Sovereignty and Cyberspace: Institutions and Internet governance

Dr. Milton Mueller, Professor, Georgia Institute of Technology School of Public Policy

This essay is derived from the 5th Annual Vincent and Elinor Ostrom Memorial Lecture, given at the University of Indiana October 3rd 2018.

1. Opening

We have been debating the relation between sovereignty and cyberspace from the very beginning of the Internet's debut as a mass medium. We went from "Internet is sovereign" and exceptional (John Perry Barlow, Johnson & Post) to the idea that cyberspace needs to be re-nationalized and subordinated to state authority. The ongoing battle over multistakeholder vs. multilateral governance was – and is – really a battle about sovereignty. Unrecognized in this battle is the tremendous relevance of the Ostrom's work. Internet governance is and always has been about institutional innovation in the face of new technology.

2. Background

By way of background my interest in Internet governance started in the 1980s, when I became fascinated by telecommunications policy. The breakup of AT&T – at the time the world's largest company and one of the most powerful – struck me as something of epochal significance. Changes in information technology were associated with transformation of industry, law and regulation. Though I didn't have the vocabulary or the theory yet, what really interested me was the relationship between information and communications technology, institutions and institutional change. I was fascinated by new resource domains created by technology (such as radio spectrum) and the way governance by competitive markets was replacing monopolies and hierarchical command and control relations.

By 1996, however, telecommunications policy had become boring to me. The main institutional changes had taken place. We broke up the phone company and introduced competition. Most of the world's developed economies abandoned PTT monopolies, vastly expanding access and lowering prices for millions. Spectrum markets went from being an idea literally dismissed as crazy to a routine process raising billions of dollars in auctions. We had a new telecom law in the US (the Telecommunications Act of 1996). We had new free trade agreements in IT equipment and basic telecom services. Little did we know that telecom liberalization was paving the way for another, even more transformative change.

3. Internet as change agent

That of course was the internet, which flourished in the new environment. The techno-economic characteristics of the Internet were radically different from telecommunications. Entirely new common pool resource spaces, such as domain names and IP addresses, were developing around it. New cooperative and market relations were forming around routing and Internet Service Provider peering and interconnection arrangements. Far from reforming pre-existing governance structures or

institutions, we were generating new bottom up governance mechanisms around a new transnational community.

Mainstream telecom economists didn't understand the economics underlying Internet resources and connectivity very well. Mainstream political scientists and IR scholars, who had their eyes glued on traditional state actors and multilateral regimes, were completely ignorant of the organically evolved institutions that the Internet community was developing.

So around 1994 – 1998, as the Internet transitioned into a major, economically significant global medium, we were confronted with the need for institutional development and innovation on a global scale. That attracted my attention.

4. The problem of misalignment

What was it about Internet governance that was – and still is – so problematic? I think the answer is quite simple. It is what I call the problem of misalignment. The mismatch between the transnational space for societal interaction created by the internet and the territorial jurisdictions of national governments. The Internet joins the world of governance into a single space; sovereignty fragments it into 200 pieces. As it came to be used by billions of people and deeply embedded in our society, all kinds of novel conflicts and disputes arose that required rules, order, and governance. Some of these problems could be addressed by existing national regulatory institutions. But many could not be.

5. Internet governance

Let's take a quick tour of the institutional innovations the Internet has led to.

- The **Internet Engineering Task Force** (IETF), which formed in the mid-1980s, was a genuinely new organizational form that evolved out of informal meetings of the computer scientists and network engineers who developed the protocols. It was the world's first large-scale open source software development community. The IETF did not sell its standards documents, it published them freely online. It was composed of individuals, not formal members who represented states or corporations. Participation was open, and its standards were voluntary.
- **Internet address registries.** Internet Protocol 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. 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 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. The need for governance of the DNS root prompted the creation of ICANN, a global, private sector regime based on contract.
- **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 Border Gateway Protocol (BGP), and contractual and cooperative arrangements amongst private sector network operators.

These governance institutions formed outside national legal and regulatory regimes. They were transnational and rooted in private actors. It's common to characterize this as the "Multi-stakeholder" model, but I will ask you to forget about that rhetoric. The key feature is not the presence of multiple stakeholders. It is the supremacy of the nonstate actor, as the problem of global governance was solved by transcending national governance mechanisms and relying on self-governance of transnational communities.

In the areas of Internet governance discussed above, compatibility and connectivity are the prime directives; there is a Nash equilibrium on cooperation. But other areas of Internet governance do not so easily equilibrate globally. These are the areas where articulation with territorial states has become problematic:

- Content regulation
- Cybercrime
- Privacy and data protection (GDPR)
- Cybersecurity

Of these, the most troublesome is the intersection of cybersecurity with national security. Cybersecurity is no longer just about the security of internet users and resources. It has invokes military powers and conflicts among states. It is this that has fueled the calls for sovereignty in cyberspace.

