Global Internet Governance in Chinese Academic Literature

Rebalancing a Hegemonic World Order?

SÉVERINE ARSÈNE

ABSTRACT: This article explores the apparently ambivalent foundations of the notion of cybersovereignty as seen from China, through some of the most recent Chinese academic literature on global Internet governance. It shows that the sampled authors conceive of the current Internet order as an anarchic or disorderly space where global hegemons reproduce their domination over the world in the digital age. In the rather dichotomous world that this portrays, most of the authors concentrate their attention on the position and strategy of the United States, with a view to underlining the contradictions in American discourse through the PRISM scandal or the status of ICANN. In this context, most scholars studied here see the current situation, where Internet governance is increasingly debated, as an opportunity to rebalance the global Internet order and advance the strategic interests of China through the establishment of an intergovernmental Internet governance framework in the long term, and through active participation in the current status quo in the short term.

KEYWORDS: Internet governance, China, cybersovereignty, China-US relations, hegemony.

As the Internet has grown to be used by almost half of humanity and to comprise so many aspects of our personal, professional, social, and political lives, it has progressively ceased to be considered the purely open, virtual space that some of its pioneers envisioned.[1] With the emergence of complex, real-life issues, from content regulation to privacy, copyright, and various forms of cybercrime (scams, fraud, identity theft, etc.), there has been growing demand for regulation.

Existing sources of regulation or governance are extremely diverse and sometimes contradictory or overlapping. The laws of nation-states apply to activities that take place on their territories. Internet service providers set norms for online behaviour through contractual terms of use, which apply globally. Economic and technical arrangements that are decided within the technical community (such as the little-known Internet Engineering Task Force) or amongst industry players (such as peer contracts between Internet service providers) have critical effects on users' opportunities and in shaping the general online ecosystem (think of the digital divide).[2]

As the political implications of Internet governance have progressively come to light, the challenge of building a coherent, global, and legitimate Internet governance framework has also come to appear an almost impossible target. Despite many attempts to bring together the global community in various kinds of institutions and fora, from issue-based institutions such as ICANN or the IETF to the more general UN-sponsored World Summit on the Information Society, to the IGF and to Netmundial[3] and to innumerable bilateral and multilateral dialogues, "We have been improving collective governance arrangements for 15 years, and these improvisations have so far failed to fully resolve the issues of legitimacy, adherence and scope on a global basis."[4]

The controversies around the proposed Internet governance frameworks have raised profound theoretical issues and question basic assumptions about the very nature of the Internet. For example, should the Internet be considered a global common good when it is composed of interconnected cables, routers, and digital services that are, for the most part, privately owned?[5] Is the Internet really a borderless space as is often assumed, and what are the implications for sovereign states?[6] How can institutional innovations such as the much-debated multistakeholder model be characterised in terms of representing the interests of various actors and political legitimacy?[7] Normative preferences on the ideal framework(s) for Internet governance are highly dependent on the theoretical understanding one may have of these issues.

Meanwhile, China has played an increasingly visible role in these debates through its government representatives, technical community, private sec-

[1] I would like to thank Anthony H. F. Li for his help on additional documentation.

[2] For more examples of forms of regulation, see Éric Brousseau, Meryem Marzouki, and Cécile Méadel (eds), *Governance, Regulations and Powers on the Internet*, Cambridge and New York, Cambridge University Press, 2012.

[3] ICANN: Internet Corporation for Assigned Names and Numbers. IETF: Internet Engineering Task Force. IGF: Internet Governance Forum.

[4] Milton Mueller and Ben Wagner, "Finding a Formula for Brazil: Representation and Legitimacy in Internet Governance," Internet Policy Observatory, January 2014, p. 11, www.internetgovernance.org/pdf/MiltonBenWPdraft_Final.pdf (accessed on 19 October 2015).

[5] Mark Raymond, "Puncturing the Myth of the Internet as a Commons," *Georgetown Journal of International Affairs*, 2013, http://tinyurl.com/onty88c (accessed on 19 October 2015); Milton L. Mueller, "Property and Commons in Internet Governance," in Éric Brousseau, Meryem Marzouki, and Cécile Méadel (eds), *Governance, Regulations and Powers on the Internet, op. cit.*, pp. 39-62.

[6] Jack L. Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World*, Oxford and New York, Oxford University Press, 2006.

[7] Mark Raymond and Laura DeNardis, "Multistakeholderism: Anatomy of an Inchoate Global Institution," *International Theory*, Vol. 7, No. 3, 2015, pp. 572-616.

tor, and users. Its impact on the Internet's infrastructure, standards, markets, and global governance has drawn more attention in recent years.[8] In particular, the fact that China pioneered Internet censorship, notably through content filtering tools known as the Great Firewall, as well as the insistence of Chinese officials on the notion of cybersovereignty, have raised debates on whether Chinese leaders intend to build a separate network similar to a Chinese "intranet." However, China's Internet infrastructures and services are increasingly globalised and interconnected, while officials have combined strong discourses on cybersovereignty with actual cooperation in a number of concrete domains, particularly by sending participants to numerous Internet governance fora and dialogues.

In this article, I intend to explore the apparently ambivalent foundations of the notion of cybersovereignty as seen from China, through some of the most recent Chinese academic literature on global Internet governance.

After a short summary of the positions taken by Chinese representatives on the topic in recent years, I will turn to a sampling of 13 academic articles from the CNKI database for a deeper analysis of the theoretical assumptions behind the Chinese positions and strategy in Internet governance (part 1). I will first show that the sampled articles conceive of the current Internet order as an anarchic or disorderly space where global hegemons reproduce their domination over the world in the digital age (part 2). In the rather dichotomous world that this portrays, most of the authors concentrate their attention on the position and strategy of the United States with a view to underlining the contradictions in American discourse through the PRISM scandal or the status of ICANN (part 3). In this context, most scholars studied here see the current debates on Internet governance as an opportunity to rebalance the global Internet order and advance the strategic interests of China through the establishment of an intergovernmental Internet governance framework in the long term, and through active participation in the current status quo in the short term (part 4). This leads me to conclude that there is as yet little belief in the notion of the Internet as a global common good among mainstream academic views of the Internet in China.

A position on cybersovereignty that deserves further scrutiny

During the 2000s, China expressed a relatively vocal criticism of the current Internet governance institutions and status quo, mostly because the "multistakeholder" model of governance (adopted by ICANN among others) only gives a marginal place to governments, and it is viewed in China as favouring American and Western interests.[9] The Chinese leadership, however, seemed to have adopted a rather more cooperative attitude in the early 2010s. For example, Chinese representatives were sent to participate in the Governmental Advisory Committee of ICANN after nearly a decade of interruption, and Chinese representatives seemed to be less vocal about their demand to put the Internet into an intergovernmental framework, even expressing some support for the multistakeholder model of representation. Lu Wei, the 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, a forum on Internet governance that also accommodates participation from a broad range of society. This increased participation was analysed either as the sign of a pragmatic approach by the Chinese government[10] 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.[11]

However, the notion of cybersovereignty has remained the bottom-line of China's cyber policy and diplomacy, and it has been consistently asserted in various official documents and declarations, starting with the milestone *White Paper on the Internet in China* published by the State Council in 2010.[12] This document notably emphasised that "the Internet of various countries belongs to different sovereignties, which makes it necessary to strengthen international exchanges and cooperation in this field. (…) China supports the establishment of an authoritative and just international Internet administration organization under the UN system through democratic procedures on a worldwide scale." Similarly, a *White Paper on Diplomacy*[13] published in 2013 emphasised the concept of territorial sovereignty and stressed that China "opposes the use of the Internet to interfere with other countries' domestic politics." Article 1 of the draft Cybersecurity law, published in July 2015 for public comment, states: "This law is formulated so as to ensure network security, to preserve cyberspace sovereignty, national security, and societal public interest."[14] Generally speaking, the notion of cybersovereignty that China advocates implies that each country should be able to police its own domestic Internet, without interference from other countries (such as circumvention tools provided by foreign entities), let alone attacks on the domestic Internet infrastructure and information system.

On the international stage, Chinese representatives did not give up efforts to push the agenda of building an intergovernmental framework for Internet governance. In 2011, China teamed up with Russia, Uzbekistan, and Tajikistan to propose (without success) a Code of Conduct for Information Security[15] to the General Assembly of the United Nations. This document, which pleaded for "multilateral, transparent and democratic international Internet governance," was later amended and proposed again to the General Assembly in January 2015.[16] The amended wording incorporates the notion of cooperating with social actors, but it still insists on the need for an intergovernmental framework, and puts the responsibility to define the

[8] Milton Mueller, "China and Global Internet Governance," in Ronald Deibert, Rafal Rohozinski, and Jonathan Zittrain (eds), *Access Contested*, Cambridge, MA, MIT Press, 2012, pp. 177-194; Scott Livingston, "Beijing Touts 'Cyber-Sovereignty' in Internet Governance: Global Technology Firms Could Mine Silver Lining," *China Law Blog*, 19 February 2015, www.chinalawblog.com/2015/02/beijing-touts-cyber-sovereignty-in-internet-governance-global-technology-firms-could-mine-silver-lining.html (accessed on 19 October 2015).

[9] For more on China and ICANN, see Séverine Arsène, "Internet Domain Names in China: Articulating Local Control with Global Connectivity," *China Perspectives*, No. 2015/4, pp. 25-34.

[10] "Due to these pre-emptive moves, and because of China's realization after WSIS that ICANN was not going to go away," Milton Mueller, "China and Global Internet Governance," *art. cit.*, p. 183.

[11] Séverine Arsène, "The Impact of China on Global Internet Governance in an Era of Privatized Control," communication at the Chinese Internet Research Conference, Los Angeles, 2012, http://hal.archives-ouvertes.fr/hal-00704196 (accessed on 19 October 2015).

[12] Information Office of the State Council, "White Paper: The Internet in China," 15 June 2010, http://china.org.cn/government/whitepaper/node_7093508.htm (accessed on 13 October 2015).

[13] "2013 Zhongguo waijiao baipishu: Zhongguo weihu lingtu zhuquan juexin jianding" (2013 China White Paper on Diplomacy: China is firmly determined to safeguard territorial sovereignty), *Renmin wang via Tianya*, 17 July 2013, http://bbs.tianya.cn/post-worldlook-827386-1.shtml (accessed on 19 August 2015).

[14] National People's Congress Standing Committee, "Wangluo anquanfa (cao'an)" (Draft cybersecurity law), 6 July 2015, www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm, trans. China Law Translate, http://chinalawtranslate.com/cybersecuritydraft/?lang=en (both accessed on 13 October 2015).

[15] People's Republic of China et al., "International Code of Conduct for Information Security," United Nations, 12 September 2011, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf (accessed on 13 October 2015).

[16] People's Republic of China et al., "International Code of Conduct for Information Security (revised version)," United Nations, 13 January 2015, https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf (accessed on 13 October 2015).

boundaries of information rights within the hands of states, according to their own definition of national security and public order. Similarly, at the 2012 Budapest Conference on Cyber Issues,[17] Chinese Ambassador Huang Huikang proposed five principles directly inspired by the 1950s notion of peaceful coexistence, of which sovereignty is first.[18] The motto of the World Internet Conference organised by China in Wuzhen in November 2014, "An interconnected world shared and governed by all,"[19] should certainly not be interpreted in an overly literal way, as a proposed – but finally abandoned – Wuzhen declaration included wording on the need to "respect Internet sovereignty of all countries."[20] As a confirmation of this position, in December 2014, Lu Wei published an op-ed in the *Huffington Post* entitled "Cyber Sovereignty Must Rule Global Internet."[21]

In April 2015, an important cyberattack on the American web platform Github further complicated the interpretation of China's claim for cybersovereignty. Github had been used for some time by activist organisations to host content blocked by the Chinese censorship system. An analysis of the tools used, nicknamed the "Great Cannon" by the Citizen Lab, showed that it most likely came from the same infrastructures as the state-sponsored Great Firewall of China.[22] This unprecedented action showed that China was ready to take action beyond its territory in order to guarantee the efficiency of information control within China. This event thus contributed to blurring the notion of "non-interference," which had been a core principle in China's diplomacy for decades.

Unfolding the theoretical assumptions behind "cybersovereignty" in China

The Chinese official press[23] provides fascinating but limited insights into these ideological and strategic trends. For example, D. Bandurski has noted a sharp increase in the use of the term "cybersovereignty" in the Chinese press since 2010, which clearly reflects the fact that the Chinese leadership had concentrated their efforts on this question even before Xi Jinping took power.[24] However, in the absence of transparency on the internal political debates within the PRC, such editorials can only raise more questions on the decision-making processes and relative influence of the various administrations and factions of the Communist Party.[25] As R. Creemers notes, in a context of administrative streamlining and competition, "it is difficult to gauge to what extent such claims [for more assertiveness] reflect true concerns about national security, rather than bureaucratic positioning in pursuit of budget appropriations."[26] In fact, these materials provide more information about the theoretical concepts and visions that circulate among the Chinese political elites and mainstream intellectuals than accurate information about the short-term strategic intentions of the current leadership, although the two aspects are related.

This article intends to dig deeper in this direction through the analysis of a sampling of recent Chinese academic literature on the topic. To identify a small set of key research articles and authors, I used the CNKI database to sample 13 key articles by ten authors. In the category about "Chinese politics and international politics" (*Zhongguo zhengzhi yu guoji zhengzhi* 中国政治与国际政治), I searched the keyword "cyberspace" (*wangluo kongjian* 网络空间), which is generally used in this database to tag articles on global cyberpolicy. The vast majority of this literature is in fact focused on the question of cybersecurity, and another important group of articles dealing with US-China relations is also mostly about cybersecurity issues. While it is important to note this orientation of Chinese scholarship, I decided to focus on a smaller group of articles that analyse global Internet governance and the notion of cybersovereignty in a more specific and comprehensive way, and therefore excluded from my selection the articles that are solely focused on China-US bilateral relations or on narrow themes such as cybersecurity or cybercrime. Among the more than 400 results, I handpicked the articles that more specifically dealt with global Internet governance, which were in the minority. Most of these articles were also tagged under the keyword "cybersovereignty" (*wangluo zhuquan* 网络主权). Another search for "Internet governance" (*wangluo zhili* 网络治理) returned 1,774 results more often focused on domestic governance issues such as e-government, control of public opinion, and cybercrime. Another field of research revolves around governance of intellectual property or e-commerce. Although all these fields of research touch upon global Internet governance in some respect, notably through specific institutions such as ICANN or the WTO, defining Internet sovereignty or global governance is generally not their central focus.

The authors of the sampled articles are generally midcareer teaching or research staff at major universities, such as Tan Youzhi, assistant professor at the Institute of International Relations, University of Business and Economics in Beijing, Gao Wanglai, assistant professor at the Department of International Relations, China Foreign Affairs University in Beijing, or Shen Yi, associate professor at the Institute for International Relations and Public Affairs, Fudan University in Shanghai. One author, Lu Chuanying, is a researcher in a prominent think tank, the Shanghai Institutes for International Studies. Although it is hard to assess the influence of these intellectuals beyond academic circles, some of them have published editorials in the Chinese and foreign press,[27] which suggests that their views are shared by at least some factions within the Chinese Party-state.

[17] Huang Huikang, "Statement at Budapest Conference on Cyber Issues," Permanent Mission of the People's Republic of China to the United Nations and Other International Organizations in Vienna, 4 October 2012, www.chinesemission-vienna.at/eng/zgbd/t977627.htm (accessed on 13 October 2015). The five principles are: sovereignty, balance "between the free flow of information and necessary regulation of the Internet," peaceful use, equitable development, and international cooperation.

[18] Rogier Creemers, "An Interconnected World with Chinese Characteristics? China Engagement with Global Governance," Chinese Internet Research Conference, Edmonton, 28 June 2015.

[19] Wuzhen conference website, www.wicnews.cn/indexen.shtml (accessed on 9 October 2015).

[20] James T. Areddy, "China Delivers Midnight Internet Declaration – Offline," *Wall Street Journal*, 21 November 2014, http://blogs.wsj.com/chinarealtime/2014/11/21/china-delivers-midnight-internet-declaration-offline (accessed on 13 October 2015).

