The impact of China on global Internet governance in an era of privatized control

Séverine Arsène

The impact of China on global Internet governance in an era of privatized control

Séverine Arsène
Ph.D in political science, Science Po, France
Yahoo! Fellow in residence, Georgetown University (2011-2012)
sa773@georgetown.edu

CIRC 2012
Communication

Over the last ten years, China has become one of the most prominent actors of the global Internet. It not only has the largest online population (513 million in January 2012[1]). Chinese corporations like ZTE and Huawei are also leaders on the global market for Internet infrastructures and mobile devices. Chinese financial institutions strongly support Chinese corporations' development overseas by providing funds for massive infrastructure projects, particularly in the telecommunication sector. Furthermore the Chinese government and other private actors are playing an increasingly important role in international fora where Internet governance is discussed, such as the ICANN and the IGF.

Consequently, the fact that China advocates national sovereignty over the Internet and the existence of a censorship system called the "Great Firewall of China" may be misleading. The main stake of China's development as a central actor of the Internet may not be the creation of a Chinese Intranet that would be isolated from the rest of the world, but on the contrary the most concerning aspect could be China's overwhelming and constantly increasing presence and influence in the global Internet ecosystem. One central issue is therefore to assess the impact that China may have on the adoption of new norms for the Internet globally, from technical standards to more "moral" codes of conduct.

This evolution takes place in a world where the control of the Internet increasingly lies in the hands of private actors and corporations. Indeed a growing number of countries are passing legislations that transfer the responsibility of controlling online publications to service providers. The latters' terms of uses and editorial choices also bear worldwide effects, often with a lack of clarity upon which jurisdiction to turn to. In this context, the fact that Chinese corporations, which are often directly or indirectly linked to the

[1] CNNIC, « Statistical report on the Internet Development in China », janvier 2012, http://www.cnnic.cn/dtygg/dtgg/201201/t20120116_23667.html.

Chinese government, are becoming global leaders in the telecommunications sector, may have a tremendous impact on essential issues, from Internet neutrality to cybersecurity and most importantly to the freedom of speech.

To investigate the various dimensions of the Chinese impact on global Internet governance, my communication will break down into three parts. I will first describe the "self-disciplinary" aspect of the control of online activities in China. I will then analyze how this control strategy is interlinked with the Chinese government's defense of Internet sovereignty. Finally, I will focus on the extension of the Chinese influence beyond the Chinese borders, notably through the government's support to Chinese corporations. I will finally put this into perspective with an analysis of the stakes of this influence in the background of an increasingly privatized Internet where a new kind of geopolitics is developing.

1) Internet control in China: self-discipline in exchange for modernization

In the *White Paper for the Internet in China*[2] published by the Chinese government in 2010, the Chinese leaders make it clear that they consider the Internet as a key growth engine and as a tool to develop national strength. The Chinese government officially encourages "the use of the Internet in ways which aim to promote economic and social progress, to improve public services and facilitate people's work and life". They also pride themselves of having "injected enormous sums of money into Internet infrastructure construction", which "ensured Internet access to 99.3% of Chinese towns and 91.5% of villages".

The Internet represents the promise of a more modern and wealthy Chinese way of life, which is crucial to the political stability that the Communist Party needs to stay in power. Internet connectivity is both part of this way of life and a tool to develop economic growth. As such, the Chinese Communist Party cannot but promote the use of the Internet among the Chinese citizens.

However it is very clear in the official discourse that this promise is conditional upon the ability of the Communist Party to maintain a certain level of control and censorship over online activities. This is part of the social contract throught which the CCP promises a better way of life in exchange for political stability.

The way this control has been implemented is consistent with this logic. Although the most well-known aspect of Internet censorship in China is the "Great Firewall" [3] that filters data and blocks access to critical foreign websites, most of the control is in fact exercised by the actors of the Internet themselves. The Chinese regulation of the

---

[2] « White paper: the Internet in China », 2010, http://china.org.cn/government/whitepaper/node_7093508.htm.

