Operational Epistemic Authority in the Internet's Infrastructure

Jesse Sowell

Abstract
Internet communication increasingly intermediates our social, economic, and political lives, yet the technical communities coordinating its critical functions remain understudied. This article provides an empirical analysis of how two of the communities managing functions essential to Internet communication—addressing and routing—create the rules and operational order that sustains global communication. Analytically, this article expands the typology of epistemic authorities at play in the global governance system to include those that have accrued authority through their direct management of global, complex infrastructures. These analyses fill gaps in both the international relations and Internet governance literatures, offering a framework for systematically evaluating epistemic quality and integrity in terms of how authority is created and sustained. The article concludes with a brief analysis of how to more effectively integrate these authorities into the global governance system.

Introduction

In the 1990's, the Internet transitioned from a government experiment started in 1969 into a communications infrastructure that increasingly intermediates our social, economic, and political lives, with implications ranging from how societies share ideas, to economic growth and international security. Absent substantive government intervention and regulation, the communities of engineers and operators that manage these core functions, self-identifying as the operations community, have grown from an epistemic community of academic and industry actors contributing research and development expertise in an experimental network to transnational epistemic authorities shaping the topology, performance, and politics of the modern Internet's infrastructure. Despite their importance, the institutions and communities maintaining the functions necessary for all Internet communication—address delegation and routing—have been understudied, relegated to the low politics of technical standard setting and operations.

In the literature, the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Governance Forum (IGF) are often framed as the center

International Organization, 20XX, page 1 of 34

doi:10.1017/xxxxxxx xxxx

of Internet governance, inspiring to van Eeten and Mueller critique this focus in their article entitled "Where is the governance in Internet governance?"[1] This article evaluates how operations communities function as epistemic authorities. One distinguishing feature of operations communities is use a bottom-up process referred to as "rough consensus"[2] to create (and maintain) the knowledge and rules necessary sustain core functions, apace with changes in the Internet's infrastructure. Rough consensus is a means of pragmatic problem identification, evaluation, and consensus-based rule-making[3] based on operational experience.

Through two empirical cases on operations communities as epistemic authorities, this articles contributes the notions of diffuse and structured operational epistemic authorities to the broader typology of epistemic authority in the literature. Operations communities are private authorities[4] with deep, experience-based knowledge, with essential distinguishing characteristics of both Haas's (1992) epistemic communities and Zürn's (2018) epistemic authorities. Following Haas, these communities have distinct means of creating and validating knowledge, and an authoritative claim to that knowledge,[5] but they are not (currently) formally embedded in policy processes. Like Zürn's epistemic authorities, operations communities are focused on impartial evaluation of their domain,[6] in this case, the security, stability, and integrity of resources critical to the Internet's core functions. Operational epistemic authorities are valuable sources of expertise, but the source of their authority differs in two significant ways. First, their authority was not delegated by a political authority;[7] it accrued by virtue of their unique access to and management of critical resources. Second, rough consensus' requires valid contributions be rooted in acknowledged expertise. This characteristic of rough consensus is a key factor contributing to endogenous legitimacy and sustaining these communities' epistemic authority.

Rough consensus has embedded appropriateness values that shape the scope of operations communities' authority. In particular, these values shape the kinds of rules made and, importantly how and under what circumstances enforcing these rules and their operational image of order may interfere with the high politics of domestic and international affairs. The values embedded are not derived from the politics of conventional transnational issues, such as human rights or economic security. Interview subjects were quick to highlight "we do not make public policy, we make [Internet] resource policy." The rule of thumb in these communities is that rules are strictly about operations and resource policy. These values are derived from the

1. See both van Eeten and Mueller (2013) and Hofmann, Katzenbach, and Gollatz (2017) addressing this question.

2. Clark 1992; Russell 2006.

3. Here, rule making is used to capture the range of rules, norms, standards, and best practices. It does not imply legal rule making.

4. Hall and Biersteker 2003; Büthe and Mattli 2011.

5. Haas 1992, 2-4.

6. Zürn 2018, 51-53.

7. And as elaborated later in this article, cannot be easily rescinded by political authorities.

politics of operational efficiency rooted in the custodianship of (common) resources that contributing to the integrity of Internet communication.

This article contributes analyses of the history and function of these epistemic authorities and their relationship to Internet governance and the broader global governance system. It then builds on these empirical cases to expand the typology of epistemic authority. First, this article disentangles the function and objectives of operations communities from broader communities engaged in more public facing elements of the infrastructure (namely the domain name system, coordinated by ICANN). Given these foundations, the notion of *operational* epistemic authorities is presented relative to existing theory, then in the context of its foundations in the early experimental Internet, ultimately leading up to the formation of the modern institutions in which rough consensus serves to ensure credible knowledge assessment and the development of rules that keep pace with growth and technological change. Rough consensus itself is then presented as an adaptive, reflexive[8] rule making process, couched in how values rooted in operational efficiency are embedded in the process and shape these authorities image of liberal order. This article concludes by returning to the question of impartiality and legitimacy in this emerging form of epistemic authority, for both the Internet, and more generally for a society with increasing dependence on complex, decentralized infrastructures for which expertise, and resource provisioning and management, are embedded in distinctly transnational epistemic authorities.

Delving *in*to the Internet's Operations Communities

Colloquial notions of "the Internet"[9] include a broad set of activities: activities facilitated by applications such as e-mail, activities on platforms such as Facebook, and, most salient here, those unseen activities playing out in the supporting infrastructure. Solum (2008) notes that

> If the topic of Internet governance were taken as the investigation of the regulation of all the[] activities [that take] place on (or were significantly affected by) the Internet, then 'Internet governance' would be more or less equivalent to 'law and politics'.[10]

Broad framings of Internet governance confound the loci the diverse governance regimes at play and their spheres of authority. Platforms such as Meta's social media platform Facebook and online shopping platforms such as Amazon Marketplace are built *on* the Internet, relying on its infrastructure for global connectivity. They are

8. Scott 2015; Black 2017; Sabel, Herrigel, and Kristensen 2018; Zürn 2018, Chapter 2.

9. See Abbate (2017) and Haigh, Russell, and Dutton (2015) for discussions on the framing what is precisely meant by "the Internet" and the scope of activities entailed in those framings.

10. Solum 2008, 49.

(thus far[11]) largely regulated and governed by those multinational firms, according to their interests. In contrast, common resources critical to the function of the Internet's infrastructure—here in particular addresses and routes—are managed by globally diverse, transnational communities *in* the Internet's infrastructure. This distinction between governance "in" versus governance "on" offers a first, coarse-grained cut at the spheres of authority at play, and how their modes of governance differ.

The "Internet governance" literature has focused on the social construction of Internet protocols vis à vis law and policy in the Internet Engineering Task Force (IETF);[12] and on ICANN and the IGF as the loci of governance and policy engagement.[13] van Eeten and Mueller (2013) rightly critique this latter, highlighting a much greater diversity of issues such as privacy, censorship, intellectual property, and security, to name a few.[14] In this literature, the operations communities, in particular those managing address delegation and routing, are often grouped alongside ICANN for completeness, but their modes of rule-making, governance, and authority are not elaborated.[15] Based on engagement through interviews and fieldwork, these communities explicitly distinguish themselves from the ICANN and IGF communities, and those managing familiar activities on platforms such as Facebook.

While not as visible as ICANN and the IGF, operations communities are not hard to access. These communities pride themselves on the openness of their meetings to anyone willing to engage and learn. That said, technical and operational knowledge is a barrier to entry for fieldwork in these understudied communities, and for these communities' engagement in the global governance system. This knowledge is necessary to understand the nuance of the topics de jure, why they are important, and their implications. It is also necessary to understand why rough consensus, as a mode of credible knowledge assessment, is fit to purpose for rule-making in this dynamic sociotechnical environment. An early interview subject rightly highlighted that simply *reading* about these processes is very different from observing the diverse, critical dialogue among participants firsthand.

The empirical work supporting this article builds on archival analysis of operational (resource) policy documents, e-mail lists (live and archived), and ten years of fieldwork and interviews with over 100 actors from globally diverse operations communities. Archival analyses include textual analysis of e-mail lists, online archives of resource coordination policies (rules produced by these communities), and documentation of resource policy development processes themselves (the ways these rules are created).

11. These platforms have seen increasing scrutiny from domestic and international policy makers; their governance has also been implicated in the contention between illiberal states and the liberal international information order (Farrell and Newman 2021).

12. Braman 2010, 2011, 2013; DeNardis 2009.

13. Mueller 2002; Klein 2002; Take 2012; Raymond and DeNardis 2015; Becker 2019; Jongen and Scholte 2021.

14. van Eeten and Mueller 2013, 723.

15. There are mentions of what they do, and broader discussions of Internet governance citing the efficiency of private governance writ broadly, but little evaluation of precisely how or why.

Much of the engagement in these communities occurs in regional and global meetings. Supplementing these face-to-face meetings, operations communities use e-mail lists to discuss common issues, facilitate broader community participation, and as a (partial) archive of policy discussions. Active e-mail lists (and the corresponding archives) were starting points for understanding community dynamics, for identifying meetings for fieldwork, for identifying substantive issue domains, and for identifying participants for semi-structured interviews.

Interview subject selection criteria included:

1. longstanding *and* relatively new community participants;
2. frequent authors of operational policy proposals and frequent contributors to policy dialogues (later differentiating between frequency and quality of contribution, as in the rough consensus process itself);
3. actors in formal and informal leadership roles;
4. actors from different technical interest groups, and Internet infrastructure subindustries, and
5. actors from employers of different sizes and geographic scope.

Snowball sampling[16] further contributed to the scope and diversity of participants necessary for content validation.

Two categories of prompts were used to explore participants' experiences. The first focused on validating rough consensus as a process. The second focused on the strengths and limitations of rough consensus. In particular, these prompts focused on rough consensus as a form of credible knowledge assessment fit to the purpose of making rules in a sociotechnical environment and sustaining epistemic authority. Interviews integrated information collected from archival analysis, fieldwork, and previous interviews to cross-validate events and processes, comparing and contrasting perspectives and expert opinions on the norms, best practices, and resource policies discussed.

