

Worldwide governance of the Internet at the crossroads

Julien Nocetti,

Institut Français des Relations Internationales (IFRI)

Abstract:

Fiercely disputed because it crystallizes a myriad of issues, complex and protean, Internet governance stands at the crossroads. The confrontation between the geoeconomy and geopolitics has, till now, hampered the development of an international regulation of the Internet (other than a technical one). The vast issue of governance overlaps with another major issue: the new balance of power in the world.

Given the shifting geopolitics of digital technology, Internet governance has special importance.¹ As it has become more and more strategically important, the digital economy figured, for a while, at the top of the international agenda. Governance of the Internet has often been confused with, or likened to, control over this network of networks — a power struggle in which some governments have been trying to gain control of “critical resources” (such as the naming and address system, routing or the design of protocols and technical standards). Edward Snowden’s revelations in June 2013 about the scope of the programs that the US administration has developed for surveillance on the Internet cast a “geopolitical” light on this governance. They have also raised questions about the preeminence, since the Net’s origins, of US institutions and organizations in this governance.

In 2018, Internet governance stands at the crossroads. It will remain a subject of international discord if the necessary shift toward more pluralism and transparency is not made, and if an awareness does not emerge about the changing uses of digital technology. Meanwhile, specific issues — the governance of data, cybersecurity or breakthrough techniques (cryptocurrencies, artificial intelligence) — have reached the top of the international agenda on problem areas in digital technology.

“Governing” the Internet: Definitely, but how?

Given that the Internet has become a major issue in international affairs, it is a daunting task to conceptualize its governance. This task has several aspects for academics specialized on international relations. A major one is that we ought to move beyond the traditional framework used to analyze relations between nation-states — even more so since the current model of Internet governance has come out of an original process (multistakeholderism) involving industry, engineering bodies, governments and “civil society” (MASSIT-FOLLÉA 2014).

Many misunderstandings and controversies arise out of uncertainty about the role and place of national governments in Internet governance. For those observers who see digital technology as an additional field in state-based international relations, digital sovereignty, since it is but a variant of sovereignty, is a topic for the big powers to argue about during international meetings. The

¹ This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor’s approval, completed a few bibliographical references.

proponents of this approach often differ with the consensus view that sees globalization and the Internet as weakening the state's power to regulate the economy (DREZNER 2004). In contrast, other pundits claim that digital technology has radically altered the international system, since the Internet has diffused at an astonishing speed throughout all layers of society. For them, the first approach exaggerates the sway of national governments over Internet governance; and some of these pundits go so far as to deny the existence of Internet governance as such (VAN EETEN & MUELLER 2013). During the World Summit on the Information Society held in 2005 under the auspices of the United Nations, discussions artificially placed nation-states at the top of the decision-making pyramid.

As for governance in the strict sense of the word, one fact is undeniable: the interests and values borne by the Internet are pluralistic. For some parties, this governance ought to allow for the free play of the marketplace or be left to self-regulation by the technical community, as imagined by the Internet's pioneers, who were libertarians and mostly American. For other parties, the emergence of the Internet as a subject of law implies using proven rules, regulations and policy instruments. However this would amount to overlooking the changes resulting from uses of the Internet, such as the wider possibilities for voicing opinions and for citizen participation. For others, the ultimate source of legitimacy would be the adoption of a treaty on the Internet, which would place governance at the planetary level (as is also the goal for the environment and climate movements).

Internet: A shifting center of gravity

The tensions now surrounding Internet governance did not originate in the Snowden affair. They reflect the asymmetry between the very strong expansion of the access to digital technology in emerging economies and the inherently Western nature of the systems that coordinate the Net's activities. More than three billion people are now connected to the Internet, approximately 40% of the planet's population according to the statistics of the UN's International Telecommunications Union (ITU). The center of gravity is shifting eastwards and southwards: nearly 75% of cybernauts live outside the West, a percentage that will increase substantially in the coming years. A simple statistic is telling: at the end of 2017, there were more cybernauts in China (772 million) than in the United States and European Union combined (745 million).²

When the context allows, the Internet lends itself to being a sounding board of the anti-American rhetoric of leaders from the so-called emerging powers. Countries like China, Russia, sometimes India, and certain Arab lands have recurrently objected to the key place held internationally by standardization organizations that are, according to them, concentrated in the hands of the United States alone.

Everything has to change for nothing to change

Often criticized for its lack of representativeness and transparency and for its ongoing connections with the US Department of Commerce, ICANN (Internet Corporation for Assigned Names and Numbers) has long been the subject of many a debate about Internet governance. It has even crystallized, sometimes exaggeratedly so, the complaints formulated about it. US authorities announced in March 2014 the "transitioning" of IANA functions (Internet Assigned Numbers Authority managed under contract by ICANN). In the autumn of 2016 — anonymously while the presidential election was in full swing in the United States — this process put an end to ICANN's

² The author's calculations using data from www.internetworldstats.com on 14 September 2018.

oversight of root zone management in the Domain Name System (DNS), the attribution of IP addresses and the maintenance of protocols by the Internet Engineering Task Force (IETF).