[3] For a more complete description of Internet censorship in China, see the country profile of China by OpenNet Initiative, 2009, http://opennet.net/research/profiles/china.

Internet is primarily based on the principle of intermediary liability, that makes Internet service providers responsible for the publications of their users. They must hire staff that makes sure that no sensitive contents are published and implement filtering systems that help delete sensitive keywords and detect potentially problematic discourse on their platforms. Besides, the "real name system" is progressively generalized to all popular social media (most recently to the microblogging services) so as to prevent Internet users from publishing subversive discourse anonymoulsy. This obviously has a chilling effects on Internet users who may self-censor out of fear of being arrested and charged, for instance, with "subversion of state power".
This censorship system is not perfect at all. There are plenty of countercensorship strategies, from the use of proxy servers to access blocked websites, to play with words, images, symbols and double meanings that enable the people to "speak truth to power"[4]. The speed with which information spreads makes it virtually impossible to cover up scandals. Above all, the control is ultimately made by individuals – police and administrative staff who identify the potentially threatening topics, moderators hired by ISPs, Internet users who self-censor – who make decisions according to their own understanding and evaluation of situations. Consequently there is some room for errors, misinterpretations or negotiations that enable some sensitive topics to make it to the front page from time to time. As a consequence the Chinese authorities are developing more sophisticated strategies to monitor and influence public opinion[5], instead of just censoring contents.

My point here is that a large part of Internet control relies on the compliance of individuals with the social contract promoted by the CCP. In other terms the infrastructure of control and the way it is exercised on a daily basis can be analyzed as a form of "governmentality" in which individuals participate in their own control and domination[6].
The insistence on the notion of "self-discipline" in the official discourse certainly is an indicator of this aspect of Internet control in China. Internet service providers are strongly encouraged to become members of organizations such as the Internet Association of China, through which informal censorsip guidelines are often transmitted, and to sign self-discipline charters such as the Public Pledge on Self-discipline for China's

[4] Ashley Esarey et Qiang Xiao, « Political Expression in the Chinese Blogosphere: Below the Radar », *Asian Survey* 48, n° 5 (octobre 2008): 752–772.
[5] David Bandurski, « China's Guerrilla War for the Web », *Far Eastern Economic Review*, juillet 2008, http://74.125.155.132/scholar?q=cache:CmJr6nHw4qMJ:scholar.google.com/+bandurski+david&hl=fr&as_sdt=2000.
[6] Michel Foucault, *The Government of Self and Others: Lectures at the College De France, 1982-1983*, trad. par Arnold I. Davidson (Palgrave Macmillan, 2010).

Internet Industry[7]. The propaganda also constantly warns Internet users against potential social disorder and crime online and insists on their responsibility to behave in a "civilized" way.
This self-discipline can be explained by various factors including fear, but also preference for stability, especially as self-censorship keeps every individual from knowing to what extent the others would be ready to break the status quo. But there are also limits to it. Whenever the control is too intrusive or interferes with the benefits brought by the Internet access, Internet users do not hesitate to voice their discontent. For example, in 2009 the attempt to implement a mandatory installation of a filtering software named "Green Dam Youth Escort" on all computers sold in China failed after Internet users vigourously protested online[8].

It is important to understand this kind of contractual nature of Internet control in China in order to analyze China's position on Internet governance on the global stage and the stakes of an increasing presence of Chinese Internet companies throughout the world. Indeed, China can not afford to build a Chinese "intranet" that would be totally isolated from the rest of the world, for fear of breaking the promise to build a more modern, comfortable society through new technologies and Internet connectivity. Instead, China is advocating Internet sovereignty domestically and promoting the interests of Chinese-controlled companies abroad, which may enable them to ensure the sustainability of its self-discipline model.

