Routledge Global Cooperation Series

POWER AND AUTHORITY IN INTERNET GOVERNANCE

RETURN OF THE STATE?

Edited by
Blayne Haggart, Natasha Tusikov
and Jan Aart Scholte

ROUTLEDGE

Power and Authority in Internet Governance

Power and Authority in Internet Governance investigates the hotly contested role of the state in today's digital society. The book asks: Is the state "back" in internet regulation? If so, what forms are state involvement taking, and with what consequences for the future?

The volume includes case studies from across the world and addresses a wide range of issues regarding internet infrastructure, data and content. The book pushes the debate beyond a simplistic dichotomy between liberalism and authoritarianism in order to consider also greater state involvement based on values of democracy and human rights. Seeing internet governance as a complex arena where power is contested among diverse non-state and state actors across local, national, regional and global scales, the book offers a critical and nuanced discussion of how the internet is governed – and how it should be governed.

Power and Authority in Internet Governance provides an important resource for researchers across international relations, global governance, science and technology studies and law as well as policymakers and analysts concerned with regulating the global internet.

Blayne Haggart is Associate Professor of Political Science at Brock University in St. Catharines, Canada, and Research Fellow, Käte Hamburger Kolleg/Centre for Global Cooperation Research University of Duisburg-Essen, Germany.

Natasha Tusikov is Assistant Professor of Criminology at York University in Toronto and a visiting fellow with the School of Regulation and Global Governance (RegNet) at the Australian National University.

Jan Aart Scholte is Chair of Global Transformations and Governance Challenges at Leiden University and Co-Director of the Centre for Global Cooperation Research at the University of Duisburg-Essen.

Routledge Global Cooperation Series

The *Routledge Global Cooperation* series develops innovative approaches to one of the most pressing questions of our time – how to achieve cooperation in a culturally diverse and politically contested global world?

Many key contemporary problems such as climate change and forced migration require intensified cooperation on a global scale. Accelerated globalisation processes have led to an ever-growing interconnectedness of markets, states, societies and individuals. Many of today's problems cannot be solved by nation states alone and require intensified cooperation at the local, national, regional and global level to tackle current and looming global crises.

Series Editors:
Tobias Debiel, Dirk Messner, Sigrid Quack and Jan Aart Scholte are Co-Directors of the Käte Hamburger Kolleg / Centre for Global Cooperation Research, University of Duisburg-Essen, Germany. Their research areas include climate change and sustainable development, global governance, internet governance and peacebuilding. Tobias Debiel is Professor of International Relations and Development Policy at the University of Duisburg-Essen and Director of the Institute for Development and Peace in Duisburg, Germany. Dirk Messner is President of the German Environment Agency (Umweltbundesamt – UBA). Sigrid Quack is Professor of Sociology at the University of Duisburg-Essen, Germany. Jan Aart Scholte is Professor of Global Transformations and Governance Challenges at Leiden University, Netherlands.

Patricia Rinck is editorial manager of the series at the Centre for Global Cooperation Research.

www.routledge.com/Routledge-Global-Cooperation-Series/book-series/RGC

Titles:

China's New Role in African Politics
From Non-Intervention towards Stabilization?
Edited by Christof Hartmann and Nele Noesselt

Hegemony and World Order
Reimagining Power in Global Politics
Edited by Piotr Dutkiewicz, Tom Casier and Jan Aart Scholte

Power and Authority in Internet Governance
Return of the State?
Edited by Blayne Haggart, Natasha Tusikov and Jan Aart Scholte

Power and Authority in Internet Governance

Return of the State?

Edited by Blayne Haggart, Natasha Tusikov and Jan Aart Scholte

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

Centre for
Global
Cooperation
Research

SPONSORED BY THE
Federal Ministry
of Education
and Research

First published 2021
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
52 Vanderbilt Avenue, New York, NY 10017

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for this book has been requested

ISBN: 978-0-367-44203-3 (hbk)
ISBN: 978-1-003-00830-9 (ebk)

Typeset in Goudy
by Apex CoVantage, LLC

Contents

List of figures vii
List of tables viii
List of contributors ix
Preface and acknowledgements xiv

Introduction: return of the state? 1
BLAYNE HAGGART, JAN AART SCHOLTE AND NATASHA TUSIKOV

PART 1
Internet governance: the bird's-eye view 13

1 **From governance denial to state regulation: a controversy-based typology of internet governance models** 15
MAURO SANTANIELLO

2 **The role of states in internet governance at ICANN** 37
OLGA CAVALLI AND JAN AART SCHOLTE

3 **The metagovernance of internet governance** 56
NIELS TEN OEVER

4 **The data-driven economy and the role of the state** 76
DAN CIURIAK AND MARIA PTASHKINA

PART 2
Internet governance and authoritarian states 95

5 **Building China's tech superpower: state, domestic champions and foreign capital** 97
LIANRUI JIA

6 "Nine dragons run the water": fragmented internet governance in China 123
TING LUO AND AOFEI LV

7 Russia: an independent and sovereign internet? 147
ILONA STADNIK

PART 3
Internet governance and democratic states 169

8 The return of the state? Power and legitimacy challenges to the EU's regulation of online disinformation 171
JULIA RONE

9 Varieties of digital capitalism and the role of the state in internet governance: a view from Latin America 195
JEAN-MARIE CHENOU

10 Seeing through the smart city narrative: data governance, power relations, and regulatory challenges in Brazil 219
JHESSICA REIA AND LUÃ FERGUS CRUZ

Conclusion: state power (and its limits) in internet governance 243
NATASHA TUSIKOV, BLAYNE HAGGART AND JAN AART SCHOLTE

Index 253

Figures

2.1	Overview of the IANA stewardship transition	44
5.1	The China-China-foreign financing model	107
5.2	An example of a VIE structure	109
6.1	The administrative hierarchy of the Chinese political system	126
6.2	Institutional structure of internet governance in China within the State Council system	129
6.3	Institutional structure of internet governance in China after 2014	130
9.1	Aggregated indexes of economic freedoms of the 12 largest economies in Latin America	203
9.2	Participation of different Latin American governments' representatives to ICANN GAC meetings (1999–2019)	206

Tables

1.1	A typology of internet governance models	24
1.2	Attributes of internet governance models	25
4.1	Economic characteristics of the DDE compared to previous eras	79
5.1	Public listing of state-owned media and telecom enterprises in China	108
9.1	Varieties of capitalism in Latin America and case studies of VoDC	204
9.2	From VoC to VoDC	207

3 The metagovernance of internet governance

Niels ten Oever

Introduction

Since the mid-1990s, multistakeholder governance, and specifically private internet governance, has been viewed as a governance innovation (Verhulst et al. 2014) and a replacement for intergovernmental telecommunications governance. However, in the 2010s the private internet governance regime, characterised by multistakeholder bottom-up self-regulation (Sowell 2012), started to show some signs of wear and tear, with the increased rule-setting done by states and multilateral bodies. For instance, as described in Chapter 2, several states have felt that they currently have an insufficient stake in the decision-making in the Internet Corporation for Assigned Names and Numbers (ICANN), the body that coordinates the usage of unique identifiers, such as top-level domains and IP addresses, that are foundational for the internet. Other states, such as Russia and China, have gone further by unilaterally proposing and enacting national regulations and creating domestic internet infrastructures in order to better exert influence on the internet, as described in Chapters 5 and 7.

