas Risse, and Beth A. Simmons, Second Edition, 453–477. London, England: SAGE UK.

Glasius, Marlies. 2002. “Expertise in the Cause of Justice: Global Civil Society Influence on the Statute for an International Criminal Court.” In *Global Civil Society Yearbook 2002*, edited by Marlies Glasius, Mary Kaldor, and Helmut K. Anheier. Oxford, UK: Oxford University Press.

Glasius, Marlies, and Marcus Michaelsen. 2018. “Authoritarian Practices in the Digital Age| Illiberal and Authoritarian Practices in the Digital Sphere — Prologue.” *International Journal of Communication* 12 (0): 19.

Gohdes, Anita R. forthcoming. “Repression Technology: Internet Accessibility and State Violence.” *American Journal of Political Science*. https://doi.org/10.1111/ajps.12509.

Goldsmith, Jack, and Tim Wu. 2008. *Who Controls the Internet?: Illusions of a Borderless World*. 1 edition. New York: Oxford University Press.

Greenberg, Andy. 2013. *This Machine Kills Secrets: Julian Assange, the Cypherpunks, and Their Fight to Empower Whistleblowers*. Reprint edition. New York: Plume.

Guest, Greg, Kathleen MacQueen, and Emily Namey. 2012. *Applied Thematic Analysis*. 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc. https://doi.org/10.4135/9781483384436.

Haas, Peter M. 1992. “Introduction: Epistemic Communities and International Policy Coordination.” *International Organization* 46 (1): 1–35. https://doi.org/10.1017/S0020818300001442.

Habermas, Jürgen. 1984. *The Theory of Communicative Action*. Boston: Beacon Press.

Hafner, Katie, and Matthew Lyon. 1998. *Where Wizards Stay up Late: The Origins of the Internet*. Simon and Schuster.

Hajnal, Peter I. 2002. *Civil Society in the Information Age*. Aldershot: Ashgate.

Hanseth, Ole, and Eric Monteiro. 1997. “Inscribing Behaviour in Information Infrastructure Standards.” *Accounting, Management and Information Technologies* 7 (4): 183–211. https://doi.org/10.1016/S0959-8022(97)00008-8.

Haraway, Donna Jeanne. 1988. “Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective.” *Feminist Studies* 14 (3): 575–599.

———. 1991. *Simians, Cyborgs, and Women: The Reinvention of Nature*. New York: Routledge.

Héritier, Adrienne, and Dirk Lehmkuhl. 2008. “The Shadow of Hierarchy and New Modes of Governance.” *Journal of Public Policy* 28 (1): 1–17.

Hess, David J. 2005. “Technology-and Product-Oriented Movements: Approximating Social Movement Studies and Science and Technology Studies.” *Science, Technology & Human Values* 30 (4): 515–35.

Hill, Richard. 2014. “The Internet, Its Governance, and the Multi-Stakeholder Model.” *Info* 16 (2): 16–46. https://doi.org/10.1108/info-05-2013-0031.

Hilpinen, Risto. 1987. *Conflict and Change in Norm Systems*. University of Turku.

Hintz, Arne. 2009. *Civil Society Media and Global Governance: Intervening into the World Summit on the Information Society*. Vol. 37. LIT Verlag Münster.

Hintz, Arne, and Stefania Milan. 2009. “At the Margins of Internet Governance: Grassroots Tech Groups and Communication Policy.” *International Journal of Media & Cultural Politics* 5 (1/2): 23–38.

Hitlin, Steven, and Jane Allyn Piliavin. 2004. “Values: Reviving a Dormant Concept.” *Annual Review of Sociology* 30 (1): 359–93. https://doi.org/10.1146/annurev.soc.30.012703.110640.

Hofmann, Jeanette. 2016. “Multi-Stakeholderism in Internet Governance: Putting a Fiction into Practice.” *Journal of Cyber Policy* 1 (1): 29–49. https://doi.org/10.1080/23738871.2016.1158303.

Hofmann, Jeanette, Christian Katzenbach, and Kirsten Gollatz. 2017. “Between Coordination and Regulation: Finding the Governance in Internet Governance.” *New Media & Society* 19 (9): 1406–23. https://doi.org/10.1177/1461444816639975.

Hurrell, Andrew. 2002. “Norms and Ethics in International Relations.” *Handbook of International Relations*, 137–154.

