

Question 1: The Distribution of Authority in Cyberspace

MIT Student
Cyberpolitics in IR
Professor Choucri
December 10, 2015

Today, 3.3 billion Internet users – about 45% of the world’s population – sent 149 billion emails, ran 3 billion Google searches, and wrote 412 million Tweets.¹ For contrast, approximately 1.2 billion active phone lines existed worldwide in 2014.² Unlike other, less powerful forms of communication – such as radio, television, or landline telephones – the Internet has no clear authority or single governance structure. Yet given the importance and ubiquity of the Internet as a tool for communication and potential harm, questions of Internet governance are crucial in the study of global politics.

Despite the emergence of other actors, such as private corporations, non-state terrorist groups, or international NGOs, international politics today is still dominated by nation-states demarcated by territorial boundaries. Notably, however, the influence of states does not map directly onto the cyber domain. Instead, a plurality of actors clamor for authority, including states, nonprofit institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN), epistemic communities such as the Internet Engineering Task Force (IETF) and the Internet Society, multinational Internet service providers, private companies, and civil society. In this diverse topography of actors, where is authority located?

This paper will seek to answer the question of how authority is dispersed across the Internet. I will utilize a layered model of the Internet, and argue that different types of authority, coming from different sources, are present at each layer. I will discuss how traces of realism, institutionalism, and constructivism at the code layer of the Internet contribute to the structure of authority. Finally, I will put this analysis in the context of the debate about multilateral versus multistakeholder models of Internet governance, and discuss the implications for governance at each layer of the Internet if one or the other position prevailed. Ultimately, I argue that while state governments have primary authority over the content layer of the Internet, non-state institutions such as ICANN and the World Wide Web Consortium (W3C) have authority over the code layer. Authority over the physical underpinnings of the Internet is primarily in the hands of corporations, tightly regulated by state governments.

Clark describes the Internet as a layered construction with seven distinct levels. At the base, the physical layer of the Internet comprises the copper fibers, the radio waves, the undersea

¹ According to Internet Live Stats, a website which gathers data on Internet users and web traffic. Internet Live Stats has been cited by the World Wide Web Consortium and by Tim Berners Lee, and can be found at <http://www.internetlivestats.com/>

² *The World Factbook* 2013-14. Washington, DC: Central Intelligence Agency, 2013.

cables, and all physical infrastructures needed to support the Internet. Above that, the datagram layer, transport layer, and three protocol layers govern the packaging, coordination, and transport of data. The sixth layer comprises the language with which Internet users navigate the content of the Internet, and the seventh and highest-level layer is the content of the Internet itself – the user-generated Tweets, web pages, photographs, and other information that is generated and distributed on the Internet.

In analyzing the locations of authority in the Internet, it will be useful to abstract from Clark's detailed depiction to Lessig's three-layered model of the Internet. Slightly less refined, Lessig's model comprises a physical layer (corresponding to the first layer in Clark's model), a content layer (corresponding to the seventh layer in Clark's model), and a code layer, which subsumes the remainder of Clark's model. Though each layer of the Internet has its own distinctive features which pose unique challenges to governance, the overall governance structures operating in the middle five layers are similar enough that to abstract to Lessig's model does not entail too great a loss of detail. This paper will therefore examine the dynamics of authority and governance at each of the three layers of the Internet.

However, it is first useful to clarify the concept of authority, and in particular, to distinguish between authority and power. It is also useful to describe the conditions under which an actor such as a government might delegate authority to an agent, ceding its own control, and the potential consequences of doing so. Hall and Biersteker describe an authority as an actor which "perform[s] the role of authorship over some important issue or domain. They claim to be, perform as, and are recognized as legitimate by some larger public as authors of policies, of practices, of rules, and of norms. They set agendas, they establish boundaries or limits for action, they certify, they offer salvation, they guarantee contracts, and they provide order and security."³ Crucially differentiating authority from power is the "legitimacy of claims of authority," which derives from consent.⁴

Cowey and Mueller argue that governments are likely to delegate to nongovernmental authorities in order to "reap efficiency gains" and to "create gains from specialization and expert

³ Hall, Bruce and Thomas Biersteker "The Emergence of Private Authority in Global Governance," Ch. 1. *The Emergence of Private Authority in Global Governance*. Cambridge University Press. 2002. Page 4.

