

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

Niels ten Oever
University of Amsterdam
mail@nielstenoever.net
<https://twitter.com/nielstenoever>
<https://orcid.org/0000-0001-5134-2199>

Abstract

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.

Keywords

infrastructural power, Internet governance, global governance, international relations, infrastructural norms, norm conflict

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’¹, 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 retracted², it shows how technical actors, such as RIRs, can have a significant impact on how governments, organizations, and individuals are connected to the Internet.

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 2005) of institutions, which together make up the transnational Internet governance regime complex (Nye 2014), also described as the polycentric Internet governance network (Scholte 2017), 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 over 92.000 separate 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,

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

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

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 understand 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. 2015), 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; M. Mueller, Schmidt, and Kuerbis 2013) or the economics of the routing infrastructure (M. L. Mueller and Kuerbis 2013; M. 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 Mathew 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 socio-economic 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 transcend 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 infrastructural norms. 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 toolkit³. 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.

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 an 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

3 <https://dataactive.github.io/bigbang/> accessed on October 31st 2019

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.⁴

4 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.*⁵

The undertone of this attitude is caught more shortly in the often repeated adage ‘my network, my rules’⁶. A long time RIPE participant further elaborated how the collaborations take shape:

*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.*⁷

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’⁸. Some interviewees express there is an

5 N2719

6 N2719, N2819, N3719, N3819, N4019

7 N3119

8 N3219

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 RIPE⁹. 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.*¹⁰

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.*¹¹

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’¹². 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.*¹³

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’¹⁴ 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’¹⁵. This sense of community among network operators allows for quicker problem solving, and help to increase personal reputation¹⁶ and build trust¹⁷ 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’¹⁸. Thus delivery on the collective expectation of respect for the inter-connectivity norm, creates an institutional normativity

9 N3919

10 N4019

11 N3819

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

13 N2719

14 N{26-42}19

15 N4019

16 N2518, N3219, N4219

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

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

among network operators, that in turn motivates willing compliance and cooperation (Jackson 2018), which in turn is rewarded with trust and reputation.

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’¹⁹, that is the sense that is being shared in the community. It is the main, leading, and common denominator.

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:

19 N4219

```

as-set:          AS-GDPR
tech-c:          NT08-RIPE
admin-c:         NT08-RIPE
mnt-by:          CYBERIA
created:         2019-05-22T21:04:44Z
last-modified:  2019-05-23T10:52:11Z
source:          RIPE
descr:           Members of this set declare to be compliant with the General Data Protection Regulation of
the European Union
mbrs-by-ref:     ANY

```

Login to update 

Figure 1: AS-GDPR, source: RIPE database <https://apps.db.ripe.net/db-web-ui/#/query?searchtext=AS-GDPR&rflag=true&source=RIPE&bflag=false> accessed on August 23, 2019

```

as-set:          AS-UNGP
tech-c:          NT08-RIPE
admin-c:         NT08-RIPE
mnt-by:          CYBERIA
created:         2019-05-22T21:05:32Z
last-modified:  2019-05-23T10:52:36Z
source:          RIPE
descr:           Members of this set declare to have adopted and implemented the United Nations Guiding
Principles on Business and Human Rights
mbrs-by-ref:     ANY

```

Login to update 

Figure 2: AS-UNGP, source: RIPE database <https://apps.db.ripe.net/db-web-ui/#/query?searchtext=AS-UNGP&rflag=true&source=RIPE&bflag=false> accessed on August 23, 2019

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 Orange²⁰. 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 GDRP or UNGPs.

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

²⁰ <https://business-humanrights.org/en/find-companies> accessed on November 17, 2019

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]’²¹. Another experienced participant explained it as follows:

*That’s—the idea that’s time has not come yet. It’s too early to introduce such a thing. [...] Because the operators 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.*²²

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 an 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.*²³ 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?*²⁴ 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 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.’²⁵, which means they could not even implement it in the running of their networks.

21 N2619

22 N3319

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

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

25 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'²⁶ and integrating these norms would 'build more things onto a system which is already just about fit for purpose'²⁷, by any means it should be maintained that Regional Internet Registries are not 'the routing police'²⁸. 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.

