Sovereignty and Cyberspace: Institutions and Internet governance

Milton Mueller (under review by Regulation and Governance)

Can there be sovereignty in cyberspace, where globalized connectivity prevails? Would national borders in cyberspace improve security and order there? That topic has been a recurring theme from the beginning of the Internet's debut as a global communications infrastructure. But it is more relevant than ever now, as states increasingly try to realign cyberspace with governmental authority.

It is a sign of the changing times that the first papers to raise the issue of sovereignty in cyberspace were animated not by an attempt to apply traditional forms of state sovereignty to the Internet, but by the claim that cyberspace was its own sovereign domain. (Barlow, 1996; Hardy, 1994; Johnson & Post, 1996) Today, the growing influence of state power on the Internet, the rise of cybersecurity concerns, and the exploitation of cyberspace by militaries have pushed us in the opposite direction, reviving claims of sovereignty in cyberspace. But can it work? And is it a good idea?

In 1996, two pioneering legal scholars argued that the Internet "cut across territorial borders, creating a new realm of human activity and undermining the feasibility – and legitimacy – of applying laws based on geographic boundaries." (Johnson & Post, 1996, 1997) They did not engage with the theory of sovereignty as such, but their vision of a globalized jurisdiction led directly to the creation of the Internet Corporation for Assigned Names and Numbers (ICANN) in 1998. ICANN's nongovernmental status was intended to globalize domain name governance so as to facilitate universal compatibility. But shortly after the creation of ICANN, and in large part because of it, an international debate over Internet governance erupted. At the UN World Summit on the Information Society states asserted their

"sovereign right" to make "international public policy" for the Internet. (WSIS, 2005) The ensuing debate over "multi-stakeholder" governance was – and still is – really a battle about sovereignty in cyberspace.

Often unrecognized in this struggle is the relevance of Nobel Laureate Elinor Ostrom's work on institutional analysis and development (Ostrom, 1990, 2005). Contention over Internet governance is a prime example of institutional innovation prompted by the emergence of new, technologically-generated resource spaces. Whether the techno-economic characteristics of the internet can unravel an institution as deeply entrenched as state sovereignty over communications, or whether the reverse occurs, remains to be seen. Yet while it is easy to dismiss naïve notions of the independence of cyberspace, it is just as simplistic to accept as inevitable a reversion to a pre-digital territorial sovereignty. It is time to have a technically and theoretically informed discussion of the role of sovereignty in cyberspace – a discussion that recognizes the historical reality of institutional change and the possibilities of collective self-governance highlighted by Ostrom's work.

Self-governance institutions

For more than a decade before the Internet became an open, economically significant information infrastructure, new bottom up governance institutions were forming around it. Though centered in the United States, the community of scientists, engineers and businesses that created those institutions were cosmopolitan and transnational.

The **Internet Engineering Task Force** (IETF), which formed in the mid-1980s, was a genuinely new organizational form. It evolved out of informal meetings of the computer scientists and network engineers who developed the protocol standards. The IETF did not sell its standards documents, it published them freely online. It was the world's first large-scale open source software development

community. Unlike its predecessor standards development organizations, it was composed of individuals, not formal members who represented states or corporations. Participation was open, and its standards were voluntary; i.e., there were no regulatory requirements to adopt them and it held no governmental mandate.

The IETF standards and protocols generated new resources spaces that required new forms of governance.

Internet protocol addresses (IP addresses) are structured numbers that uniquely identify nodes on the network. The supply of numbers is determined by the IETF standard defining internet protocol. IP addresses are common pool resources in the Ostrom sense. (Mueller, 2010) Their allocation and assignment must be coordinated so that each host computer's address is globally unique; and their supply is fixed so there may be a need to ration their appropriation. The internet technical community solved this problem through the development of regional Internet registries (RIRs), which are organized as private sector nonprofits that issue number blocks and govern their use through private contracts. The first RIR was formed in Europe in 1991, the second in the Asia Pacific in 1996; others followed later.

Routing is the step-by-step movement of data packets over thousands of separate networks that comprise the Internet. It is truly a miracle of networked self-governance: billions of individual packets successfully move from their origin to their destination every minute, with no external, legal governance other than Internet service providers' adherence to the IETF's BGP protocol, and contractual and cooperative arrangements amongst private sector network operators.