2) China, Internet sovereignty and the global Internet governance

Although the goal is not to build an isolated Chinese Internet, the type of control chosen by the CCP requires that the definition and implementation of Internet infrastructures, regulations and codes of conduct that Chinese Internet users are subject to remain in the hands of the Chinese government.
Domestically this means that the Chinese government firmly opposes any interference with their control of Internet activities. The *White Paper on the Internet in China* makes a direct link between Internet control and the notion of Internet sovereignty. "The Internet sovereignty of China should be respected and protected. Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China". As part of this doctrine, any

[7] Launched in 2002 and signed by more than 300 signatories. « Chinese sites agree to censor content », *The Guardian*, juillet 16, 2002, http://www.guardian.co.uk/technology/2002/jul/16/onlinesecurity.internetnews.
[8] Tom Doctoroff, « China's Digital Green Dam: The Party Capitulates », *Huffington Post*, juin 30, 2009, http://www.huffingtonpost.com/tom-doctoroff/chinas-digital-green-dam_b_223535.html.

call for more freedom of expression on the Chinese Internet is treated by the propaganda as an attempt by the West to undermine the country's stability.

On a global scale, this position is relatively incompatible with the multi-stakeholder governance model that currently prevails in the Internet sector. Today some of the most important political and technical decisions concerning the global Internet are not taken by government representatives only, but by engineers, members of non-profit organizations, lobbies and individuals along with governments, through participation in organizations that are called "multi-stakeholder". For example the elaboration of technical standards is essentially conducted by the Internet Engineering Task Force (IETF) which self-advertises as "a loosely self-organized group of people" which "is not a corporation and has no board of directors, no members, and no dues". The Domain Name System is managed by the Internet Corporation for Assigned Names and Numbers (ICANN), which is considered as one of the pioneering multi-stakeholder organization, with representations of the private sector and non-profit sector along with governments. In 2005, at the World Summit on the Information Society (WSIS) organized by the UN in Tunis, the Internet Governance Forum was created as a forum where all different stake-holders would be able to discuss Internet governance issues[9].
Although this governance model appears to be generally more inclusive, it is still quite experimental and raises new questions, notably on the relative weight every group should be given, on the degree of consensus that is necessary to validate a decision or on the degree of representativity of self-declared stakeholders towards the rest of the society.
China and other developing countries are particularly critical of these organizations, that they see as an instrument in favor of American and Western hegemony. First the cost of participation turns out to create a bias in favor of developed countries, where stakeholders have more resources to actively engage in research and lobbying activities. Moreover they question the independence of such organizations as the ICANN, which headquarters are situated in California and that is linked to the American Department of Commerce by a memorandum[10].
China was particularly dissatisfied with the non-alignment of the ICANN with the international *status quo* concerning Taiwan. From 2001 to 2009, it refused to send representatives to its "Governmental Advisory Committee" because of the representation of Taiwan with a government status. China finally started sending representatives again in 2009, only after a compromise was reached, through which Taiwan was renamed in Chinese Taipei.

---

[9] On multi-stakeholderism: Wolfgang Kleinwächter, éd., *Internet Policy Making*, Co:llaboratory discussion paper series no.1 2 (Berlin et Nairobi: Internet & Society Co:llaboratory, 2011); Jeremy Malcolm, *Multi-Stakeholder Governance and the Internet Governance Forum* (Perth 2008: Terminus Press, 2008); Milton L Mueller, *Networks and states : the global politics of Internet governance*, 1 vol., Information revolution and global politics (Cambridge, Mass. ; London: MIT Press, 2010).
[10] http://www.ntia.doc.gov/page/docicann-agreements

Besides, China opposed the renewal of the mandate of the IGF that occurred in 2010, five years after its creation[11]. As the IGF's mandate was finally renewed, China seems to try and make its governance more intergovernmental and to put it more clearly under the responsibility of the UN[12].

Beyond these specific criticisms, the very principle of multi-stakeholderism is totally contradictory with the Chinese notion of Internet sovereignty. The main objective of the Chinese government is to remain the only legitimate representation of the Chinese population on the international stage. Therefore China claims that Internet governance should be inter-governmental.

As more and more countries are concerned with cybersecurity and law enforcement issues, China is not the only country that advocates for more cyber-sovereignty and inter-governmental dialogue, as exemplified by the e-G8 organized in France in 2011 or the London conference in 2012. 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). Another example is the Anti-Counterfeiting Trade Agreement, which was discussed by some fourty countries, but did not involve such important countries as China, India or Brazil.

