scripted

Volume 9, Issue 2, August 2012

CHINA AND THE INTERNET: EXPANDING ON LESSIG'S REGULATION NIGHTMARES

Vasileios Karagiannopoulos [*]

Abstract

This paper focuses on the Internet policies of the People's Republic of China (PRC). It discusses the ways the governing Communist Party of the PRC manipulates factors that regulate behaviour online to an extent that actually enables it to control the flows and content of information and subsequently, also, the politicisation of the Internet community. Consequently, such practices enable the ruling regime to maintain the status quo, allowing only minor, localised modifications to its policies and avoiding major political and ideological ruptures. The essay discusses the Internet conditions in China through the prism of Prof. Lawrence Lessig's theory, adopting the same quadripartite system for analysing regulatory factors in relation to cyberspace behaviours. The analysis further demonstrates how the ruling party is realising Lessig's fears in relation to the four identified categories of regulatory modalities and also how the government even adopts additional measures in order to preserve and extend its control through implicit, as well as aggressive tactics. The ultimate goal of this paper is to demonstrate how China might be formulating its own model of Internet governance and how this model might be gaining more power, becoming capable of eliminating, controlling or co-opting any serious challenges to it from internal and external influences.

DOI: 10.2966/scrip.090212.150

[*] PhD Candidate/Tutor of Law - University of Strathclyde, School of Law, e-mail: v.karagianno@gmail.com

1. Introduction

In its early years, the Internet had been considered a globally interconnected medium with the potential to facilitate a new democratic reality, a hope that was eloquently expressed by many theorists and plain users.[1] The open, decentralised technology of the medium, the geographical distribution of its users and the multi-faceted nature of its content, seem to pose serious challenges to any attempt to be regulated by any societal or state actors.[2] However, it would appear that these hopes have not materialised, since limitations on the structuring of the Internet and also on the free, universal exchange of information have been widely developed and employed based on various cultural, religious, political or financial reasons, such as national security or copyright.[3] The country with potentially the strictest regime worldwide in relation to information production and circulation, demonstrating the various ways cyberspace communications could be regulated, is the People's Republic of China (PRC).

The Chinese Communist Party (CCP), which is currently ruling the PRC under a strange mixture of a single party communist model with capitalist aspirations, has been forced to adopt multiple measures and restrictions in order to structure the Internet in accordance with its cultural and political principles, but also facilitate China's information technology-based economic development scheme.[4] The question of whether such policies could be successful in regulating online behaviour and eventually managing to adequately censor and control the Internet experience of users within the PRC seems very much related to Lessig's discussion of Internet regulation. A core part of his argument is that the Internet could be controlled very effectively and extensively, when laws, market policies, norms and code can be manipulated adequately by certain actors, such as the state.

This paper assesses whether the Chinese state can or has already gained an adequate degree of control over all potentially engaged regulatory actors, enabling the government to extensively structure the Internet experience of its citizens and potentially shape global norms and standards, presenting a paradigm for other regimes. The analysis will attempt to show that the CCP has not just relied on traditional blocking of information and spreading of propaganda, which are the main regulatory dangers Lessig describes in relation to technological controls. It has additionally even adopted a more implicit tactic, attempting to use the informational

---

[1] J Barlow, "The Declaration of Independence of Cyberspace" (1996) available at https://projects.eff.org/~barlow/Declaration-Final.html (accessed 26 Jul 12); A Murray, *The Regulation of Cyberspace: Control in the Online Environment* (London: Routledge, 2007), at 5-7.

[2] C Li, "Internet Content Control in China" (2003-4) 8 *International Journal of Communications Law and Policy,* 39-69, at 47.

[3] See various examples in T Wu and J Goldsmith, *Who Controls the Internet? Illusions of a Borderless World* (Oxford: Oxford University Press, 2006); Other examples would be the decisions of the UK government to filter or block social media during political events: J Halliday and J Garside, "Rioting Leads to Cameron Call for Social Media Clampdown" (2011) available at www.guardian.co.uk/uk/2011/aug/11/cameron-call-social-media-clampdown (accessed 26 Jul 12).

[4] Information Office of the State Council of the People's Republic of China "The Internet in China" (2010) Editor: Piny Han, available at http://english.gov.cn/2010-06/08/content_1622956.htm (accessed 26 Jul 12).

and civic potential of the medium for the benefit of the ruling Party. Finally, the discussion will demonstrate how the ruling regime has cracked down aggressively on- and offline against practices of users and even corporations that might have the potential to compromise its control. In order to set the groundwork for such discussion, Lessig's views on the regulability of cyberspace will be elaborated and will subsequently be combined with an overview of the Internet realities in China. This process will connect the theory of regulation of cyberspace with the actual facts relating to China in order to demonstrate whether, how and to what extent the CCP realises the author's fears, having also added a new twist to the modes and tactics elaborated.