Huston, Geoff. 2017. “The Internet’s Gilded Age.” *The ISP Column* (blog). March 2017. http://www.potaroo.net/ispcol/2017-03/gilding.html.

Hutchby, Ian. 2001. “Technologies, Texts and Affordances.” *Sociology* 35 (2): 441–456.

ICANN. 2016. “Bylaws for Internet Corporation for Assigned Names and Numbers | A California Nonprofit Public-Benefit Corporation.” February 11, 2016. https://www.icann.org/resources/pages/bylaws-2016-02-16-en.

Internet Architecture Board. 1996. “RFC1958 - Architectural Principles of the Internet.” RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc1958.

———. 2004. “RFC3724 - The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture.” RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc3724.

Internet Society. 2012. “Internet Invariants: What Really Matters.” *Internet Society* (blog). February 3, 2012. https://www.internetsociety.org/internet-invariants-what-really-matters/.

———. 2013. “The Value of Openness for a Sustainable Internet.” *Internet Society* (blog). 2013. https://www.internetsociety.org/resources/doc/2013/the-value-of-openness-for-a-sustainable-internet/.

Isin, Engin, and Evelyn Ruppert. 2015. *Being Digital Citizens*. London, UK ; New York: Rowman & Littlefield International.

Jackson, Jonathan. 2018. “Norms, Normativity, and the Legitimacy of Justice Institutions: International Perspectives.” *Annual Review of Law and Social Science* 14: 145–165.

Jasanoff, Sheila. 2004. “Ordering Knowledge , Ordering Society.” In *States of Knowledge: The Co-Production of Science and the Social Order.*, edited by Sheila Jasanoff. Vol. International library of sociology. London: Routledge.

Jasanoff, Sheila, and Sang-Hyun Kim. 2015. *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*. University of Chicago Press.

Jasanoff, Sheila, Sang-Hyun Kim, and Stefan Sperling. 2007. “Sociotechnical Imaginaries and Science and Technology Policy: A Cross-National Comparison.” *NSF Research Project, Harvard University*.

Jasper, James M., and Jan Willem Duyvendak, eds. 2015. *Players and Arenas: The Interactive Dynamics of Protest*. Amsterdam University Press.

Jessop, Bob. 1997. “Capitalism and Its Future: Remarks on Regulation, Government and Governance.” *Review of International Political Economy* 4 (3): 561–581.

Jørgensen, Rikke Frank. 2006. *Human Rights in the Global Information Society*. Cambridge, MA: MIT Press.

Jørgensen, Rikke Frank, Cathrine Bloch Veiberg, and Niels ten Oever. 2019. “Exploring the Role of HRIA in the Information and Communication Technologies (ICT) Sector.” In *Handbook on Human Rights Impact Assessment*. Edward Elgar Publishing.

Kaye, David. 2016. “Freedom of Expression, States and the Private Sector in the Digital Age.” Report of the Special Rapporteur on the promotion and protection of

the right to freedom of opinion and expression A/HRC/32/38. Geneva, Switzerland: Human Rights Council. https://www.ohchr.org/en/issues/freedomopinion/pages/privatesectorinthedigitalage.aspx.

Keck, M., and K. Sikkink. 1998. *Activists beyond Borders. Advocacy Networks in International Policy*. London: Cornell University Press.

Kelley, Judith. 2008. “Assessing the Complex Evolution of Norms: The Rise of International Election Monitoring.” *International Organization* 62 (2): 221–255.

Keohane, Robert O. 2001. “Governance in a Partially Globalized World.” *American Political Science Review* 95 (1): 1–13.

Kingdon, J. W. 1995. *Agendas, Alternatives and Public Policies*. New York: Longman.

Kooiman, Jan, and Svein Jentoft. 2009. “Meta-Governance: Values, Norms and Principles, and the Making of Hard Choices.” *Public Administration* 87 (4): 818–836.

Krasner, Stephen D. 1982. “Structural Causes and Regime Consequences: Regimes as Intervening Variables.” *International Organization* 36 (2): 185–205.

Kuerbis, Brenden, and Milton Mueller. 2011. “Negotiating a New Governance Hierarchy: An Analysis of the Conflicting Incentives to Secure Internet Routing.”

Kulesza, Joanna. 2018. “Balancing Privacy and Security in a Multistakeholder Environment. ICANN, WHOIS and GDPR.” *The VISIO JOURNAL*, 49.