⁴ *Ibid*, p. 5.

knowledge.”⁵ Cowey and Mueller also describe two distinct processes by which a principal may come to delegate to an agent. First, a principal may delegate to an agent by a “formal act of deliberative delegation.” However, it may also be the case that a principal becomes “interested in an area where there is a preexisting “agent” who emerged for other reasons.”⁶ In this case, the principal, such as a state government, could accept the existing agent as an authority, could try to modify the agent’s scope of authority, or could try to replace the agent altogether.

In the context of the Internet, these claims are consistent with Cerny’s argument that a growing gap between the capacity of the state to provide and the demands for public goods will result in an erosion of state power and a curtailment of state activities, since the sheer volume of demand for Internet services overwhelms the capacity of a single state.⁷ But to who could the state delegate authority and what consequences might delegation entail? Haas argues that under conditions of uncertainty – when the state seeks to “create gains from...expert knowledge” – epistemic communities may gain authority as legitimate international actors.⁸ Epistemic communities may provide information, or take part in setting and enforcing policy. Haas argues that epistemic communities may “bound the range of collective choice” by excluding options from policy debate, or help identify state interests. However, Cowey and Mueller describe several strategies by which states might reduce the autonomy of such agents, including through “stacking the deck” in the agency’s personnel system or in “outside advisory processes” to ensure that people “favorable to the goals of the principals have a disproportionate role.”⁹

Thus, even before analyzing the dynamics of Internet authority, several predictions can be made. First, non-state organizations may have more authority in areas that require technical knowledge or expertise. Second, even in cases where non-state actors appear to have authority, state governments may have taken steps to curtail their autonomy. Finally, authority may be most contested in areas where pre-existing ‘agents’ accrued authority prior to the involvement of the state.

⁵ Cowey, Peter and Milton Mueller. "Delegation, Networks and Internet Governance" in Kahler, *Networked Politics: Agency, Power, and Governance*. Cornell University Press. 2009. Pages 174-175.

⁶ *Ibid*, p. 176.

⁷ Cerny, Philip G. 1995. "Globalization and the Changing Logic of Collective Action." *International Organization* 49 (4): 595-625.

⁸ Haas, Peter M. 1989. *The Fourth Image Reversed: Epistemic Communities and Knowledge Based Bargaining as a Response to Uncertainty.* prepared for delivery at the 1989 Annual Meeting of the American Political Science Association, Atlanta, Georgia. August 30-September 3, 1989.

⁹ Cowey and Mueller, p. 176.

Authority in the Content Layer

The content layer of the Internet comprises the content of webpages, Tweets, blog posts, videos, photographs, and all user-generated material. Policy objectives of authority in the content layer include “controlling illegal and harmful content, consumer protection, data protection, and control of spam.”¹⁰ These objectives mainly fall into the domain of authority of the state – controlling crime and protecting citizens from criminal activity is a well-established prerogative of state governments, and the legitimate authority of the state to protect its citizens in the “real world” extends into the cyber domain as well. In addition, the instruments available for achieving the policy objectives, combined with the prevailing standards and enforcement mechanisms, create an environment where state governments exercise most authority, though their jurisdiction is fragmented across territories.

To protect data and consumer information, and to control spam and illegal content, organizations can implement certification systems, encryption schemes, and programs to filter unwanted content.¹¹ While the creation of these programs may be delegated to private authorities, state governments are the primary standard setters when it comes to Internet content. To demonstrate this, consider the following legislation passed by U.S. Congress: the Communications Decency Act (1997), the No Electronic Theft Act (1997), the Children’s Online Privacy Protection Act (1999), the Digital Millennium Copyright Act (1998), the Anti-Cybersquatting Consumer Protection Act (2000), the Electronic Communications Privacy Act (2000), and the USA Patriot Act (2001). These policies set the standards for appropriate Internet content, protecting users from harmful content, from malicious attacks, and enforcing intellectual property law. Since these standards are encoded in law, enforcement also falls to the state.