As a consequence, the Chinese government considers the United Nations as the ideal framework for a global Internet governance. It states in its *White Paper* that "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 organization under the UN system through democratic procedures on a worldwide scale."

As a consequence of this position, at the 2005 WSIS in Tunis, the Chinese government tried, unsuccessfully, to obtain that the responsibilities of the ICANN be transferred to the International Telecommunications Union, under the framework of the UN. As the treaty known as International Telecommunications Regulations (ITRs), that dates back in 1988, is being renegotiated in 2012, China is pushing towards enlarging the role of the ITU to such issues as cybersecurity and the domaine name system[13].

---

[11] Rebecca MacKinnon, « China calls for an end to the Internet Governance Forum », *RConversation*, mai 14, 2009, http://rconversation.blogs.com/rconversation/2009/05/china-calls-for-an-end-to-the-internet-governance-forum.html.

[12] On China, the ICANN and the IGF: Milton Mueller, « China and Global Internet Governance », dans *Access contested*, éd. par Ronald Deibert, Rafal Rohozinski, et Jonathan Zittrain (Cambridge (Mass.): MIT Press, 2012), 177–194, http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-chapter-09.pdf.

[13] Robert McDowell, « The U.N. Threat to Internet Freedom », *WSJ.com*, février 21, 2012, http://online.wsj.com/article/SB10001424052970204792404577229074023195322.html; Ben Woods, « Schmidt: UN treaty a "disaster" for the internet », *ZDNet UK*, février 29,

Such a framework would also enable the Chinese government to prevent dissident voices from China or other authoritarian countries to express their views on the global Internet governance. Rebecca MacKinnon, a journalist, specialist of China and Internet freedom activist, experienced it during the Tunis Summit in 2005. She was supposed to be the moderator of a workshop entitled "expression under repression". Although this workshop had been authorized and put on the agenda by the organisers, it was removed from the program by the Tunisian government under the excuse that it did not fit the general topic of the conference, "ICT for development". The workshop was finally held after the intervention of the Dutch ambassador but without advertisement[14]. Another incident happened during the IGF meeting in Sharm-el-Sheikh in 2009. Researchers from the Open Net Initiative were prevented from distributing flyers and displaying a poster for the launch of their book *Access Controlled*, because they reproduced a text from the back cover of the book that mentioned Internet censorship in China[15].

The Chinese government is clearly advocating for an Internet governance scheme that would guarantee their sovereignty over online activities in China and their position as the only legitimate representatives of the Chinese Internet users' interests. However they are not in the business of building a Chinese Internet that would be isolated from the rest of the world, a so-called "intranet", as proved by their pragmatic way of defending their interests within the current governance scheme.

3) Chinese governmentality beyond the Chinese territory

Although the Chinese government is not in favour of multi-stakeholderism, they have been actively participating in the currently existing organizations to defend their interests.

The Chinese representatives took part again in the ICANN's Governmental Advisory Committee in 2009, just when the ICANN was opening a series of very important negotiations concerning the domain name system[16]. One important issue was the creation of "internationalized top level domain names", in other words domain names written in non-latin scripts. In 2010 China obtained an accelerated procedure to create the <.中国> (.China) country code top level domain name (ccTLD), which enabled them to create a website for the Shanghai World Expo with a URL in Chinese: <http://上海世

2012, http://www.zdnet.co.uk/news/regulation/2012/02/29/schmidt-un-treaty-a-disaster-for-the-internet-40095155/.

[14] Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books, 2012), p. 203.

[15] Ronald Deibert et al., *Access contested*, MIT Press. (Cambridge, Mass., 2012), p. 3.

[16] Rebecca MacKinnon, « China @ ICANN: thoughts from former CEO Paul Twomey », *RConversation*, juillet 3, 2009, http://rconversation.blogs.com/rconversation/2009/07/china-icann-thoughts-from-former-ceo-paul-twomey.html.