Kulesza, Joanna, and Roy Balleste. 2015. *Cybersecurity and Human Rights in the Age of Cyberveillance*. Rowman & Littlefield.

Kummer, Markus. 2007. “The Debate on Internet Governance: From Geneva to Tunis and Beyond.” *Information Polity* 12 (1–2): 5–13. https://doi.org/10.3233/IP-2007-0107.

Lambach, Daniel. 2019. “The Territorialization of Cyberspace.” *International Studies Review*, 1–25. https://doi.org/10.1093/isr/viz022.

Land, Molly Beutz. 2009. “Protecting Rights Online.” *The Yale Journal of International Law* 34 (1): 1–46.

Lave, Jean. 2011. *Apprenticeship in Critical Ethnographic Practice*. University of Chicago Press.

Law, John. 1990. “Power, Discretion and Strategy.” *The Sociological Review* 38 (1_suppl): 165–191.

———. 1994. *Organizing Modernity*. Oxford: Blackwell.

Lemley, Mark A. 1997. “The Law and Economics of Internet Norms.” *Chicago-Kent Law Review* 73: 1257.

Lentz, Roberta G. 2011. “Civil Society in the Digital Age.” In . Oxford University Press. http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780195398571.001.0001/oxfordhb-9780195398571-e-27.

Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace*. New York: Basic Books.

———. 2006. *Code 2.0*. New York: Basic Books. http://codev2.cc/download+remix/Lessig-Codev2.pdf.

———. 2008. *Remix*. Bloomsbury Academic.

Levinson, Nanette S., and Derrick L. Cogburn. 2016. “The Next ‘Turn’ in Internet Infrastructure Governance.” In *The Turn to Infrastructure in Internet Governance*, edited by Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, 219–23. Information Technology and Global Governance. New York: Palgrave Macmillan US. https://doi.org/10.1057/9781137483591_12.

Levy, Steven. 1996. *Hackers, Heroes of the Computer Revolution Chapters 1 and 2*. http://www.gutenberg.org/ebooks/729#download.

Litwak, Robert S. 2002. “The New Calculus of Pre-Emption.” *Survival* 44 (4): 53–80. https://doi.org/10.1080/00396330212331343492.

MacKenzie, Donald, and Judy Wajcman, eds. 1999. *The Social Shaping of Technology*. Buckingham, UK: Open University Press.

Malcolm, Jeremy. 2008. *Multi-Stakeholder Governance and the Internet Governance Forum*. Terminus Press.

Mann, Michael. 1984. “The Autonomous Power of the State: Its Origins, Mechanisms and Results.” *European Journal of Sociology/Archives Européennes de Sociologie* 25 (2): 185–213.

Mansell, Robin. 2013. *Imagining the Internet: Communication, Innovation, and Governance*. Oxford: Oxford University Press.

Marcus, George E. 1995. *Technoscientific Imaginaries: Conversations, Profiles, and Memoirs*. Vol. 2. University of Chicago Press.

Marres, Noortje. 2017. *Digital Sociology: The Reinvention of Social Research*. John Wiley & Sons.

Mathew, Ashwin J. 2014. *Where in the World Is the Internet? Locating Political Power in Internet Infrastructure*. Berkeley: University of California. https://www.ischool.berkeley.edu/research/publications/2014/where-world-internet-locating-political-power-internet-infrastructure.

McCarthy, Daniel R. 2011. "Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet." *Foreign Policy Analysis* 7 (1): 89–111. https://doi.org/10.1111/j.1743-8594.2010.00124.x.

McKelvey, Fenwick. 2018. *Internet Daemons: Digital Communications Possessed*. U of Minnesota Press.

McLuhan, Marshall. 2013. *Understanding Media: The Extensions of Man*. Critical edition. Gingko Press.

Meier-Hahn, Uta. 2014. "Internet Interconnection: How the Economics of Convention Can Inform the Discourse on Internet Governance." In *GigaNet: Global Internet Governance Academic Network, Annual Symposium*.

———. 2015. "Creating Connectivity: Trust, Distrust and Social Microstructures at the Core of the Internet." In *Proceedings of the 43th Research Conference on Communication, Information and Internet Policy (TPRC 2015)*. Washington DC.

