Contested Governance: Internet Governance and Cybersecurity

Tim Maurer

Internet governance is bit of an odd duck in the context of global governance. Over the past twenty years, the internet has become the platform for the global economy and the Achilles' heel of many states' national security apparatuses. Yet, governments have played and continue to play a surprisingly small part in the governance of the internet as compared to other areas of similar importance.

INTERNET GOVERNANCE

To start, it is helpful to distinguish between the governance of the internet and governance on the internet, or, put differently, how the internet is designed and what it is used for.[1] Illustrating the former are the many standard-setting bodies, such as the Internet Engineering Task Force, with (mostly nongovernmental) technical experts developing and deciding—through "rough consensus"—the protocols that run the internet.[2] An example of the latter is the growing number of heads of state calling on social media companies to do more to tackle the spread of extremist content and disinformation.[3] In addition, it is worth mentioning that the scholarship on internet governance sometimes exhibits a normative undertone promoting, explicitly or implicitly, multistakeholderism—the notion that nongovernmental actors, such as private companies and civil society organizations, are recognized as equal partners to governments in the transnational governance of the internet.

How important actors other than governments are in the context of internet governance becomes clear when considering the language of the 2005 outcome document of the World Summit on the Information Society (WSIS) that took place under the auspices of the United Nations. The WSIS 2005 Tunis Agenda for the Information Society states: "Internet governance is the development and application by governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the internet."[4]

This passage is remarkable in the broader context of global governance, especially for an outcome document of a UN summit. Governments are not referred to as being at the top of a hierarchy compared to all other actors when it comes to governing the internet.

The term *multistakeholderism* framed and gave a name to this specific mode for how the internet is governed, with governments not in the driver's seat but as part of a broader ecosystem of actors that have influential and decisive roles. This multistakeholder approach has since become a rallying cry for internet governance activists and governments that try to push back against those states promoting the traditional intergovernmental, top-down governance model.

Putting WSIS in the broader context of trends in global governance, it is worth noting that WSIS was one of the last in a series of world summits that the United Nations convened starting in the early 1990s. With the end of the Cold War, space opened for innovations in global governance beyond the

intergovernmental, often hard law treaty–based, and bureaucratized mechanisms that were characteristic of much of the past years of the century. The multistakeholderism of internet governance that emerged is essentially the latest step in a broader evolutionary trend that ranged from subtle shifts, such as humanitarian assistance being provided with the consent instead of at the request of the host state, to new organizational forms such as the Financial Action Task Force.[5]

The modern internet's global proliferation coincided with this broader systemic change in international relations. The internet's worldwide expansion truly started after 1994, when legal restrictions in the United States for its commercial use were removed. Even more than before, companies subsequently drove the technology's evolution, building the infrastructure such as undersea cables and internet exchange points to connect more countries and people while adding more applications for the technology itself. The dot-com boom of the late 1990s was an early indication of how important the internet would become for the global economy.

CYBERSECURITY

By the late 1990s, the most technologically advanced states also realized that the internet could be exploited for political and military purposes. Intelligence agencies were the first to recognize the potential of the new technology. Militaries soon followed suit, when increasingly more devices became connected to the network and hackers moved beyond stealing data. In 2010, news about the Stuxnet malware having infected the Iranian nuclear facility in Natanz revealed to the world how hacking had moved from script kiddies into one of the most sensitive and consequential tools of international affairs. Edward Snowden's actions in 2013 shed light on the extensive scope of the intelligence complex that the internet has enabled. More broadly, it also shed light on some of the most secret yet most important governance structures in the security field, namely the Five Eyes Agreement.[6]

As the security dimension of the internet's use became apparent, sovereignty and the role of the nation-state witnessed a resurgence. States such as China, Iran, and Russia started pushing back against the emerging governance structures for the internet. This included Russia's proposal for an international treaty on information security in the late 1990s and its joint effort with China to push for a greater role by intergovernmental organizations, namely the International Telecommunications Union and the United Nations, generally for policy processes relating to the internet. Other countries such as India, Brazil, and South Africa resisted taking a specific position on these issues for many years, but Brazil publicly endorsed the multistakeholder approach at the Multistakeholder Meeting on the Future of Internet Governance (NETmundial) in 2014, and India followed suit in 2015.[7] Ultimately, discussions about internet governance and cybersecurity are in many ways part of the broader discussion about sovereignty, its limits in the twenty-first century, and the role of the United States and democracies in the world.