博会.中国>. Another important issue is the creation in 2012 of a new set of "generic top-level domain names" (gTLDs), like <.sport> or <.music> but also, potentially, trademarks like <.haier> or internationalized gTLDs like <.教育> (.edu)[17].
Actually China had already implemented a Chinese domain name system that was only available from China, with such domain names as <.中国> (.china), <.公司> (.entreprise) and <.网络> (.net), as well as subdomains like <.com.cn>, as early as 2006[18]. This initiative was first considered as a step towards the creation of a Chinese Intranet. However the Chinese participation in the creation of a global system that includes internationalized domain names underlines the fact that their position is more complex. As the Internet is a central part of the Chinese government's strategy to enhance its own legitimacy by providing growth opportunities, it is crucial for them to be able to defend the interests of Chinese companies, communities and trademarks that could draw considerable benefits from these new "online territories". At the same time this may extend the effects of intermediate liability beyond the Chinese territory, over some part of the Chinese-language online activities. One key issue is therefore what proportion of the new internationalized gTLDs will be administered by Chinese registrars (through the CNNIC) and therefore fall under some kind of Chinese supervision.

China is also expanding its influence over the global Internet by developing its own technical standards and by supporting the adoption of global standards that are favorable to Chinese companies. One motive is to reduce China's dependency on foreign patterns and, if possible, to draw revenues from royalties on native Chinese technologies. For instance China has invested a lot to pioneer such technologies as the Ipv6 protocol. They opened a test platform within the CERNET network as soon as 1998 and ran the 2008 Olympic games information system with this protocol[19]. China can also use the attractiveness of its market to force companies that want to do business in China to adopt Chinese standards. For example, in 2003 the Chinese authorities considered imposing the use of the standard known as Wireless Local Area Network Authentication and Privacy Infrastructure (WAPI) on all wireless local network devices sold in China, which can be considered as a technical barrier to trade on the Chinese market and therefore contradictory with the rules of the WTO[20]. The mandatory use of this standard was finally replaced by a simple "preference" but China has not

---

[17] More than 1200 applications have been received by the ICANN so far. http://newgtlds.icann.org/en

[18] Rebecca MacKinnon, « China's New Domain Names: Lost in Translation », *CircleID*, février 28, 2006, http://www.circleid.com/posts/chinas_new_domain_names_lost_in_translation/.

[19] Laura DeNardis, *Protocol politics : the globalization of Internet governance*, Information revolution and global politics (Cambridge (Mass.): MIT Press, 2009), p. 110.

[20] Christopher Gibson, « Technology Standards - New Technical Barriers to Trade? », éd. par Sherrie Bolin, *The standards edge: golden mean* (2007), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=960059.

abandoned the standard. They have submitted it (unsuccessfully) to the ISO in 2006 and 2009 and showcased it during the Olympic Games in 2008. Another example of the way China defends standards that are favorable to its companies is how they strongly support the adoption of the Multiprotocol Label Switching (MPLS) standard before the IETF and later before the UIT, at the expense of the relationships between the two organizations[21].

With proprietary technologies, China would also be in a better position to conquer foreign markets, particularly in developing countries where new infrastructures depend less on previous technological choices. The two Chinese telecommunications giants, Huawei and ZTE, are building Internet network backbones and wireless networks in such countries as Ethiopia, Angola or Tanzania, often with the financial support of the Chinese Exim Bank[22]. Chinese Internet and mobile phone service providers, China Telecom and China Mobile, are also looking at overseas markets, in developing countries as well as in Europe and the United States[23].

This increasing presence of Chinese companies on the global telecommunications market raises some concerns in terms of cybersecurity, both for governments and citizens. The United States and Australia have barred Huawei and ZTE from participating in projects to build network construction projects on their territories[24]. The US Congress is investigating whether the "networking equipment sold could secretly contain Chinese military technology to spy and interfere with U.S. telecommunications" [25]. Besides, these companies are known for having sold surveillance technologies to Iran (they subsequently promised to reduce this partnership with Iran, just like American

---

[21] Iljitsch van Beijnum, « ITU bellheads and IETF netheads clash over transport networks », *ars technica*, mars 3, 2011, http://arstechnica.com/tech-policy/news/2011/03/itu-bellheads-and-ietf-netheads-clash-over-mpls-tp.ars.