This contest, at its heart, involves a contest between conflicting norms. The private internet governance regime has as its highest value the creation of interoperability and interconnection through industry coordination and norm development. In contrast, the multilateral regime seeks to achieve a number of other goals (including but not limited to maximising state sovereignty, promoting economic prosperity and limiting the spread of harmful and illegal content), through laws, policies, and norm-setting.

The rise of multilateral, or state-focused, internet governance is often seen as being a direct challenge to existing multistakeholder, or private, internet governance (e.g., Mueller 2017). This view sees the state as an (illegitimate) challenger to this private internet governance regime. In contrast, this chapter argues that rather than one regime potentially displacing another, we can better understand transnational internet governance as a regime complex that functionally and effectively consists of two normative regimes, namely a "private internet governance" regime that produces interconnection and interoperation and which is limited in turn by a "multilateral internet governance" regime. These two normative regimes jointly shape the internet as we know it. Both regimes operate with functionally

narrow remits that are shaped by their respective guiding norms. The guiding norms of the private internet governance regime is to increase of interconnectivity and interoperability, whereas the guiding norm of the multilateral internet governance regime is also to ensure the technical infrastructure accommodates national and regional norms and values.

To understand how these two regimes fit together, I employ the concept of "metagovernance." This lens offers us a to functionally differentiate between these two regimes and to analyse how power and influence are exerted in decentralised decision-making environments. Metagovernance, or "the governance of governance" (Jessop 1997), "entails the coordination of one or more governance modes by using different instruments, methods, and strategies" (Gjaltema, Biesbroek and Termeer 2019, 12). The concept of metagovernance allows one to transcend the perspective that sees "governance" as a practice that overcomes government in favour of one that understands the dialectical relationship between the two regimes. In using this concept, I build on the work of Sandra Braman (2020), who first applied the lens of metagovernance to the field of internet governance. Braman provides an excellent overview of the usefulness of the concept for the field, which I seek to validate by showcasing how institutional design and norm regimes serve as tools for metagovernance (Sørensen and Torfing 2009).

The private internet governance regime, which emerged after the privatisation of the internet in the early 1990s, is narrowly aimed at producing voluntary interconnection and interoperation among internet users and transnational corporations. While it has proven to be very successful in these regards, it has proven unable, in its current configuration, to accommodate norms that do not contribute to an increase in interconnection and interoperation, that is, to address other important social-policy objectives, such as privacy and internationalisation. The inability of the private internet governance regime to deal with these issues has sparked the creation of a new regime, namely the multilateral internet governance regime, based on norm-setting by state-based entities. The result has been the emergence of a regime complex that includes both regimes that themselves are a combination of different governance modes – private actors working through voluntary norms on one hand, states working through treaties and laws on the other – that are sometimes in conflict over norms, goals, and methods. These conflicts give the regime complex a dynamic, changing character. Oftentimes these regimes are painted as opposites, but I argue that both fulfill a particular role that cannot be fulfilled by the other regime. The private internet governance regime systematically fails at incorporating structural considerations on its societal impact, especially when these limit interoperability and interconnection. The multilateral internet governance regime, on the other hand, is unable to produce a general-purpose global communication network. The lens of metagovernance helps us to theorise how the interaction of these regimes, in the internet governance regime complex, are producing the internet infrastructure that is the backbone for information societies.

To substantiate this claim, I will first provide definitions of key theoretical terms I use in my analysis. Second, I provide an overview on debates of how internet

governance should be understood. Third, I describe the rise of the private internet governance regime and its guiding norms of interconnection and interoperability. Finally, I describe the pushback to the private internet governance regime, and the rise of the multilateral regime, and how this led to the emergence of a regime complex.

Norms, regime, and metagovernance of the internet infrastructure

The internet infrastructure is designed to function as a network of independent networks. The word "internet" itself is derived from "internetworking," the practice of interconnecting multiple networks (Peterson and Davie 2007, 169). These independent networks, also called Autonomous Systems (AS), are operated by many different kinds of institutions, ranging from internet service providers and telecommunication companies to research institutions and financial companies. For instance, AS2 is the University of Delaware, AS3 is the Massachusetts Institute of Technology, and AS32251 is assigned to the bank BNP Paribas. Furthermore, the internet does not have a central authority, the independent networks that make up the internet are not necessarily limited to one country or continent, and the "rules of the road" (Wu et al. 2007) for the internet are for the most part not binding, but rather voluntary norms that are developed through the private internet governance regime. 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). The voluntary technical norms that underpin the guiding norm of interoperability and interconnection on the internet are produced in private internet governance bodies. Examples of such protocols are the Internet Protocol (IP), the Domain Name System (DNS), and the Hypertext Transfer Protocol (HTTP). The dependence on voluntary norms produces in private governance bodies, rather than mandates in laws or treaties that are developed and ratified by nation states, to promote the interconnection of independent transnational networks make the governance of the internet a complex affair that has resulted in a "mosaic" (Dutton and Peltu 2005) or "bricolage" (Radu 2019) of governance institutions.

The internet has grown from being a communication network based in one and then several societies to the point where it now deeply permeates almost every part of every society in the world, a process described as metastisation (Raymond 2019). Typically, when discussing an issue area in global politics, we can speak of "regimes," which produce "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). However, the internet's ubiquity and pervasive permeation, and the involvement of a wide range of bodies, institutions, and authorities in the governance of the internet, mean that it is more useful and appropriate to speak of internet governance as a "regime complex." A regime complex is "an array of partially overlapping and non-hierarchical institutions that includes more than one international agreement or authority" (Alter and Raustiala 2018, 329). Regime theory allows one to theorise collaboration and conflict within

one issue field and regime complexes help to understand the interrelation between these regimes that might not always directly interact with each other, but all impact a specific area, in this case the internet infrastructure. Because they involve various institutions, or regimes, the metagovernance framework is particularly useful for thinking about regime complexes such as internet governance.

Politically contested definitions: the where, who, and what of internet governance

The internet's infrastructure has become a fundamental part of the critical infrastructure of information societies. This transformation embeds not only a particular technology or communication system within a society but also the norms enshrined in the processes of designing, standardising, and coordinating internet infrastructure. These norms are politically contested, including at the fundamental level of what exactly is "internet governance."