At the same time, the picture is more nuanced among Western governments as well. The U.S. government has made the promotion of the multistakeholder approach a central talking point for any meeting on internet policy. In fact, it even agreed to relinquish its role as principal in the contractual principal-agent relationship with the Internet Corporation for Assigned Names and Numbers and, in 2016, the U.S. Department of Commerce transitioned the Internet Assigned Numbers Authority to a global multistakeholder body.[8] On the other hand, the U.S. Department of State has also drawn a clear line and considers the discussions on the internet's implications for international peace and security in

the UN General Assembly First Committee to be a discussion exclusive to states despite calls from other actors such as Microsoft for a seat at the table.[9]

UNCERTAIN OUTCOMES

The best way to describe the status quo of internet governance and cybersecurity is therefore as contested governance. The roles and responsibilities of the actors involved remain unclear and hotly contested. The past decade has witnessed a resurgence of the nation-state and the concept of sovereignty. The discussion is part of a broader geopolitical battle but also reveals that how to govern this technology remains a challenge for liberal democracies. The broader trend is certainly moving toward more informal industry codes, best practices, and soft law. At the same time, questions of accountability, effectiveness at scale, and legitimacy loom large. Participation by the global south in various bodies remains low and dependent on resources. And many more informal entities face the question of how to avoid being captured by the most powerful, the wealthiest, or the loudest. How resilient the existing governance mechanism will prove depends on the outcome of these different dynamics in the coming years.

Finally, much like the concept of multistakeholderism that emerged in the specific context of internet governance but as an extension of innovations in other global governance areas, an open question remains whether this concept might spill over into other governance areas in which nonstate actors play similarly influential roles.

ENDNOTES

1. This distinction has become a standard differentiation in the field. See, for example: Bertrand de La Chapelle and Paul Fehlinger, "What Do We All Mean by 'Roadmap to Further Evolve the Multistakeholder Internet Governance Ecosystem'?," http://content.netmundial.br/contribution/what-do-we-all-mean-by-roadmap-to-further-evolve-the-multistakeholder-internet-governance-ecosystem/250.
2. Paul Hoffman, ed., "The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force," 2012, http://ietf.org/tao.html.
3. "G7 Puts Pressure on Internet Firms to Remove Extremist Content," Reuters, May 26, 2017, http://reuters.com/article/us-g7-summit-terrorism-idUSKBN18M259.
4. "Tunis Agenda for the Information Society," World Summit on the Information Society, November 18, 2015, http://itu.int/net/wsis/docs2/tunis/off/6rev1.html.
5. "Strengthening of the Coordination of Humanitarian Emergency Assistance of the United States," United Nations General Assembly, December 19, 1991, http://un.org/documents/ga/res/46/a46r182.htm.
6. The Five Eyes agreement itself is a fascinating example of an informal, soft law–based institution.
7. Hannes Ebert and Tim Maurer, "Contested Cyberspace and Rising Powers," *Third World Quarterly* 34, no. 6 (2013): 1054–1074; "NETmundial," May 20, 2014, http://netmundial.br; "Indian Government Declares Support for Multistakeholder Model of Governance at ICANN53," ICANN, June 22, 2015, http://icann.org/resources/press-material/release-2015-06-22-en.
8. The U.S. Department of Commerce is now also starting to apply the concept of multistakeholderism to its domestic policymaking processes. See "Multistakeholder Process: Cybersecurity Vulnerabilities," National Telecommunications and Information Administration, http://ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.
9. Brad Smith, "The Need for a Digital Geneva Convention," Microsoft on the Issues, February 14, 2017, http://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention.