Séverine Arsène: China, Internet Governance and the Global Public Interest[31]

Making the Internet for the Public Good

Since the end of the 1970s, a widespread belief in the economic, social and political benefits of the "information society" encouraged many countries, including China, to invest massively in the development of telecommunications. Nowadays the internet has become an essential part of daily life for almost half of the world's – and China's – population. It has become a key facilitator in maintaining social networks, finding a job, using public services, accessing useful information, or simply enjoying popular entertainment. Because it is so ubiquitous, there is now a sense that not having access to the internet is a form of exclusion, and some even wonder whether internet access may be considered a human right.

While there is consensus on the general idea that the internet bears a character of public interest, there is much less convergence on the particular implications of this idea. As half of the world's population still does not have internet access, the idea that access is a right is quite problematic, as well as the question of who should bear the costs of universal access, and how to rebalance the uneven distribution of infrastructure, technology, contents and digital literacy. How to regulate activities online is also a matter of controversy, as economic and political interests diverge, as well as normative preferences. This is further complicated by the great number of layers that the internet is composed of, and therefore the great number of actors implicated in making and managing it.

In this chapter I will describe the main components of global internet governance, and highlight some of the questions it raises in terms of global public interest. I will then discuss the increasingly important role China has played in this framework so far and highlight how the Chinese case points to democratic cracks in the current internet governance system.

The concept of internet governance is most often used[32] to refer to the definition of technical standards for the internet and to the management of "critical resources", like the

[31] This article was written in February 2016.

[32] Denardis and Musiani identify six main objects of Internet governance: administration of critical Internet resources such as names and numbers; establishment of Internet technical standards; access and interconnection coordination; cybersecurity governance; policy role of private information intermediaries; architecture-based intellectual property rights enforcement. Laura DeNardis and Francesca Musiani, "Governance by Infrastructure," in Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, and

allocation of IP addresses and domain names. These features require global coordination to ensure interoperability and proper information routing. To manage them, members of the industry, engineers, academics and civil society members crafted ad hoc decision-making organisations. The Internet Engineering Task Force (IETF) is composed of informal working groups, generally coordinated via mailing lists, which collectively develop and validate new technical standards. The members of the World Wide Web Consortium (W3C), generally industry players, software editors or academic institutions, elaborate standards and specifications to guarantee universal interoperability of internet technologies. ICANN, a private not-for-profit corporation based in California, was mandated by the U.S. Department of Commerce to coordinate a global network of institutions dedicated to the allocation of IP addresses and domain names. It pioneered a "multistakeholder" model of governance that includes a variety of actors of the industry, along with civil society and engaged individuals, with a consultative role on the part of states.

Beyond the variety of these set-ups, these institutions share the principle that any interested party should be able to participate in the decision-making process, and each of them takes pride in their openness, transparency and inclusiveness. However the technical nature of the issues, the cost of participation and the complicated voting mechanisms go against these stated principles, and debates tend to take place among rather small communities of experts. ICANN in particular has attracted criticism for its bias towards developed countries and lobbies (in 2012 the decision to launch a global bid for new top-level domain names, like .sport or .paris, was particularly controversial) (DeNardis 2014). In general, although these institutions claim that they work for the interests of all internet users, there has been no real reflection or debate on the definition of a global public interest for the internet.

The industry and service providers also play an important role in internet governance, taken in a larger sense. Their decisions on infrastructure, technology, design, business models, and terms of use, all have a direct impact on internet users' agency, including access to information, privacy, or freedom of speech. For example, Apple and Google's gatekeeper role come under criticism when they refuse to include applications in the App Store and Play Store, for reasons related to contents that they consider inappropriate (like nudity) or politically sensitive (localising drones in Pakistan for example). Being in the hands of private companies, most decisions are taken by a handful of individuals, with

Nanette S. Levinson (eds), The Turn to Infrastructure in Internet Governance, New York: Palgrave Macmillan, 2016, p. 7.

little knowledge or approval of users, and with little possibility to appeal. Despite their claims of acting for the good of humanity (see Google's "do no evil" motto), the great power exercised by these global internet companies lacks transparency and democratic legitimacy. This is detrimental to the companies themselves, as they are confronted with difficult political, ethical, and diplomatic issues that would normally be the responsibility of states.