[22] Andrea Marshall, « China's mighty telecom footprint in Africa », *E-learning Africa*, février 21, 2011, http://www.elearning-africa.com/eLA_Newsportal/china%E2%80%99s-mighty-telecom-footprint-in-africa/.

[23] Jonathan Browning et Edmond Lococo, « China Mobile seeks partners abroad », *China Daily*, février 16, 2011, http://www.chinadaily.com.cn/bizchina/2011-02/16/content_12024698.htm; « China Telecom Will Launch Mobile Services In UK », *China Tech News*, janvier 11, 2012, http://www.chinatechnews.com/2012/01/11/15975-china-telecom-will-launch-mobile-services-in-uk.

[24] Yueyang (Maggie) Lu, « Australia Bars Huawei From Broadband Project », *NYTimes.com*, mars 26, 2012, http://www.nytimes.com/2012/03/27/technology/australia-bars-huawei-from-broadband-project.html.

[25] Michael Kan, « US Committee to Investigate China's Huawei, ZTE », *PCWorld*, novembre 18, 2011, http://www.pcworld.com/businesscenter/article/244210/us_committee_to_investigate_chinas_huawei_zte.html.

companies had done before them)[26]. More generally speaking, the intricate links between the Party and the leadership of the Chinese corporations, especially in such a sensitive field, raise some concerns. For example Huawei's founder, Ren Zhengfei, is known for having hold the position of deputy director in the Chinese People's Liberation Army's engineering corps. In reaction, Chinese companies firmly deny the existence of any cyberthreat and make more transparency efforts than ever[27].

Whatever the reality of the cybersecurity risk, it might overshadow another important stake of an increasing Chinese presence on the global Internet. It is already clear that it has a central role in the Chinese "soft power" strategy that was made an official priority during the 2011 Plenum of the Party[28]. By developing patterns, by being in charge of a large part of the Chinese-language domain names, and by using Chinese corporations as flagships to advertise the Chinese technological assets, the Chinese authorities may be able to influence the global narratives in its favor.
Moreover, as these moves may render some actors dependent on the Chinese corporations, patents, licences and regulations, one could expect the extension of some kind of self-disciplinary behavior to these actors.

Internet geopolitics in an era of privatized control

This aspect is all the more important that todays's global Internet is characterized by what one could call "privatized control". As a small number of Internet service providers concentrate a large part of the people's online activities and time, their personal data and social networks, they exercise a considerable power on their users through the mere application of their terms of uses. They can censor contents that they find objectionable, delete users' profiles or sell their personal data to third parties, and most importantly, change the terms of uses unilaterally. Some services even play roles that used to be the monopoly of states, such as guaranteeing their users' identity or maintaining social order online. Such companies as Apple, Facebook or Google have so

---

[26] Steve Stecklow, Farnaz Fassihi, et Loretta Chao, « Huawei, Chinese Tech Giant, Aids Iran », *WSJ.com*, octobre 27, 2011, http://online.wsj.com/article/SB10001424052970204644504576651503577823210.html; Bryan Bishop, « ZTE follows Huawei's lead, promises to curb Iran business after surveillance system sale », *The Verge*, mars 24, 2012, http://www.theverge.com/2012/3/24/2898835/zte-follows-huaweis-lead-promises-to-curb-iran-business-surveillance-system.

[27] Kevin Brown, « Huawei's opacity a colourful issue for US », *Financial Times*, avril 19, 2011, http://www.ft.com/cms/s/0/65e93b90-6a84-11e0-a464-00144feab49a.html#axzz1uafyc2XQ.

[28] David Bandurski, « All in favor of culture, say "Aye" », *China Media Project*, octobre 26, 2011, http://cmp.hku.hk/2011/10/26/16743/.

many users and such an important role in their life that they could be compared to virtual "countries"[29].