Process tracing[17] was used to systematically evaluate how rough consensus contributed to rule-making and sustaining epistemic authority. In particular, process tracing was used to validate the black letter of formally documented rough consensus processes relative to participants' experiences and observations of the process, and to identify differences across organizations. Fieldwork, interviews, and comparative analysis contributed to the detailed evaluation of rough consensus and understanding the epistemic community's political culture, in particular its aspirations to limit the scope and impact of its activities (these communities' sphere of authority) to operational rule making. Placing these in their historical context highlights the distinctly path dependent[18] character of how authority gradually accrued and is sustained. This process also highlighted how rough consensus contributes to self-

16. TenHouten 2017; Noy 2008.
17. George and Bennett 2005; Bennett and Checkel 2015.
18. David 2007.

reinforcing feedback.[19]

Simple, Generative, and Liberal

Writ narrowly, the Internet (as an infrastructure) has one intentionally simple, yet highly adaptive, general-purpose function: move data from here to there.[20] The simple functions described in this section—addresses to uniquely identify devices and routing data across the Internet from one device to another—are necessary for *all* Internet-based communication: checking one's e-mail, interacting with web pages and social media, streaming the latest episode of your favorite series, secure online banking . . . the list goes on and on. From an infrastructure economics perspective, the infrastructure is an essential common factor of production contributing to the diverse (downstream) "public, private, and social goods"[21] built on Internet communication technologies.

The function itself is simple; the collaboration necessary for ensuring security and stability is a complex sociotechnical process. This section describes these functions and the role of the operations community sustaining those functions. It then argues how the general-purpose (generative) character of these functions' contribute to the liberal character often attributed to the Internet, and the role of the operations community in sustaining that liberal character.

Simple Function

Jon Postel, an Internet pioneer that coordinated common resources critical to early inter-networks that would become the Internet, concisely summarized the role and function of these resources:

> A *[domain] name* indicates what we seek. An *address* indicates where it is. A *route* indicates how to get there.[22]

Domain names such as *facebook.com*, *amazon.com*, and *gmail.com* are the most visible. Domain names (in community vernacular, simply *names*) were initially created to add semantically meaningful labels to seemingly meaningless numeric addresses; governance and regulation of the domain name system (DNS), often focusing on ICANN, has been studied quite extensively.[23] Names have become integral to the

19. rixen2016historical

20. For the design principle behind this simple function (the end-to-end principle), see Saltzer, Reed, and Clark (1984) and Blumenthal and Clark (2001). For an analysis of differing interpretations, see van Schewick (2010).

21. See Frischmann (2012) for discussion of infrastructure as a common factor of production for a wide variety of public, private, and social goods.

22. Emphasis added here. Famously attributed to Postel (1981, 7), paraphrasing Shoch (1978, 1).

23. The most well known work on the domain name system (DNS) is Mueller (2002). See also X

behaviors and features users expect in platforms, but are not essential to the Internet's core function. In contrast, addresses and routes provide the information necessary for data to get from here to there; without them, there would be nothing to give a meaningful name to.

Addresses uniquely identify devices such as laptops, tablets, mobile phones, the increasingly broad array of "smart" IoT devices, and importantly, the networking equipment along the paths (routes) necessary to move data from one device's home network, through intermediary networks, and on to the destination device's network (for instance, from an academic's laptop to the server hosting an article submission platform). It would be inconvenient not to use domain names, but the data would still get there. Consider a simple analogy. The proper name of a place, such as the Museum of Modern Art (MoMA) in New York City, tells one what kind of place it is and a bit about what they will find there. Without the address and an authoritative map one can use to identify the most efficient route amongst a variety of possible paths, modes of transport, and considering neighborhoods and congestion, it would be very difficult to get from, say, one's home or office, to the MoMA. The name is convenient and useful, but the addresses and routes are essential.

Following the MoMA analogy, there are multiple routes, over multiple modes of ground transport—walking, subway, bus, personal vehicle—that one can select from. In the Internet, there are also many routes to choose from, some more desirable than others.[24] With the exception of frustrating construction on the ground, the map of New York City (and that of physical, resource intensive infrastructures in general) is relatively static. In contrast, the map of the Internet, i.e. the collection of all possible routes, is constantly changing, dynamically, on a near continuous basis. Routes change for various reasons: changes in contractual relationships between networks, outages,topological changes (new physical infrastructure, such as fiber optic cables in the ground or submarine cables), to improve performance, or for economic and national security[25] reasons. Coordinating across one hundred thousand plus networks[26] creates endemic, unavoidable uncertainties, requiring human intervention and rules to maintain consistent function, a form of operational order.

Adding to this complexity is that, on the technical side, this map is drawn and maintained using a protocol colloquially referred to as "routing by rumor."[27] Networks

24. Of the many routes available, some are longer (take more time), some are less stable (data is lost, meaning it has to be resent, potentially affecting the performance of applications like video streaming), and for security purposes, it is often considered undesirable to route traffic through jurisdictions known to monitor Internet traffic.

25. For instanced, routing to avoid jurisdictions known to monitor Internet traffic, or to ensure local, sensitive traffic stays local.

26. Calculated based on the number of autonomous systems in the Internet, as reported by the Number Resource Organization (2022).

27. The protocol for distributing routing information, the Border Gateway Protocol (BGP) (Rekhter (Ed.), Li (Ed.), and Hares (Ed.) 2006), is a distance vector algorithm referred to colloquially in the community as "routing by rumor." Among the operational epistemic communities discussed here, this colloquialism is

"advertise" to their neighbors the addresses in their networks, and the information about the routes *through* their networks they are willing to make available to get to other networks. Those neighbors incorporate that routing information into what they know from *their* neighbors, update their own advertisements, and advertise onwards. In effect, the map of the Internet is updated based on the continuous chatter between networks about what routes are available, which have changed, and which have been rescinded. Like all chatter and rumors, it is best to confirm what one hears from an authoritative source, but that is a transaction cost for networks, just as it is for individuals. "Routing by rumor," was initially developed when routing chatter was exchanged in a community of a few hundred known, trusted peers. It is still effective today, but to ensure consistent, stable routes, in addition to the flexibility baked into Internet protocols, operations communities also developed norms, best practices, and resource policies to mitigate and remediate negative network externalities when rumors turn out to be false.

A well known adage illustrating the operational order in addressing and routing is that "the Internet interprets censorship as damage and routes around it."[28] The incident between Pakistan and YouTube in 2008, over blocking a video offensive to the Prophet Mohammad (illegal in Pakistan), illustrates the implications of routing by rumor and how these actors resolve network externalities. When YouTube refused Pakistan's request to take down the video, Pakistan attempted to manipulate *local* routes to redirect Pakistani traffic intended for YouTube to a local destination, managed by the Pakistan Telecommunication Authority (PTA), that indicated YouTube was hosting illegal content. When Pakistan implemented their intervention, not only were local YouTube users in Pakistan redirected to the PTA's website, but users *around the world* were redirected. From the perspective of the operations communities, Pakistan had "hijacked" YouTube's addresses, violating routing norms and contractually binding address policy, resulting in damage to the integrity of the Internet's routing system. Operators around the world identified the "damage", shared what they knew about the "illegitimate" route advertisements within the community (across firm and jurisdictional boundaries), and began correcting their own routing advertisements to ensure traffic intended for YouTube's addresses did in fact get directed to YouTube's servers. This global network externality between Pakistan, YouTube, and the transnational network of Internet operators played out, and was resolved, in approximately three hours.[29]

The Pakistan-YouTube incident illustrates more than just technical mechanics. First, it illustrates one of the operations community's core images of *order*: accurate

frequently used in explaining the nuance of BGP. More recently, it is also used to explain some vulnerabilities, calling for more secure (cryptographically signed) announcements of routing information akin to officially signed letters than rumors.

28. John Gilmore, quoted by Elmer-DeWitt and Jackson (1993).

29. The RIPE NCC produced an excellent video (now on YouTube) (RIPE NCC 2008) illustrating precisely how this happened.

distribution of routing information. Second, it illustrates the *capabilities and capacities* of the operations community to correct damage and maintain their image of operational order. Third, it illustrates the *willingness* to use these capabilities and capacities to maintain its image of operational order. Finally, it demonstrates one end of the spectrum of operational epistemic authority developed here: diffuse authority, applied by a "close-knit yet loosely organized" community when its norms were violated. These characteristics of the operations community are not only important for maintaining operational order, but enforcing these norms is also one of the ways the liberal character of the Internet's infrastructure is maintained.

Generative and Liberal

These core functions and the associated rules are also important for understanding the liberal character of the Internet, frequently attributed to the open, free flow of information.[30] Zittrain offers the notion of generativity as "a function of a technology's capacity for leverage across a range of tasks, adaptability to a range of different tasks, ease of mastery, and accessibility."[31] The generative character of the Internet rests on *(1)* the programmable personal computer (PC) and, important here, *(2)* the Internet's simple, general purpose communications protocol (the Internet Protocol, IP). Used in conjunction with one another, these complementary technologies not only drastically lowered the barriers to transnational engagement, but also lowered the barriers for developing tools and platforms that cultivate and sustain transnational polities.[32] In *Inventing the Internet,* Abbate highlights that when the early ARPANet was primarily used for sharing access to geographically distributed computing resources and data among researchers, it was under utilized. Utilization increased substantively with the use of e-mail, highlighting the Internet's potential for catalyzing human collaboration.[33]

The generative character of the Internet opened the door to developing the diversity of interactive platforms that make up today's Internet. This same generative potential also facilitates many of the malicious activities, such as spyware and ransomware. In this sense, it is liberal, to an extreme. Absent significant regulatory order *on* the Internet, it is arguably liberal to a fault. Any set of actors, regardless of their normative intent, liberal or illiberal, can collaborate to create innovative online tools and platforms, for licit or illicit purposes. Consider two contemporary instances. Social media platforms range from mainstream platforms such as Facebook to "alternative" platforms such as Parler. As another instance, platforms have been developed to facilitate engagement in legitimate electoral processes, and malicious actors have developed platforms commoditizing disinformation campaigns intended to distort

30. Farrell and Newman 2021.
31. Zittrain 2006, 1981.
32. Nye and Keohane 1971.
33. Abbate 2000, 105-112.

democratic processes.