Faced with increasing concerns regarding cybercrime, like privacy infringement, bullying, scams, traffics, or copyright disputes, states are now paying more attention to all dimensions of internet governance in the name of national public interest and public order. More and more states are therefore passing laws criminalising certain kinds of online activities, enabling the blocking of foreign websites or requesting to host sensitive data on their territories. After revelations by Edward Snowden on the extent of the NSA's global surveillance, and with increased awareness of cybersecurity issues, states have extra motivation to look at the internet through the lens of national interest. As there is a shared concern for the stability and security of the internet, as well as a recognised need to avoid any escalation in potential cyberattacks, cybersecurity is mostly discussed in the framework of intergovernmental dialogue, be it bilateral or multilateral. While this all makes things difficult for industry players who are confronted with multiple and sometimes contradictory regulations, civil society actors warn of a possible "balkanisation" (or in fact localisation) of the internet, which would "kill" the ideal of a global public space.

Global-scale initiatives abound to discuss these issues. In the beginning of the 2000s, the United Nations initiated the World Summit on the Information Society (WSIS) and created the yearly Internet Governance Forum (IGF)[33], with a view to finding a comprehensive, "multistakeholder" framework for internet governance. In 2012, the Dubai summit of the International Telecommunications Union (ITU) was the stage of a showdown between supporters and opponents of a proposal to let the ITU take over more responsibilities over the global internet. The status quo prevailed after a Manichean debate where the issue was framed as opposing a "free" and "open" multistakeholder model with an intergovernmental, United Nations-based framework associated with authoritarian governments. In spring 2014, Brazil launched an initiative called Netmundial[34], where some 700 delegates from governments, the private sector, civil society, the technical community, and academia produced a roadmap for future internet governance, based on the princi-

[33] http://www.intgovforum.org.
[34] https://www.netmundial.org.

ples of multistakeholderism, human rights, transparency and accountability, among others. In their final declaration, participants "recognised that the internet is a global resource which should be managed in the public interest."[35] But these initiatives have borne few concrete results so far, perhaps because of their ambition to tackle internet governance in an all-encompassing, consensual way, thus ignoring the diversity of mechanisms and issues at stake, and shying away from addressing contentious, political issues. Meanwhile, practical decisions on technology, standards, regulation, design, business models, etc. are taken daily by a myriad of actors for whom public interest is but a secondary concern, and with practically no checks and balances in place.

As these political stakes are coming to light, the global balance of power is also changing, with the advent of new powerful actors such as transnational companies that handle the personal data of billions of people, rights-defence organisations and activists, and governments of developing countries. Among these new actors, the emergence of China as a "new cyber power" has increasingly affected discussions of global internet governance, not only because China's internet users constitute about 20% of the world's online population, but also because the Chinese government and businesses have become much more visible and assertive on the global stage.

Chinese Approach to Internet Governance/Sovereignty

In line with global discourses on the "information society", the Chinese authorities have long seen the internet as a key growth engine and as a strategic tool to develop technological, economic, and cultural power. Domestically, the internet also represents the promise of a more modern and wealthy Chinese way of life, which is crucial to respond to the aspirations of the younger generations and thus sustain the Communist Party's legitimacy in power.[36]

In 2010 the Chinese government published a White Paper for the Internet in China, which formulated "cyber sovereignty" as an essential principle to enable China to embrace the internet while containing political risks. With this concept, it claims the right and legitimacy to control online activities in the name of social order and stability, and it calls

[35] For more on these initiatives see Derrick L Cogburn, "The Multiple Logics of Post-Sowden Restructuring of Internet Governance," pp. 25-46, and Nanette S. Levinson and Meryem Marzouki "International Organizations and Global Internet Governance: Interorganizational Architecture," pp. 47-72, in Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson (eds), The Turn to Infrastructure in Internet Governance, New York: Palgrave Macmillan, 2016.