The domain name system (DNS) is another resource space brought into existence by the Internet. It gives web sites and computers globally unique names and plays a critical role in maintaining universal connectivity. The DNS root, where the naming hierarchy begins, has the characteristics of a common

pool resource. As noted before, the need for governance of the DNS root prompted the creation of ICANN, a global, private sector regime based on contract.

All these Internet institutions depart from sovereignty. Their scope of governance is transnational rather than national, and authority is rooted in private actors. They bear out Ostrom's belief that collective action amongst a community could solve common pool governance problems.

It is common to characterize this as the "multi-stakeholder model," (Strickling & Hill, 2017) but the rhetoric of multistakeholderism is misplaced and often misleading. The key feature of this regime is not the presence of multiple stakeholders. It is the elevated status of the nonstate actor, which supplants the sovereign state or intergovernmental treaties and regimes in its authority to define rules and policies.

Despite the impressive record of institutional development and self-governance in cyberspace, one must recognize that *compatibility* and *connectivity* are the prime directives in all the domains of governance mentioned above. With standards, addresses, domains and routing there is a Nash equilibrium on cooperation. Other areas of Internet governance do not so easily settle on a cooperative solution, however. These are the areas where articulation with territorial states has become troublesome:

- Content regulation. Global connectivity makes anything published anywhere accessible to anyone. States cannot abide this erosion of their authority over information flows, and so have asserted their power over ISPs, platforms and users to block access to content and applications, censor web sites, and restrict access to online services.
- Cybercrime. Private governance institutions cannot lock people up, they can only exclude them from resources and services. States are still the only institution with the authority to prosecute, arrest, jail or fine criminals. The emergence of widespread and highly creative forms of cybercrime re-invokes the state.

- Privacy and data protection. Laws and regulations relating to data protection and privacy exist almost everywhere and have become increasingly important as the economy and social media are digitized. Yet the rules vary from place to place while data flows are global.
- Cybersecurity. Security has always been deemed one of the key responsibilities of the state. Despite the existence of myriad cooperative, non-hierarchical and market-based cybersecurity solutions, the state is tempted to reassert its traditional role, especially when cybersecurity intersects with national security and military power, as it increasingly does.

Yet while sovereignty advocates may see these problems as evidence of the 'inevitability' of a reversion to the state-centric norm, the joke is really on them. Far from being the solution to cybersecurity, nation-states have become one of the chief threats to it. They have ignored sovereign boundaries to aggressively utilize the Internet's global connectivity to attack each other and ordinary businesses. These attacks, while serious, are so far under the threshold of armed aggression or military force that established international law has little relevance. Similarly, European governments are having a hard time enforcing a "right to be forgotten" in their territory without also imposing it on Internet users in America, where it violates free speech guarantees in the constitution. An attempt to protect privacy by one region's government – the European General Data Protection Regulation – has had massive extraterritorial effects and threatens to trigger blockages or retaliatory legislation in other jurisdictions. It seems that the globalism of the net exacts its revenge even when sovereigns attempting to carve it up.

The theory of sovereignty

What is it about Internet governance that is so problematic? I think the answer is simple, though its ramifications are many and highly complex. It is the problem of misalignment: the mismatch between the transnational spaces for societal interaction created by the internet and the territorial boundaries of

national governments. The internet joins the world of communication and information into a single space; sovereignty fragments it into 200 pieces.

The principle of state sovereignty is one of the most important concepts underpinning the world's governance institutions. The theory dates to Bodin in the 16th century (Grimm, 2015), although after centuries of empires, colonialist expansion, and wars of territorial aggression its realization as a principle of international organization did not actually occur until the end of World War 2 (Jackson, 1999).

There is a direct connection between the concept of sovereignty and the theory of the state. If one accepts Weber's classic definition of the state as a monopoly on the legitimate use of force, then sovereignty bounds that privileged status to a specific, well-defined territory. Sovereignty as an institution is intended to mitigate anarchy among states by confining them to a defined territory. It assumes that each functioning government is supreme and legitimate in its own space, then applies reciprocal rules of non-intervention and voluntary interaction to each sovereign unit. If Leviathan solves the problem of anarchy domestically, sovereignty is supposed to do the same internationally.