6. Alignment

These problems have given rise to what I call *alignment*, an attempts to push global cyberspace into a shape recognizable to the territorial state. Alignment takes the following forms.

- Bordering and controlling Internet content through blocking and filtering access to services, usually enforced through control of national telecommunications infrastructure
- Data localization - the practice of limiting storage, movement and/or processing of data to specific geographies. As examples:
    - Vietnam's Ministry of Public Security's cyber security legislation requires all foreign online service providers to store data of citizens exclusively in local data centers
    - The Brazilian Central Bank has proposed cybersecurity regulations that prohibit financial institutions from using foreign data processing and cloud computing services
    - Belgium, Denmark, Germany, UK and Finland all require companies to store commercial data locally
    - In Sweden companies are required to store information locally to share it with authorities who have interpreted a requirement to provide "immediate access" as meaning physical access to servers
    - China's National Security and cybersecurity Laws limit operation of "Critical Internet Infrastructure" to mainland China; impose local data storage requirements on operators, and impose broad restrictions on outgoing data

- Mistrust of foreign equipment and software service providers
    - Despite the absence of any evidence of spying, US intelligence agencies succeeded in driving Chinese equipment manufacturer Huawei out of the U.S. market.
    - Similar concerns led the Defense and Homeland Security Departments to expel Kaspersky software from their agencies.
    - Snowden uncovered evidence of NSA intercepting and putting implants into US equipment being exported to foreign countries.
- Restrictions on the flow of foreign investment
    - The Committee on Foreign Investment in the US (CFIUS) has targeted incoming Chinese investment in various high tech industries.
    - The Chinese are even more restrictive, imposing strict foreign ownership limits on cloud and other information services.
- Jurisdictional competition over privacy and data protection laws.
    - Unlike alignment efforts, Europe's General Data Protection Regulation (GDPR) was specifically designed to have extraterritorial and even global effects. But retaliatory responses from the US might start creating islands of alternative sets of rules.

The battle between global access and state alignment is the main problem in Internet governance right now. And as I've written in my latest book, that conflict is all about sovereignty in cyberspace.

7. The theory of sovereignty

The principle of state sovereignty is one of the most important concepts underpinning the world's governance institutions. The theory dates back to Bodin in the 16th century (practice is much more recent). Yet one will search the canons of the institutionalist literature (Ostrom, North, Knight, Bates) for an extended discussion, of sovereignty. There is some attention paid to the state, its origins and its functions. But though Vince Ostrom did address it in some early papers from the mid-1980s, sovereignty – the institution that regulates the relations among states – is largely absent from the discussion.

Weber defined the state as a monopoly on the legitimate use of force. Sovereignty bounds that legitimate use of force to a specific territory. As an institution, it is intended to mitigate anarchy among states, to regulate the effects of these monopolies on violence by confining them to a defined territory that doesn't overlap with any others. If Leviathan solves the problem of anarchy domestically, in other words, sovereignty is supposed to do the same internationally. It assumes that each functioning government is legitimate in its own territory, then applies reciprocal rules of non-intervention and voluntary interaction to each sovereign unit. Though this is often called the "Westphalian" system, it took us 300 years after the Peace of Westphalia to come anywhere close to that structure.

Even so, the impact is limited. Anarchy among states is still a reality. A careful study of the forms and practices of sovereignty led Stephen Krasner 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 them when it provides benefits.

8. Sovereignty in cyberspace?

There is now a growing trend to think that the problems of Internet governance justify a turn towards sovereignty. The push comes both from intellectuals and from the pursuit of political self-interest by some major states, notably Russia and China. I want to challenge the case for sovereignty in cyberspace on both practical and intellectual grounds. Sovereignty in cyberspace could only be achieved by sacrificing most of what makes the Internet valuable. It is not quite impossible, but certainly undesirable. I make three arguments against it: 1) that there are domains where sovereignty doesn't belong; 2) that the Internet protocols create a global commons and a non-territorial virtual space; 3) there is no monopoly on the legitimate use of force in cyberspace.

1) The high seas have long been recognized as not subject to sovereign claims. The US Government and other maritime powers have advocated of freedom of navigation in the face of what they have regarded as excessive claims by other states of jurisdiction over ocean space or international passages. The Outer Space Treaty, passed in 1967, banned participants from putting nuclear weapons in space and in 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 that a global commons approach is neither unprecedented nor unthinkable and prevails in some very critical domains.

2) The Internet protocols create a global commons. They are open source, non-exclusive and non-proprietary. Anyone can implement them. They allow for a practically unlimited number of networks (standard allows for 3.7 billion Autonomous System (AS) numbers). When implemented, the Internet protocols create a non-territorial virtual space. It is a network of networks the boundaries of which are autonomous systems, not geographic territories. An AS is not a physical layer phenomenon. It exists at Layers 3 (the network layer) and 4 (the transport layer), 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 Internet protocols are running over those physical facilities, they become part of a non-geographic virtual space. Whatever boundaries or limits exist in cyberspace will be defined and maintained primarily by software instructions, and these instructions could come from anywhere.