[21] Lu Wei, "Cyber Sovereignty Must Rule Global Internet," *The Huffington Post*, 15 December 2014, www.huffingtonpost.com/lu-wei/china-cyber-sovereignty_b_6324060.html (accessed on 14 October 2015).

[22] Bill Marczak et al., "China's Great Cannon," Citizen Lab, University of Toronto, 10 April 2015, https://citizenlab.org/2015/04/chinas-great-cannon (accessed on 14 October 2015).

[23] See the work by Qian Gang and David Bandurski at the China Media Project http://cmp.hku.hk, or by Rogier Creemers on China Copyright and Media https://chinacopyrightandmedia.wordpress.com. Also, Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," *China Leadership Monitor*, No. 42, Fall 2013, http://media.hoover.org/sites/default/files/documents/CLM42MS.pdf (accessed on 14 October 2015).

[24] "China Actively Pushes Building of New System of International Governance of Cyberspace," *Legal Daily*, 28 September 2015, translated in David Bandurski, "Re-Defining Cyberspace," *Medium*, 7 October 2015, https://medium.com/@cmphku/re-defining-cyberspace-7d085c75440b (accessed on 14 October 2015).

[25] See Qing Duan, *China's IT Leadership,* Saarbrücken, VDM Verlag Dr. Mueller, 2007; Greg Austin, *Cyber Policy in China*, Cambridge, UK, Malden, MA, Polity, 2014.

[26] Rogier Creemers, "An Interconnected World with Chinese Characteristics? China Engagement with Global Governance," *art. cit.*

[27] Lu Chuanying, "Yao lizhiqizhuang tan wangluo zhuquan" (It is legitimate to talk about cybersovereignty), *Huanqiu wang*, 16 December 2015, http://opinion.huanqiu.com/1152/2015-12/8185356.html (accessed on 15 February 2016); Shen Yi, "For China and the U.S., Cyber Governance Is Better Than Cyberwar," *Huffington Post*, 22 September 2015, www.huffingtonpost.com/shen-yi/cyber-governance-cyber-war-china_b_8177732.html (accessed on 16 October 2015).

Due to the exclusive focus on academic publications and exclusion of cybersecurity articles, some important authors do not appear in this sampling, such as Zhang Li,[28] from the China Institutes of Contemporary International Relations, or Xu Longdi,[29] from the China Institute of International Studies, a think tank that belongs to the Chinese Ministry of Foreign Affairs.

This narrow selection can obviously not be considered exhaustive or without flaws. However, I hope that it will provide a glimpse of current academic points of view on Internet governance in China, and an opportunity for more detailed analysis of the wording and theoretical assumptions used in this emerging literature. As this field of research is largely oriented towards public policy expertise, and almost all authors provide recommendations for the defence of the interests of China and the Chinese government, these articles are also particularly worth studying for their normative dimensions. Of course, as the last few years have been marked by enhanced crackdowns on opinion leaders, it can be assumed that published scholarship – as well as editorials – will mostly feature rather mainstream points of view, albeit with slight variations (mainly in the type of recommendations) depending on the authors' position and disciplinary background. Overall, the views expressed in this sample are highly homogenous.

The global Internet, an anarchic space where hegemons are imposing their order

An anarchic space

For most authors, the reflection on global Internet governance starts with the common observation that the Internet has historically developed in a largely non-organised way, and its transnational character (*kuaguoxing* 跨国性) makes it more difficult for sovereign countries to enforce their domestic rules and maintain social order. Social and political movements (such as the Arab Spring), hackers and cyberattacks, cybercrime, cyberspying, and misuse of personal data are cited among the most worrying phenomena confronting governments with political, social, economic, or cultural challenges.

For example, the global Internet is described by Tan Youzhi 檀有志[30] as an "anarchy" (*wuzhengfu zhuangtai* 无政府状态) and "an uncharted territory" (*wuzhi lingyu* 无知领域) "from the legal, political, security points of view" where "authority, transparency, and responsibilities are not clarified."[31] For that reason, he describes the Internet as a "fifth frontier" (*di wu jie* 第五界) in addition to those of land, sea, air and space (p. 30), using notions drawn from security studies.[32]

The notion of order (*zhixu* 秩序) – or the lack of it – is ubiquitous in this group of articles, and in most cases it is used to justify why China should pay attention to global Internet governance. For instance, Gao Wanglai 高望来[33] speaks of a "lost order of cyberspace in the information era" (*xinxishidai wangluo kongjian de shixu* 信息时代网络空间的失序).[34] But beyond threats to social and political stability, which are the focus of many articles oriented towards cybersecurity, these articles also point to a broader, more systemic analysis of the changing world order and to the changing position of China in this landscape. For Shen Yi 沈逸,[35] for example, the Internet has developed as an "anarchy" where "all sorts of actors use their own practices to enlarge their space for action, to obtain more resources, acquire and use the right to define the rules, and turn the definition of their own particular interests into determined codes of action in cyberspace."[36]

The digital divide and political, economic, cultural domination

The idea that the global Internet is a totally unruly space, out of reach of jurisdictions, is however increasingly debated. In fact it could even be argued that one issue is that the Internet is subject to too much regulation, with conflicts of jurisdictions that render national laws difficult to enforce.[37] The authors here also describe how states are retaliating by adjusting national regulation and asserting a more important role in Internet governance. But until states obtain more control of the Internet, the current status quo is described here as one in which infrastructure and platform design and ownership, copyright, and other technical features of the Internet, which often incorporate the libertarian views of involved engineers,[38] have been shaping and channelling Internet behaviours in a more powerful way than the laws of any country. This angle of analysis seems in part derived from the work of Lawrence Lessig on normative effects of technical code,[39] but whereas Lessig concludes with the necessity of better defining common interests and protecting citizens' rights, the focus here is more on the effects of technological inequalities on China's position in the international world order. The general argument defended here is that the low institutionalisation of the Internet has in fact rearranged the world order in a way that has benefited the more technologically advanced countries and actors and thus exacerbated global inequalities from a number of social, cultural, political, economic, and strategic perspectives.

A common focus of the articles is the "asymmetry" (*bu duichenxing* 不对称性, ex. Gao Wanglai p. 54) between developed and developing countries, and the "monopoly" (*longduan* 垄断) of developed countries on certain key infrastructures, which have long given them the capacity to take advantage of the opportunities of the digital age and to set the rules of Internet governance. Shen Yi takes several indicators of the global digital divide, such as Internet access rates and infrastructures, as proof of the dependency of de-

[28] Zhang Li, "A Chinese Perspective on Cyberwar," *International Review of the Red Cross*, Vol. 94, No. 886, 2012, https://www.icrc.org/eng/resources/documents/article/review-2012/irrc-886-zhang.htm (accessed on 19 February 2016).

[29] Xu Longdi, "China's Internet Development and Cybersecurity: Policies and Practices," in Daniel Ventre (ed.), *Chinese Cybersecurity and Defense*, London, Wiley-ISTE, 2014, pp. 1-53.

[30] Assistant professor, Institute of International Relations, University of International Business and Economics (Beijing).

[31] Tan Youzhi, "Wangluo kongjian quanqiu zhili: guoji qingshi yu Zhongguo lujing" (Global Internet governance: International trends and the Chinese path), *Shijie jingji yu zhengzhi*, No. 12, 2013, p. 31. For brevity, each article of this sample will only be referenced once, with pagination of further citations indicated in the text. All translations are done by me.

[32] This is interesting in a context when the People's Liberation Army is preparing to create a body overseeing cyber and space defense. See Megha Rajagopalan, "Chinese Military Force to Take Lead on Cyber, Space Defense," *Reuters*, 29 January 2016, www.reuters.com/article/us-china-military-idUSKCN0V714B (accessed on 5 April 2016).

[33] Assistant professor, Department of International Relations, China Foreign Affairs University (Beijing).

[34] Gao Wanglai, "Wangluo zhili de zhidu kunjing yu Zhongguo de zhanlüe xuanze" (The institutional dilemma of Internet governance and China's strategic choices), *Guoji guanxi yanjiu*, No. 4, 2014, p. 51.