The definition of "internet governance" is itself contested: Struggles over internet governance thus involve debates regarding what internet governance itself means, as there is no authoritative or definitive definition of internet governance. In the words of Hofmann, "definitions of internet governance, either narrow or broad, always implicitly include preliminary decisions about institutions, constellations of actors and forms of authority" (2005, 1). The nature of these "preliminary decisions" and thus the perspectives of key actors can be illustrated by comparing a few definitions of internet governance. The first, and still most used, definition of internet governance was minted during the United Nations World Summit on the Information Society (WSIS) in 2005:

> Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the internet.
>
> (United Nations 2005)

This definition describes a wide range of actors involved in the process of internet governance, but their involvement is immediately qualified by the addition of the phrase "in their respective roles." While the nature of these roles is not defined explicitly, this definition least indicates that the actors do not engage on equal footing in the process because of their different respective roles. In the negotiations during the development of these definition, governments were the main actors pushing for the inclusion of this qualifier of the respective roles, because they believed a government representative should, for instance, have more weight than a member of a civil society organisation or a company. Nonetheless, this definition does acknowledge that non-governmental actors do have a role to play in the governance of the internet.

The definition of internet governance that was reached at WSIS cemented the idea that internet governance was a multistakeholder effort (Hofmann 2016).

This, however, led to a backlash among several influential internet governance scholars. In response to the definition of civil society and governments as key actors in the practice internet governance, they proposed one that argues that practically speaking, the private sector, in interplay with the networks' users, not civil society and governments, sets the rules in the governance of the internet:

> Internet governance is collective decision-making by owners, operators, developers, and users of the networks connected by Internet protocols to establish policies, rules, and dispute resolution procedures about technical standards, resource allocations, and/or the conduct of people engaged in global internetworking activities.
>
> (Mueller, Mathiason and Klein 2007, 245)

While this definition did not gain much traction, it does foreground the dominant role the private sector plays in private internet governance. In contrast to the previous one, this definition does not mention governments and civil society or their roles or obligations. The authors do so because, for them, "the internet is largely composed of . . . privately owned and administered networks . . . which means that it has less need than many other systems for global governance" (Mueller, Mathiason and Klein 2007, 246). With this statement, these scholars are not just offering an assessment of the current situation but are also making a normative statement. They are claiming, as many after these scholars have done, that internet governance *should* be left to the private sector. This belief dovetails with the idea that sole role of the private internet governance regime is to increase interconnection and interoperability. The definition also implies that governments and civil society might not (or, perhaps, should not) have an active role to play in the governance of the internet.

The centre of the private internet governance regime consists of private, non-state institutions. The governance bodies are not treaty bodies, nor are they international organisations. The internet infrastructure's technical standards and governance bodies, such as the Internet Engineering Task Force (IETF), ICANN, and Regional Internet Registries (RIRs) are dominated by the transnational corporations that design and sell networking equipment, provide services or operate networks. The IETF, ICANN, and the RIRs together set the "rules of the road" (Wu et al. 2007); that is, they produce the preconditions of the interoperability of independent networks by providing the coordination and distribution of unique numbers to all connected networks and devices on the internet, the service that translates human-readable addresses into numbers, as well as the open voluntary protocols that allow these interconnected devices and networks to communicate. The IETF, ICANN, and the RIRs are bodies that have grown and developed in conjunction with the internet and are fully and exclusively dedicated to its coordination and operation. Because these bodies provide the bare minimum of technical preconditions for the internet to function, they are often understood as the core internet governance bodies. Whereas internet governance, or at least the self-regulatory private internet governance regime, is often a synonym for these bodies, these specific institutions are not mentioned in definitions of internet

governance. The institutional configuration of these organisations, such as their processes, procedures, and organisational culture and other affordances, does play a significant role in the shaping on the internet infrastructure. One could understand this as a blind spot in the internet governance definitions provided earlier, because they do not take into account the "mosaic" (Dutton and Peltu 2005), or "bricolage" (Radu 2019), of governance institutions involved in, and traditionally associated with, internet governance, such as the IETF, ICANN, and RIRs. The guiding norms of interconnection and interoperability are also encoded in the bylaws, technical documents, and policy documents. For instance, in the founding document of the RIR for Europe, West Asia (i.e., the Caucasus and Iran) and the Middle East, Reseaux IP Europeans, it reads: "RIPE promotes and coordinates interconnection of IP networks within Europe and to other continents" (RIPE 1992). This is just to illustrate that the private internet governance regime is not a "neutral" meeting platform, if such a thing could exist, but rather a normative regime. The prominent internet governance scholar Laura DeNardis, meanwhile, provides a definition that includes private internet governance bodies but also clearly highlights that internet governance does not stop there and includes the role of technology, states, and international agreements. This definition thus combines the first two definitions but adds institutions, practices, and the role that design of architecture plays:

> the practice of internet governance extends beyond institutions such as the Internet Corporation for Assigned Names and Number and standards-setting organisations to include private industry policies, national policies, international treaties, and the design of technical architecture.
>
> (DeNardis 2014, 19)

Van Eeten and Mueller, for their part, put the centre of gravity of internet governance beyond these institutions to emphasise the influence of the private sector. They argue that "the aggregate effect of decentralised decisions and adjustments made by ISPs . . . have much more profound effects on the evolution and use of the internet than the ICANN" (Van Eeten and Mueller 2013, 727). While it might be true that actors such as internet service providers (ISPs) undertake regulatorily consequential actions, many of the decisions made outside of the aforementioned formal internet governance bodies are still mediated by trust relations and connections that are built at the meetings that are organised by these governance bodies, as convincingly shown by Ashwin Mathew in his work on the governance of internet routing (Mathew 2014). In other words, making the definition of internet governance too inclusive risks reducing its conceptual utility. Hofmann, Katzenbach, and Gollatz offer an escape out of this conundrum by defining governance as "critical moments" when routine activities become problematic and need to be revised, thus, when regular coordination itself requires coordination" (Hofmann, Katzenbach and Gollatz 2016, 1406). This approach helpfully locates internet governance in a combination of practices of reflexive coordination, and thus ensures that not all practices involving the internet infrastructure are understood

as internet governance, but does include a wide array of practices, venues, and actors. That said, while this seems an elegant theoretical solution that includes activities both inside and outside of governance bodies, it does not describe *where* these practices of internet governance take place and *who* undertakes them. This makes internet governance a large, nebulous object with blurry edges that is hard to describe or interrogate, which in turn makes it hard to research larger trends about how the internet infrastructure is being shaped through its transnational governance.