Milan, Stefania. 2009. "Community Media Activists in Transnational Policy Arenas." *Understanding Community Media*, 308–317.

———. 2014a. "The Fair of Competing Narratives: Civil Society(les) after NETmundial." *CGCS Media Wire* (blog). Spring 2014. http://www.global.asc.upenn.edu/the-fair-of-competing-narratives-civil-societyies-after-netmundial/.

———. 2014b. "NETmundial: Is There a New Guard of Civil Society Coming to the Internet Governance Fore?" *CGCS Media Wire* (blog). April 24, 2014. http://www.global.asc.upenn.edu/netmundial-is-there-a-new-guard-of-civil-society-coming-to-the-internet-governance-fore/.

Milan, Stefania, and Arne Hintz. 2013. "Networked Collective Action and the Institutionalized Policy Debate: Bringing Cyberactivism to the Policy Arena?" *Policy & Internet* 5 (1): 7–26. https://doi.org/10.1002/poi3.20.

Milan, Stefania, and Niels ten Oever. 2017. "Coding and Encoding Rights in Internet Infrastructure." *Internet Policy Review* 6 (1).

Minar, Nelson, and Marc Hedlund. 2001. “A Network of Peers: Peer-to-Peer Models through the History of the Internet.” In *Peer-to-Peer: Harnessing the Power of Disruptive Technologies*, by Andy Oram, 9–20. O’Reilly Media.

Mogul, J. C., M. Theimer, R. Finlayson, and T. Mann. 1984. “RFC903 - A Reverse Address Resolution Protocol.” RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc903.

Mol, Annemarie. 2002. *The Body Multiple: Ontology in Medical Practice*. Durham, North Carolina: Duke University Press.

Morris, John, and Alan Davidson. 2003. “Policy Impact Assessments: Considering the Public Interest in Internet Standards Development.” In *Proceedings of the 31th Research Conference on Communication, Information and Internet Policy (TPRC 2003)*. Washington DC. https://cdt.org/wp-content/uploads/publications/pia.pdf.

Mosco, Vincent. 2005. *The Digital Sublime: Myth, Power, and Cyberspace*. The MIT Press.

Mueller, Milton. 2002. *Ruling the Root Internet Governance and the Taming of Cyberspace*. Cambridge, Mass.: MIT Press.

———. 2010. *Networks and States: The Global Politics of Internet Governance*. MIT press.

———. 2017. *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*.

Mueller, Milton, and Brenden Kuerbis. 2013. “Buying Numbers: An Empirical Analysis of the IPv4 Number Market.”

Mueller, Milton, Brenden Kuerbis, and Hadi Asghari. 2013. “Dimensioning the Elephant: An Empirical Analysis of the IPv4 Number Market.” *Info* 15 (6): 6–18.

Mueller, Milton, John Mathiason, and Hans Klein. 2007. “The Internet and Global Governance: Principles and Norms for a New Regime.” *Global Governance* 13 (2): 237–54.

Mueller, Milton, Christiane Pagé, and Brenden Kuerbis. 2004. “Civil Society and the Shaping of Communication–Information Policy: Four Decades of Advocacy.” *The Information Society* 20 (3): 169–85. https://doi.org/10.1080/01972240490456845.

Mueller, Milton, Andreas Schmidt, and Brenden Kuerbis. 2013. “Internet Security and Networked Governance in International Relations.” *International Studies Review* 15 (1): 86–104. https://doi.org/10.1111/misr.12024.

Musiani, Francesca. 2015. “Practice, Plurality, Performativity, and Plumbing: Internet Governance Research Meets Science and Technology Studies.” *Science, Technology, & Human Values* 40 (2): 272–286.

———. 2016. “Alternative Technologies as Alternative Institutions: The Case of the Domain Name System.” In *The Turn to Infrastructure in Internet Governance*, edited by Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, 73–86. Springer.

Musiani, Francesca, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, eds. 2016. *The Turn to Infrastructure in Internet Governance*. New York: Palgrave Macmillan.

Nederhand, José, Victor Bekkers, and William Voorberg. 2016. “Self-Organization and the Role of Government: How and Why Does Self-Organization Evolve in the Shadow of Hierarchy?” *Public Management Review* 18 (7): 1063–1084.

Nye, Joseph S. 2014. “The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance.” Canada: Global Commission on Internet Governance. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

Nye, Joseph S., Jr. 2011. *The Future of Power*. New York: PublicAffairs.