Although the epistemic authorities maintaining the Internet's infrastructure do not use the term generativity, maintaining the (liberal) general purpose character of Internet communication, and the innovation attributed to this design,[34] has become, in and of itself, a normative ideal. Particularistic governance issues (such as what constitutes abusive messaging, or what constitutes disinformation on a given platform or in a given jurisdiction) are considered the domain of public authorities and/or the managers of platforms built on the Internet. This latter distinction highlights two coarse-grained spheres of authority in the global governance of Internet-related activities: those ensuring the general-purpose character of simple communication *in* the Internet's infrastructure and those regulating the particularistic behaviors that play out *on* the Internet. As illustrated by the two contemporary instances above, these latter intersect directly with conventional domestic and transnational policy and security issues.

This distinction is also critical for understanding the scope of private Internet governance often cited in the literature. Consider Farrell and Newman's argument that attributes self-undermining contestation in the liberal international information order (LIIO) to openness and private-actor governance, citing activities motivated by "data-driven advertising" and "[n]ew media ecosystems, driven by the imperative to maximize 'engagement,' [that] favor[] controversial fringe material while offering opportunities for political entrepreneurs to exploit and widen fissures in political knowledge."[35] The argument certainly holds, but it is important to note that, in this case, self-undermining contestation, as characterized above, is a consequence of private governance of platforms developed by individual multinational firms managing social media platforms *on* the Internet, that, relative to the general-purpose character of the Internet's infrastructure, have rather particularistic goals and values shaped by the objectives of the firm (such as Meta) or the politics of a particular group (such as Parler). In contrast, distinctly pluralistic, transnational epistemic authorities *in* the Internet focus on sustaining its simple communication function, and the general-purpose (generative) character of that function. First, embedding particularistic values would limit the general-purpose function, foreclosing on a number of real and potential downstream uses.[36] Second, interviews indicate that it is not in these actors political or economic interest to limit the general-purpose character or (unnecessarily) interfere with transnational issues playing out atop the Internet *unless* those actions interfere with the integrity of the infrastructure itself (viz. Pakistan-YouTube). Rather, those issues fall more appropriately within the spheres of authority of domestic and international policy makers and regulators.

The operational epistemic authority illustrated in the Pakistan-YouTube case is

34. See van Schewick for one of the most complete analyses of innovation and the Internet's architecture.

35. Farrell and Newman 2021, 341.

36. It also runs against the fundamental design principles in the end-to-end principle (Saltzer, Reed, and Clark 1984; van Schewick 2010).

interesting because it is not delegated in the sense of Zürn's politically assigned epistemic authorities.[37] Rather, epistemic authority accrued to these communities as they grew and matured, alongside the Internet itself, in an emerging age of postnational liberalism.[38] This epistemic authority was not actively cultivated as political authority, either. Adhering to the extreme liberal character resulting from normative focus on preserving the general-purpose (generative) character of communication *in* the infrastructure means the community is extremely reluctant to hew to political objectives. Some of these kinds of actions, that do have consequences for conventional political activities and align with normative notions of liberalism[39], are often celebrated by civil society and activist organizations. These latter have imbued the Internet with these ideals, but, as a diffuse form of operational epistemic authority, they were not directed by any particular state or conventional liberal international organization. For the operations community, this was a normative imperative to restore the integrity of the (routing) system as a common good critical to the integrity of Internet communication and their value propositions.

The operational epistemic authorities discussed here vary in the formality of rule making and institutional structure. At one end of the spectrum are the routing communities, an instance of "close-knit yet loosely organized" (diffuse) operational epistemic authorities. At the other end of the spectrum is the addressing communities, an instance of structured operational epistemic authorities, which have developed formal institutional constructs comprising non-profits coordinating address delegations and transfers, documenting the rules ordering those resource management activities, and facilitating rule-making processes. The next section first contextualizes this distinctly operational mode of epistemic authority in the global governance literature, then traces how this authority emerged from the early organization and development of the Internet as an experiment through its modernization and development of resource management institutions in the late 1990s.

Operational Epistemic Authorities *in* the Internet

Epistemic communities are increasingly critical to the management of complex global infrastructures, here in particular the Internet. Private authorities are characterized as more efficient than their public counterparts,[40] but also less transparent[41] and face potential legitimacy issues.[42] In contrast to the closed private authorities evaluated by Büthe and Mattli (2011), these communities are adamantly open, actively encouraging new participants willing to learn. Like those authorities evaluated by Büthe and

37. Zürn 2018, 51-52.
38. Börzel and Zürn 2021.
39. See Lake, Martin, and Risse (2021, 229-232) for a recent typology of the kinds of liberalism.
40. Cutler, Haufler, and Porter 1999; Hall and Biersteker 2003.
41. Mattli and Büthe 2003; Büthe and Mattli 2011.
42. Underhill and Zhang 2008; Zürn 2018.

Mattli (2011), technical knowledge and vernacular used in those communities is a high barrier to entry.

This section first defines diffuse and structured operational epistemic authorities relative to the literature, then evaluates how operations communities transitioned from research and development contractors in a small experimental Internet into transnational authorities managing resources critical to a global infrastructure. The historical context is critical to distinguishing between authority that has been politically delegated (and as such, can be rescinded) and authority accrued by these communities, intrinsic in their capabilities and capacities, and that is sustained by their ongoing operational practices and rule-making through rough consensus.

Sources of Epistemic Authority

As an epistemic community, operations communities "share[] . . . normative and principled beliefs" regarding the integrity of Internet communication, have refined their notion of rough consensus as a means of "shar[ing] causal beliefs" based on experience managing the system, use constructive conflict within the rough consensus process as a "shared [image] of validity," and have the general-purpose operational integrity of the Internet as both "a common policy enterprise" and a bound on the scope of that policy enterprise (infrastructure management, minimal interference with public policy and authority).[43] Typically framed as offering expert advice, epistemic communities help domestic and international policy makers navigate complex domains or issue areas, potentially influencing broader international politics as they become more embedded in the policy process.[44] Under this framing, epistemic communities are sources knowledge salient to policy makers, but not necessarily managers of resources in the domain or issue-area.[45] In contrast, operations communities base their knowledge on direct experience coordinating a complex, global Internet infrastructure. Their knowledge base is more akin to the teleological experimental methods that characterized early engineering science than methods attributed to more traditional scientific communities.[46]

Zürn's characterization of epistemic authorities focuses on the role of these communities' "expert knowledge and impartiality,"[47] highlighting the idea of "pure epistemic authorities . . . [e]specially transnational civil society organizations."[48]

43. Quoted text from Haas's definition of epistemic communities (1992, 3).
44. Haas 1992, 4.
45. Haas 1992.
46. This follows Haas (1992, 3, footnote 4). In terms of their operational knowledge of the address and routing system as a commonly managed resource, their knowledge base is developed similar to Ostrom's common pool resource managers (1990, p). In terms of the way they perform experiments, their (resource) policy experiments are akin to those described by Moss (2004). For the teleological methods of improving performance used by early engineering scientists, see Layton (1979).
47. Zürn 2018, 51.
48. 52.

Communities become what Zürn refers to as politically assigned epistemic authorities (PAEAs) when "assigned that status by other authorities,"[49] typically by political authorities. In this framing, "they do not make binding decisions, but [are delegated] competences to make often very consequential interpretations."[50] Here, demand for these epistemic communities' knowledge led to explicit delegations of authority that can also be rescinded based on politics or performance.

Rather than being placed "in" authority by an existing political authority, the role of operations communities as "an" authority accrued over time, as a consequence of their role and experience developing, deploying, and maintaining a functioning, increasingly complex, global infrastructure. Here, "in" authority and "an" authority are used in the sense developed by Flathman (1980, 16-19).[51] To be "in" authority is by virtue of holding an office; it is delegated and can be rescinded. To be "an" authority is "based on, is possessed by virtue of, demonstrated knowledge, skill, or expertise concerning a subject matter or activity."[52] Operations communities' collective knowledge, capabilities, and capacities developed first in regional networks that made up the early Internet (for instance, in the United States and Canada, in Western Europe, and in developed economies in the Asia Pacific). These regional communities integrated into a global community[53] as transnational demand for improved performance and capacity led to a more dense mesh of network relationships.[54] In the 1990's, the increased importance of Internet communication led to explicit demand for institutions[55] and organizations for maintaining operational order, here in particular the regional Internet registry system as an instance of structured operational epistemic authority.

The two forms of operational epistemic authorities developed here, diffuse and structured, are two ends of a larger spectrum of epistemic authorities managing technologies and operations in the Internet's infrastructure. *Diffuse operational epistemic authorities (DOEAs)* are informally organized institutions whose participants are "close-knit, yet loosely organized"[56] There is no single, authoritative source of norms and best practices; knowledge is generated largely through experience. In the routing community, knowledge is shared among peers in fora such as network operator groups (NOGs, discussed later in this section), RIR meetings, among others. Their shared causal belief and shared image of validity follows the spirit of rough consensus:

49. 51.
50. 52.
51. Sea also Lake's notion of relational authority (2009).
52. Flathman 1980, 16.
53. Operations communities are surprisingly granular. In countries such as the US, regional operator groups are quite active. Globally, there are typically operator groups corresponding to most economies with significant Internet presence.
54. In this case, greater capacity means greater bandwidth and interconnection relationships that reduced inefficiencies as more traffic flowed over a denser mesh of connections between countries. This latter density means more efficient paths, not necessarily more direct bilateral connections.
55. Mattli and Woods 2009.
56. In the sense of Ellickson (1991).

it must be based on pragmatic experience and demonstrated (performed) expertise.

Structured operational epistemic authorities (SOEAs) are rooted in formal organizations that manage or coordinate resources critical to system function and serve as the loci of rule-making (here, organizations that facilitate rough consensus). Like DOEAs, the validity of rule-making requires credible contributions by participants the community recognizes "an" authority. The organizations in SOEAs provide the fora in which these rules are made; manage resources based on the rules developed by the community; and manage the authoritative repository of the documentation of rule-making proceedings and the resulting rules themselves. SOEA organizations also play an important role ensuring the integrity of "an" authority-based rule-making procedures. It is in this process validation role that SOEA organizations are instances of those "in" authority, but those actors must be "an" authority to effectively fulfill these roles.