Still, the impact of sovereignty on international order is limited. Anarchy among states is still ever-present and unavoidable. A careful study of the forms and practices of sovereignty led Stephen Krasner (Krasner, 1999) to conclude that sovereignty is best understood as "organized hypocrisy" – a space somewhere between anarchy and institutionalization where rulers adhere to conventional norms of sovereignty when it offers them resources and support and deviate from it when violating them provides benefits.

Even the most traditionalist thinkers about sovereignty realize that a global internet challenges what Krasner called *interdependence sovereignty*, the ability of states to regulate the flow of information, money and goods across their borders. (Betts & Steven, 2011) But a growing number of politicians and security experts seem to think that the appropriate response to this problem is to find new ways to

reassert national borders or embed them in technology. This push comes both from intellectuals and from politicians who want to strengthen their control of communications. Corroborating Krasner's account of 'organized hypocrisy,' the appeal to sovereignty in Internet governance is heard when states stand to benefit from a more controlled internet; but this does not prevent them from exploiting the capabilities of a globalized network for transnational surveillance, economic and military espionage, and the exercise of military power. There is actually little difference between authoritarian states and Western liberal democracies in this regard.

The Case against Sovereignty in cyberspace

Sovereignty in cyberspace is a bankrupt idea that provides no useful solutions to the problems of Internet governance. Below, I make three arguments against it: first, that there are other domains where sovereignty is not recognized; second, that the Internet protocol standards create a global commons from which exclusion is extremely difficult; third, that the underlying construct of sovereignty does not make sense in cyberspace.

1. Other global commons

The first and most obvious argument is that there have always been global domains where sovereignty isn't recognized. States have accepted this either because of practical limitations on their control, and/or because it was in their mutual interest to do so. The high seas were long recognized as not subject to sovereign claims, going back to the 17th century. The US Government and other maritime powers have been vigorous advocates of freedom of navigation in the face of excessive jurisdictional claims by other states over ocean space or international passages. The Outer Space Treaty, passed in 1967, banned participants from putting nuclear weapons in space. Article II stated that "outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty... use,...occupation, or by any other means." The point here is not that the examples of

these other domains are perfectly analogous to the case of cyberspace; the point, rather, is simply that a global commons approach is neither unprecedented nor unthinkable and prevails in some very critical domains. In those cases there is general acceptance that sovereignty would not be beneficial as an organizing principle.

2. The Internet protocols create a global commons

The next step in my argument is that the Internet protocols create a virtual space that is a global commons. The basic, incontrovertible fact underlying this claim is that the Internet standards are open and nonproprietary, and the protocols as implemented are open source software. Anyone with the necessary facilities can run the protocols and in legal or practical terms it is virtually impossible to exclude everyone else from using them.

Internet is not a physical layer phenomenon. It exists at Layers 3 (the network layer) and 4 (the transport layer) in the stack, which are both instantiated in software. While physical facilities are necessary to run the software and transmit and store the information that moves over the Internet, as soon as the protocols are running over those facilities, they become part of a nongeographic virtual space where simultaneous action is possible irrespective of location. Data used in real time in one location can be stored on computers far away; and software applications running on a computer in one location can be hosted somewhere else. A single session can draw on multiple sources of code or data in multiple places. Whatever boundaries or limits exist in cyberspace will be defined and maintained primarily by software instructions, and these instructions could come from anywhere. Thus, the oft-repeated claim that the location of the physical facilities supporting cyberspace in some jurisdiction makes it simple and straightforward to apply traditional notions of territorial sovereignty to cyberspace is misguided.

Internet connectivity is not bilateral-international (like air flights or shipping), nor is it territorial with some transnational border-spillover effects (like broadcast signals sent via radio spectrum). The virtual

space created by running the Internet protocols includes every connected entity also running the protocols, unless the AS's through which they enter cyberspace actively block specific domains, addresses or applications. With other access technologies (e.g., a traditional circuit-switched telephone network) the system provides access on a territorial basis, and connections beyond the territory are optional and additive; with cyberspace the default is global, and blockages are optional and subtractive.

It follows that the security and governance problems in cyberspace are not territorial or national; insofar as they can be localized, they revert to the basic operational unit of the Internet, the autonomous system (AS). An AS is defined as a set of routers under a single technical administration, using an interior gateway protocol and common metrics to route packets within its own network, and an exterior gateway protocol to route packets to other ASs (Hawkinson & Bates, 1996). In more colloquial terms, an AS is the name for the 60,000 distinct networks that make up the “network of networks.” They do not conform to national boundaries. Many are transnational in scope, most are subnational. The mismatch between territory and governance is built into the structure of the Internet.