Obar, Jonathan A., and Andrew Clement. 2013. “Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty.” In *TEM 2013: Proceedings of the Technology & Emerging Media Track-Annual Conference of the Canadian Communication Association*. Victoria, Canada.

Okuyama, Fabio Yoshimitsu, Rafael H. Bordini, and Antônio Carlos da Rocha Costa. 2011. “Situated Normative Infrastructures: The Normative Object Approach.” *Journal of Logic and Computation* 23 (2): 397–424.

Orwat, Carsten, and Roland Bless. 2016. “Values and Networks: Steps toward Exploring Their Relationships.” *ACM SIGCOMM Computer Communication Review* 46 (2): 25–31.

Padlipsky, M. A. 1982. “RFC871 - Perspective on the ARPANET Reference Model.” RFC-series. RFC Editor. https://tools.ietf.org/html/rfc871.

Parks, Lisa. 2015. “‘Stuff You Can Kick’: Toward a Theory of Media Infrastructures.” *Between Humanities and the Digital*, 355–373.

Pavan, E. 2012. *Frames and Connections in the Governance of Global Communications: A Network Study of the Internet Governance Forum*. Lanham, MD: Lexington Books.

Perrin, Stephanie E. 2018. “The Struggle for WHOIS Privacy: Understanding the Standoff Between ICANN and the World’s Data Protection Authorities.” Thesis. https://tspace.library.utoronto.ca/handle/1807/89738.

Pipek, Volkmar, and Volker Wulf. 2009. “Infrastructuring: Toward an Integrated Perspective on the Design and Use of Information Technology.” *Journal of the Association for Information Systems* 10 (5). https://doi.org/10.17705/1jais.00195.

Porter, Tony, and Karsten Ronit. 2006. “Self-Regulation as Policy Process: The Multiple and Criss-Crossing Stages of Private Rule-Making.” *Policy Sciences* 39 (1): 41–72.

Price, Monroe, and Stefaan Verhulst. 2000. “The Concept of Self-Regulation and the Internet.” *Protecting Our Children on the Internet: Towards a New Culture of Responsibility*, January, 133–98.

Price, Richard. 1998. “Reversing the Gun Sights: Transnational Civil Society Targets Land Mines.” *International Organization* 52 (3): 613–644. https://doi.org/10.1162/002081898550671.

Raboy, Marc, and Claudia Padovani. 2010. “Mapping Global Media Policy: Concepts, Frameworks, Methods.” *Communication, Culture & Critique* 3 (2): 150–169. https://doi.org/10.1111/j.1753-9137.2010.01064.x.

Radu, Roxana. 2019. *Negotiating Internet Governance*. Oxford University Press.

Raymond, Mark. 2019. “The Metastasization of the Global Cyber Regime Complex and the Creation of Critical Governance Infrastructure.” Presented at the International Studies Association, Toronto, March. https://www.isanet.org/Conferences/Event-Detail/mid/6587/EventID/11827/ItemID/111384?popUp=true.

Raymond, Mark, and Laura Denardis. 2015. “Multistakeholderism: Anatomy of an Inchoate Global Institution” 7 (3): 572–616. https://doi.org/10.1017/S1752971915000081.

Regent, Sabrina. 2003. “The Open Method of Coordination: A New Supranational Form of Governance?” *European Law Journal* 9 (2): 190–214. https://doi.org/10.1111/1468-0386.00175.

Resnick, Pete. 2014. “RFC7282 - On Consensus and Humming in the IETF.” RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc7282.

Risse, Thomas. 2000. “‘Let’s Argue!’: Communicative Action in World Politics.” *International Organization* 54 (1): 1–39.

Rochon, T. R. 1998. *Culture Moves. Ideas, Activism, and Changing Values*. Princeton, NJ: Princeton University Press.

Rogers, Michael, and Grace Eden. 2017. “Digital Citizenship and Surveillance| The Snowden Disclosures, Technical Standards, and the Making of Surveillance Infrastructures.” *International Journal of Communication* 11 (0): 22.

Rosa, Fernanda R. 2019. “Global Internet Interconnection Infrastructure: Materiality, Concealment, and Surveillance in Contemporary Communication.” PhD Thesis, American University.