Another way of locating internet governance is by 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" (DeNardis 2014, 7). To do this, one can trace patterns of ownership, power, and reconfigurations in the internet infrastructure and particularly in the exercise of control (Musiani et al. 2015), which is especially relevant when it comes to control over main "chokepoints" (Tusikov 2016, 36), or "control points" (Choucri and Clark 2018, 168). In addition to large data transit providers that interconnect networks and operate (submarine) cables, content distribution networks and internet exchange points, governance and standard-setting institutions such as ICANN, IETF, and RIRs are prime examples of such points of focus, because these are persistent fields of convergence of coordination, collaboration, and policy development in internet governance. Not only are the formal processes that these bodies facilitate important, but also the building of trust, reputation and personal relations, which is an essential part of these coordination processes, happens to a significant degree at the meetings that these institutions organise (Mathew 2014; Meier-Hahn 2014). While not all internet governance takes place in governance and standard-setting institutions, these are main focus points for coordination and a place where many of the players in inter-networking meet to engage in industry self-regulation, or, in the *parlance* of the field, bottom-up coordination (Sowell 2012). Also, reverberations and responses to significant changes in the internet infrastructures are discussed and sometimes addressed in, through, and by these institutions.

The previous sections show how internet governance definitions are both descriptive and normative and how they include, exclude, or emphasise the role of governments, corporations, civil society, technological design, governance institutions, and reflexive practices. Another approach to internet governance is through how power is exercised through the internet infrastructure. This approach emphasises the role of institutional configuration, epistemic communities, and interpersonal relations that are important building blocks of the private internet governance regime that I will further describe in the following section.

The rise of the private internet governance regime

The commercialisation of the internet at the beginning of the 1990s led to the rise of the private internet governance regime, which one can understand by looking at the relevant arrangements of power. Many expected that the distributed

architecture of the internet and its private governance would lead to perfect markets, free competition, and decentralised structures (Litan and Rivlin 2001; Wu 2018). However, as we now know, this did not happen. Rather, "market concentrations, control, and power struggles are categories to adequately describe the fundamental dynamics of the commercial internet" (Dolata and Schrape 2018, 85). Instead of leading to competition and innovation (Cowhey, Aronson and Richards 2009; Van Schewick 2012; Powers and Jablonski 2015), it actually led to the emergence of internet oligopolies (Mansell and Javary 2002; Smyrnaios 2018), such as Google, Amazon, Cloudflare, Cisco, Huawei, and Juniper. The internet has long had a privatised component; already in the 1980s corporations were connected to the internet, and networks were often produced and maintained by companies such as Bolt Beranek and Newman (BBN), then called Interface Message Processor (IMP), that built the first router. Nonetheless, in these early days the oversight over the development of the internet architecture was still managed through publicly funded agencies and academic institutions. In the 1980s, the internet was also already connected to commercial services, such as mail providers like SprintMail and Compuserve (Kahin 1990), but commercialisation was still limited because commercial traffic was not allowed on the network due to the Acceptable Use Policy (AUP) that governed the internet backbone, which was funded by the National Science Foundation (NSF).[1]

However, the growth of the use of the internet by the end of the 1980s and beginning of the 1990s seriously congested the internet backbone that was run by the NSF. Several options were explored to increase the capacity of the internet and the backbone. Of the different options, such as establishing national research networks, commercialisation of the internet backbones was perceived as the best option to scale the network (Kahin 1990; Chinoy and Salo 1997), which fitted with the "end of history" (Fukuyama 2012) sentiment that was en vogue in that period, which translated in a limited role of government and a belief in neoliberal market economies. The decision to pursue commercialisation led to the creation of the Commercial Internet Exchange, which overcame the limitations set by the AUP because there was no longer a central backbone funded by public money. This alleviated a burden on public funding and replaced it with private capital, which resulted in the commercialisation and further privatisation of the internet (Frischmann 2001). Some understand this as the retreat of government from internet governance, which fits into a straightforward story implicit in the Mueller definition and argument mentioned earlier in which state and civil society interests (beyond maximising interoperability) are treated as illegitimate. Others, however, have argued that this has actually led to the galvanisation of the power of the United States, through the dominance of the American companies (e.g., Carr 2015). I build on the thinking of Madeline Carr by interpreting the de-funding of the backbone by the US government as an act of metagovernance – that is, "the coordination of one or more governance modes" via different methods and strategies. From this perspective, the US government did not retreat from internet governance. Instead, it engaged in governance by other means, in this case, outsourcing the growth of the internet to the private sector through the establishment

of a transnational private internet governance regime. This decision spurred the formal institutionalisation of the IETF, RIRs, and ICANN. Commercialisation of the internet was not a retreat from governmental control, but a transition from direct governance to indirect governance through norm-setting and institutional design. Industry was tasked with meeting particular US goals of increasing interconnection between independent networks, without incurring direct costs for government. And so it did, but with consequences that were not directly foreseen.

Norms in the private internet governance regime

The commercialisation and the privatisation of the internet that started at the end of the 1980s led to the formal institutionalisation of the private internet governance regime with the official institution of RIRs, the IETF, and ICANN. These bodies were supposed to coordinate interconnection between independent networks following voluntary standards. A popular saying among IETF engineers captures the single-minded focus on this mission: "The IETF is not the protocol police." (Among RIR network operators the equivalent saying is, "We are not the routing police.") However, these sayings fail to identify who actually *is* the protocol or routing police. The answer, it turns out, is surprisingly simple: There is no police, at least if one thinks of police in terms of a restricting authority. The private internet governance regime is not aimed at limiting or restricting interconnection; to the contrary, and true to the private regime's embedded norms, it is aimed at creating more interconnection and interoperability. The private internet governance regime does not create limitations but creates incentives for cooperation among competitors (Meier-Hahn 2014). The participants in these bodies do what they describe as acting "for the good of the internet" (Mathew 2014), and this dominant norm translates in an increase in network capacity, meaning higher bandwidths and lower latency, for more interoperable devices. This norm benefits certain groups: network operators, vendors, and service providers (Powers and Jablonski 2015) through a network effect. More interconnected networks, and interconnection among networks, produces an increase in value for all interconnected networks (Lemley 1997). Within this normative framework, within the private internet governance regime, debates centre not on *whether* more interconnection and interoperation should be created: This is taken as a given. Rather, they focus on *how* this should happen. The private internet governance regime is an instrument for the increase of data traffic through the production of interconnection and interoperability between transnational corporations.