[35] Associate professor, Institute for International Relations and Public Affairs, Fudan University (Shanghai).

[36] Shen Yi, "Hou Sinuodeng shidai de quanqiu wangluo kongjian zhili" (Global Internet governance in the post-Snowden era), *Shijie jingji yu zhengzhi*, No. 5, 2014, p. 147.

[37] See multiple examples provided by the Internet and Jurisdiction Observatory: www.internetjurisdiction.net/observatory (accessed on 6 April 2016).

[38] John Perry Barlow's *Declaration of the Independence of Cyberspace* is often quoted. *Electronic Frontier Foundation*, 8 February 1996, https://projects.eff.org/~barlow/Declaration-Final.html (accessed on 13 October 2015).

[39] Lawrence Lessig, *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999.

veloping countries on assets owned and provided by developed countries. For instance, he underlines that European and American companies enjoy de facto dominance over the market of submarine cables, and that the US and Japan lead the market in server hardware providers. This creates a configuration of "centre-periphery" (*zhongxin – waiwei* 中心 – 外围, p. 150), which he believes is detrimental to China. This argument is in sharp contrast to the view of many countries such as the US, Australia, or European countries, which are concerned by the rise of Chinese manufacturing giants such as Huawei and ZTE in global markets.

For Yang Rongjun 杨嵘均, [40] the dividing line is not only between developed and developing countries, but also between developing countries according to their level of modernisation. It translates into very different visions of cyberspace and cybersovereignty:

> Developed countries think that cyberspace is a "global public domain" (*quanqiu gongyu* 全球公域), whereas developing countries think that cyberspace has a sovereign nature. (…) As developing countries, socialist countries generally support a cybersovereignty with more content, and a higher level of intervention of the state in cyberspace. On the other side, more Westernised countries such as India or South Korea, as developing countries that received more influences from Western thinking on freedom and democracy, put more emphasis on entrusting citizens and giving them more rights (…). The lower the level of modernisation, the larger the scope of cybersovereignty. [41]

Yang sees in this phenomenon "the mutation of colonialism into the information society":

> [Western countries] use various means to advance colonialism in cyberspace through cybertechnologies and information technologies. For a large number of developing countries, because of their backwardness in cybertechnologies and information technologies, there is no other option than to accept the international Internet system and cyberspace order established by powerful capitalist countries (p. 85).

According to him, this new form of colonialism is not only the result of historical contingencies but is still at play through the influence exerted by Western media production and propaganda:

> In general, because developed countries occupy superior economic, political, and cultural positions, and also have absolute superiority in the production of online information, they can infiltrate the ideology of target countries with their political positions, visions of life and values etc., through unlimited propaganda. (p. 82)

In other authors' views, the cultural influence of the global Internet on developing countries is not limited to the circulation of content but is also a result of the values and principles incorporated within the technological infrastructure and governance mechanisms, as in the article by Lu Chuanying 鲁传颖: [42]

> The unity of the Internet means that cyberspace was discovered and created in the West, and its standards, values, and culture are all based on Western civilisation. When they adopt the Internet, other countries must also adopt the Internet's leading culture and they cannot introduce their own cultures into cyberspace. In this context, the cultural sovereignty (*wenhua zhuquan* 文化主权) of developing countries is strongly challenged (*yanzhong chongji* 严重冲击) by the civilisation and values of the West. [43]

This vision somewhat echoes research in political economy that focused on the structural inequalities and dependencies of media infrastructures, and on one-way information flows that have long inundated developing countries from the West. [44] These conclusions focused global attention on the digital divide as early as the end of the 1970s. This stream of scholarship, largely inspired by the work of Gramsci, emphasised the importance of cultural content and infrastructure as an element of cultural domination and capitalist "hegemony." [45]

The concept of hegemony (*baquan* 霸权) has long been a common keyword in the official doctrine of the Communist Party, and it is clearly a major starting point in Chinese studies of global Internet governance. However, in this group of articles it is not used in reference to the Gramscian concept of hegemony. In lieu of a critique of global capitalism, the notion is used here to denounce American and Western domination over the global Internet, mostly using references from strategic studies and reports published in the United States (including references by Western authors criticising information control).

Moreover, when asserting that media content has unidirectional effects on audiences, they tend to exaggerate the supposed uniformity of content produced and circulated on the global Internet, and to overlook the development of academic research on media reception, [46] which shows that audiences have much more agency than suggested here through the complex processes of consumption, interpretation, and discussion of media content. The culturalist and simplistic vision presented here of a "Western" culture, different from and opposed to "Chinese" culture, is also quite weak theoretically.

The US as a hegemon seeking to perpetuate its domination

Although the articles vary slightly in the way they regroup the winners and losers of the current global Internet (dis)order, they all reflect a dichotomous vision of the world, where the United States is the leading actor and where China falls into the disadvantaged group. Explanations range from mere historic contingencies to China being purposely antagonised by other superpowers, as in Huang Zhixiong's 黄志雄 [47] analysis:

[40] Associate researcher, Institute of Public Policy, Nanjing Normal University (Nanjing).

[41] Yang Rongjun, "Lun wangluo kongjian zhili guoji hezuo mianlin de nanti ji qi yingdui celüe" (On problems and strategies of international cooperation in cyberspace governance), *Nanning shifan daxue xuebao (Shehui kexue ban)*, Vol. 13, No. 4, December 2014, pp. 79; 80; 81.

[42] Associate researcher, Shanghai Institutes for International Studies (Shanghai).

[43] Lu Chuanying, "Zhuquan gainian de yanjin jiqi zai wangluo shidai mianlin de tiaozhan" (Evolution of the concept of sovereignty and challenges faced in the Internet Age), *Guoji guanxi yanjiu*, No. 1, 2014, p. 77.

[44] Armand Mattelart, *Communication, idéologies et hégémonies culturelles. Une anthologie en trois volumes (1970-1986) - Tome 1* (Communication, ideologies, and cultural hegemonies: A 3-volume anthology – Vol. 1), Fabien Granjon and Michel Sénécal (eds), Paris, Presses des Mines, 2015.

[45] Antonio Gramsci, *Cahiers de prison* (Prison notebooks), Paris, Gallimard, 1986 [1950].

[46] Starting from Stuart Hall, "Encoding and Decoding in the Media Discourse," Stencilled Paper 7, Birmingham, Centre for Contemporary Cultural Studies, 1973.

[47] Associate professor, Wuhan University School of Law (Wuhan).

> When China joined the international governance of the Internet, at first it was out of a need to "passively respond" (*beidong yingdui* 被动应对) to the pressures and attacks launched by the West on a variety of concrete issues. (…) Some Western governments and media, out of a need to establish imaginary enemies (*jiaxiangdi* 假想敌), continue to spin the theory of the "Chinese cyberthreat" (*Zhongguo wangluo weixie* 中国网络威胁) (…) The chess game that is centred on the international order and regulation of cyberspace has created two camps, with the United States, Europe, and other Western countries on one side and China, Russia, and other newly developed countries on the other side. [48]

Tan Youzhi also sees the current situation as a competition between hegemons (*baquanguo* 霸权国) and other big Internet countries (*wangluo daguo* 网络大国). Despite nominal equality between them, "in reality there is a hierarchical structure where countries occupy different ranks depending on their strength." Even if other countries have acquired equivalent resources, from this perspective, they remain in a subaltern position. According to Tan, the unequal world order is now actively maintained by the United States:

> The US is not only seeking to guarantee its own security but is also actively seeking a leadership role in the management of the global Internet. This leadership role is not only based on technological superiority but also on all the fields where free activities bear no boundaries or reprisals. (...) As an Internet hegemon, the US meticulously suppressed the proposal by China, the Russian federation, Kazakhstan, and Uzbekistan at the 66th UN plenary session on 12 September 2011 to establish an International Code of Conduct for Information Security, which aimed at combating terrorism, separatism, extremism, and destruction of other country's political, economic, and social stability. (pp. 35-36)

The Code of Conduct is often mentioned as an example of the perceived active strategy of the United States to undermine any attempt to change the current balance of power through institutional means, and of its hypocritical use of principles such as freedom of information or civil society participation.