Ruggie, John. 2011. “United Nations Guiding Principles on Business and Human Rights.” *United Nations*.

Russell, Andrew L. 2006. “’Rough Consensus and Running Code’and the Internet-OSI Standards War.” *IEEE Annals of the History of Computing* 28 (3): 48–61.

———. 2014. “Open Standards and the Digital Age: History, Ideology, and Networks.” *Afterimage* 42 (3): 39.

Rüth, Jan, Ingmar Poese, Christoph Dietzel, and Oliver Hohlfeld. 2018. “A First Look at QUIC in the Wild.” *ArXiv:1801.05168 [Cs]*, January. http://arxiv.org/abs/1801.05168.

Saltzer, J., D. Reed, and David Clark. 1984. “End-to-End Arguments in System Design.” *ACM Transactions on Computer Systems (TOCS)* 2 (4): 277–288. https://doi.org/10.1145/357401.357402.

Sandvig, Christian. 2013. “The Internet as Infrastructure.” In *The Oxford Handbook of Internet Studies*, edited by William H. Dutton. Oxford University Press. http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780199589074.001.0001/oxfordhb-9780199589074-e-5.

Scharpf, Fritz W. 1994. “Games Real Actors Could Play: Positive and Negative Coordination in Embedded Negotiations.” *Journal of Theoretical Politics* 6 (1): 27–53.

Schattschneider, Elmer E. 1975. “The Semi-Sovereign People: A Realist’s View of Democracy in America.”

Schmitz, Joachim, Cengiz Alaettinoglu, Carol Orange, David Meyer, and Mark Prior. 1999. “RFC2650 - Using RPSL in Practice.” RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc2650.

Scholte, Jan Aart. 2016a. “Relations with Civil Society.” In *The Oxford Handbook of International Organizations*, edited by Jacob Katz Cogan, Ian Hurd, and Ian Johnstone. Oxford University Press. http://opil.ouplaw.com/view/10.1093/law/9780199672202.001.0001/law-9780199672202-chapter-33.

———. 2016b. “Process and Power in Internet Governance. Reflections on the IANA Transition.” Presented at the RIPE meeting, Amsterdam, May 26.

———. 2017a. “Complex Hegemony: The IANA Transition in Global Internet Governance.” Presented at the Giganet 2017, Geneva, Switzerland. https://igf2017.sched.com/event/CRB7/the-12th-annual-symposium-of-the-global-internet-governance-academic-network-giganet.

———. 2017b. “Polycentrism and Democracy in Internet Governance.” In *The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance*, edited by Uta Kohl. Cambridge England ; New York: Cambridge University Press.

———. 2020. “Multistakeholderism: Filling the Global Governance Gap?” Stockholm, Sweden: Global Challenges Foundation.

Seawright, Jason, and John Gerring. 2008. “Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options.” *Political Research Quarterly* 61 (2): 294–308.

Shackelford, Scott J., Enrique Oti, Jaclyn A. Kerr, Elaine Korzak, and Andreas Kuehn. 2015. “Back to the Future of Internet Governance.” *Georgetown Journal of International Affairs* 16: 83.

Shapiro, Carl, and Hal R. Varian. 1998. *Information Rules: A Strategic Guide to the Network Economy*. Boston, Mass: Harvard Business Review Press.

Smyrnaios, Nikos. 2018. *Internet Oligopoly: The Corporate Takeover of Our Digital World*. Emerald Publishing Ltd.

Snow, D., and R. Benford. 1988. “Ideology, Frame Resonance, and Participant Mobilization.” In *From Structure to Action: Comparing Social Movement Research across Cultures*, edited by Bert Klandermans, Hanspeter Kriesi, and Sidney Tarrow, International social movement research:197–217. Greenwich, Conn: JAI Press.

Sørensen, Eva, and Jacob Torfing. 2009. “Making Governance Networks Effective and Democratic through Metagovernance.” *Public Administration* 87 (2): 234–258.

Sovacool, Benjamin K., Katherine Lovell, and Marie Blanche Ting. 2018. "Reconfiguration, Contestation, and Decline: Conceptualizing Mature Large Technical Systems." *Science, Technology, & Human Values* 43 (6): 1066–97. https://doi.org/10.1177/0162243918768074.

Sowell, Jesse H. 2012. "Empirical Studies of Bottom-up Internet Governance." In *Proceedings of the 40th Research Conference on Communication, Information and Internet Policy (TPRC 2012)*. Washington DC.