[36] This section is a synthesis based on previously published articles, referenced below.

for an intergovernmental governance framework and the principle of non-interference in the domestic cyber policy of other countries.

The technical and regulatory set-up of the Chinese internet reflects these principles. In the 1990s, while the Chinese government was massively investing in networks all over the country, it also launched the Golden Shield project to develop cutting-edge filtering and blocking technologies aimed at limiting access to foreign websites and at monitoring online public opinion. Since then, licensing rules for internet service providers and content providers, and systematic verification of "real names" on all popular platforms have ensured political caution from companies and users. More recently, Chinese authorities have imposed further constraints on internet businesses, such as mandatory local storage of sensitive data like banking information, interdiction of foreign investment in internet content providers, or, as proposed in a 2016 draft law on the Domain Name System, registration of domain names with a Chinese service provider for China-based websites.

Taken together, these measures show a will to bring internet infrastructure, businesses and critical data on the Chinese territory within the reach of the Chinese authorities. This facilitates information control (for both censorship and surveillance), guarantees better protection against supposed cybersecurity threats, and provides advantages to Chinese businesses. However it does not, I believe, constitute a separate Chinese 'intranet' as is often suggested by metaphors like the "Great Firewall of China". Indeed, despite these control and localisation measures, the Chinese internet is highly interconnected with global infrastructures. For example, Chinese domain names are set up in compliance with ICANN's rules; Chinese internet service providers set up servers around the world for better service to overseas customers; foreign IT companies have branches in China to cater to the Chinese market. Chinese authorities want the best of both worlds, with access to the economic and social benefits of the global internet, and even the capacity to project China's soft power globally, and simultaneously to limit political threats in China. In other words, China has a vested interest in the stability of the global internet infrastructure.

Moreover, the temptation to implement localising measures is not technically a specificity of China. This is part of a strong trend towards more "localisation" of the internet, for a variety of political, legal, cultural and marketing reasons. For instance many countries have also mandated the surveillance and blocking of some content in the name of the protection of citizens, and more and more governments are also calling for a local storage of data out of cybersecurity concerns. Copyright issues also motivate content providers to

limit the availability of cultural products to one specific country or to the customers of one specific network.

The specificities of China and other authoritarian countries in this regard are political. They lie in the extensive focus on political websites and surveillance of opponents, the particularly blurry legal framework and opaque decision-making, as well as the absence of appeal, all of which come down to the absence of a true rule of law. Beyond the heated but simplistic debates on how to preserve the "openness" of the internet, the political set-up of the Chinese internet highlights, if needed, the importance of crafting democratic governance mechanisms to set and enforce legitimate norms and rules for the internet, at both a national and global level.

Pushing for an International Governance Framework

China's leaders and cyber policy experts tend to see the global internet as an "anarchic space" where Western countries, and particularly the U.S., exercise "hegemonic" power as the marginalisation of governments and apparent inclusiveness may in fact mask overwhelming domination by participants from developed, Western countries. Suspicion is especially strong in the case of ICANN because of its links with the American government.[37]

As a result, Chinese experts and policy-makers have always expressed clear preference for intergovernmental frameworks, especially the UN, where, due to the principle of "one state, one vote", developing countries are represented on a more equal footing with developed countries, and where civil society and corporate interests usually have no more than a consultative voice. Such frameworks are also bound by standard diplomatic negotiation norms, as opposed to the "rough consensus" principle that prevails in technical and multistakeholder communities, whereby it is difficult for a single actor or state to effectively block or withdraw from any specific measure. China is an active participant in various bilateral and multilateral dialogues, in particular in the field of cybersecurity. However this format is not entirely satisfying for China, as it is not systematically part of the conversation (it is not a member of the G8), and bilateral cooperation is open to suspension from either side in case of diplomatic tensions. For example, when five members of the People's Liberation Army were indicted in the U.S. for cyberespionage in May 2014, China stopped participation in a U.S.-China cybersecurity working group established only