Accruing Epistemic Authority: From Research Contracts to Institutions

The initial Internet experiment was funded by the United States' Department of Defense's (DoD) Advanced Research Projects Agency (ARPA) and coordinated by the Information Processing Techniques Office (IPTO). The DoD contracted academics and industry actors for research and development of a decentralized, heterogeneous network-of-networks more resilient than the centralized architecture of the telephone system.

> We wanted to have a common protocol and a common address space so that you couldn't tell, to first order, that you were actually talking through all these different kinds of nets. That was the principal target of the Internet protocols.[57]

Abbate highlights that the DoD was largely a coordinator, leaving much of the development and decision making to those doing the work.[58]

> IPTO managers preferred to take the informal approach whenever possible. Having been researchers themselves, they subscribed to the view that the best way to get results in basic research was to find talented people and give them room to work as they saw fit. *They also tended to believe that differences of opinion could be debated rationally by the parties involved and decided on their technical merits, and that they, as IPTO managers, would need to intervene with an executive decision only if the contractors could not resolve differences among themselves.*[59]

57. Vint Cerf, one of the fathers of the Internet and directly involved in its early development, quoted by Abbate (2000, 128).
58. Abbate 2000, 54-60.
59. 55, emphasis added.

These function- and operations-specific groups evolved into the working group structure of the IETF, the organization that currently manages develops core Internet standards and protocols.

As the Internet grew from a distributed lab experiment hosted largely at academic institutions, into an experimental government network, and on into the modern commercial Internet in the mid-1990s, the IETF emerged as the organization coordinating and documenting the development of Internet protocols.[60] In the course of these transitions, the IETF formalized its protocol standards development processes,[61] developing a variant of consensus-based decision-making common to technical standards development processes.[62] At this time, the epistemic communities convening at the IETF performed many of the functions necessary for Internet development and operations: managing and contracting physical infrastructure; development and implementation of communications protocols; developing naming, addressing, and routing standards and related protocols; delegation of corresponding resources as needed; and development of protocols underpinning common applications such as e-mail (along with a plethora of attendant security standards). Norms encouraging experimentation with implementations, and how rules and best practices were made, were not only encouraged, but necessary. These norms carried through from the relationship between early management and contractors, later under the coordination of the National Science Foundation (NSF), and ultimately into the private operations communities that took up stewardship of operations related to names, addresses, and routing, as the IETF increasingly focused on standards and protocols. Hearkening to their origins in the IETF, the operations communities, here in particular addressing and routing focused, on epistemic quality, through norms that encouraged operations and policy experiments.

As the importance of Internet communication became more broadly understood, other standards for creating "Internets" came into competition with IETF standards. Competition with another standards process gave rise to the mantra of "rough consensus and running code" that has come to characterize the ethos, and the mode of authority, in the IETF and operations communities. In 1977, the International Standards Organization (ISO) began developing an the Open Systems Interconnection (OSI) model, "to set the ground rules for network interconnection,"[63] an alternative to the IETF's TCP/IP (Transmission Control Protocol/Internet Protocol). Russell documents the standards culture war that ensued, highlighting a key point of contention: the distinct differences in the organizational structure and perceptions of authority in the IETF and ISO. According to Russell, ISO's organizational culture "resembled contemporary democratic bodies insofar as it featured voting, partisan compromises,

60. For detailed histories, see Abbate (2000) and Hafner and Lyon (1999).
61. Resnick 2014.
62. See Yates and Murphy (2019), in particular Chapter 7.
63. Russell 2006, 52.

and rule-making behavior designed to protect financial interests."[64] Russell goes on to describe that early Internet pioneers' (participants in the IETF) distaste

> stemmed from their frustration with the technical aspects of OSI as well as with ISO as a bureaucratic entity. Where TCP/IP was developed through continual experimentation in a fluid organizational setting, Internet engineers viewed OSI committees as overly bureaucratic and out of touch with existing networks and computers.[65]

In 1992, the IETF's leadership, the Internet Architecture Board (IAB), developed a draft proposal to replace IP addresses with an addressing model from the OSI model. IETF participants rebelled against the idea that the IAB was acting "in" authority, requiring the IAB to "relent . . . in the face of a massive 'palace revolt'."[66] The IAB did relent, and in doing so clarified the ethos of standards development in the IETF, and its way of evaluating knowledge and resource policies in the emerging operational epistemic authorities.

In a presentation responding to this revolt, Dave Clark presented a clear and distinct articulation of this ethos, now part of the IETF's mission statement.[67]

> We reject: kings, presidents, and voting. We believe in: rough consensus and running code.[68]

It is important to be clear that this is not intended as a rejection of government authority writ broadly, but a statement about the kind of authority that characterizes the IETF. It is a reaffirmation that, within this community, there is no set of actors "in" authority that can override the epistemic consensus of the community, arrived at by credible "an" authorities. Flathman indicates "[t]hose who have such authority [(an authority)] issue statements or propositions about the subject matter, or *perform the activity in question*—statements and *performances* that allegedly have such qualities as truth, *correctness, validity*, profundity, exceptional grace or beauty, and so forth."[69] For the IETF, "running code" is that performance, rooted in correctness and validity that has been evaluated through rough consensus among "an" authorities. Documentation of these processes and in IETF RFCs are the means by which these evaluations become authoritative.

Moreover, it highlights that majoritarian voting, and the politics and vote trading that come along with this model of decision-making,[70] are inappropriate for developing protocols, standards, and operational policies that require high levels of collaboration,

64. Russell 2006, 53.
65. 53.
66. 55.
67. Alvestrand 2004, 2.
68. Clark 1992, Slide 19.
69. Flathman 1980, 16, emphasis added here.
70. Lijphart 1999.

among actors considered "an" authorities. In the absence of a central governing body, for these be authoritative, they require rigorous knowledge assessment to be considered both credible and actionable (they will yield stable, running code) and rough (but not necessarily complete) consensus. This teleological perspective is also embedded in the modern operations communities' "rough consensus" processes[71]: developing norms, best practices, standards, and policies on an experimental, best effort basis, by an epistemic community that prefers developing rules based on operational experience, and evaluating outcomes (experiments, running code that yields functional, stable systems). The debates within these communities are rigorous and contentious, requiring deep knowledge of the topic at hand. If a participant cannot justify the rationale for contesting a solution in terms of empirical evidence, in reference to existing community knowledge of the system, and/or existing best practices, their contestations are dismissed. If a participant makes a regular habit of making these kinds of contestations, their status as "an" authority diminishes. Former prestige as "an" authority and former accomplishments does foster some tolerance, but if these actors engage in invalid or incredible contestations, those contestations will be dismissed as well.

Early in the development of these communities, a common objective was Internet stability; today, it is coordinating rule-making and maintaining system integrity. With the approach of the NSF's divestiture of Internet management to the private sector in the 1990s (made official in 1998), demand emerged for new *operational* coordination institutions. Two functionally related, but organizationally different, groups of operational institutions emerged to fill these gaps. The global set of network operator groups (NOGs) emerged as convening fora for the routing community, an instance of diffuse operational epistemic authority. The regional Internet registry (RIR) system emerged as a structured operational epistemic authority managing the delegation of (IP) addresses.

Diffuse Operational Epistemic Authority: Routing and Network Operator Groups

In the mid-1990s the routing community developed network operator groups (NOGs) as fora in which actors could discuss operational issues critical to ensuring global connectivity, i.e. ensuring an increasingly global network-of-networks remained glued together in a secure and stable way. Although operations communities, here in particular the routing and address communities have substantive overlap in participants,

71. This *kind* of consensus has been in play in scientific and technical standards making since at least 1880 (Yates and Murphy 2019, 4, Chapter 1). *Rough* consensus was coined in a presentation at the IETF by David Clark (Clark 1992) (currently a Research Scientist at MIT's Computer Science and Artificial Intelligence Lab (CSAIL), and formerly Chief Protocol Architect and chair of the Internet Activities Board from 1981-1989). Russell (2006) offers a historical analysis of this term in the context of the Internet-ISO Standards War.

within these, actors make clear conceptual distinctions between the roles in, and knowledge created in those roles, in each function-specific community. In their role coordinating routing and interconnection, actors refer to themselves as the routing community, differentiating from roles in other function-specific communities such as those managing names (the DNS or naming community) or addresses (the numbers[72] or addressing community).

One of the first of these communities, the North American Network Operator Group (NANOG) was created expressly for the purpose of filling the coordination gap left by the NSF: to facilitate sharing operational interconnection information necessary to sustain global connectivity during and after the transition of coordination by the NSF to the private sector. Today, there are more than fifty network operator groups[73] around the world.[74] These range from global communities such as NANOG; to regional groups, such as LACNOG (Latin America and Caribbean), AFNOG (Africa), and MENOG (Middle East); to economy specific NOGs such as JANOG (Japan), ghNOG (the Ghambia), ArNOG (Argentina), and DENOG (Germany).

NOGs serve three primary knowledge sharing and coordination functions: sharing information and best practices about interconnection operations; supporting engagement among actors coordinating interconnection and routing between networks; and developing the relationships necessary to quickly and efficaciously mitigate and remediate network externalities. For instance, NANOG's mission highlights that it facilitates discussion among experts on topics such as "experiences with new protocols and backbone technologies, implications of routing policies on the Internet as a whole, measurement techniques and measurements of Internet health and performance, areas in which inter-provider cooperation can be mutually beneficial (such as NOC [network operations center] coordination or security incident response), and maintaining a competitive and level business environment."[75] Their bylaws go on to indicate that all presentations and tutorials are "reviewed in advance and are limited to those entirely of a general technical nature, *explicitly prohibiting material that relates to any specific product or service offerings*."[76] Within these fora, commercial presentations, i.e. marketing, is often banned, or strongly discouraged. Program review committees enforce these norms. When presenters deviate from these norms, the audience is not shy about sustaining epistemic quality, calling out the presenters (and the NOG). NOGs are convening fora for the routing community as a DOEA and many provide archives

72. As a resource, addresses are important, but conceptually quite simple. The address community often refer to them as simply "numbers". The primary address range in use, IPv4 addresses, range from 1 to $2^{32} - 1$. In their simplest form, they are a range of integers, numbers, for used for uniquely identifying devices. The function is simple; management of delegations to networks is where the cooperation and coordination problems become more complex.