Stadnik, Ilona. 2019. "Internet Governance in Russia – Sovereign Basics for Independent Runet." In *Proceedings of the 47th Research Conference on Communication, Information and Internet Policy (TPRC 2019)*. Washington DC.

Star, Susan Leigh. 1990. "The Structure of Ill-Structured Solutions: Boundary Objects and Heterogeneous Distributed Problem Solving," 37–54.

———. 1999. "The Ethnography of Infrastructure." *American Behavioral Scientist*, no. 3: 377–391.

———. 2010. "This Is Not a Boundary Object: Reflections on the Origin of a Concept." *Science, Technology, & Human Values* 35 (5): 601–617.

Star, Susan Leigh, Geoffrey C. Bowker, and J.L Neuman. 2003. "Transparency beyond the Individual Level of Scale: Convergence between Information Artifacts and Communities of Practice." In *Digital Library Use:Social Practice in Design and Evaluation*, edited by Ann Peterson Bishop, Nancy A. Van House, Barbara P. Buttenfield, and Bruce Schatz, 241–69. MIT Press. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6279898.

Star, Susan Leigh, and James R. Griesemer. 1989. "Institutional Ecology,Translations' and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39." *Social Studies of Science* 19 (3): 387–420.

Star, Susan Leigh, and Karen Ruhleder. 1994. "Steps towards an Ecology of Infrastructure: Complex Problems in Design and Access for Large-Scale Collaborative Systems." In , 253–264. CSCW '94. ACM. https://doi.org/10.1145/192844.193021.

Stone, Deborah A. 1988. *Policy Paradox and Political Reason*. Scott Foresman & Co.

Susskind, Jamie. 2018. *Future Politics: Living Together in a World Transformed by Tech*. Oxford, New York: Oxford University Press.

Szyszczak, Erika. 2006. “Experimental Governance: The Open Method of Coordination.” *European Law Journal* 12 (4): 486–502. https://doi.org/10.1111/j.1468-0386.2006.00329.x.

Tarrow, Sidney. 1998. *Power in Movement. Social Movements and Contentious Politics*. Cambridge: Cambridge University.

———. 2005. *The New Transnational Activism*. New York: Cambridge University Press.

Taylor, Tom, Hanns Juergen Schwarzbauer, Malleswar Kalla, Lixia Zhang, Ken Morneault, Ian Rytina, Randall R. Stewart, Chip Sharp, and Qiaobing Xie. 2000. “RFC2960 - Stream Control Transmission Protocol.” RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc2960.

ten Oever, Niels. 2018. “Productive Contestation, Civil Society, and Global Governance: Human Rights as a Boundary Object in ICANN.” *Policy & Internet* 11 (June): 37–60. https://doi.org/10.1002/poi3.172.

———. 2020. “‘This Is Not How We Imagined It’ - Technological Affordances, Economic Drivers and the Internet Architecture Imaginary.” *New Media & Society*.

ten Oever, Niels, and Corinne Cath. 2017. “RFC8280 - Research into Human Rights Protocol Considerations.” RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc8280.

ten Oever, Niels, Stefania Milan, and Davide Beraldo. 2020. “Studying Discourse in Internet Governance through Mailing-List Analysis.” In *Research Methods in Internet Governance*, edited by Francesca Musiani, Derrick L. Cogburn, and Nanette S. Levinson. Cambridge, MA: MIT Press.

ten Oever, Niels, and Kathleen Moriarty, eds. 2018. “The Tao of IETF: A Novice’s Guide to the Internet Engineering Task Force.” *Internet Engineering Taskforce*. https://www6.ietf.org/tao.

Thaler, Dave. 2011. “RFC6250 - Evolution of the IP Model.” RFC-Series. RFC Editor. https://tools.ietf.org/html/rfc6250.

Thomas, Ward. 2001. *The Ethics of Destruction: Norms and Force in International Relations*. Cornell University Press.

Tilly, Charles. 1989. *The Contentious French*. Cambridge, Mass.: Belknap Press.

Torfing, Jacob. 2016. “Metagovernance.” In *Handbook on Theories of Governance*. Edward Elgar Publishing.

Tréguer, F, A Panayotis, and J Söderberg, eds. 2016. “Alternative Internets.” *The Journal of Peer Production*, no. 9.