Other norms that are often professed in internet governance, such as openness and decentralisation, are deprioritised when they come in conflict with the prevailing normative framework of interconnection and interoperability. The distributed design of internet governance was supposed to prevent centralised decision-making as much as possible, to ensure that no one party or group would have significant sway over another. The sedimentations of these design choices can be found in the formalisation of the policy and specification development processes in these bodies that all have been organised around the principle of

openness (Russell 2014; ten Oever 2021 forthcoming). Openness here should be understood as the public availability of process and outcome documents, discussion archives, as well as participatory decision-making. This has led to drawn-out, specialised, highly proceduralised, and resource-intensive processes. Ironically this "openness" design has had the effect of closing down these decision-making processes for everyone who has not been initiated into the processes and vocabulary of this environment because it leads to a torrent of often interrelated documents, emails, calls, and meetings in which one can participate. This flood of information can be hard to navigate, as it takes not only experience to filter the information based on relevance but also expert knowledge to understand the content. For example, the guide to abbreviations used in internet governance that is produced regularly by the not-for-profit DiploFoundation, currently runs to 34 pages and over 150 abbreviations (DiploFoundation n.d.). Because of the need for expert knowledge of technologies and processes in order to effectively participate, compounded with the resources and time needed to acquire this knowledge and participate in these meetings and conversations, the practice of open and distributed internet governance revolves around a relatively small group of experts that form a global elite (Scholte 2017) that regularly attend internet governance meetings that take place several times per year in large hotels and conference venues on different continents. While the bodies might have different areas of operations, and different institutional configurations, the number of people actively partaking in decision-making in these bodies is quite small, and the number of organisations they represent is significantly smaller and getting smaller every year due to consolidation in the market. Thus, the open decision-making process in the private internet governance regime has not led to more openness, but it has facilitated private self-coordination for the production of more interoperation and interconnectivity.

Governmental requests and the rise of the multilateral internet governance regime

When governments largely delegated the scaling of the internet to the private sector (while holding some indirect involvement and oversight), the internet could grow without governments worrying about the economic and financial overhead costs and risks for themselves. However, when this private governance regime was optimised for its intended purposes of increasing interconnection and interoperation, it came with significant consequences for the ability of governments to influence this regime.

Private internet governance can be largely understood as an example of normative industry self-coordination that is optimised through the institutional configuration of distributed bodies to increase interconnection and interoperability between networks and devices. When the private internet governance regime is expected or requested to perform other roles that do not fit with the underlying norms of increasing connectivity and interoperability, it regularly fails to deliver, for instance, when the private internet governance regime is asked to consider the societal impact of their policies and technologies. This becomes glaringly clear when governments make requests to the private internet governance regime to inscribe or encode social

or legal norms which might not increase interconnectivity or interconnections. Such conflicts between two normative systems is typical within regime complexes. I will provide four recent examples of this in the internet governance regime complex. These examples demonstrate that when states have concrete policy objectives they seek to pursue by means of the internet infrastructure, the private internet governance regime resists their requests because states' requests were in conflict with their norm for increasing interconnection and interoperation.

WHOIS and GDPR

An interesting example where internet governance was unable to accommodate the needs of states started with ICANN's lack of response to the formal requests of the European Commission to limit access to the private information of registrants of websites via the publicly available WHOIS registry. The WHOIS registry is a service that everyone can access to look up the contact information, often including the physical address, of the person or entity who registered a domain name. For the European Commission, this presented a violation of the right to privacy of domain registrants and European privacy laws (Perrin 2018), as they documented in their letters to ICANN in 2006 and 2007 (Article 29 Data Protection Working Party 2006, 2007). ICANN never responded to these letters. Only when the European Commission developed its own rules, namely the Europe-wide, enforceable, General Data Protection Regulation in 2016, ICANN started a process to devise an alternative to the existing WHOIS registry.

For the private internet governance regime, embodied in ICANN in this example, the WHOIS registry was understood as an artefact that enabled interconnection and interoperability. This was actually one of the reasons that the WHOIS registry was invented in the internet's early years: to be able to find the contact information connected to a malfunctioning network. The European Commission found that the WHOIS registry violated the privacy of website owners. The private internet governance regime prioritised here interconnection and interoperability – they emphatically did not want different WHOIS systems for different parts of the world – over the norms of the European Commission.

Snowden revelations of US mass surveillance

Another example that shows how internet governance bodies are bad interfaces for government policies was the response to the Snowden revelations by the IETF. In response to the revelations of widespread American state surveillance, the IETF adopted a document called "Pervasive Monitoring Is an Attack" (Farrell and Tschofenig 2014). At the same time, the Internet Architecture Board, a prominent committee of the IETF, adopted a statement urging "protocol designers to design for confidential operation by default" (Morgan 2014), which heralded a widespread use of encryption in protocols to thwart the US government's ability to continue its surveillance practices. These documents by themselves were reminiscent of a document released in May 2000, in which the IETF stated that

it would not standardise interfaces for wiretapping or interception technologies in the technologies they develop and standardise (Internet Architecture Board and Internet Engineering Steering Group 2000). With these actions, the IETF went straight against requests by and perceived needs of the United States government, namely the ability of law enforcement agencies and other government services to access private internet communications.

The IETF has made it clear, time and again, that they do not want to facilitate the weakening of encryption or the construction of back doors to provide access to law enforcement agencies to data streams. One of the main arguments offered by the IETF is that a weakening of protocols would provide access not only to law enforcement agencies but also to others, which would weaken trust in the network. That would in turn negatively impact interconnectivity. The US government, as well as other governments, however, has never ceased asking and looking for such capabilities.

Chinese draft law and verification service providers

US government and European Commission requests are not the only ones that are denied by the private internet governance regime. In 2006, the Chinese government published draft legislation (Creemers 2016) which contained a provision that would mandate all internet domain names in China to be registered through government-licensed service operators. Verisign, the world's largest domain registry, developed a proposed technical standard[2] to implement verification service providers through the Extensible Provisioning Protocol (EPP). EPP is the protocol that is used by domain registries and registrars to register domains. This would have added the possibility of verification service providers to acknowledge that someone's identity has been verified. The verification service provider would check whether someone, based on their identity, would be allowed to register a specific domain.

Permissionless innovation – the ability to develop and implement protocols and services without having to ask for permission – has been one of the principles underlying the internet's interconnectiveness and interoperability. When one is asked to register in the WHOIS registry upon registering a domain, your identity is not verified, and receiving it does not depend on *who you are* or whether you are allowed to have that domain. The Chinese government's proposal would have gone against this policy. And even though American company Verisign, the registry of the largest top-level domain in the world, was eager to enter this market and create a technical norm to accommodate that proto-legal norm, there was a significant amount of criticism in the IETF working group which caused Verisign to discontinue the work on the proposed standard.

Schengen routing

A final example is the proposal that has been brought up by several governments and which has been resisted by engineers and network operators time after time: internet routing based on geographical borders, such as Schengen routing (Dönni et al. 2015). The proposal prescribes that internet traffic originating from and destined for

a certain country, or group of countries, would stay within that territory. Time and again, it has been argued that the internet does not recognise geographical borders (Mueller 2017). This is not because it is a technological or social impossibility to make this happen, but it is rather a design choice made primarily by network operators. Networks could be limited to one jurisdiction, and routing rules could be developed to preferably or exclusively route internet traffic among specific networks in a specific jurisdiction. This possibility, however, has been repeatedly rejected by network operators and network equipment vendors in the private internet governance regime because this could lead to less internet interconnection and interoperability between networks. This illustrates perfectly how norms requested by the multilateral internet governance regime for technical infrastructure to accommodate national or regional social and legal norms get resisted by the private internet governance regime because it hampers interconnection and interoperation.