3) Does the theory of the state make sense in cyberspace? The security problem in cyberspace is not territorial or national; it embraces the entire virtual arena. Data packets can contain threats regardless of whether they come from inside or outside a country's borders. Packets that come from inside the borders can be generated by agents outside the borders if they are able to control domestic computers. Threats, intrusions and malware can and do come from anywhere in the world. It is the AS boundary and the security of information assets – not jurisdictional boundaries – that matter.

In this environment, does anyone have a monopoly on the legitimate use of cyber-force? The answer seems clear: no. Once you are dealing with global connectivity and instantaneous and invisible action across network boundaries, there is no relevant distinction between state actors and nonstate actors. Neither one has a monopoly, neither one has legitimacy. State actors and criminals do the same kinds of attacks, use the same techniques. If a cyber-attacker and all her victims happen to be in the territory of a single state, then yes, the normal rule of law applies. The aggressor can be identified, arrested, prosecuted. But with transnational actors it is difficult to maintain any distinction; there are no

legitimate state actors and illegitimate private actors, there are only attackers and defenders, adversaries and victims.

Let's assume for a moment that some unknown entity can, somehow, monopolize cyber-force and gain general legitimacy in its use. How could such a capability be contained in a geographic territory? How, in a globally compatible cyberspace? It could not be; it would have to be a global monopoly, a global sovereign.

9. Common objections to the commons

When I advance these arguments against sovereignty in cyberspace and characterize it as a global commons, I often hear the following objections.

- The Internet isn't a commons

The most common objection is that most Internet services and facilities are private goods. They are organized not as commons, but through contracts 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 while many of the facilities and services interconnected through these protocols are private goods, their value is highly dependent on the existence of the common space.

- Aren't states asserting their sovereignty?

Others object that the issue is settled. States are already creating sovereignty by asserting their power over domestic facilities and residents' use of the Internet. But this objection also misses a crucial distinction. 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. This kind of control is imperfect and limited. States can only identify and block things after the fact, because they are not in control of who joins cyberspace outside of their territory. In short, states cannot assert sovereignty over, or in, cyberspace; they can only regulate the way people (or things) subject to their authority access or use global cyberspace. This distinction may sound weak, but it exists and it is important. A country's ability to control the building, ownership or launch of satellites, for example, does not mean it has sovereignty over outer space, nor does its ability to license ships and regulate their access to its harbors mean that they have sovereignty over the seas.

10. What difference does it make?

What happens if we abandon notions of sovereignty in cyberspace? What changes, what benefits accrue? While it's not a panacea for all the problems of Internet governance, I see three potential effects: 1) mitigation of inter-state conflict; 2) shifts in the decision making criteria for global governance of cyberspace; and 3) a shift in the relative power of key decision makers.

1) I think we can all understand how undesirable it would be if the US or any other country asserted sovereignty over outer space or the seas. Such a claim could only be maintained via constant military conflict. Rather than searching for justification of their actions through assertions of their absolute authority over distinct "pieces" of the world, turning away from sovereignty requires states to recognize their co-existence in cyberspace – not only with other states, but more importantly with business and civil society.

2) A global commons concept elevates the value of connectivity and compatibility relative to other goals. It articulates the global Internet-using public's interest in an interconnected and open space. It affirms the importance of freedom of action and permissionless innovation in cyberspace, both of which enhance human rights and foster economic and technological development.

3) Finally, a non-sovereign approach gives states and private actors the same status. Both are equal status inhabitants and creators of the space; a state has no special status – it is just another network operator and user group. When generally applicable cyberspace governance is needed, it must arise through cooperation at the global or transnational level amongst all relevant stakeholders. Such an approach strengthens the hand of civil society and private sector actors. At the same time, it does not interfere with purely domestic regulatory efforts by states. Even if a commons model does not automatically eliminate states' political incentives to engage in alignment, it helps to contain it, limit its scope. Its acceptance as a norm makes it clear that states cannot and should not have the kind of authority over cyberspace that many of them are seeking.

11. Reconciling sovereignty and Internet governance

Nobel Laureate Elinor 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 in many respects already exists.

Most of the Ostrom literature, however, has assumed that cooperation and self-governance take place within a context of civil order, which assumes an authority with a monopoly on the legitimate use of force somewhere in the background. The problem with extending that approach to international affairs, however, is that we are dealing with an anarchic system, the inevitable and dangerous friction caused by states' incomplete monopoly on violence. 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?

I think we can, but here I leave you with questions that frame the problem rather than definitive answers. How do we keep state control bounded by territory while at the same time freeing the producers and users of global cyberspace to govern themselves? How can we use the territorial civil

order established by states as a foundation for transnational civil governance of cyberspace? How can we de-militarize and de-nationalize cyberspace?