Similarly, Lu Chuanying writes that the US is using its "monopoly" (*longduan*) on basic infrastructure and governance organisations "to further blur the boundaries, and to extend its own cyberpower into the space of weak countries" (p. 79):

> The US believes that cyberspace is a "global public domain" (*quanqiu gongyu* 全球公域), and that countries should not exert their sovereignty in cyberspace. But in reality, the strategic goal of the US is to seize the resources and power of those spaces that cannot be characterised as states (*mei you mingque guojia shuxing kongjian* 没有明确国家属性空间) through the hegemony it has established in the global public domain. (...) Without the protection of sovereignty, the US can use its superiority in coercive cyberpower and institutional cyberpower (*qiangzhixing wangluoquan he zhiduxing wangluoquan* 强制性网络权和制度性网络权) to undermine (*weishe* 威慑) the cybersecurity of other countries, and to enter and control other countries' cyberspace resources at will. (p. 80)

For Lu, the supposedly open, inclusive concept of multistakeholderism is in fact a tool to advance the interests of strong countries. Despite the fact that its promoters "believe that the role of state actors, private companies, NGOs, academic groups, and individuals is as essential to the openness, prosperity, transparency as that of states alone," they still tend to turn to states whenever security issues arise (p. 79).

This vision of China being the constant target and victim of American domination is directly symmetrical to frequent accusations of China being one of the main sources of cyberattacks in the world. [49] It is in line with the official discourse of the Chinese government, which in turn claims that China is the world's largest victim of cyberattacks. [50]

ICANN as an instrument of American institutional domination

The case of Internet domain names [51] has attracted the most interest, probably because this issue is better known to the larger public. One frequent criticism relayed by Chinese authors is that the great majority of root servers, which help direct traffic towards the appropriate locations, are situated in the United States, which is seen as a major cybersecurity risk for the rest of the world (Tan Youzhi p. 39).

Besides this criticism on the geographical concentration of key Internet traffic infrastructure, a global controversy around the governance framework of domain names is also developing. ICANN, or the Internet Corporation for Assigned Names and Numbers, oversees the allocation of Internet addresses at a global level and thus plays a critical role in the Internet's stability and security as well as equitable distribution of resources. Founded in 1998, the private non-profit corporation based in the United States is perhaps the most well-known example of a "multistakeholder" model of governance that seeks to include a variety of actors of the industry, along with civil society and engaged individuals, with a consultative role for states. It has, however, consistently been criticised by many actors, notably developing countries, for its unbalanced and complicated decision-making processes, which tend to favour industry actors and Western interests, and for its sustained links with the US government, through the "stewardship" (control) role of the US National Telecommunications and Information Administration, over one of ICANN's core missions, the Internet Assigned Numbers Authority (IANA). [52]

The Chinese government has long been among the fiercest critics of ICANN's multistakeholder scheme, which is described in this set of articles as an instrument of the American domination strategy, as in Wang Mingguo 王明国: [53]

[48] Huang Zhixiong, "Wangluo kongjian guoji fazhi: Zhongguo de lichang, zhuzhang he duice" (Rule by international law in cyberspace: China's status, standpoint, and strategy), *Yunnan minzu daxue xuebao*, Vol. 32, No. 4, July 2015, pp. 137-138.

[49] A report published by the cybersecurity firm Mandiant on state-sponsored hacking was particularly powerful: David Sanger, David Barboza, and Nicole Perlroth, "China's Army Is Seen as Tied to Hacking Against U.S.," *The New York Times*, 18 February 2013, www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=4&_r=0&pagewanted=all (accessed on 6 April 2016)

[50] Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," *art. cit.*

[51] See Séverine Arsène, "Internet Domain Names in China: Articulating Local Control with Global Connectivity," *art. cit.*

[52] Laura DeNardis, *The Global War for Internet Governance*, New Haven, Yale University Press, 2014, Chapter 2: "Controlling Internet Resources"; Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance*, Cambridge, MA, and London, MIT Press, 2010, pp. 231*ff.*

[53] Associate Professor, Institute for International Strategy and Policy Analysis of the Law school, Shanghai University of International Business and Economics (Shanghai).

> To put an end to the American monopoly on the Internet sphere and implement a pluralistic, democratic, and transparent international governance system, it is necessary to accelerate the reform of ICANN. (…) Overall, ICANN embodies the American Internet governance project, which the US created thanks to its technological superiority, and which prevents other countries from obtaining some control over cyberspace. In that way, it perpetuates American hegemony and dominance (*baquan he tongzhi diwei* 霸权和统治地位).[54]

Lu Chuanying takes the example of the .iq (Iraq) domain name to argue that the US is effectively using the domain name system to advance its strategic interests:

> The United States government has in the past forbidden the resolution of particular domain names, which makes other countries disappear on the Internet, causing them great political and economic losses as well as social turbulence. (…) In 2001, before the war, the American government instructed ICANN to stop the resolution service for the Iraq .iq country code top-level domain name, which led websites in Iraq to completely stop service, and caused severe social, political, and economic unrest. (p. 79)

Although Chinese experts often cite this episode, the official account of the story by IANA is that the corporation that had received delegation for the .iq domain name never really implemented it, and its managers, based in the US, were suspected of criminal activities. As a consequence, the .iq domain was left dormant until ICANN redelegated it in cooperation with the post-war government in 2005.[55]

The American administration announced in 2014 that it is willing to transfer its overseeing role on IANA to another body under certain conditions, thereby launching a large-scale debate and reform process within ICANN (which was still generating controversy at the time of writing). Although generally welcomed by Chinese observers, this announced reform is also seen with a certain degree of scepticism, as in Gao Wanglai's analysis:

> This action may look like a withdrawal, but in reality it is only a strategic measure to acquire leadership on the multilateral chess board (*boyi zhong zhengduo zhudao quan suo caiqu de zhanlüe cuoshi* 博弈中争夺主导权所采取的战略措施 p. 56).

PRISM and the "double standard" in American discourse

The PRISM scandal,[56] in which Edward Snowden revealed the global extent of the American NSA's online surveillance, is also mentioned in nearly all articles to debunk American rhetoric, for example in Huang Zhixiong's article:

> The United States has used its technological superiority and monopoly on cyber-resources to conduct sustained and large-scale monitoring and secrets theft against many countries, including China. (p. 138)

For Shen Yi, PRISM also revealed the cooperation between the US government and the private sector, which enabled their surveillance capacity to reach the entire world. For him, empowering the private sector is in fact a way to seek "overwhelming hegemony" (*yadaoxing baquan youshi* 压倒性霸权优势 p. 152) rather than the disinterested support of civil society.

In Lu Chuanying's view, the PRISM scandal underlines the fact that the US has adopted "double standards" (*shuangchong biaozhun* 双重标准) when it comes to the concept of Internet sovereignty:

> When the US gathers countries' online data, or interferes with other countries' cyberpolicies, it claims that cyberspace is a "global public domain." When it wants to increase online supervision or enhance public-private cooperation domestically, then it either thinks that cyberspace is a sovereign sphere or that basic Internet infrastructure is privately-owned and that the country has jurisdiction over it. (p. 80)

Other, less well-known examples are also mentioned, such as the fact that Microsoft blocked access to its Messenger services to users in Cuba, Iran, Sudan, North Korea, and Syria as part of an American trade embargo in 2009[57] (Yang Rongjun p. 82).

Liu Yangyue 刘杨钺[58] and Yang Yixin 杨一心[59] also point at the perceived hypocrisy of American discourse in a context of proliferation of cybersecurity threats:

> The United States, (…) on the one hand calls out for cyber-liberalism and pleads in favour of the existing international Internet governance system in the name of openness and freedom, but on the other hand the practice of cyberthreat and cyberattacks and other military strategies has objectively promoted the trend of cyber-securitisation, enhanced support for cybersovereignty, and accelerated the decline of the Internet governance system that it intends to protect. Seen from this perspective, the inherent logic of the hegemonic cyber-strategy of the US is undoubtedly contradictory.[60]

In the same excerpt, Liu and Yang insist on the necessity of limiting the US's strategic hegemony by initiating international control over cyber-weapons (*wangluo junbei kongzhi* 网络军备控制). Such control would be "both a clear-headed recognition of the current situation of militarisation of cyberspace and a limitation to the de facto American deterrence (*weishe* 威慑) and pre-emptive strategy (*xianfazhiren zhanlüe* 先发制人战略)."