73. Typically referred to NOGs; some are referred to as network operator forums, such as UKNOF in the United Kingdom.

74. Greene 2021.

75. NANOG 2020.

76. NANOG 2020, emphasis added here.

of presentations, some of which describe best practices. That said, NOGs do not present themselves as coordinated, authoritative sources or archives of authoritative, formally agreed upon norms and best practices.

The second primary function of the NOGs is to serve as meeting places for expert network representatives[77] to engage in negotiating, establishing, and maintaining interconnection relationships between networks.[78] These contractual relationships determine which routes are shared, and with whom. These relationships range from those focused on moving traffic from one network to another to those in which a provider guarantees its clients connectivity to the global Internet.[79] The continuous process of redrawing the "map" of the Internet is a combination of these contractual dynamics and "routing by rumor."

A consequence of this construct is that, even for the largest global networks, no single firm has a complete map of the Internet. The third function of function of the NOGs is sustaining the relationships within the routing community. *Maintaining* the integrity of the routing system requires substantive coordination and cooperation across network, firm, and international boundaries, often based on community relationships established and sustained at NOGs. Identifying, mitigating, and remediating operational failures and intentional shutdowns,[80] such as the Pakistan-YouTube incident, requires this cooperation. Networks regularly monitor their connectivity and can *identify* outages on their own. *Restoring* connectivity, though, requires coordination, often with multiple parties, to identify the source of the externality and who is necessary to restore normal operations.

Structured Operational Epistemic Authority: Regional Internet Registries (RIRs)

A key component of routing is distributing the information necessary to get traffic from one location to another, i.e. making sure everyone has the pieces of the map necessary to move data closer to its destination. For such a global network to function properly, for traffic to consistently get from an origin (such as a website) to a destination (a user's laptop browsing that website), the addresses of those origins, the intermediate stops along the way, and the final destination, must be globally unique. The primary function of the RIR system is to maintain accurate, up-to-date, globally accessible registries of the address information necessary for this consistency. Each

77. Based on interviews and fieldwork, across the NOG community, sending marketing representatives is strongly discouraged by the community. They still show up, but if they cannot keep up with the technical vernacular and discussions, or prove to be disruptive, they are generally ignored, and on occasion, shunned.

78. For detail on the contracting relationships see Clark, Lehr, and Bauer (2011) and Faratin et al. 2008.

79. Faratin et al. 2008.

80. See AccessNow's recent shutdown reports (Berhan 2020)taye2021shattered for analyses of recent shutdowns around the glob.

RIR maintains the authoritative information about which firms[81] have been delegated which addresses and network identifiers.[82] When Pakistan "hijacked" YouTube, it broke this global uniqueness rule,[83] violating resource policies established by the RIR system. Pakistan's (illegitimate, from the perspective of the RIR system) advertisement effectively claimed that it held the addresses that had been delegated to YouTube and corresponded to its services. Pakistan introduced conflicting information (a false rumor) into the routing system, (temporarily) creating an inconsistent map of the Internet.

The role of the RIR system is largely administrative, but critical to rule-making in the Internet. The RIRs also provide the fora in which the fundamental political questions of who gets what (addresses and network identifiers), and how, play out. They provide the fora in which the operational order (related to address resources) is discussed, negotiated, established, and maintained. The RIR system *coordinates* the bottom-up consensus processes for developing resource policy, the rules that determine how number resources are delegated, to whom, and under what conditions. The RIR (as a nonprofit firm) itself does not determine the substance of rules, but rather, it facilitates the consensus among operators in the address community that serve as both rule makers and rule takers, and maintains the authoritative records of these proceedings.

The five modern RIRs, listed in the order they were established, are:[84]

- Réseaux IP Européens Network Coordination Centre (RIPE NCC), established in 1992, located in The Netherlands, coordinating number resources for Europe, the Middle East, and Russia
- Asia-Pacific Network Coordination Centre (APNIC), established in 1993, located in Australia, coordinating number resources for the Asia Pacific region
- American Registry for Internet Numbers (ARIN), established in 1997, located in the United States, coordinating number resources for the United States, Canada, and some Caribbean and North Atlantic islands
- Latin American and Caribbean Internet Addresses Registry (LACNIC), established in 2002, located in Uruguay, coordinating number resources for Latin America and some Caribbean islands
- African Network Coordination Centre (AFRINIC), established in 2005, located in Mauritius, coordinating number resources for Africa

81. Typically firms, but number resources have been delegated to individuals in the past. Most of these delegations are artifacts of the early, experimental Internet. Delegation to private individuals, especially during the period in which IPv4 addresses were becoming increasingly scarce, has been much less common in the modern Internet.

82. These networks are numbers that uniquely identify a network as a whole. More technically, those identifiers, referred to as autonomous system numbers (ASNs) uniquely identify networks with a common routing policy, typically one per network (firm), but there are exceptions.

83. More technically, it illegitimately appropriated resource rights exclusively delegated to YouTube by the RIR system.

84. NRO 2021.

The RIRs coordinate through the Number Resource Organization (NRO), an organization jointly funded by the RIRs to help coordinate and support joint activities of the RIRs and to be an authoritative voice for the RIR system in broader Internet governance fora.[85]

In contrast to the diffuse structure and operational epistemic authority of the routing community and the NOGs, the criteria for establishing an Internet registry[86] and the constitutional norms of the RIRs[87] are formally (and authoritatively) established in IETF RFCs. The criteria for establishing a regional Internet registry highlight the foundations of bottom-up governance and endogenous legitimacy: networking authorities (i.e. experts, not necessarily government actors) in the region must legitimize the organization and that "the organization will commit appropriate resources to provide stable, timely, and reliable service to the geographic region."[88] The constitutional norms of the RIRs (below, from RFC2050) provide insight into the function of the RIR, its commitment to fair and responsible delegation of resources, and, most importantly, the commitment to bottom-up (rough) consensus processes.

Conservation: Fair distribution of globally unique Internet address space according to the operational needs of the end-users and Internet Service Providers operating networks using this address space. Prevention of stockpiling in order to maximize the lifetime of the Internet address space.

Routability: Distribution of globally unique Internet addresses in a hierarchical manner, permitting the routing scalability of the addresses. This scalability is necessary to ensure proper operation of Internet routing, although it must be stressed that routability is in no way guaranteed with the allocation or assignment of IPv4 addresses.

Registration: Provision of a public registry documenting address space allocation and assignment. This is necessary to ensure uniqueness and to provide information for Internet trouble shooting at all levels.[89]

In 2013, RFC7020 updated these constitutional norms to reflect modern number resources dynamics, in particular the impending depletion of the global pool of IPv4 addresses. Given the increasing scarcity of addresses, *conservation* was updated to *allocation pool management*, reaffirming that fairness means delegating resources to actors that can demonstrate operational need, not the highest bidder. *Routability* was updated to *hierarchical allocation* to limit unnecessary redundancy. *Registration* was updated to *registration accuracy*. The global pool of IPv4 addresses reached depletion on 3 February 2011, leaving only those remaining in regional pools for delegation. The means of acquiring IPv4 addresses began to shift from delegation from diminishing regional pools managed by the RIRs to transfers between firms.

85. NRO 2020.
86. Cerf 1990; Gerich 1993.
87. Hubbard et al. 1996; Housley et al. 2013.
88. Gerich 1993, 1-2.
89. Hubbard et al. 1996.

Transfer policies have been some of the most contentious sets of policies developed in the RIR system. RIR policy requires transfers be mediated and approved by the RIR(s) that originally delegated those resources (and maintain registry data about those resources) to ensure registry accuracy necessary for network operations and the kinds of partial attribution necessary for security incident response.

The RIRs' constitutional norms were produced in the IETF RFC series as the authoritative documentation of standards, best practices, and procedures for the Internet. In keeping with the development of norms and procedures based on operational expertise, the authors of these documents are known experts on the RIR system, and were made authoritative through the IETF's consensus process. RFC2050 was the product of operational expertise early in the history of the modern Internet, laying the foundations of the RIR system. RFC7020 is an update of those constitutional norms to reflect new understandings of the dynamics of number resource management, especially in the face of IPv4 depletion, debates over precisely how transfers markets should function, and the increasing need for security protocols that could reinforce resource rights (reducing the potential for hijackings such as illustrated in the Pakistan-YouTube incident).

Both RFC2050 and RFC7020 highlight that:

> These goals may sometimes conflict with each other or with the interests of individual end users, Internet service providers, or other number resource consumers. *Careful analysis, judgment, and cooperation among registry system providers and consumers at all levels via community-developed policies are necessary to find appropriate compromises to facilitate Internet operations.*

Bottom-up consensus processes, derived from the IETF's rough consensus process, are the means by which the operational epistemic community develops resource delegation policy, evaluates the trade-offs when these norms conflict, and adapts policy to address those trade-offs and the needs of modern operational issues related to the delegation and use of numbers.

Sustaining Authority via Rough Consensus

Rough consensus not only serves to shape the rules at play, but also serves as a means to sustain and update knowledge of how the systems works within and across the operational epistemic communities that manage the Internet. It is the mechanism by which participants, as "an" authorities, debate and establish resource policies as "the authoritative." Embedded in this process is a shared way of knowing, through shared operational experiences, and debates over the validity and implications of those experiences as applied to resource policy development. The rough consensus process itself, as a mechanism for constructive conflict, represents a shared notion of validity, especially in the active consensus process described below. Are assertions contributing to the development of a particular policy from "an" authority, and based

on operational experience? Do assertions align with or update existing knowledge of Internet operations and functions?

There are three categories of actors involved in the RIRs resource policy development process. RIR staff coordinate and document the consensus process. Members of the routing community contribute to the evaluation of policy proposals and are the authors of proposals. Policy shepherds (members of the routing community that are also members of a given RIR), are experienced community members formally tasked with evaluating the appropriateness of the scope of policy proposals and providing guidance for authors through the policy. The following elaborates the model of the RIRs' "bottom-up" rough consensus process.[90]

Problem Identification

In the problem identification and evaluation phase, participants and policy shepherds determine

1. whether a problem exists and it is affecting a significant number of constituents (i.e., it is not particularistic to a group or technology) and
2. whether the problem is within the scope of the RIRs' remit.