Authority in the Code Layer

The code layer of the Internet is the area in which the state had the least pre-existing legitimacy. In comparison, organizations such as ICANN, W3C, and IETF had both the technical knowledge and the capacity to establish themselves as legitimate authorities. In some cases, the

¹⁰ Caral, J. "Lessons from ICANN: is self-regulation of the Internet fundamentally flawed?" *International Journal of Law and Information Technology*, Volume 12 (1) 1-31. Page 12.

¹¹ *Ibid*, p. 13.

state was content to delegate authority to these institutions. However, where the interests of the state conflict with the established interests of these non-state institutions, contestation over authority comes to a head.

The IETF, W3C, and ICANN are the primary standard-setters for the code layer of the Internet, with the IETF developing communications standards, W3C developing document standards for the World Wide Web to ensure that text, graphics, audio, and video are accessible and displayable, and ICANN developing standards for the Internet's domain name and addressing system.¹² Delegation to these institutions is predicted by Haas's theory of epistemic communities, and indeed, the U.S. government did recognize its own inability to act as a standard-setter for the Internet. The *Framework for Global Electronic Commerce*, developed by the Clinton administration in 1997, delegated standard-setting authority away from the government, establishing that:

The marketplace, not governments, should determine technical standards and other mechanism for interoperability on the Internet. Technology is moving rapidly and governments' attempts to establish technical standards to govern the Internet would only risk inhibiting technological innovation.¹³

Caral argues that because of the technical expertise required to effectively govern the code layer, and because non-compliance with set standards results in non-inclusion in the Internet, that government enforcement is not necessary and self-regulation among the three principal non-state actors is the source of authority in the code layer. However, this depiction belies the contestation between global, decentralized governance and the interests of the nation-state system.

In particular, contentions have arisen around delegation of authority over critical Internet resources, defined by Mueller as "the governance of Internet standards, domain names, and IP addresses" as well as "the interconnection and routing arrangements among Internet service providers."¹⁴ These critical Internet resources are the choke points of the Internet – among the

¹² Caral, p. 9.

¹³ President William J. Clinton & Vice President Albert Gore, Jr., *A Framework for Global Electronic Commerce*. July 1, 1997.

¹⁴ Mueller, Milton L. *Networks and States*, 2010. Cambridge, MA.: MIT Press, Chapter 8.

“few points of global leverage,” according to Mueller, and the points of the networks that states “had almost no control over.”¹⁵ However, as predicted previously, the United States government constructed ICANN in a way that would give it a disproportionate influence – it “stacked the deck” in favor of its priorities.¹⁶ In particular, the U.S. government “disproportionately empowered the Internet technical community and intellectual property owners.” In addition, it “retain[ed] policy authority over the root zone file,” requiring ICANN to submit any proposed changes to the Department of Commerce for approval, and any approved changes are implemented by a U.S. corporation. Thus, non-state actors are the primary authorities in the code layer of the Internet, but state governments in general, and the U.S. government in particular, still exert low levels of control.

The code layer of the Internet is relevant to the content layer, since the architecture of the code layer determines how, when, and to whom content is accessible. It is in the code layer that ideals from constructivism, institutionalism, or realism would have the most impact on how people use the Internet. The architecture of the Internet was built to ensure free and rapid communication. It was intentionally designed to allow the spread of ideas, and innovation within the network, close to ideals of constructivism, which views the spread of ideas as a causal agent for change. One effect of the Internet, to promote new forms of collaboration and overcome problems of collective action, is identified with the institutionalist mode of thought. Absent from the design of the Internet were concerns for security, jurisdiction, and identity of individuals – key realist concerns.