It would be inaccurate, however, to depict these virtual territories as totally independent from the offline world. Internet service providers are subject to the regulations of the countries where they host their servers, where they register domain names, where they hire staff and where users access their services from.

Everywhere, concerns about cybercrime (pornography, counterfeiting), cybersecurity (spying, terrorism) or freedom of speech abuses lead to a greater focus on Internet sovereignty and more strict regulations of online activities. Intermediary liability is one of the priviledged tools used by governments to control online activities, particularly when law enforcement is challenged by their international character. In Australia, Internet service providers have been authorized to "voluntary" block a list of child-abuse websites, while a more general law on Internet filtering is pending[30]. In India, the Delhi High Court has ordered 21 companies to censor online contents that may be considered offensive to religious beliefs[31]. In Italy, Google employees have received suspended six-months sentences for allowing an offensive video to be posted online[32].

As a consequence, such companies as Google and Twitter have announced filtering policies that are adapted to every country[33]. Companies that cannot afford such a sophisticated system find themselves in a situation where they have to comply with multiple, sometimes contradictory legislations or see their websites blocked on certain territories.

Some countries' regulations also have an impact beyond their borders. For example the US seize hundreds of domain names every year, directly from VeriSign, an American company which manages domain names ending in .com, .net, .cc, .tv and .name[34]. As a consequence American laws apply to websites that do not belong to American companies, are not hosted in the US and that are not necessarily used by American citizens.

---

[29] MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom*.

[30] Jennifer Dudley-Nicholson, « Telstra, Optus to start censoring the web next month », *News.com.au*, juin 22, 2011, http://www.news.com.au/technology/internet-filter/telstra-optus-to-begin-censoring-web-next-month/story-fn5j66db-1226079954138.

[31] Emil Protalinski, « Indian court forces Facebook, Google to censor content », *ZDNet*, février 6, 2012, http://www.zdnet.com/blog/facebook/indian-court-forces-facebook-google-to-censor-content/8643.

[32] « Google bosses convicted in Italy », *BBC*, février 24, 2010, http://news.bbc.co.uk/2/hi/8533695.stm.

[33] Danny Sullivan, « Twitter Now Able To Censor Tweets, If Required By Law, On A Country-By-Country Basis », *Marketingland*, janvier 26, 2012, http://marketingland.com/twitter-now-able-to-censor-tweets-by-country-4531.

[34] David Kravets, « Uncle Sam: If It Ends in .Com, It's .Seizable | Threat Level | Wired.com », *Wired*, mars 6, 2012, http://www.wired.com/threatlevel/2012/03/feds-seize-foreign-sites/.

In other words, despite numerous claims in favour of an open, borderless and neutral Internet, the web is currently subject to a new form of geopolitical struggle, a struggle for sovereignty over the virtual "territories" that are domain names, search engines, social networks and other websites.
One can understand China's position towards the global Internet governance, their advocacy for Internet sovereignty, their efforts to obtain a globally accessible domain name system in Chinese or their investments in research to develop proprietary technologies against this background. Although the Chinese government's advocacy for Internet sovereignty enables them to exercise a very strict domestic control of online activities, the main objective is not to isolate the Chinese Internet users from the global Internet. It is rather to secure a dominant position over a significant part of the developing online territories. From the perspective of the CCP, this is a way to reinforce their legitimacy by arguing that they are defending the Chinese people's interests, while ensuring a "good enough" control through intermediate liability and self-discipline.

Needless to say, this analysis of the Chinese position is not an appeal to take part in the geopolitical struggle and compete with China for virtual territories, for it would only reinforce a logic that is occurring at the expense of the citizens' freedoms and mostly without their consent[35]. It is rather an appeal for an inclusive, democratic and transparent global Internet governance that would ensure, among other commons, net neutrality and freedom of speech online.

[35] See *MacKinnon, Consent of the Networked: The Worldwide Struggle for Internet Freedom*. See also arguments by the Electronic Frontier Foundation or La Quadrature du Net for example. http://www.laquadrature.net/