These two criteria contribute to ensuring activities are part of the RIRs' common policy enterprise (resource policy) and do not fall outside the RIRs' sphere of authority. In the RIRs, problem identification occurs in a number of places: in "hallway conversations" where an individual feels out whether others in their professional network are experiencing similar issues; in general discussion on e-mail lists; and in formal presentations of current issues being faced in the day-to-day operation of the Internet. In each of these cases, an individual (or individuals) are sharing their experience with others, especially more experienced participants, to determine whether the issue warrants a proposal. It is common for an operator's presentation of their experience, originally intended to be informative, to be turned into a proposal to update resource policy.

The second part of problem identification is determining whether the problem is clearly stated and within the scope of the RIR's resource policy making remit. Formally, determining scope takes place shortly after a policy proposal is submitted. The proposal must present a problem relevant to address resource delegation (conservation, routability, and registration), the mechanics of registry function, or a correction to existing policy to improve clarity or remove ambiguities. The proposal must be tractable for the RIR to implement, without overstepping the bounds of the RIR's remit or authority. Prospective policy proposals are made publicly available, typically on the policy mailing list for that RIR. If the proposal is rejected, it is presented as such

90. The RIRs' process was adapted from the IETF's rough consensus process. Some of the mechanics differ, but the implications for authority are the same. Of the variants of consensus processes observed in the broader set of operational epistemic authorities in the Internet's infrastructure, the RIRs process is most similar to that of the IETF.

with a justification. If it is accepted for evaluation by the community, it is announced as an active proposal and the process moves into the *active census* phase.

Active Consensus

In the active phase, participants debate the content of a given proposal until rough consensus is reached. Achieving active consensus means that participants have iteratively reviewed the proposal, considered valid proposed changes (either enhancements or contestations), and the discussion has reached a point where there are no further proposed changes. In terms of the content of the proposal, the solution must fit within the established objectives of the RIR. Efficacy and efficiency, in terms of the proposal's operational, technical, and economic implications, are the criteria by which proposals are evaluated. Debates consider the tractability and implications of the solution for RIR members (in their role as rule takers) and in terms of implementation by the RIR itself (in its role as rule implementer, monitor, and potential enforcer). During the active consensus phase, the RIR typically produces an impact analysis, providing evaluators with information about what would be necessary for the RIR to implement the proposal, such as changes to the registry, operational requirements, etc. as a means to understand the impact on the RIR as a firm. The impact analysis includes an evaluation of *(1)* the costs of implementing a given policy and *(2)* potential legal implications of the policy for the RIR.

Rough consensus, in both the IETF and the RIRs, does not mean that everyone has to agree. Rather, it means that all contestations have been addressed, a significant portion of those engaged in the discussion agree, and importantly, that the consensus process itself has been followed. Like the IETF, participants in RIRs' consensus processes eschew majoritarian voting as a form of credible knowledge assessment. Evaluating the merits and implications of a policy, takes place in in-person RIR meetings and/or on e-mail lists dedicated to policy evaluation.

Simply asserting "No, I do not agree," without a rationale for that contestation, is insufficient and will be ignored. Unqualified contestations, and those that are not grounded in the epistemic communities' shared way of knowing (operational experience, demonstrable effects) are not considered authoritative. To be considered valid and credible, contributions to the policy debate must either fit, or constructively update the epistemic community's authoritative image of the operational dynamics at hand. When debating substantive change, such as policies affecting resource rights transfers markets or resource rights security, the constructive conflict embedded in these dialogues often updates community knowledge based on real-world observations, evaluated for veracity and consistency by those participating.

In interviews, leadership and policy process shepherds were quick to highlight that a "shallow 51-49 victory" is not rough consensus. Under rough consensus, the *number* of actors supporting or contesting a given proposal *is not* the deciding factor. The credibility of the critique (vis-à-vis community knowledge) and the evaluation of the proposal are the deciding factors. For instance, minority participants have an equal voice that *must* be addressed by the group for the process to proceed. The

group must reconcile the contestation by evaluating validity, credibility, and impact. If recognized as a valid contestation (i.e. others in the group support this, for instance by indicating they have also experienced the problem presented), the active consensus process continues to explore the solution space until that contestation is resolved to the satisfaction of the minority participant(s) *and* other expert ("an" authority) participants.

A fundamental premise of *rough* consensus is that *all* credible critiques must be reviewed, but *not all of them* will result in a change in the proposed policy. In the "easy" case, a critique may simply contest the wording to reduce ambiguity and improve clarity. In more substantive cases, the rationale and particular trade-offs characterizing a given solution are contested, and the group must iterate over alternate solutions. For instance, a common debate is improvement in the integrity (often related to security) of the system versus transaction costs of that solution. Discussions in the active phase evaluate the current solution, the current trade-offs and possible alternative trade-offs to identify other possible solutions that satisfy the overall objectives of the proposal. An important part of this process is that, at this point, the active participants in the process essentially become contributors, creating a sense of community contribution and ownership of this proposal. As such, the community of experts acting as "an" authorities are shaping proposals that may become policy, and consequently, authoritative.

The content of contestations may be incorporated into a proposal, may be iteratively refined to satisfy those presenting the contestation and the broader set of contributors, or may be discarded. In some valid contestations, the original solution is discarded, but iterative discussions identify an alternate solution that satisfies the premises of the critique is identified and incorporated into the proposal. In other cases, this process is followed, but the critique dismissed. To illustrate, returning the integrity-transaction costs trade-off, a minority of actors from smaller firms (networks) may argue that the for them, the relative transaction costs of a given proposal are much higher than for larger firms. This is a valid point: it is generally considered unfair to introduce policy that creates disproportionately high costs for some, but not all actors. That said, it is up to the community to decide how disproportionate it is and whether that prevails over the countervailing integrity concerns. If, for example, integrity is paramount and the community cannot identify an alternative that creates the same (or a similar) improvement in overall integrity, then the critique may be acknowledged (through discussion and evaluation), but ultimately dismissed (the proposal is not changed) on the grounds that overall integrity supersedes those transaction costs.

Another characteristic of rough consensus is that vote packing is not possible. Consider a simplified example adapted from Resnick (2014). Five participants are evaluating two proposals, one that is general purpose and less efficient, one that requires special hardware but is more efficient. Four of the five argue that general purpose is more valuable, while the fifth, that has easy access to the specialized hardware, argues for the fifth. The group has decided that general purpose solution is, overall, more desirable for a solution to be used by the broadest set of actors. Even

if the fifth recruits ten, or even twenty more actors to support their argument, if no new information or arguments are brought to bear, then the rough consensus still holds. In rough consensus processes, the number of supporters is not the deciding factor. Rather, increasing the number of expert actors in the rough consensus process is intended to improve the chances of bringing *additional* credible information and knowledge to the process. The objective is to maximize the potential size of the solution trade-off space, adding credibility to the ultimate solution and ensuring that the best operational information and knowledge used in the process.

Taken together, reaching active consensus means that the evaluative dialogue has *(1)* explored the solution trade-off space by *(2)* systematically addressing credible contestations offered by active participants. Like consensus in the IETF[91], the integrity of the consensus process itself highly contingent on the actor(s) designated to determine that consensus has been reached. In the IETF, this is the working group chair(s); in the RIRs, this is the policy shepherd(s). In interviews, experienced shepherds have stressed that while there is no hard and set rule, a good rule of thumb is to ensure that approximately 70-80 percent of participants agree with the resulting solution. Equally important to the integrity of the process is that all of the participants feel that, even if their preferred solution(s) were not accepted, that the rough consensus process was followed.

Passive Consensus

Passive consensus is the opportunity for community members that did not follow every incremental change in the proposal to evaluate, and potentially offer a critique of, the proposal resulting from active consensus. Rough consensus, as the name implies, does not mean that everyone agrees, nor does it require participation by every member of the community. Many of the participants in rough consensus processes are volunteers—they are engineers and technicians for whom this is important to their day job, but not their primary activity. Over the life cycle of a policy proposal, there is typically of core set of engaged actors, but other contributors may come and go throughout the incremental and iterative active consensus process.

Under passive consensus, silence on a proposal is sufficient. The implication is that there are no new critiques of the current proposal. That said, critiques may arise. In some cases, such as the "easy" language clarification critique described earlier, changes can be made in the passive consensus phase. In others, a more substantive critique that introduces new information or knowledge that has not been addressed in the active phase, must be addressed. For these critiques, the proposal will return to the active consensus phase to be resolved. Once resolved, the proposal returns again to passive consensus. After this period, the proposal enters the final phase of rough consensus, process review.

91. Resnick 2014.

Process Review

The last step of the rough consensus process is process review. Process review is typically conducted by either the board of the RIR and/or the policy shepherds as a collective to ensure the integrity of the consensus process itself. Process review does not further evaluate the content of the policy proposal itself. The process review is a double check on the legal implications of a policy and potential risks a particular policy may create for the RIR as the firm implementing and managing the registry itself. As such, process evaluators are playing the roles of legal and risk evaluators for the registry itself.

Implications for Global Governance

Modern societies increasingly depend on complex distributed technical systems. Understanding how order is created in these systems, and the sources of authority that shape that order, is essential for developing the policy and institutions necessary to effectively integrate these authorities into the broader global governance system. In the management of complex engineering systems, here in particular the Internet, understanding the loci of governance, the scope of those regimes' sphere of authority, the source of that authority, and how that authority is maintained is critical for understanding the implications for global governance. For policy analysis, distinguishing between governance *on* the Internet and governance *in* the Internet is a necessary first cut at mapping out the spheres of authority in this distributed, complex system. In this last section, the analytic implications are presented, with a brief foray into the normative implications for global governance. Governance on and governance in, and the concept of operational epistemic authorities, are presented in terms of their contributions to understanding Internet governance in the broader global governance system. Normatively, the good news is that these authorities have contributed to sustaining a valuable global communications system; the bad news is that the current ad hoc relationships with broader global governance institutions is unstable, especially in the face of contestations by illiberal regimes.