In each of these four examples, the private internet governance regime resisted the introduction of norms by governments in the internet infrastructure. This shows that the bodies that make up the private internet governance regime produce interconnection and interoperation and support norms favouring these outcomes. States, rather, seek to introduce limitations to fit the network (and its inherent normative biases) to their particular norm regimes, which must address other policy issues beyond maximising interconnection. The inability, or unwillingness, of the private internet regime to accommodate these requests by nation states has led to the rise of a multilateral internet governance regime. The private internet governance regime and the multilateral internet governance regime jointly make up the transnational internet governance regime complex. In the multilateral internet governance regime, states seek to align the technical infrastructure with national and regional social and legal norms.

This attempt by state governments to contest interoperability norms has led scholars such as Milton Mueller, one of the co-authors of the second internet governance definitions cited earlier, to argue that there is a misalignment between internet governance and national sovereignty (Mueller 2017). According to Mueller, internet governance produces (or, rather, should produce) one global internet, while nation states seek to apply rules based on their own limited territorial reach.

Mueller's argument is worth unpacking, because it gets to the heart of what it means, from a metagovernance perspective, to see internet governance as a regime complex of sometimes-overlapping institutions and regimes, rather than as a unidimensional regime that converges around one single set of norms (in this case, related to interoperability). While Mueller sees states' actions as a challenge to an existing internet governance regime, these state actions can also be understood as a next step in the "process of defining, delimiting, and inscribing space" in cyberspace, involving a "process of deterritorialisation and reterriorialisation" (Lambach 2019, 2–3). However, the limited normative scope of a private internet governance regime, supporting and focusing exclusively on the norms of increased interconnection and interoperation, means that states are unable to realise their public-policy objectives via the regime as it currently exists.

Unable to work through the narrow interconnection-focused regime, we have seen actions such as the introduction of the General Data Protection Regulation of the European Commission (Kulesza 2018; Perrin 2018) and the Russian "sovereign internet" regulation (Stadnik 2019; this volume). Such moves are new milestones in the governance of the internet infrastructure, since they could form the beginning of a trend in state-based rule-setting on internet infrastructure, which is inherently different from the private "multistakeholder" internet governance regime. A similar trend in states engaging in intergovernmental initiatives for norm-setting for the internet can also be observed in initiatives such as the United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security and the United Nations Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security. These multilateral efforts should also be understood as inherent part of the emerging multilateral internet governance regime. In contrast to Mueller's interpretation of this emerging regime as a threat to privatised internet governance, a metagovernance approach highlights that it, together with the private internet governance regime, make up an internet governance *regime complex*.

From this perspective, we can understand the internet governance regime *complex* as follows. The private internet governance regime is guided by the norm of creating more interconnection and interoperation. The multilateral internet governance regime, on the other hand, serves to shape the internet to the norms of states and limits interconnection and interoperation. These two regimes should not be understood as opposing forces, but rather as two different parts of the internet governance regime complex. Aside from being composed of distinguishable parts, such as the Internet Governance Forum on the multilateral side and the IETF on the private governance side, they do not focus on different areas. If they did, we would be able to classify them as sub-regimes. Instead, these two regimes have different purposes, while they both seem to design and optimise the internet infrastructure to function according to their respective objective, namely the increase in interconnection and interoperability or the accommodation of technical norms to local norms, which makes these different regimes instruments of metagovernance.

The private internet governance regime's features and limitations are the product of a "mobilisation of bias," through which "some issues are organised into politics while others are organised out" (Schattschneider 1975, 71). In this case, the interconnection and interoperation norms are organised in. They lie at the heart of the private internet governance regime and the internet's technical standards: "The goal is connectivity, the tool is the Internet Protocol"; "connectivity is its own reward" (Internet Architecture Board 1996, 1). Crucially, this private regime was shaped in this manner by governments, most significantly the US government, via processes of commercialisation and privatisation. This perspective helps to restore governments into the internet-governance picture. The limitation of interoperation and interconnection by governments through the multilateral internet governance regime should be understood as an internet governance practice and not as something that is misaligned with internet governance. It is solely misaligned with (parts of) the private internet governance regime.

Discussion

States' (particularly the United States') decision to commercialise and privatise the internet's infrastructure led to the emergence of the private internet government regime and, later, the multilateral internet governance regime. The commercialisation of the internet was not an example of the retreat of government, but rather a transition from direct governance to a process of metagovernance through the dialectics between two normatively limited regimes: one focused on interconnectivity and the other on other norms. Efforts by governments to govern the internet through the multilateral internet governance regime, irrespective of how they are framed or the goals that are claimed, limit the increase in interoperation and interoperability of the private internet governance regime but rather seek the technical infrastructure to accommodate to social and legal norms.

The metagovernance heuristic used in this chapter is not solely an analytical lens to allow us to discern the functional differentiation between the regimes of the internet governance regime complex. It also offers the practical opportunity to explore why some norms get embedded in policies and technologies and why some are not. This brings about possible reflections on the societal impact of the development of technological norms through this regime complex. The social and legal impact of the internet has been a topic of discussion since its early inception. In her analysis of early technical internet standards documents, the so-called RFC-series, Braman shows how norms, privacy, security, rights, and freedoms have been part and parcel of early technical discussions about the internet (2011, 2012). There also exists an extensive literature on the norms and values that have been embedded in the internet infrastructure (Orwat and Bless 2016; Shilton 2018; Zittrain 2008), and scholars have also asked whether the internet infrastructure should be designed to accommodate different value systems (Clark et al. 2005), or rather have specific values embedded in them, for instance through the use of value-sensitive design approaches (Brown, Clark and Trossen 2010; Friedman, Kahn and Borning 2008). There also have been calls to encode specific sets of values in the internet infrastructure (Cath and Floridi 2017) or at least consider the implications of policies and technical proposals structurally on their societal impact (Morris and Davidson 2003). Despite all this, norms beyond interoperability and interconnectivity have never been operationalised through the private internet governance regime.

The heuristic of metagovernance allows us to make a functional differentiation between the private and the multilateral internet governance regimes. This differentiation highlights the tools of metagovernance, such as norms and institutional design, that are used to structure these regimes and fundamentally make the internet work in the way it does. The differentiation also helps to explain why the private internet governance regime does not take the structural impact of technology on society into account.