3. There is no monopoly on the legitimate use of force in cyberspace.

Does the theory of the state make sense in cyberspace? To ask this is to ask whether anyone has, or ever could have, a monopoly on the legitimate use of cyber-force, and if so, how that supremacy and legitimacy could be bounded. It is difficult to imagine how a globally compatible internet is consistent with both territorial boundedness and accepted legitimacy. The possibility of coercive use of cyber capabilities exists wherever the Internet protocols are in use, wherever one can acquire the equipment and software resources to mount a DDoS attack, code an exploit, generate a phishing email and so on. Given the existence of global connectivity and instantaneous action across national boundaries, there is no relevant distinction between state actors and nonstate actors, except in the special case when a cyber-attacker and all victims happen to be in the territory of a single state. In the transnational context,

states and criminals do the same kinds of attacks and use the same techniques. Neither one has a monopoly; neither one has legitimacy.

Assume for a moment that some entity can, somehow, monopolize cyber-force and gain general legitimacy in its use. In a globally compatible cyberspace, how could such a capability be contained in a geographic territory? It would have to be a global monopoly, a global cyber-sovereign.

Objections

Two objections are frequently heard when I characterize cyberspace as a commons, or critique sovereignty in cyberspace.

1. Internet services and facilities are not a commons

Perhaps the biggest sticking point for the global commons proposition is the obvious fact that many Internet services and facilities are private goods. They are organized not as commons, but by contract and/or the exchange of property rights in markets. The owners of these private goods can and do exclude others from access to resources and services unless a payment is made.

This objection, however, confuses the private goods and services *enabled by Internet connectivity* with the *common cyberspace* in which they function. On the Internet, property and commons co-exist, as they do in almost all economies. A public street enables private commerce in the private shops along the road; a common language facilitates private commerce amongst the speakers or writers of that language; the appropriation rules governing a common pool fishery (to invoke Ostrom again) enable private markets for the fish that appropriators take from the common pool. In just the same way, the open and nonproprietary Internet protocols enable private commerce in online goods and services among the people, places and things joined together in the commons. The protocols are non-rival in use and no user can exclude any other user from implementing them. But many facilities and services

interconnected through these protocols are private goods, their value is highly dependent on the existence of the common space.

It is hard to understand why this distinction has acted as such a barrier to the recognition of cyberspace as a commons. The parallel to other common spaces is obvious. Space satellites are physical objects owned by a specific company or country, and the services they provide (e.g., video broadcasts) can be exclusive private goods. But the satellite-using world has no problem recognizing outer space as a commons and governing it as such. Ships are physical, owned private goods, and are registered under a sovereign jurisdiction; but the sea is recognized as a commons. Cyberspace should not be confused with the objects that occupy it and the private services that function within it.

2. Aren't states asserting their sovereignty?

Another common objection is that states are already asserting and creating sovereignty over cyberspace, so the whole issue is settled. Here again, the argument for sovereignty rests on overlooking important distinctions. In this case, state sovereignty over cyberspace is being conflated with the ability of states to regulate the way people or things subject to their authority access or use global cyberspace. Of course, states can and do regulate service providers and users. But there is no “national cyberspace” over which they exercise supreme control; rather, there is a shared global cyberspace, and they leverage their sovereignty over actors and devices in their territory to restrict connections to certain sites or applications. But this happens in an imperfect and limited way. Anyone in their territory who runs the Internet protocols are still “in” the global commons. States can only identify and block access after the fact, because they are not in control of who joins cyberspace or what goes on there. As noted above, efforts to assert jurisdiction are creating numerous extraterritorial effects and compatibility problems precisely because they try to insert territory into a global virtual space. There is a distinction between exercising control over access to cyberspace and exercising sovereignty over cyberspace *per se* .

What difference does it make?

What happens if we abandon notions of sovereignty in cyberspace? What changes? There is no contention here that such a move would magically solve most Internet governance problems. It is, rather, an attempt to gain acceptance of a basic reality – a *principle* in regime-theoretic terms – that provides a foundation for appropriate forms of governance going forward. Such a recognition matters because its acceptance would mitigate inter-state conflict, shift the criteria for decision making, and redistribute power among decision makers.