[37] Séverine Arsène, Internet Governance in Chinese Academic Literature. Rebalancing a Hegemonic World Order?, China Perspectives, 2016/2, pp. 25-36.

a year earlier. Top-level cooperation resumed in the autumn of 2015 with the establishment of a U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues.

Given the uncertainties of such discussion platforms, the Chinese government considers the United Nations to be the ideal framework for global internet governance. The 2010 White Paper states: "China holds that the role of the UN should be given full scope in international internet administration. China supports the establishment of an authoritative and just international internet administration organisation under the UN system through democratic procedures on a worldwide scale." Chinese representatives spared no efforts throughout the 2000s to push this agenda. At the 2005 World Summit on the Information Society (WSIS) in Tunis, the Chinese government tried, unsuccessfully, to obtain agreement that the responsibilities of ICANN should be transferred to the International Telecommunications Union. At the 2012 Dubai ITU summit, China pushed for enlarging the role of the ITU to include such issues as cybersecurity and the domain name system. In 2011 and in 2015, China teamed up with Russia, Uzbekistan, and Tajikistan to propose (without success) a Code of Conduct for Information Security to the General Assembly of the United Nations. This document pleaded for "multilateral, transparent and democratic international internet governance."

Despite these efforts, the chances are very slim that China will succeed in this quest. It is true that China has been able to obtain small concessions, like the inclusion of the word "multilateral" in the final report of the Ten-Year Review of the World Summit on the Information Society in December 2015. This highlights the fact that China can find alliances in global governance institutions, notably with developing countries such as some members of the Group of 77 (which brings together developing countries), as well as more advanced cyber powers such as Russia. However these allies remain in the minority and generally amongst less powerful countries. In particular, although European countries are more nuanced than the United States in their support for the multistakeholder model, and insist more often on the role states can play to defend the interests of citizens, they still stand against the idea of a purely intergovernmental governance model, as this could enable some states to block measures in favour of the Human Rights, or to push for a nation-based architecture of the Internet, deemed by some as "balkanisation."

The Chinese Way in Multistakeholderism?

In light of this situation, Chinese leaders have had to find their own way within the current governance model. Even as official representatives were publicly expressing criticism of multistakeholder organisations, individual Chinese engineers and academics continued

to participate in meetings and working groups, and contributed to developing essential technology, such as encoding for Chinese-character domain names (to create urls like www.网站.中国).

In the early 2010s, the Chinese leadership seemed to adopt a rather more cooperative attitude. For example, Chinese representatives were sent to participate in the Governmental Advisory Committee of ICANN after nearly a decade of interruption. Lu Wei, former head of the Cyberspace Administration of China (CAC), and Jack Ma, CEO of the Chinese internet giant Alibaba, are both members of the board of Netmundial. This increased participation by officials and key public figures can be analysed either as a sign of a pragmatic approach by the Chinese government or as a more profound change in strategy and attitude on the international stage, related in part to China's new confidence in its own capacity to defend its interests within the existing global governance framework.

Indeed, in light of the growth of China's internet sector, it seems that China can take advantage of the multistakeholder scheme to advance its agenda, in particular through the private sector. During the last three decades, China has striven to develop "indigenous innovation" in order to reduce its dependency on foreign technology and competencies. It now has the world's most numerous internet users and some of the most dynamic internet businesses (think of Alibaba, Tencent), which are very attractive to the global internet industry, so much so that many internet platforms are ready to make concessions on freedom of speech and handling of personal data in order to access the Chinese market. The apparent rapprochement of Xi Jinping and Lu Wei, former head of the Cyberspace Administration of China, with the American internet giants during the Chinese-American technology forum in September 2015, as well as the trips by Mark Zuckerberg, Facebook's CEO, to China, suggest that the Chinese leadership is now looking to the private sector for alliances at a global level.