Governance in versus governance on is a simple, but important distinction that is often lost in broad characterizations of Internet governance as a form of private ordering, driven by private interests. Following the earlier distinction between multinationals managing platforms on the Internet and the operations communities presented here, these are both forms of private governance, but the kinds of issues they engage with, the scope of governance, and to whom they are accountable are significant. It also encourages the analyst to dig deeper into the diverse roles of actors within multinationals. Firms such as Google, Meta, and Amazon employ marketing teams and platform developers whose decisions shape the kinds of behaviors that play out on those platforms. These firms also employ network operators, security teams, and abuse desk operations teams that both distinguish themselves from the former (often adamantly), and express a normative dedication to the stability and security

of the Internet. These actors balance their obligations to their job and the norms of OEAs; in a number of OEAs, it is a common norm to announce one's affiliation and in what capacity one is making a contribution or contestation.

The notion of OEAs contributes to the literature on private authority and ordering, the work on epistemic communities pioneered by Haas, and most specifically contributes to the typology of epistemic authorities offered by Zürn. The operational component means not just having access to resources, but includes the scope of authority and the norms shaping the willingness of an OEA to use their capabilities and capacities to sustain operational order. The operational component also speaks to the source of authority and how it accrued to these institutions. This distinguishes OEAs from Zürn's politically assigned epistemic authorities, which have been delegated authority, for whom political influence goes both ways (offering significant interpretations and having those interpretations influenced by exogenous factors), and for whom authority may be rescinded. Operational also distinguishes OEAs from Zürn's pure epistemic authorities, exemplified by human rights and civil society groups. Like pure epistemic authorities, whose authority is not politically assigned, OEAs derive their authority from a distinct (often transnational) polity. Unlike pure epistemic authorities, they are not trying to shape the order and governance of a system from the outside: OEAs directly manage the system, here in particular the routing and addressing systems of the Internet.

Incorporating Flathman's notions of "in" authority, "an" authority, and "the authoritative" provides a conceptual framework for understanding how authority is sustained, and, taken together with the norms and values of the community, how the scope of that authority remains the same, or changes. Following Flathman's overall characterization of authority,[92] these ideal forms are analytically useful, but are more powerful when the analyst evaluates how the mix of these two plays out to contribute to "the authoritative." It also highlights fundamental trade-offs. DOEAs minimize "in" authority relationships, in both the IETF and the routing community. Some routing norms and best practices are documented by the routing community, most notably in IETF RFCs and the Internet Society's MANRs project,[93] but there is no formal obligation to follow any of these practices short of those necessary for baseline functionality. They are authoritative in that it has been agreed they are a best practice, but they are not obligatory. In contrast, those receiving IP address delegations and transfers from the RIRs are contractually bound to adhere to resource policy. Resource policies are created by rough consensus, with checks to ensure the integrity of in the process validation phase, but compliance is monitored and enforced by a non-profit firm whose contracts confer a degree of "in" authority.

As implied by the comparison above, evaluating OEAs as a mix of "in" and "an" authority also provides a framework for evaluating epistemic quality and legitimacy.

92. Flathman 1980.
93. Internet Society 2022.

Zürn indicates that "an epistemic authority need not, in all cases, convince people factually and in detail. It is, therefore, not the quality of the specific argumentation, but rather the general reputation of an institution . . . that is decisive."[94] Characterization of the mix of "in" and "an" offers a means of evaluating the integrity of the process of creating and maintaining the authoritative, without necessarily "convinc[ing] people factually and in detail." The distinction here is not necessarily one of more or less "an" authority or "in" authority. Rather, it is a question of the integrity of the process of formulating the authoritative in terms of endogenous legitimacy and impartiality. Complementing evaluations of the institution's reputation, the OEA framework facilitates distinguishing institutions' authority structure in terms of opportunities for bias (lack of impartiality). Ongoing work is applying the OEA framework in a systematic comparative analysis of the broader set of OEAs engaged in managing Internet operations, including a novel comparative analysis of ICANN.

Normatively, the good news is that the epistemic authorities evaluated here are driven by a cooperative ethos, have demonstrated the capabilities and capacities to sustain the address and routing system, and regularly act to mitigate global externalities. Their focus on endogenous legitimacy is both a strength and a weakness. They have focused their scope of authority and intervention to operational issues, with exceptions limited to when the integrity of the system is impacted. Their aversion to intentionally interfering with public policy and broader transnational issues is laudable for their awareness of the limits of their knowledge and representativeness to make such decisions.

The bad news is that these institutions have largely informal relationships with the broader global governance system. Historically, these communities have avoided engagement with state actors. More recently, they have recognized the need to engage, in part recognizing the limitations of their own capabilities, capacities, and authority, and in part because policy entrepreneurs in both these communities and in governments and international organizations have recognized the need for engagement. While the relationships between these epistemic authorities and state-based authorities *do* exist, like these epistemic communities themselves, they are largely informal, and based on interpersonal relationships. In the case of the routing community, their diffuse structure limits engagement, although experts in these communities have engaged with regulatory bodies such as the United States' Federal Communications Commission (FCC) and the European Union's Body of European Regulators for Electronic Communications (BEREC) in their capacity as well known "an" authorities from industry. Not surprisingly, the RIRs have created more durable fora for engagement, developing working groups for educating and engaging with law enforcement, regulators, and policymakers.[95]

94. Zürn (2018, 52), citing Haas (1992).

95. For instance, ARIN has a longstanding history of working with and educating law enforcement. The RIPE NCC sustains an ongoing Round Tables forum for engaging with government representatives and regulators from its region on issues related to "the governance and operation of the Internet," (Réseaux IP

While these are valuable steps engaging with the broader global governance system, the informal character of these relationships makes these relationships tenuous. While there are certainly some actors in these communities that eschew government engagement, there are policy entrepreneurs among the leadership in these communities that recognize the need for engagement. Here, the these communities' self-imposed aversion to "making public policy" can be turned to diplomatic benefit. Many of these actors do want to provide credible advice to state and international actors wrestling with the distinctions between governance in and governance on, and the implications of policy for the liberal, innovative character of the Internet. Committing further analysis to how OEAs can effectively engage with state-based authorities, while continuing to ensure the integrity of their own image of authority, can substantively contribute to greater integration into the global governance system.

Supplementary Material

(This is dummy text) Supplementary material for this research note is available at <https://doi.org/10.1017/Sxxxxxxxxx>.

References

Abbate, Janet. 2000. *Inventing the Internet.* The MIT Press, July.

Abbate, Janet. 2017. What and Where Is the Internet? (Re)Defining Internet Histories. *Internet Histories* 1, nos. 1-2 (January):8–14. https://doi.org/10.1080/24701475.2017.1305836.

Becker, Manuel. 2019. When Public Principals Give up Control over Private Agents: The New Independence of ICANN in Internet Governance. *Regulation & Governance* 13 (4):561–576. https://doi.org/10.1111/rego.12250.

Bennett, Andrew, and Jeffrey T. Checkel, eds. 2015. *Process Tracing : From Metaphor to Analytic Tool.* Strategies for Social Inquiry. Cambridge University Press.

Berhan, Taye. 2020. Targeted, Cut Off, and Left in the Dark: The #KeepItOn Report on Internet Shudowns in 2019. Technical report. Https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf. Access Now.

Black, Julia. 2017. 'Says Who?' Liquid Authority and Interpretive Control in Transnational Regulatory Regimes. *International Theory* 9, no. 2 (April):286–310. https://doi.org/10.1017/S1752971916000294.

Blumenthal, M. S., and D. D. Clark. 2001. Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World. *ACM Transactions on Internet Technology (TOIT)* 1 (1):70–109.

Börzel, Tanja A., and Michael Zürn. 2021. Contestations of the Liberal International Order: From Liberal Multilateralism to Postnational Liberalism. *International Organization* 75 (2):282–305. https://doi.org/10.1017/S0020818320000570.

Européens Network Coordination Centre 2022).

Braman, Sandra. 2010. The Interpenetration of Technical and Legal Decision-Making for the Internet. *Information, Communication & Society* 13, no. 3 (April):309–324. https://doi.org/10.1080/13691180903473814.

Braman, Sandra. 2011. The Framing Years: Policy Fundamentals in the Internet Design Process, 1969–1979. *The Information Society* 27, no. 5 (October):295–310. https://doi.org/10.1080/01972243.2011.607027.

Braman, Sandra. 2013. The Geopolitical vs. the Network Political: Internet Designers and Governance. *International Journal of Media & Cultural Politics* 9, no. 3 (September):277–296. https://doi.org/10.1386/macp.9.3.277_1.

Büthe, Tim, and Walter Mattli. 2011. *The New Global Rulers: The Privatization of Regulation in the World Economy.* Princeton University Press.

Clark, David D. 1992. A Cloudy Crystal Ball: Visions of the Future. https://groups.csail.mit.edu/ana/People/DDC/future_ietf_92.pdf. Plenary Presentation. Cambridge, MA, July.

Clark, David D., William Lehr, and Steven Bauer. 2011. Interconnection in the Internet: The Policy Challenge. SSRN Scholarly Paper ID 1992641. Https://papers.ssrn.com/abstract=1992641. Rochester, NY: Social Science Research Network, August.

Cutler, A. Claire, Virginia Haufler, and Tony Porter, eds. 1999. *Private Authority and International Affairs.* State University of New York Press.

David, Paul A. 2007. Path Dependence: A Foundational Concept for Historical Social Science. *Cliometrica* 1, no. 2 (April):91–114. https://doi.org/10.1007/s11698-006-0005-x.

DeNardis, Laura. 2009. *Protocol Politics: The Globalization of Internet Governance.* Information Revolution and Global Politics. The MIT Press.

Ellickson, Robert C. 1991. *Order without Law: How Neighbors Settle Disputes.* Harvard University Press.

Elmer-DeWitt, Philip, and David S. Jackson. 1993. First Nation in Cyberspace. *Time* 142, no. 24 (December):62.

Faratin, Peyman, David Clark, Steven Bauer, William Lehr, Patrick Gilmore, and Arthur Berger. 2008. The Growing Complexity of Internet Interconnection. Http://ezproxy.library.tamu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eoh&AN=1095251&site=eds-live, *Communications and Strategies,* no. 72, 51–71.