Overall, and despite the fact that I voluntarily excluded articles exclusively focused on China-US relations, the question of global Internet governance

[54] Wang Mingguo, "Quanqiu hulianwang zhili de moshi bianqian, zhidu luoji yu chonggou lujing" (Global Internet governance: Model change, institutional logic and path reconstruction), *Shijie jingji yu zhengzhi*, No. 3, 2015, pp. 49; 54-55.

[55] "IANA Report on Redelegation of the .IQ Top-Level Domain," IANA, July 2005, https://www.iana.org/reports/2005/iq-report-05aug2005.pdf (accessed on 14 October 2015).

[56] PRISM is the code name for a surveillance program developed by the United States National Security Agency. It collects Internet communications from American technology companies, including Microsoft, Yahoo! and Google. The revelation of its existence and scope created global outrage.

[57] Eric Lai, "Microsoft Not Only Firm Banning IM Access to U.S. Enemy Nations," *Computerworld*, 29 May 2009, www.computerworld.com/article/2524620/web-apps/microsoft-not-only-firm-banning-im-access-to-u-s--enemy-nations.html (accessed on 13 October 2015).

[58] Lecturer, National University of Defence Technology (Changsha).

[59] Senior engineer, National Centre for Networked Informatics and Information Security Management (Beijing).

[60] Liu Yangyue and Yang Yixin, "Wangluo kongjian 'zai zhuquanhua' yu guoji wangluo zhili de weilai" (The resurgence of sovereignty in cyberspace and its implications for Internet governance), *Guoji luntan*, Vol. 15, No. 6, November 2013, p. 6.

is mainly studied through the lens of American domination and its impact on China, not only in terms of cybersecurity – which is a main concern – but also in terms of economic and cultural domination, which are also perceived as potentially conducive to social unrest.

Between intergovernmental preferences and the multistakeholder status quo

Historic opportunity

As they are focused on making policy recommendations for the defence of China's interests, and marginally for the general interest, all authors see the current context as a key opportunity for China to acquire a place and voice (*huayuquan* 话语权) that is commensurate with its new status as a cyberpower (*wangluo daguo* 网络大国).

First, the American role in Internet governance is increasingly questioned by global actors, particularly after the revelations of the NSA's cyberspying. Secondly, in a context of global concern over cyberterrorism and cybercrime, states have stepped up efforts to intervene in Internet governance. Most articles also mention the fact that many Western countries have published cyberstrategy reports and that China should do so too. Moreover, the announcement of a reform of ICANN is seen as a sign that current institutional arrangements can now be questioned with a view to finding a new balance of power between the various stakeholders, or perhaps even to seek a completely different governance framework. The demographics of the Internet have also changed considerably, with the largest online populations now being in China, India and other developing countries, which calls for better representation of these countries in global Internet governance.

All these arguments lead the Chinese scholars to consider that China has a move to play on the "chess board" (*boyi* 博弈) of global Internet governance, and that it must "seize the opportunity" (*shenshi duoshi, bawo jiyu* 审时度势, 把握机遇, Tan Youzhi p. 37) offered by this "strategic window" (*zhanlüe zhi chuang* 战略之窗, Shen Yi p. 153). For Huang Zhixiong:

> The place occupied by China in the chessboard of international regulation of cyberspace (*wangluo kongjian guoji guize boyi* 网络空间国际规则博弈) determines its place and power in the future international order of cyberspace. (p. 138)

In the article by Gao Wanglai, who looks at the issue from a cybersecurity point of view, the sense of urgency is even more palpable, notably because of risks of cyberwar:

> The international community must establish international rules to prevent rivalries from turning into a global armed conflict. (...) China must seize this historic moment (*lishi qiji* 历史契机) and actively join in this process in order to guarantee that the rules of cyberspace represent the interests of China and other developing countries. (p. 57; p. 61)

Moreover, the authors propose to reform existing Internet governance institutions and to establish a diplomatic dialogue on cybersecurity within the United Nations and other intergovernmental organisations. They also encourage bilateral and multilateral dialogue with such countries as the US, Great Britain, South Korea, and BRICS countries.

China, the "common interest of humanity," and intergovernmental governance

Considering that the multistakeholder model is regarded with suspicion in this group of articles, the great majority of the authors studied here advocate the establishment of an intergovernmental framework for Internet governance, with some variations depending on their disciplinary background and focus.

For example, the solutions envisioned by authors who privilege a cybersecurity approach, such as Gao Wanglai, are often inspired by other strategic fields of diplomacy such as non-proliferation or money-laundering, where intergovernmental frameworks have been used to guarantee peaceful resolution of conflicts, including the UN and regional and bilateral dialogues. Gao also mentions the possible participation (*canyu* 参与 p. 58) of other parties such as transnational corporations, NGOs, scientists, or law experts, but only in a consultative role.

In an article that focuses on Internet global governance mainly from the perspective of the increasing militarisation of networks, Liu Yangyue and Yang Yixin state that the return of states and of the notion of cybersovereignty is an inevitable trend:

> At the institutional level, international organisations of Internet governance such as ICANN will inevitably go through a legitimacy crisis, and it will be difficult to maintain the status quo. Deep reform, or even complete replacement by institutions that represent the interests of sovereign states constitutes a reasonable prospect for institutional change. (p. 6)

While most authors do not consider cyberwar a credible eventuality, many see the establishment of an intergovernmental model as a solution to maintain peace and social order in a way that is not so different from the notion of peaceful coexistence advocated by Huang Huikang at the Budapest conference. Some also find supporting arguments in the fact that nation-states and other actors are implementing more and more territorialisation measures such as Internet filtering, server localisation, and nation-based copyright protections.[61]

For instance, Wang Mingguo argues that even the United States is no longer defending the idea of a global public domain (*quanqiu gongyu* 全球公域):

> It would be more accurate to consider the Internet a condominium resource (*gongguan ziyuan* 共管资源), a shared structure that lacks common rules and governance, and the basic infrastructure of which is under the control of nation states. (...) The Internet is undergoing a process of "re-sovereignisation and re-territorialisation" (*zai zhuquanhua he zai lingtuhua* 再主权化和再领土化). (...) At the organisational level, [China should] insist on giving a leading position to the United Nations, and try to turn the UN's International Telecommunications Union into the basic organisation in the construction of the global Internet governance system. (...) Only with the active support of the international community, and in particular of developing countries, can the ITU take a leading role in the sphere of Internet governance. (pp. 69; 70; 71; 72)

[61] The book by Jack L. Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World, op. cit.*, is often quoted.

Some authors do relate the establishment of intergovernmental Internet governance to the notion of a global common interest, and try to balance more universal notions related to citizens' rights, such as freedom of speech or privacy, with national interests in a rather politically conservative way.

Looking at the issue from the perspective of legal studies, Huang Zhixiong underlines that "the proposals to apply international laws to cyberspace reflect the objective need to build an international order in cyberspace, and it corresponds to the common interests of human societies" (*fuhe renlei shehui de gongtong liyi* 符合人类社会的共同利益 p. 136). He recommends a strategy based on the establishment of an international law of cyberspace through the United Nations and bilateral cooperation. As national sovereignty is the cornerstone of international law, such a framework would enable every country to establish its own domestic rules according to its level of development, traditions, culture, etc. (pp. 138-139). In his view, international law needs to be adapted and individual freedoms need to be balanced with public order and security concerns, with a view to building a "harmonious" (*hexie* 和谐) and "inclusive" (*gongjin* 共进) cyberspace (p. 140). Here, the "common interest of humanity" is stated in terms that are compatible with the political motto of former Chinese President Hu Jintao, "building a harmonious society," which was often used in the 2000s to justify measures of policing, public order, and political stability. The author then proceeds to a number of recommendations to develop cyberdiplomacy and related research, to publish a Chinese cyberspace strategy, to recognise the important role of non-state actors and "soft-law" in cyberspace, and finally to develop rule by law (*yi fa zhi guo* 依法治国) in China, which is a core concept of the Xi Jinping leadership.