Conclusion

In 2014, China initiated a yearly World Internet Conference, held in the Chinese town of Wuzhen, where the former head of the Cyberspace Administration of China, Lu Wei, and in 2015 the Chinese president himself, Xi Jinping, asserted the role of China as a new cyber power, and expressed strong support for the cyber sovereignty principle.

The motto of the conference is "an interconnected world shared and governed by all," in a formulation that adroitly stops short of clarifying whether "all" are states or other actors or both, and how their respective roles should be balanced. However it is clear that

the Chinese leadership sees the internet through the lens of national interest, and more particularly through the interests of the Communist party in power. For Chinese leaders, global cooperation on internet governance is mainly necessary to guarantee the stability of the internet from a technical point of view, and to build "peaceful coexistence" between cyber-sovereigns. But few among the Chinese cyber experts and policy makers believe in the internet as a global public good, as they tend to see this concept as a rhetorical offensive in favour of American hegemony.

Chinese positions seem to have a polarising effect on the global debates on internet governance, with concepts like multistakeholderism, multilateralism and cyber sovereignty referred to in terms of whether the internet can remain "open" or "free". Such Manichean discussions do not seem to effectively tackle the democratic issues that are raised by the highly transnational and privatised character of internet governance. Indeed, the fact that the Chinese government is now finding its way through the current multistakeholder system, and even more in direct cooperation with global internet giants like Apple or Facebook (despite the latter being blocked in China), underlines the shortcomings of the current global internet governance system in terms of democratic procedures and guarantees. As a result, the formulation of a global public interest for the internet remains a challenge.

Further reading

Arsène, S. (2015): From the 'Great Firewall' to the 'Great Cannon': The Misleading Metaphors of Internet Filtering in China, China Policy Institute Blog, April 29 https://blogs.nottingham.ac.uk/chinapolicyinstitute/2015/04/29/from-the-great-firewall-to-the-great-cannon-the-misleading-metaphors-of-internet-filtering-in-china/

Arsène, S. (2015): Global Internet Governance in Chinese Academic Literature. Rebalancing a Hegemonic World Order?, China Perspectives, 2016/2, pp. 25-36

Arsène, S. (2015): Internet Domain Names in China: Articulating Local Control with Global Connectivity, China Perspectives, 2015/4, pp. 25–34

Arsène, S. (2012): The Impact of China on Global Internet Governance in an Era of Privatized Control, Chinese Internet Research Conference, Los Angeles http://hal.archives-ouvertes.fr/hal-00704196/

Brousseau, É., M. Marzouki and C. Méadel (eds.) (2012): Governance, regulations and powers on the Internet, Cambridge and New York, Cambridge University Press

DeNardis, L. (2014): The global war for internet governance, New Haven: Yale University Press

Hofmokl, J. (2010): The Internet commons: towards an eclectic theoretical framework, International Journal of the Commons, 4 (1), pp. 22650

MacKinnon, R. (2012): Consent of the Networked: The Worldwide Struggle for Internet Freedom, New York: Basic Books

Musiani, F., D. L. Cogburn, L. DeNardis and N. S. Levinson (eds.) (2016): The Turn to Infrastructure in Internet Governance, New York: Palgrave Macmillan

Raymond, M. and L. DeNardis (2015): Multistakeholderism: Anatomy of an Inchoate Global Institution, International Theory, May 2015, pp. 1–45

Séverine Arsène
is the managing editor of AsiaGlobal Online at the Asia Global Institute, The University of Hong Kong, and an associate researcher at the French Center for Research on Contemporary China in Hong Kong. Her research focuses on Chinese cyberpolicy and the role of China in global Internet governance.