Farrell, Henry, and Abraham L. Newman. 2021. The Janus Face of the Liberal International Information Order: When Global Institutions Are Self-Undermining. *International Organization* 75 (2):333–358. https://doi.org/10.1017/S0020818320000302.

Flathman, Richard E. 1980. *The Practice of Political Authority: Authority and the Authoritative.* Univ of Chicago Pr, August.

Frischmann, Brett M. 2012. *Infrastructure: The Social Value of Shared Resources.* Oxford University Press.

George, Alexander L., and Andrew Bennett. 2005. *Case Studies and Theory Development in the Social Sciences.* The MIT Press, February.

Greene, Barry. 2021. Network Operations Groups (NOGs). https://www.senki.org/network-operations-scaling/network-operations-groups-meeting/.

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

Hafner, Katie, and Matthew Lyon. 1999. *Where Wizards Stay Up Late: The Origins Of The Internet.* Simon & Schuster, August.

Haigh, Thomas, Andrew L. Russell, and William H. Dutton. 2015. Histories of the Internet: Introducing a Special Issue of Information & Culture. *Information & Culture: A Journal of History* 50 (2):143–159. https://doi.org/10.1353/lac.2015.0006.

Hall, Rodney Bruce, and Thomas J. Biersteker, eds. 2003. *The Emergence of Private Authority in Global Governance.* Cambridge University Press, January.

Hofmann, Jeanette, Christian Katzenbach, and Kirsten Gollatz. 2017. Between Coordination and Regulation: Finding the Governance in Internet Governance. *New Media & Society* 19, no. 9 (September):1406–1423. https://doi.org/10.1177/1461444816639975.

Internet Society. 2022. MANRS – Mutually Agreed Norms for Routing Security. https://www.manrs.org/.

Jongen, Hortense, and Jan Aart Scholte. 2021. Legitimacy in Multistakeholder Global Governance at ICANN. *Global Governance: A Review of Multilateralism and International Organizations* 27, no. 2 (June):298–324. https://doi.org/10.1163/19426720-02702004.

Klein, Hans. 2002. ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy. *Information Society* 18, no. 3 (May):193–207. https://doi.org/10.1080/01972240290074959.

Lake, David A. 2009. Relational Authority and Legitimacy in International Relations. *American Behavioral Scientist* 53, no. 3 (November):331–353. https://doi.org/10.1177/0002764209338796.

Lake, David A., Lisa L. Martin, and Thomas Risse. 2021. Challenges to the Liberal Order: Reflections on *International Organization*. *International Organization* 75 (2):225–257. https://doi.org/10.1017/S0020818320000636.

Layton, Edwin T. 1979. Scientific Technology, 1845-1900: The Hydraulic Turbine and the Origins of American Industrial Research. *Technology and Culture* 20, no. 1 (January):64–89. https://doi.org/10.2307/3103112.

Lijphart, Arend. 1999. *Patterns of Democracy: Government Forms and Performance in Thirty-Six Countries.* Yale University Press, July.

Mattli, Walter, and Tim Büthe. 2003. Setting International Standards: Technological Rationality or Primacy of Power? *World Politics* 56, no. 1 (October):1–42. https://doi.org/10.1353/wp.2004.0006.

Mattli, Walter, and Ngaire Woods. 2009. In Whose Benefit? Explaining Regulatory Change in Global Politics. In *The Politics of Global Regulation,* Kindle, 1–44. Princeton, NJ: Princeton University Press.

Moss, David A. 2004. *When All Else Fails: Government as the Ultimate Risk Manager.* Harvard University Press, October.

Mueller, Milton. 2002. *Ruling the Root.* The MIT Press.

NANOG. 2020. NANOG Bylaws. https://www.nanog.org/legal/bylaws/, July.

Noy, Chaim. 2008. Sampling Knowledge: The Hermeneutics of Snowball Sampling in Qualitative Research. *International Journal of Social Research Methodology* 11, no. 4 (October):327–344. https://doi.org/10.1080/13645570701401305.

NRO, The Number Resource Organization. 2020. About the NRO. https://www.nro.net/about/, November.

NRO, The Number Resource Organization. 2021. Regional Internet Registries. https://nro.net/about/rirs/, April.

Number Resource Organization. 2022. RIR Statistics | The Number Resource Organization. https://www.nro.net/about/rirs/statistics/.

Nye, Joseph S., and Robert O. Keohane. 1971. Transnational Relations and World Politics: An Introduction. *International Organization* 25 (3):329–349.

Ostrom, Elinor. 1990. *Governing the Commons: The Evolution of Institutions for Collective Action.* Cambridge University Press.

Raymond, Mark, and Laura DeNardis. 2015. Multistakeholderism: Anatomy of an Inchoate Global Institution. *International Theory* 7, no. 3 (November):572–616. https://doi.org/10.1017/S1752971915000081.

Réseaux IP Européens Network Coordination Centre. 2022. Roundtable Meetings. https://www.ripe.net/participate/meetings/roundtable/roundtable-meetings.

Cerf, V.G. 1990. IAB Recommended Policy on Distributing Internet Identifier Assignment and IAB Recommended Policy Change to Internet "Connected" Status. RFC 1174. Fremont, CA, USA: IETF (Internet Engineering Task Force), August. https://doi.org/10.17487/RFC1174.

Gerich, E. 1993. Guidelines for Management of IP Address Space. Request for Comments, Internet Request for Comments 1466. Fremont, CA, USA: IETF (Internet Engineering Task Force), May. https://doi.org/10.17487/RFC1466.

Hubbard, K., M. Kosters, D. Conrad, D. Karrenberg, and J. Postel. 1996. Internet Registry IP Allocation Guidelines. Request for Comments 2050. Fremont, CA, USA: IETF (Internet Engineering Task Force), November. https://doi.org/10.17487/RFC2050.

Alvestrand, H. 2004. A Mission Statement for the IETF. Best Current Practice, Internet Request for Comments 3935. Fremont, CA, USA: Internet Engineering Task Force (IETF), October. https://doi.org/10.17487/RFC3935.

Rekhter (Ed.), Y., T. Li (Ed.), and S. Hares (Ed.) 2006. A Border Gateway Protocol 4 (BGP-4). RFC, Internet Request for Comments. Fremont, CA, USA: RFC Editor, January. https://doi.org/10.17487/RFC4271.

Housley, R., J. Curran, G. Huston, and D. Conrad. 2013. The Internet Numbers Registry System. RFC. Fremont, CA, USA: RFC Editor, August. https://doi.org/10.17487/RFC7020.

Resnick, P. 2014. On Consensus and Humming in the IETF. RFC 7282. Fremont, CA, USA: Internet Engineering Task Force (IETF), June. https://doi.org/10.17487/RFC7282.

Postel, J. 1981. Internet Protocol. RFC 791. Fremont, CA, USA: Internet Engineering Task Force (IETF), September. https://doi.org/10.17487/RFC0791.

RIPE NCC. 2008. YouTube and Pakistan Telecom. https://www.youtube.com/watch?v=IzLPKuAOe50, February.

Russell, A.L. 2006. 'Rough Consensus and Running Code' and the Internet-OSI Standards War. *IEEE Annals of the History of Computing* 28, no. 3 (July):48–61. https://doi.org/10.1109/MAHC.2006.42.

Sabel, Charles, Gary Herrigel, and Peer Hull Kristensen. 2018. Regulation under Uncertainty: The Coevolution of Industry and Regulation. Http://onlinelibrary.wiley.com/doi/abs/10.1111/rego.12146, *Regulation & Governance* 12 (3):371–394.

Saltzer, J. H., D. P. Reed, and D. D. Clark. 1984. End-to-End Arguments in System Design. *ACM Transactions on Computer Systems* 2 (4):277–288.

Scott, Colin. 2015. The Contribution of Transnational Private Regulation to Revisiting Risk Regulation. Https://irgc.org/wp-content/uploads/2018/09/IRGC-IRR-2.pdf, *International Risk Governance Council,* Improving Risk Regulation:14.

Shoch, John F. 1978. Inter-Network Naming, Addressing, and Routing. In Proceedings of the Seventeenth IEEE Computer Society International Conference (COMPCON). Http://mailman.postel.org/ien/pdf/ien019.pdf. Washington D.C.: IEEE Computer Society, September.

Solum, Lawrence B. 2008. Models of Internet Governance. Technical report Law & Economics Research Paper No. LE08-027. University of Illinois Law.

Take, Ingo. 2012. Regulating the Internet Infrastructure: A Comparative Appraisal of the Legitimacy of ICANN, ITU, and the WSIS. *Regulation & Governance* 6, no. 4 (December):499–523. https://doi.org/10.1111/j.1748-5991.2012.01151.x.

TenHouten, Warren D. 2017. Site Sampling and Snowball Sampling - Methodology for Accessing Hard-to-Reach Populations. Http://www.jstor.org/stable/26411978, *BMS: Bulletin of Sociological Methodology / Bulletin de Méthodologie Sociologique,* no. 134, 58–61.

Underhill, Geoffrey R. D., and Xiaoke Zhang. 2008. Setting the Rules: Private Power, Political Underpinnings, and Legitimacy in Global Monetary and Financial Governance. Http://www.jstor.org/stable/25144816, *International Affairs* 84 (3):535–554.

van Eeten, Michel JG, and Milton Mueller. 2013. Where Is the Governance in Internet Governance? *New Media & Society* 15, no. 5 (August):720–736. https://doi.org/10.1177/1461444812462850.

van Schewick, Barbara. 2010. *Internet Architecture and Innovation.* The MIT Press, July.

Yates, JoAnne, and Craig N. Murphy. 2019. *Engineering Rules: Global Standard Setting since 1880.* Johns Hopkins University Press, June.

Zittrain, Jonathan L. 2006. The Generative Internet. *Harvard Law Journal* 119:1974–2040.

Zürn, Michael. 2018. *A Theory of Global Governance: Authority, Legitimacy, and Contestation.* Oxford University Press. https://doi.org/10.1093/oso/9780198819974.001.0001.

Date received: MMMM DD, YYYY; Date accepted: MMMM DD, YYYY.

Dummy dates; please ignore.