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.²⁹

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."³⁰

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

[H]ow can it [RIPE NCC] say, "Well, we're just gonna stick with Western European values?" Well, hang on a second. [RIPE] NCC serves 76 different countries or 73 different

26 N2619

27 N4019

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

29 N4019

30 N2819

*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.*³¹

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'³², this should 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*³³

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.'³⁴

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'³⁵,
- institutionally, because the scope of the RIPE database is kept limited: adding norms 'is not what the RIPE database was made for'³⁶ and integrating these norms would 'build more

31 N3419

32 N3119

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

34 N3819

35 N4019

36 N2619

things onto a system which is already just about fit for purpose'³⁷, by any means it should be maintained that Regional Internet Registries are not 'the routing police'³⁸;

- 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 complexity³⁹;
- supranationally, because these norms would encourage the 'politicizing [of] identifiers'⁴⁰, which would be 'a slippery slope'⁴¹. This in turn could create thresholds and boundaries in internetworking, which would not work 'for the good of the network'⁴².

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 norm 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 identify 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'⁴³.

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

37 N4019

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

39 N3819

40 N3119

41 N3019, N3819

42 N3219

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

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.

Funding Acknowledgment

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), and the Amsterdam School of Cultural Analysis Finishing Fellowship. 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.

References

- Baur-Ahrens, Andreas. 2017. "The Power of Cyberspace Centralisation: Analysing the Example of Data Territorialisation." *Security/Mobility: Politics of Movement*, 37–56.
- 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>.
- Braman, Sandra. 2012. "Internationalization of the Internet by Design: The First Decade." *Global Media and Communication* 8 (1): 27–45. <https://doi.org/10.1177/1742766511434731>.
- DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven: Yale University Press.
- 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>.
- 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.
- 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>.
- Easterling, Keller. 2014. *Extrastatecraft: The Power of Infrastructure Space*. Verso Books.
- 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*. Tallinn: 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>.

- Haas, Peter M. 1992. "Introduction: Epistemic Communities and International Policy Coordination." *International Organization* 46 (1): 1–35. <https://doi.org/10.1017/S0020818300001442>.
- Haraway, Donna. 1988. "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective." *Feminist Studies* 14 (3): 575–99. <https://doi.org/10.2307/3178066>.
- Haraway, Donna Jeanne. 1991. *Simians, Cyborgs, and Women: The Reinvention of Nature*. New York: Routledge.
- Hilpinen, Risto. 1987. *Conflict and Change in Norm Systems*. University of Turku.
- Hurrell, Andrew. 2002. "Norms and Ethics in International Relations." *Handbook of International Relations*, 137–154.
- Jackson, Jonathan. 2018. "Norms, Normativity, and the Legitimacy of Justice Institutions: International Perspectives." *Annual Review of Law and Social Science* 14: 145–165.
- Kuerbis, Brenden, and Milton Mueller. 2011. "Negotiating a New Governance Hierarchy: An Analysis of the Conflicting Incentives to Secure Internet Routing."
- Lambach, Daniel. 2019. "The Territorialization of Cyberspace." *International Studies Review*, 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: 1257.
- 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.
- 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>.
- 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 *TPRC*. Vol. 43.
- 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 L., and Brenden Kuerbis. 2013. "Buying Numbers: An Empirical Analysis of the IPv4 Number Market."
- 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, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, eds. 2015. *The Turn to Infrastructure in Internet Governance*. 1st ed. 2015 edition. New York, NY: Palgrave Macmillan.
- Nye, Joseph S. 2014. *The Regime Complex for Managing Global Cyber Activities*. *Global Commission on Internet Governance*. CIGI, Global Commission on Internet Governance. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.
- 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.
- Oever, Niels ten, 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.
- 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.
- 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*.
- Schmitz, Joachim, Cengiz Alaettinoglu, Carol Orange, David Meyer, and Mark Prior. 1999. "RFC2650 - Using RPSL in Practice." RFC. IETF. <https://tools.ietf.org/html/rfc2650>.
- Scholte, Jan Aart. 2017. "Polycentrism and Democracy in Internet Governance." In *The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance*, edited by UtaEditor Kohl, 165–184. Cambridge University Press. <https://doi.org/10.1017/9781316534168.012>.
- Sowell, Jesse H. 2012. "Empirical Studies of Bottom-up Internet Governance." In *Proc. TPRC*.
- Thomas, Ward. 2001. *The Ethics of Destruction: Norms and Force in International Relations*. Cornell University Press.
- Tusikov, Natasha. 2016. *Chokepoints: Global Private Regulation on the Internet*. Univ of California Press.
- Van Eeten, M.J., and Milton L. Mueller. 2013. "Where Is the Governance in Internet Governance?" *New Media & Society* 15 (5): 720–36.
- 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.