The lack of structural evaluation of the societal impact of technological norms in the private internet governance regime is not because existing institutions lack the capacity to evaluate and implement policies and frameworks supporting different norms or because there is a lack of interest among various individuals involved in the internet governance regime complex. Rather, as I noted earlier, norm evaluation is happening, but it occurs through the lens of the embedded and guiding

norm of the specific regime. In the case of the private internet governance regime, this is the norm of interconnection and interoperation. Proposed new voluntary norms are evaluated against these deeply enshrined and institutionally and infrastructurally embedded norms that guide the community of the bodies that make up the private internet governance regime. Freedom of speech and freedom of expression are rights that are widely supported within the private internet governance regime because expression fits very well with increasing interoperation and interoperability. On the other hand, the operationalisation of the right to privacy, such as in the case of WHOIS and the GDPR or Schengen routing, or the right to nondiscrimination, is more likely to be enacted through the limitation of interconnectivity and interoperation through the multilateral internet governance regime. This is because privacy requires data minimisation, and Schengen routing implies limited interoperation between networks.

Conclusion

Existing definitions and understandings of internet governance largely focus on stakeholder groups, institutions, and practices. In this chapter I have sought to show how one can make effective functional differentiations between governance regimes within the internet governance regime complex, using the lens of metagovernance. By understanding these regimes through their embedded norms, one obtains a higher-level view to the vast field of internet infrastructure and its governance. Subsequently, one is able to interrogate the respective regimes using their own respective norms. This shows that the governance of the internet infrastructure is by no means monolithic, nor is it random. Insight in the two norm regimes that make up the regime complex provide one with the ability to understand how power and control are exercised in this global network, namely through deeply embedded guiding norms, bound to norm regimes that transcend individual internet governance bodies and instruct the behaviour of those who engage in it. This analysis has also shown that the resurgence of the nation state through the rise of the multilateral internet governance regime is a direct consequence of the inability of the private internet governance regime to accommodate social and legal norms that do not increase interconnection and interoperability.

Notes

1 The Acceptable Use Policy. GENERAL PRINCIPLE:
(1) NSFNET Backbone services are provided to support open research and education in and among US research and instructional institutions, plus research arms of for-profit firms when engaged in open scholarly communication and research. Use for other purposes is not acceptable.
UNACCEPTABLE USES:
(10) Use for for-profit activities, unless covered by the General Principle or as a specifically acceptable use.
(11) Extensive use for private or personal business.

Source: www.livinginternet.com/doc/merit.edu/acceptable_use_policy.htm, accessed 28 November 2019.

2 For the Verification Code Extension for the Extensible Provisioning Protocol, see https://tools.ietf.org/html/draft-ietf-regext-verificationcode-06, Accessed 29 November 2019.

References

Alter, Karen J., and Kal Raustiala. 2018. "The Rise of International Regime Complexity." *Annual Review of Law and Social Science* 14 (1): 329–349. https://doi.org/10.1146/annurev-lawsocsci-101317-030830.

Article 29 Data Protection Working Party. 2006. *European Commission. Letter to ICANN Board of Directors Chairman*. 22 June. www.icann.org/en/system/files/files/schaar-to-cerf-22jun06-en.pdf. Accessed 29 November 2019.

Article 29 Data Protection Working Party. 2007. *Subject: Comments on the GNSO Whois Task Force Preliminary Task Force Report on Whois Services of 22 November 2006; and on the Draft ICANN Procedure for Handling Whois Conflicts with Privacy Law of 3 December 2006*. European Commission. Letter to ICANN Board of Directors Chairman. 12 March. 22 June. www.icann.org/en/system/files/files/schaar-to-cerf-12mar07-en.pdf. Accessed 29 November 2019.

Braman, Sandra. 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.

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

Braman, Sandra. 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.

Brown, Ian, David D. 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: ACM. https://doi.org/10.1145/1921233.1921246.

Carr, Madeline. 2015. "Power Plays in Global Internet Governance." *Millennium* 43 (2): 640–659. https://doi.org/10.1177/0305829814562655.

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.

Chinoy, Bilal, and Timothy J. Salo. 1997. "Internet Exchanges: Policy-Driven Evolution." In *Coordinating the Internet*, edited by Brian Kahin and James H. Keller, 325–345. Cambridge, MA: MIT Press. http://dl.acm.org/citation.cfm?id=275025.275053.

Choucri, Nazli, and David D. Clark. 2018. *International Relations in the Cyber Age: The Co-Evolution Dilemma*. Cambridge, MA: MIT Press.

Clark, D.D., 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.

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. https://doi-org.proxy.library.brocku.ca/10.1111/j.1541-1338.2008.00371.x.

Creemers, Rogier 2016. "Internet Domain Name Management Rules (Opinion-seeking Revision Draft)." *China Copyright and Media*. 25 March. https://chinacopyrightandmedia.

wordpress.com/2016/03/25/internet-domain-name-management-rules-opinion-seeking-revision-draft/. Accessed 4 August 2020.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

DiploFoundation. n.d. *Internet Governance Acronym Dictionary*. Version 3.0. www.diplomacy.edu/sites/default/files/IG_Acronym_glossary_2019.pdf. Accessed 27 November 2019.

Dolata, Ulrich, and Jan-Felix Schrape. 2018. *Collectivity and Power on the Internet: A Sociological Perspective*. SpringerBriefs in Sociology. Springer International Publishing. www.springer.com/de/book/9783319784137.

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. Cham: Springer International Publishing.

Dutton, William H., and Malcolm Peltu. 2005. "The Emerging Internet Governance Mosaic: Connecting the Pieces." *SSRN Scholarly Paper ID 1295330*. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=1295330.

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

Farrell, Stephen, and Hannes Tschofenig. 2014. "RFC7258 – Pervasive Monitoring Is an Attack." *RFC – Series*. IETF. https://tools.ietf.org/html/rfc7258.

Friedman, Batya, Peter H. Kahn, and Alan Borning. 2008. "Value Sensitive Design and Information Systems." In *The Handbook of Information and Computer Ethics*, edited by Kenneth Einar Himma and Herman T. Tavani, 69–101. Hoboken: John Wiley & Sons.

Frischmann, Brett. 2001. "Privatization and Commercialization of the Internet Infrastructure." *Science and Technology Law Review* 2: 1–25. https://doi.org/10.7916/stlr.v2i0.3537.

Fukuyama, Francis. 2012. *The End of History and the Last Man*. New York: Penguin.

Gjaltema, Jonna, Robbert Biesbroek, and Katrien Termeer. 2019. "From Government to Governance . . . to Meta-Governance: A Systematic Literature Review." *Public Management Review* 1–21. https://doi.org/10.1080/14719037.2019.1648697.

Hofmann, Jeanette, Christian Katzenbach, and Kirsten Gollatz. 2016. "Between Coordination and Regulation: Finding the Governance in Internet Governance." *New Media & Society* 19 (9): 1406–1423. https://doi-org.proxy.library.brocku.ca/10.1177%2F1461444816639975.