Shifting its focus back on techniques following a period of intense politicization, Internet governance has fostered a “decentralization” (symbolized by the reform under way at ICANN), even as it remains in the economic and cultural orbit of the United States. Meanwhile, major events have affected less this governance than nearly all other fields of digital technology. In a way, the question of governance has been overshadowed by the upsurge of problems perceived to be more economically and politically important (such as the manipulation of news and information, the role of economic monopolies). Another new event was Donald Trump’s election as president of the United States. His dismantling of the Obama legacy in matters related to digital technology and his ambivalent relations with Silicon Valley (NOCETTI 2017a) have diluted his country’s message about Internet freedom. US policy used to form a doctrine, but it was discredited under Obama (owing to the Snowden affair) and has now been deprived of consistency since Donald Trump’s inauguration.

A consequence of these events is that what is being said about Internet governance has changed. This governance must address several weighty issues, which follow major lines in international politics.

The challenge of an alternative model

The first challenge comes from a proposal that competes with the traditional multistakeholder model. Authoritarian governments, as in China or Russia, see the free circulation of information as a menace to their survival. Arguing that the state’s interests legitimately override all others, Peking and Moscow advocate an Internet governance based on national sovereignty and security. Their demands with regard to Internet governance often serve to justify tighter domestic controls (NOCETTI 2015). Since their model has limited attraction in UN bodies and agencies (the General Assembly, ITU), these countries have turned to other means to defend their view of Internet governance.

For Peking, the Internet, today and tomorrow, requires a custom-made approach to governance. The World Internet Conference (or Wuzhen Summit) — an annual event since 2014 that assembles officials and the heads of global tech firms around the Chinese president — seeks to legitimate the Chinese view of cyberspace and justify the international standards that Peking wants. It also tries to show that the planet’s technological center of gravity has shifted. In October 2017, the discussions between Xi Jinping, Mark Zuckerberg and Tim Cook reflected this de-Westernization of international relations (NOCETTI 2018). Furthermore, China is using its economic leverage to attract new allies. A substantial part of its Silk Road project has to do with digital technology. Besides opening railways and seaways for connecting China to Europe and even Africa, it will be possible to transmit electronic data over an optical fiber network. For China, the goal is to control digital infrastructures, in particular the cloud, data centers and undersea cables.

As a consequence, rivalry is mounting on all fronts between the Chinese view and the Western idea of a free, open Internet. Although China and Russia do not always act jointly, they have designed and now defend an alternative form of governance. This is a constant subject in their discourse. The appeal of this alternative view is all the stronger insofar as Western “double standards” have disoriented parties who used to lean toward the Western view.

The end of the age of innocence

A second challenge is directly related to the fact that the libertarian period of Internet governance is drawing to a close. The age of innocence is not ending abruptly, but recent events seem to have accelerated this trend. This trend can be described as the attempt by democratic states to come to grips with the “exceptionalism” of the digital realm, which was supposed to be kept out of the hands of governments so that all its social, economic (and political) promises could be kept as we would be guided toward a glowing future riddled of government.

The multiplication of criminal and terrorist uses of digital technology has put innocence down. These uses have sparked political arguments, often fiery but seldom satisfactory. Nonetheless, opinions about the Internet have moved beyond the traditional rift between democratic and authoritarian states. In recent years, Western countries (the United Kingdom, France) have adopted very intrusive laws about this technology. These democratic states have realized that an intervention by public authorities in the digital realm is needed to guarantee freedom and openness.

Meanwhile, the view held by Westerners (no longer so clear given their diverging points of view) is confronted with a well-structured alternative. The digital realm does not lie beyond the reach of politics, national and international. Democratic countries have never made it clear that “free and open” does not mean “absence of regulation”, nor that, in a national setting, multistakeholder governance does not imply that civil society and the marketplace carry the same weight in decision-making. This schizophrenia, now evident, has opened a window of opportunity for authoritarian governments, who enjoy referring to Western regulations to justify their own laws for regulating digital platforms.

One or more forms of governance?

A third challenge is to inquire into the very contents of Internet governance. Is it still, in 2018, relevant to talk about “global Internet governance”, given that the stakes and subjects to be addressed are so different? Internet governance is all the harder to define because there is not one but several forms of governance, depending on the issues and subjects. How could a single model of governance handle topics as varied as cybersecurity, technical standards, freedom of speech or the power of big platforms?

Within a few years, the digital realm has been transformed: breakthrough (or increasingly sophisticated) forms of technology (cryptocurrencies, deep learning, etc.) raise new issues for “digital governance” and push into the background the usual issues related to “Internet governance”. Meanwhile, artificial intelligence (AI), for example, is growing fast but is not yet subject to any governance. China and the United States, to the detriment of Europe, are rivaling for the control of this technology. In the case of AI, two shortcomings of Internet governance are to be avoided. First of all, the influence of private businesses should be hampered by ditching an exclusively participatory form of governance for one that is actually pluralistic. Secondly, we should forget the status quo and realize that the planet’s digital and technological center of gravity has inexorably moved toward Asia.