Turner, Fred. 2006. *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago: University of Chicago Press.

Tusikov, Natasha. 2016. *Chokepoints: Global Private Regulation on the Internet*. Univ of California Press.

United States Government, Department of Commerce. 2014. “NTIA Announces Intent to Transition Key Internet Domain Name Functions.” March 14, 2014. https://www.ntia.doc.gov/print/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.

Van Eeten, M.J., and Milton Mueller. 2013. “Where Is the Governance in Internet Governance?” *New Media & Society* 15 (5): 720–36.

Van Rooy, A. 2004. *The Global Legitimacy Game. Civil Society, Globalization, and Protest*. New York: Palgrave Macmillan.

Van Schewick, Barbara. 2012. *Internet Architecture and Innovation*. Mit Press.

Verhulst, Stefaan G., Beth S. Noveck, Jillian Raines, and Antony Declerq. 2014. “Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem.” *Centre for International Governance Innovation*, December. https://www.cigionline.org/publications/innovations-global-governance-toward-distributed-internet-governance-ecosystem.

Weiss, Linda. 2006. “Infrastructural Power, Economic Transformation, and Globalization.” *An Anatomy of Power: The Social Theory of Michael Mann*, 167–86.

———. 2018. *The Myth of the Powerless State*. Cornell University Press.

Weissbrodt, David, and Muria Kruger. 2003. “Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regards to Human Rights.” *American Journal of International Law* 97 (4): 901–22. https://doi.org/10.2307/3133689.

Winner, Langdon. 1980. “Do Artifacts Have Politics?” *Daedalus* 109: 121.

Winseck, Dwayne. 2019. “Internet Infrastructure and the Persistent Myth of U.S. Hegemony.” In *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century*, edited by Blayne Haggart, Kathryn Henne, and Natasha Tusikov, 93–120. International Political Economy Series.

Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-14540-8_5.

Woolgar, S., and D. Neyland. 2013. *Mundane Governance: Ontology and Accountability*. Oxford: Oxford University Press.

Wu, Tim, David Gross, Esther Dyson, Michael Froomkin, A. A. Dyson, and A. A. Gross. 2007. "The Future of Internet Governance." *Proceedings of the ASIL Annual Meeting* 101: 201–13. https://doi.org/10.1017/S0272503700025660.

Wynsberghe, Aimee L. van, and GC Moreira Moura. 2013. "The Concept of Embedded Values and the Example of Internet Security." *Responsible Research and Innovation in ICT, Oxford, Technical Report* 1101.

Yin, Robert K. 2009. *Case Study Research: Design and Methods*. SAGE.

Zalnieriute, Monika, and Thomas Schneider. 2014. "A Council of Europe Analysis on ICANN's Procedures and Policies in the Light of Human Rights, Fundamental Freedoms and Democratic Values." Strasbourg: Council of Europe. https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/ICANN-PoliciesProcedures%2816June2014%29.pdf.

Zittrain, Jonathan. 2008. *The Future of the Internet–and How to Stop It*. Yale University Press.

List of Sources of Figures

Figure 1 'ICANN Policies and Human Rights Diagram', ICANNs Cross Community Working Party on ICANN's Social and Cultural Responsibility to Respect Human Rights, http://icannhumanrights.net/wp-content/uploads/2018/07/ICANN-and-Human-Rights-Jan2018.pdf accessed on May 26, 2020

Figure 2 Diagram produced by the author using the tool Python based tool 'BigBang'

Figure 3 Diagram produced by the author using the tool Python based tool 'BigBang'

Figure 4 'ICANN organizational chart', ICANN, https://www.icann.org/sites/default/files/assets/org-chart-1800x1000-04mar14-en.png accessed on May 26, 2020

Figure 5 Schematic overview produced by the author

Figure 6 Screen capture of object AS-GDPR in the RIPE Database, RIPE NCC, https://apps.db.ripe.net/db-web-ui/#/query?searchtext=AS-GDPR&rflag=true&-source=RIPE&bflag=false accessed on August 23, 2019

Figure 7 Screen capture of object AS-UNGP in the RIPE Database, RIPE NCC, https://apps.db.ripe.net/db-web-ui/#/query?searchtext=AS-UNGP&rflag=true&-source=RIPE&bflag=false accessed on August 23, 2019