From an international relations perspective, Tan Youzhi analyses the tension between necessary interconnectivity and concerns of nation-states:

> It is reasonable that countries will value and publicly defend cybersovereignty, but this contradicts the model of collaborative governance that has been proposed so far by sovereign countries and territories and international organisations, institutions, individuals, and various actors. The common interest of humanity (*renlei gongtong liyi* 人类共同利益) can only prevail over small calculations by nation-states if the latter voluntarily abandon or delegate some part of their governance to other organisations and find the best point of balance and the greatest common divisor between them. (pp. 32-33)

Tan's final recommendations are nonetheless more oriented towards restoring China's right to participate in the definition of rules (*zhengqu wangluo kongjian quanqiu zhili guoji guize de zhiding quan* 争取网络空间全球治理国际规则的制定权 p. 37) than towards pushing for reciprocally giving up some degree of sovereignty:

> Together we must push for the definition of international rules and regulations of cyberspace, an international supervision system of cyberspace, and a global sanctions program, and finally push for the realisation of a global governance system of cyberspace to effectively limit the superpowers' unilateral actions (*danbian zhuyi xingjing* 单边主义行经 pp. 37-38).

Like many authors in this sample, Tan also encourages international cooperation, particularly on a technical level, as well as investment to enhance domestic innovation in order to eradicate technological dependency (*nuli baituo shouzhi yu ren de beidong jumian* 努力摆脱受制于人的被动局面 p. 41).

In all the studied contributions, the term "intergovernmental platforms" mainly refers to the United Nations International Telecommunications Union, but can also include multilateral and bilateral dialogues such as the Association of South-East Asian Nations (ASEAN). Most authors also do not exclude direct cooperation with the private sector, thus replicating the all-encompassing strategy that is identified in the analysis of the American model, for example in Lu Chuanying's article:

> China participates in Internet global governance, both as a developing country and as a new cyberpower (*xinxing daguo* 新兴大国).(…) [China should] promote international cooperation and dialogue, participate in the definition of standards and rules of the Internet, change its passive position in the definition of international standards, actively enhance its right to speak on the international stage, and increase our country's weight in the renewed structure of future cyberspace.[62]

In the strategy proposed by Lu Chuanying, China would count on various possible forms of alliances, from the support of developing countries to more developed "new cyberpowers" such as Russia, which was one of the promoters of the Code of Conduct.

Multistakeholderism as a strategy

While the implementation of a more intergovernmental framework is often considered a more long-term goal, if possible at all, some authors hold that in the short term China should increase participation in the currently existing platforms and possibly try to change them from within.

In the article that probably expresses the most support for the idea of multistakeholder representation, Cai Cuihong 蔡翠红[63] exposes the multiple ways in which the interests and values of different actors can be divided or opposed in the field of cyberspace governance. Her vision of the future of global Internet governance is nonetheless optimistic, as she believes that the confrontation of these points of view and the interdependence between all actors can be overcome through a suitably balanced governance model:

> The differences in power and interests in cyberspace between the different institutional actors means that only an Internet governance model that can balance the diverse, multi-level cooperation of states, the market, and society can be really effective and acceptable to all parties. States cannot exist separately from the market and society. The market is the effective carrier of economic development for states, and the economy is the basic guarantee of the strength of states. At the same time, states exist through society and are controlled by society.[64]

[62] Lu Chuanying, "Shijin dangqian wangluo kongjian quanqiu zhili kunjing" (Analysis of the dilemmas of current cyberspace global governance), *Xiandai guoji guanxi*, No. 11, 2013, p. 54.

[63] Associate professor, Centre for American Studies, Fudan University (Shanghai).

[64] Cai Cuihong, "Guojia-shichang-shehui hudongzhong wangluo kongjian de quanqiu zhili" (Cyberspace governance amid the interaction of states, markets, and society), *Shijie jingji yu zhengzhi*, No. 9, 2013, p. 112

Shen Yi offers a more strategic and sophisticated perspective on the necessity of participating in currently existing institutions. For him, both unconditional support and opposition to the current order are infeasible. China should:

> (…) take security-oriented governance (*zhili mouqiu anquan* 治理谋求安全) as a starting point and embrace the principle of common heritage of humanity (*renlei gongtong yichan* 人类共同遗产). [Through strategic coordination with new great powers, it would be possible to] unite and coalesce like-minded countries, such as developing countries with a low technological level and high dependency on the Internet, and which are concerned about how the US takes advantage of their hegemony. (...) The objective of this strategy would be to put data sovereignty at the centre (*yi shuju zhuquan wei hexin* 以数据主权为核心), to build an open and attractive Internet governance ecosystem (*juyou youhuoli de kaifang de wangluo kongjian zhili shengtai xitong* 具有诱惑力的开放的网络空间治理生态系统), and to strive for the improvement of global Internet governance on an open basis, to guarantee mutual security and ordered development. (pp. 154-155).

Among the potential difficulties envisioned by Shen Yi is the fact that giving more power to sovereign governance or establishing supervision by an intergovernmental organisation such as the UN could easily lead the US to stop its withdrawal from global Internet affairs (and indeed, the United States has clearly expressed that multistakeholderism is a condition for its withdrawal from IANA stewardship; NGOs and rights advocates also have shown an ability to mobilise whenever intergovernmental schemes were pushed forward at important summits). So in Shen Yi's opinion, other countries should "find another non-governmental institution, including an enterprise or a private corporation, that would be powerful enough to try and compete with the level of control of Internet governance that the US has inherited, and to use innovative, non-traditional means to push for, guarantee, and realise the data sovereignty of states." This wording suggests that a formally multistakeholder organisation could actually serve the strategic interests of China if it contributes to balance the power of the US over Internet governance.

In a 2015 article, Shen Yi further expresses the view that it is impossible for China to replace the US as the global leader of cyberspace. In the short term, it is only possible to develop substitutes in certain key sectors, such as Huawei for traffic hubs, in order to put data transmission technologies into Chinese hands. This means that:

> The relevant departments should establish the necessary adjustments for governance, design of infrastructure, and methods. These adjustments should not only correspond to the interests of China, but also to the international rules of the game, at least from a formal and procedural point of view.[65]

Shen Yi's analysis clearly indicates a strategic vision of how China can defend its interests within the current state of global Internet governance institutions, without having to be vocal about replacing the whole system, and instead trying to change it from within. His vision seems to strike a chord in certain political spheres, as he is quoted in prominent Chinese articles[66] and has also expressed his opinions in the *Huffington Post*[67] for a global audience.

It also echoes the tone of editorials and analyses published in various venues by Chinese experts. For many, with limited strategic room to manoeuvre, and lacking an existing global, legal, or diplomatic framework to rely on, it seems more fruitful to adopt a flexible strategy where concrete issues are dealt with in a very ad hoc way, using all possible levers, from implementing filtering measures to intergovernmental dialogue (particularly on cybercrime and cybersecurity) and to hands-on involvement of the private sector in the more technical operational decisions of Internet governance. For example, Li Yan[68] argues that China never opposed the multistakeholder model, but defends a "flexible, pragmatic, multiple application" of it, "eliminating the misconception of its 'statist' view of the Internet, while also strengthening cooperation with both governmental and non-governmental [Internet governance] actors and supporting the reform of ICANN."[69]

Conclusion: Global order, cybersovereignty and public interest

Overall, these articles remain relatively general in the way they deal with global Internet governance. There are relatively few in-depth remarks on the sociological, economic, legal, or organisational functioning of ICANN, the IGF, or Netmundial, for example. International relations and legal perspectives are in the majority, with more attention paid to the articulation between the various multistakeholder, international, and bilateral platforms of discussion in relation to the strategic interests of China.

This scholarship reflects a rather dichotomous and culturalist vision of the post-Cold War world, where the United States and other Western countries such as those in Europe (or sometimes Japan) have acquired a hegemonic position thanks to their technological superiority, and draw benefits from the apparent lack of order in cyberspace. China, frequently seen abroad as the main source of cybersecurity issues with its increasing technological capabilities, is depicted in this group of articles as the main victim of Western technological superiority, in line with official discourse.