Two other fields (so strategic that international debate about them is intense) have been brought under “governance”. First of all, cybersecurity. Cyberthreats range from economic espionage through political warfare to organized crime. The most serious menaces come from national governments that have no qualms about launching major offensive actions to destabilize and destroy while hiding behind the uncertainty about whom to blame. Major international tensions are crystallizing around this issue, as illustrated by massive, worldwide cyberattacks during 2017. Secondly, the problems related to data (circulation, storage, processing by private businesses and by governments) now compel recognition as a fundamental issue for global Internet governance. The threat represented by the big digital platforms to national sovereignty, though now widely recognized, is no less real.

Conclusion

The most salient issues for Internet governance now lie outside the “hallowed” field of domain names and addressees. Accomplished in a period of two and a half years (2014-2016), the transfer (without major disturbances) of the ANA functions has signaled a “return to techniques” (*i.e.*, a partial depoliticization of the issues related to Internet governance) following a period of international polarization that culminated between the time of the ITU’s meeting in Dubai (2012) and the fallout from the Snowden affair, which continued till into 2014. Tensions between governments, private operators and “civil society” now tend to arise around issues related to cybersecurity or the control of data.

Bibliography

- BHUIYAN A. (2014) *Internet Governance and the Global South: Demand for a New Framework* (New York: Palgrave Macmillan).
- BRAMAN S. (2004) *The Emergent Global Information Policy Regime* (Basingstoke: Palgrave Macmillan).
- BROUSSEAU E., MARZOUKI M. & MÉADEL C. (2012) Editors of *Governance, Regulations and Power on the Internet* (New York: Cambridge University Press).
- DENARDIS L. (2014) *The Global War for Internet Governance* (Yale, CT: Yale University Press).
- DREZNER D. (2004), “The global governance of the Internet: Bringing the state back in”, *Political Science Quarterly*, 119(3), pp. 477-498.
- HANSON F. (2015) *Internet Wars: The Struggle for Power in the 21st Century*, (Habersfield, AU: Longueville).
- JEET SINGH P. (2014) “Global Internet governance: A developing country perspective”, *Third World Resurgence*, 287-288, pp. 15-21.
- MASSIT-FOLLÉA F. (2014) “Internet et les errances du *multistakeholderism*”, *Politique étrangère*, 4, pp. 29-41.
- MCCARTHY D. (2010) “Open networks and the open door: American foreign policy and the narration of the Internet”, *Foreign Policy Analysis*, 7(1), pp. 89-111.
- MUELLER M. (2010) *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: MIT Press).
- MUSIANI F. & POHLE J. (2014) “NETmundial: Only a landmark event if ‘Digital Cold War’ rhetoric abandoned”, *Internet Policy Review*, 3(1), DOI: 10.14763/2014.1.251.
- NOCETTI J. (2014) Editor of *Internet. Une gouvernance inachevée*, special issue of *Politique étrangère*, 4.
- NOCETTI J. (2015) “Contest and conquest: Russia and global Internet governance”, *International Affairs*, 91(1), pp. 111-130.
- NOCETTI J. (2017a) “Trump contre la Silicon Valley, ou l’inverse?” in T. GOMART & L. NARDON, *Trump, un an après. Un monde à l’état de nature?* (Paris: Études de l’IFRI), available at https://www.ifri.org/sites/default/files/atoms/files/ifri_trump_un_an_apres_2017.pdf.
- NOCETTI J. (2017) “Souveraineté et gouvernance mondiale du numérique” in P. TÜRK & C. VALLAR, *La souveraineté numérique. Le concept, les enjeux* (Paris: Mare & Martin).
- NOCETTI J. (2018) “La Chine, superpuissance numérique?” in T. DE MONTBRIAL & D. DAVID, *Ramses 2019* (Paris: Ifri/Dunod).
- OWEN T. (2015) *Disruptive Power: The Crisis of the State in the Digital Age* (Oxford: Oxford University Press).
- POWERS S. & JABLONSKI M. (2015) *The Real Cyber War: The Political Economy of Internet Freedom* (Champaign, IL: University of Illinois Press).

- RADU R., CHENOU J.M. & WEBER R. (2014) Editors of *The Evolution of Global Internet Governance: Principles and Policies in the Making* (Berlin: Springer Verlag).
- SEGAL A. (2013) Editor of *Defending an Open, Global, Secure, and Resilient Internet*, Independent Task Force Report n° 70 (New York: Council on Foreign Relations Press).
- SUSSKIND J. (2018) *Future Politics: Living Together in a World Transformed by Tech* (Oxford: Oxford University Press).
- VAN EETEN M. & MUELLER M. (2013) "Where Is the governance in Internet governance?", *New Media & Society*, 15(5), pp. 720-736.