Hofmann, Jeanette. 2005. "Internet Governance: A Regulative Idea in Flux." *SSRN Scholarly Paper ID 2327121*. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2327121.

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.

Internet Architecture Board. 1996. *RFC1958 – Architectural Principles of the Internet*. https://tools.ietf.org/html/rfc1958.

Internet Architecture Board, and Internet Engineering Steering Group. 2000. "RFC2804 – IETF Policy on Wiretapping." *RFC – Series*. IETF. https://tools.ietf.org/html/rfc2804.

Jessop, Bob. 1997. "Capitalism and Its Future: Remarks on Regulation, Government and Governance." *Review of International Political Economy* 4 (3): 561–581. https://doi-org.proxy.library.brocku.ca/10.1080/096922997347751.

Kahin, B. 1990. "RFC1192 – Commercialization of the Internet Summary Report." *RFC-Series*. IETF.

Krasner, Stephen D. 1982. "Structural Causes and Regime Consequences: Regimes as Intervening Variables." *International Organization* 36 (2): 185–205. https://doi-org.proxy.library.brocku.ca/10.1017/S0020818300018920.

Kulesza, Joanna. 2018. "Balancing Privacy and Security in a Multistakeholder Environment. ICANN, WHOIS and GDPR." *The VISIO Journal* 49. http://4liberty.eu/balancing-privacy-and-security-in-multistakeholder-environment-icann-whois-gdpr/.

Lambach, Daniel. 2019. "The Territorialization of Cyberspace." *International Studies Review* vix022: 1–25. https://doi.org/10.1093/isr/viz022.

Lemley, Mark A. 1997. "The Law and Economics of Internet Norms." *Chicago-Kent Law Review* 73 (4): 1257.

Litan, Robert E., and Alice M. Rivlin. 2001. "Projecting the Economic Impact of the Internet." *American Economic Review* 91 (2): 313–317.

Mansell, Robin, and Michele Javary. 2002. "Emerging Internet Oligopolies: A Political Economy Analysis." In *An Institutionalist Approach to Public Utilities Regulation*, edited by E. Miller and W. J. Samuels, 162–201. East Lansing, MI: Michigan State University Press.

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

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*. https://dx.doi.org/10.2139/ssrn.2809867.

Morgan, Cindy 2014. *IAB Statement on Internet Confidentiality*. Internet Architecture Board. 14 November. www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/.

Morris, John, and Alan Davidson. 2003. "Policy Impact Assessments: Considering the Public Interest in Internet Standards Development." *SSRN Scholarly Paper ID 2060656*. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2060656.

Mueller, Milton. 2017. *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. Hoboken: Wiley.

Mueller, Milton, John Mathiason, and Hans Klein. 2007. "The Internet and Global Governance: Principles and Norms for a New Regime." *Global Governance* 13 (2): 237–254.

Musiani, Francesca, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, eds. 2015. *The Turn to Infrastructure in Internet Governance*. 1st ed. New York: Palgrave Macmillan.

Orwat, Carsten, and Roland Bless. 2016. "Values and Networks: Steps toward Exploring Their Relationships." *ACM SIGCOMM Computer Communication Review* 46 (2): 25–31. https://doi-org.proxy.library.brocku.ca/10.1145/2935634.2935640.

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

Peterson, Larry L., and Bruce S. Davie. 2007. *Computer Networks: A Systems Approach*. New York: Elsevier.

Powers, Shawn M., and Michael Jablonski. 2015. *The Real Cyber War: The Political Economy of Internet Freedom*. Chicago: University of Illinois Press.

Radu, Roxana. 2019. *Negotiating Internet Governance*. Oxford: 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. www.isanet.org/Conferences/Event-Detail/mid/6587/EventID/11827/ItemID/111384?popUp=true.

RIPE. 1992. "RIPE Terms of Reference." *RIPE NCC*. 29 November. www.ripe.net/publications/docs/ripe-001. Accessed 5 August 2020.

Russell, Andrew L. 2014. *Open Standards and the Digital Age*. Cambridge: Cambridge University Press.

Schattschneider, Elmer E. 1975. *The Semi-Sovereign People: A Realist's View of Democracy in America*. Boston, MA: Wadsworth, Cengage Learning.

Scholte, Jan Aart. 2017. *Complex Hegemony: The IANA Transition in Global Internet Governance*. Presented at the Giganet Annual Symposium, Geneva. https://igf2017.sched.com/event/CRB7/the-12th-annual-symposium-of-the-global-internet-governance-academic-network-giganet.

Shilton, Katie. 2018. "Engaging Values Despite Neutrality: Challenges and Approaches to Values Reflection during the Design of Internet Infrastructure." *Science, Technology, & Human Values* 43 (2): 247–269. https://doi.org/10.1177/0162243917714869.

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

Sørensen, Eva, and Jacob Torfing. 2009. "Making Governance Networks Effective and Democratic through Metagovernance." *Public Administration* 87 (2): 234–258. https://doi-org.proxy.library.brocku.ca/10.1111/j.1467-9299.2009.01753.x.

Sowell, Jesse H. 2012. "Empirical Studies of Bottom-up Internet Governance." In *Proceedings of the 40th Research Conference on Communications, Information, and Internet Policy*. Arlington, VA: Telecommunications Policy Research Consortium.

Stadnik, Ilona. 2019. "Internet Governance in Russia – Sovereign Basics for Independent Runet." In *TPRC47 Proceedings*. Washington, DC: TPRC. https://papers.ssrn.com/abstract=3421984.

ten Oever, Niels. 2021 Forthcoming. "'This Is Not How We Imagined It' – Technological Affordances, Economic Drivers and the Internet Architecture Imaginary." *New Media & Society*.

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

United Nations. 2005. "Tunis Agenda for the Information Society." *World Summit on the Information* Society. WSIS-05/TUNIS/DOC/6(Rev.1)-E. 18 November. www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

Van Eeten, Michael J.G., and Milton L. Mueller. 2013. "Where Is the Governance in Internet Governance?" *New Media & Society* 15 (5): 720–736. https://doi-org.proxy.library.brocku.ca/10.1177%2F1461444812462850.

Van Schewick, Barbara. 2012. *Internet Architecture and Innovation*. Cambridge: 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. www.cigionline.org/publications/innovations-global-governance-toward-distributed-internet-governance-ecosystem.

Wu, Tim. 2018. *The Curse of Bigness: Antitrust in the New Gilded Age*. New York: Colombia Global Reports.

Wu, Tim, David Gross, Esther Dyson, Michael Froomkin, A.A. Dyson, and A.A. Gross. 2007. "The Future of Internet Governance." In *Proceedings of the ASIL Annual Meeting* 101: 201–213. https://doi.org/10.1017/S0272503700025660.

Zittrain, Jonathan. 2008. *The Future of the Internet – And How to Stop It*. New Haven, CT: Yale University Press.