The notions of common good and public domain are generally treated with suspicion as concepts put forward by the global hegemons to perpetuate their technological, political, and cultural superiority. In most cases, the global common good is equated at best with international peace or peaceful coexistence, concepts very commonly used in Chinese diplomacy, and translates into a preference for multilateral – or intergovernmental – governance frameworks, such as the United Nations International Telecommunications Union. When support is expressed for China's active and open cooperation within the existing "multistakeholder" governance institutions, it is more out of the need to influence Internet governance in the short term, and out of confidence that China has enough assets (with its private sectors and sizeable

[65] Shen Yi, "Quanqiu wangluo kongjian zhili yuanze zhizheng yu Zhongguo de zhanlüe xuanze" (The controversy on the global cyberspace governance principles and China's strategic choices), *Waijiao pinglun*, No. 2, 2015, pp. 1-15; pp. 14-15

[66] Zhao Li and Gu Peng, "Zhuanjia: Zhongguo li tui jianli guiji wangluo kongjian zhili xin tixi" (China actively pushes building of new system of international governance of cyberspace), *Fazhi ribao* (Legal Daily), 28 September 2015, www.chinanews.com/gn/2015/09-28/7547457.shtml (accessed on 16 October 2015), translated in David Bandurski, "Re-Defining Cyberspace," *art. cit.*

[67] Shen Yi, "For China and the U.S., Cyber Governance Is Better Than Cyberwar," *art. cit.*

[68] Deputy director, Institute of Information security and social development, China Institutes of Contemporary International Relations.

[69] Li Yan, "Reforming Internet Governance and the Role of China," *Focus Asia*, Institute for Security and Development Policy, Stockholm, February 2015, p. 7, http://mercury.ethz.ch/serviceengine/Files/ISN/188532/ipublicationdocument_singledocument/c12383a2-7716-4a40-bfc2-a814025bdf40/en/2015-LiYan-Reforming-Internet-Governance-and-the-role-of-China.pdf, (accessed on 19 October 2015).

market) and allies (with like-minded countries) to defend its interests, than out of genuine belief in the global public usefulness of such institutions.

The frequent use of the concept of hegemony is therefore not associated with any critique of the capitalist world order, as is the case in Gramscian theory and in the political economy of communication. Instead, it reflects a "realist" vision of international relations where states, as the only relevant actors, mainly act to defend their interests and security in a digital world primarily qualified as anarchic (which in itself is a problematic statement). In this context, cybersecurity and social order are presented as pressing issues that require the elaboration of a more sophisticated Chinese cyberstrategy.

The ideas expressed in this sampling of academic articles seem to provide some inspiration to the higher circles of Chinese politics. The concept of cybersovereignty was promoted to the top of the agenda at the 2nd World Internet Conference,[70] where Xi Jinping himself delivered a speech entitled "Promoting the transformation of the global system of Internet governance" (*tuijin quanqiu hulianwang zhili tixi biange* 推进全球互联网治理体系变革), which contains key concepts outlined here:

> (...) respecting each country's right to choose its own internet development path, its own internet management model, its own public policies on the Internet, and to participate on an equal basis in the governance of international cyberspace – avoiding cyber-hegemony, and avoiding interference in the internal affairs of other countries.[71]

Year on year it seems that the Chinese leadership is showing more confidence and assertiveness in putting forward the cybersovereignty agenda in every possible venue. For instance, the negotiations for the Ten-Year Review of the World Summit on the Information Society, a forum on Internet governance organised under the umbrella of the United Nations, represented a significant step forward, as the word "multilateral" was included once in the final report.[72]

This compromise highlights that China can find alliances in global governance institutions. In the sampled articles, China is qualified alternatively as a developing country (*fazhanzhong guojia* 发展中国家), a "newly developed country" (*xinxing fazhan guojia* 新兴发展国家), or a new cyberpower (*wangluo daguo* 网络大国). The digital divide, which impairs the former, as well as the lack of recognition, which is deemed unfair to the latter, both serve as arguments in favour of rebalancing the Internet world order. This somewhat ambivalent positioning is seen as advantageous to China in its quest for allies. Indeed, China's positions are supported by other developing countries such as some members of the Group of 77 (which gathers developing countries),[73] as well as more advanced cyberpowers such as Russia.

True, its allies are found among relatively less powerful countries in terms of Internet development, and they remain in the minority. 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 firmly against the idea of a purely intergovernmental governance model.[74] Chinese netizens noted that most of the heads of state who attended the Wuzhen World Internet Conference were in fact from countries where the Internet is less developed, and even proposed, not without irony, to rename it the "Third World" Internet Conference.[75] Short of more powerful allies, changing the framework of Internet governance to an intergovernmental model may remain an inaccessible goal.

However, China can also take advantage of the (still ill-defined) multistakeholder scheme to advance its agenda through other actors, in particular in the private sector, as suggested by the apparent rapprochement of Xi Jinping and Lu Wei, the head of the Cyberspace Administration of China, with the American giants of the Internet during the Chinese-American technology forum in September 2015.[76] The recent trip to China by Mark Zuckerberg, Facebook's CEO,[77] (which was mocked in the Chinese social media), also suggests that the biggest global Internet businesses may find some of their interests converging with those of the Chinese leadership. To assess the influence and power of China in this multistakeholder Internet governance context, it is no longer enough to look at intergovernmental alliances alone. One needs instead to look at specific policy measures and at what kind of actors push them forward – governments but also private companies, experts, and NGOs, among others. In this global and complex movement to reshape the Internet world order, China might find itself much less isolated than during the last decade.

Séverine Arsène is a researcher at CEFC and chief editor of *China Perspectives*.
CEFC, 20/F Wanchai Central Building, 89 Lockhart Road, Wanchai, Hong Kong (sarsene@cefc.com.hk).

[70] Xi Jinping, "Xi Jinping zai di er jie shijie hulianwang dahui kaimushi shang de jianghua" (Xi Jinping's inaugural discourse at 2nd World Internet Conference), *Xinhuanet*, 16 December 2015, http://news.xinhuanet.com/politics/2015-12/16/c_1117481089.htm (accessed on 16 February 2016).

[71] Cited in Fang Kecheng, "Diplomacy Is the Point of China's World Internet Conference," translated by David Bandurski, *China Media Project*, 21 December 2015, http://cmp.hku.hk/2015/12/21/39527 (accessed on 16 February 2016).

[72] Dan Levin, "At U.N., China Tries to Influence Fight Over Internet Control," *NYTimes.com*, 16 December 2015, www.nytimes.com/2015/12/17/technology/china-wins-battle-with-un-over-word-in-internet-control-document.html (accessed on 17 February 2016).

[73] There is a clear effort from the Chinese leadership to win support among African and Asian developing countries, as shown, for example, by the publication of an editorial on the Wuzhen Conference by a council member of the government-controlled Asia-Africa Development and Exchange Society of China. Cao Xin, "'Wangluo zhuquan' de guoji beijing yu Zhongguo hulianwang tese" (The international background of "cybersovereignty" and the specificities of the Chinese Internet), *Financial Times (Chinese Edition)*, 23 December 2015.

[74] See for example: "French Government Submission to NETmundial," *Netmundial*, 4 March 2014, http://content.netmundial.br/contribution/french-government-submission-to-netmundial/154 (accessed 6 April 2016).

[75] Fang Kecheng, "Diplomacy Is the Point of China's World Internet Conference," *art. cit.*

[76] Paul Mozur and Jane Perlez, "China Flexes Tech Muscles Before a State Visit," *NYTimes.com*, 8 September 2015, www.nytimes.com/2015/09/09/science/china-flexes-tech-muscles-before-state-visit-with-meeting-of-industry-giants.html?_r=0 (accessed on 22 March 2016).

[77] Associated Press, "Facebook's Mark Zuckerberg Meets China Propaganda Chief in Beijing," *The Guardian*, 20 March 2016, www.theguardian.com/world/2016/mar/20/facebooks-mark-zuckerberg-meets-china-propaganda-chief-in-beijing (accessed on 6 April 2016).