Clearly, it would be undesirable for the US or any other country to assert sovereignty over outer space or the high seas. Control over these vital shared spaces could only be maintained via constant military conflict. Turning away from sovereignty requires states to recognize their (and their societies') co-existence in a shared space. Rather than justifying their actions through assertions of absolute authority over distinct "pieces" of cyberspace – a goal which will never be attainable – states would be led to participate in some form of joint governance.

In questions of policy and governance, a global commons approach elevates the value of connectivity and compatibility relative to other goals. It highlights the global public's interest in an interconnected and open information and communication environment. It calls attention to the value of freedom of action and permissionless innovation, both of which enhance liberty and foster economic and technological development. Assertions of national sovereignty, on the other hand, devalue these features and elevate national restrictions and control.

Whereas sovereignty makes states supreme authorities, governance of a global commons is rooted in the community involved, a community which is transnational. Such an approach strengthens the hand of nonstate actors. It does not, of course, eliminate states' coercive power or their political incentives to

engage in alignment. But it does help to contain it, to limit its scope. It makes it clear that states cannot and should not have the kind of authority over cyberspace that some of them are seeking.

Reconciling sovereignty and Internet governance

Whatever governance regime we settle upon in cyberspace must take state power and the realities of military conflict among states into account. But does this mean we are doomed to revert to the territorially fragmented governance of a sovereignty-based model? Or can some way be found to reconcile the two?

Nobel Laureate Ostrom emphasized the ability of communities to develop self-governing institutions that need not be based on the hierarchical authority of states. As we have seen, self-governance by a transnational Internet community is both possible, and already exists in several key areas. The problem with the self-governance approach in global affairs, however is that it intersects with the organized violence of states and their military rivalries. Most of the Ostrom literature on self-governance has assumed that self-governance takes place within a context of civil order, which assumes an authority with a monopoly on the legitimate use of force somewhere in the background.

Going forward, the pressing question for Internet governance is how to keep state power bounded by territory while at the same time freeing the producers and users of cyberspace to govern themselves. The territorial civil order established by states must be used as a foundation for transnational civil governance of cyberspace.

References

Barlow, J. P. (1996). Declaration of the Independence of Cyberspace. Retrieved from https://www.eff.org/cyberspace-independence

Betts, D. J., & Steven, T. (2011). *Cyberspace and the State: Towards and Strategy for Cyber Power*. Oxford: Routledge.

Grimm, D. (2015). *Sovereignty: The Origin and Future of a Political and Legal Concept* (B. Cooper, Trans.). New York: Columbia University Press.

Hardy, I. T. (1994). The Proper Legal Regime for 'Cyberspace'. *University of Pittsburgh Law Review, 55*.

Hawkinson, J., & Bates, T. (1996). Guidelines for creation, selection, and registration of an Autonomous System (AS) (Vol. RFC 1930). United States: The Internet Society.

Jackson, R. (1999). Sovereignty in World Politics: a Glance at the Conceptual and Historical Landscape. *Political Studies, 47*, 431-456.

Johnson, D. R., & Post, D. (1996). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review, 48*(Journal Article), 1367.

Johnson, D. R., & Post, D. (1997). And How Shall the Net Be Governed?: A Meditation on the Relative Virtues of Decentralized, Emergent Law. In B. Kahin & J. H. Keller (Eds.), *Coordinating the Internet* (pp. 62-91). Cambridge, Mass.: MIT Press.

Krasner, S. D. (1999). *Sovereignty: Organized Hypocrisy*. Princeton: Princeton University Press.

Mueller, M. L. (2010). Critical resource: An institutional economics of the Internet addressing-routing space. *Telecommunications Policy, 34*(8), 405-416.

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

Ostrom, E. (2005). *Understanding Institutional Diversity*. Princeton, NJ: Princeton University.

Strickling, L., & Hill, J. F. (2017). Multi-stakeholder internet governance: successes and opportunities. *Journal of Cyber Policy, 2*(3), 296-317.

WSIS. (2005). *Tunis Agenda for the Information Society*. (WSIS-05/TUNIS/DOC/6(Rev. 1)-E). Geneva: United Nations.