It is relevant that the state, which has authority in the content layer, has diminished authority in the layer of the Internet where design choices are made that affect the ability of the state to regulate its borders, provide for its security, and identify its citizens. Presumably, had the state more influence in the code layer of the Internet, realist concerns about security and jurisdiction would be more strongly manifest in the underlying architecture of the Internet.

Authority in the Physical Layer

¹⁵ *Ibid*, p. 216.

¹⁶ Cowey and Mueller, p. 187.

There is precedent for the state to have authority in matters of national infrastructure-building. The state has a history in overseeing the development by private companies of railroads, telephone lines, and telecommunications networks, and this precedent creates the legitimate authority for the state to regulate the infrastructure of the Internet.

However, the private companies which build the infrastructure for the Internet differ from historical examples in that they are multinational, and their operations cross through multiple jurisdictions. Nevertheless, there are mechanisms for states to regulate private companies – even ones which cross jurisdictions. Caral looks to the example of international banking to see how governments have imposed order on entities which cross territorial borders, and suggests that the level of co-operation among public and private regulators be increased to deal with ambiguities arising from unclear jurisdiction.

Thus, at the physical layer of the Internet, private companies have a large role in building infrastructure, but state governments have the authority to regulate and oversee these companies.

A Multilateral Model of Governance

Given this structure of authority distribution in the Internet, a multistakeholder versus multilateral model of Internet governance would most likely be manifest at the code layer. A multilateral model of governance, in which states are the primary authorities, might see a fundamental shift in the organization of the DNS system and root zone files. The current arrangement represents a multistakeholder model, and is what allows for relatively free and open communication. States, which are generally more concerned with issues of security and jurisdiction, might arrange the domain name system to support a number of separate networks, corresponding to each territorial state, connected at a few, tightly controlled, bottleneck points. This would clarify the issue of jurisdiction, and give states a monopoly over the ability to control access to their network by non-citizens.

Conclusion

Ultimately, authority is distributed in different ways at different levels of the Internet. At the content layer and physical layer, the state can rely on its legitimate power to protect its

citizens and control crime, and regulate corporations, respectively. However, at the code layer, where the state has neither the technical expertise nor the preexisting mandate, non-state nonprofit organizations have accrued authority. Nevertheless, the state has tried to reassert its authority over these institutions, and the United States government in particular retains some key elements of control over crucial Internet resources. The distribution of authority in the Internet may shape key functionalities of the Internet itself, and if it were to change, could be reflected in changes to the underlying design of the Internet which would alter how it could be used. Yet in some sense, checks and balances of power exist between authorities at different layers of the Internet, since each layer depends on all others to operate to its full potential.

Works Cited

- Caral, J. "Lessons from ICANN: is self-regulation of the Internet fundamentally flawed?" *International Journal of Law and Information Technology*, Volume 12 (1) 1-31. Page 12.
- Cerny, Philip G. 1995. "Globalization and the Changing Logic of Collective Action." *International Organization* 49 (4): 595-625.
- President William J. Clinton & Vice President Albert Gore, Jr., *A Framework for Global Electronic Commerce*. July 1, 1997.
- Cowey, Peter and Milton Mueller. "Delegation, Networks and Internet Governance" in Kahler, *Networked Politics: Agency, Power, and Governance*. Cornell University Press. 2009. Pages 174-175.
- Haas, Peter M. 1989. *The Fourth Image Reversed: Epistemic Communities and Knowledge Based Bargaining as a Response to Uncertainty.* prepared for delivery at the 1989 Annual Meeting of the American Political Science Association, Atlanta, Georgia. August 30-September 3, 1989.
- Hall, Bruce and Thomas Biersteker "The Emergence of Private Authority in Global Governance," Ch. 1. *The Emergence of Private Authority in Global Governance*. Cambridge University Press. 2002. Page 4.
- Mueller, Milton L. *Networks and States*, 2010. Cambridge, MA.: MIT Press, Chapter 8.

MIT OpenCourseWare
<http://ocw.mit.edu>

17.445 / 17.446 International Relations Theory in the Cyber Age
Fall 2015

For information about citing these materials or our Terms of Use, visit: <http://ocw.mit.edu/terms>.