Before proceeding to the analysis, one methodological clarification is required. It is a common concern that papers about non-western, non-English speaking regimes, such as China here, which are written and are based on sources in English, would potentially provide a westernised, biased view of the facts. This choice of sources is, of course, partly due to the inevitable language barrier, which poses a difficulty for accessing sources written in Chinese. Nevertheless, in this analysis, care has been taken to include many sources that have direct references to Chinese sources or are authored or translated in English by Chinese citizens and academics, especially where views are expressed. Therefore, the facts and arguments included are related to reports and analyses that originate from Chinese sources to a large extent, albeit indirectly. Another difficulty in employing Chinese sources relates exactly to the problem that this essay discusses extensively, the fact that mainstream Chinese sources may be filtered and censored. Censorship in Chinese media would inevitably hinder any reporting and thorough analysis of views about freedom of information, regime oppression etc that are discussed in this paper, since such views would be considered controversial by the Chinese regime and would often be filtered and thus, harder to find or access. With these methodological difficulties in mind, the author has made extensive efforts to include a variety of sources, originating from China as well as from Chinese sources abroad. It is hoped that through such a process any concern of bias towards western views could be minimised to a degree that would render the essay as objective as possible under the circumstances.

2. Lessig's Theory: Code and other modalities of regulation online

Lessig, in his book Code 2.0, a follow-up of his seminal work Code and other laws of Cyberspace, provides an analysis of Internet regulation, identifying four elements that can influence behaviour online. These are laws, market forces, social norms, and code, the equivalent of architecture in real-life, the physical and digital infrastructure of what we call cyberspace.[5] Lessig is not the only one to have articulated this quadripartite theory of regulation, since similar analyses have been made by various theorists.[6] Many have also criticised Lessig's views on the role and interplay of these

[5] L Lessig, *Code V.2.0* (New York: Basic Books, 2006), at 5-6, 24.

[6] Murray and Scott characterise the four types of controlling online behaviour as hierarchical controls, competition-based controls, community based controls and design-based controls, while Reidenberg articulates his regulatory modalities as States, private sector, citizen forces and technical interests; A Murray and C Scott, "Controlling the New Media: Hybrid Responses to New Forms of Power" (2002) 65 *The Modern Law Review,* 491-516; J Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules through Technology" (1997) 76 *Texas Law Review* 553-584.

modalities and their actual importance in regulation and the prevention of it.[7] Irrespective of the view one might be adopting, it is undeniable that Lessig has articulated his theory very explicitly and his work has formed a large part of regulatory discussion about cyberspace, despite any flaws. Consequently, an analysis on the Chinese reality through the basic structure and theorisation of Lessig could, at least, provide some insights and an initial basis for assessing the interplay of various regulatory actors and the potential outcomes. But let us look at the specifics of this theory more closely before viewing its applicability to the Chinese reality.

Lessig focuses on code as a dominant element of regulation online and argues that the nature of Internet architecture is crucial in defining the regulability of certain behaviours.[8] He admits that regulability of cyberspace might have appeared harder initially, due to the basic open-ended architectures of the Internet and the functions of the various applications, which did not differentiate between kinds of information and promoted a decentralised model of communications.[9] However, he submits, this started to change after the commercialisation and popularisation of the medium, since economic interests and the need to facilitate and protect transactions and user interaction from phenomena such as cybercrime, induced companies to generate code that has made stricter regulation easier.[10] As Zittrain has also argued in his book 'The Future of the Internet and How to Stop it', that the various security threats that abound in cyberspace have been a driving force for more intensely regulated systems, organised and managed by corporations and accessed through 'appliances' with prescribed functionalities, such as the game consoles or smart-phones. Such closed networks accessed by hardware that would be monitored and modified by corporations deprive users of the capacity to innovate, instead offering consumers bundles of quick and reliable information, which has been prescribed by the service-providing businesses. Beyond this aspect, on a more legislative level, many states have promulgated laws that pose various restrictions on code and also on online behaviour, with penalties gradually intensifying globally.[11]

However, Lessig believes that the final step will be taken by the governments in providing coding incentives that will integrate regulability into the heart of the Internet by influencing not just the applications, but more infrastructural principles dictating the functionality of the Internet, such as the non-prioritisation of information.[12] Generation of controlling code has been a result not only of direct ordering, but mostly, as Lessig says, indirect, through the promulgation of regulations

---

J Goldsmith, "Against Cyberanarchy" (1998) 65 *The University of Chicago Law Review,* 1199-1250.

[7] V Mayer-Schonberger, "Demystifying Lessig" (2008) *Wisconsin Law Review* 713-746; D Post, "What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace" (2000) 52 *Stanford Law Review* 1439-1459; D Wall, "Digital Realism and the Governance of Spam as Cybercrime" (2004) 10 *European Journal on Criminal Policy and Research* 309-335.

[8] L Lessig, see note 5 above, at 24.

[9] *Ibid,* 32.

[10] *Ibid*, 38.

[11] The UK has been a typical example with the penalties for cybercrimes having doubled after 2006, whereas in the US there has been a constant intensification of strictness, especially after the USA Patriot Act in 2001.

[12] L Lessig, see note note 5 above, at 60-1.

by the state and facilitation of norms and market demands that create incentives and market opportunities that can change code-writing orientations.[13] In his words: "*... as code has become the product of companies, the power of East Coast Code (law-making) has increased. When commerce writes code, then code can be controlled, because commercial entities can be controlled.*"[14] He further adds that: "*Commerce has a purpose, and government can exploit that to its own end. It will, increasingly and more frequently, and when it does, the character of the Net will change. Radically so.*"[15] As it appears, Lessig believes that states could take advantage of the very obvious aims of markets to minimise risk, increase profits and induce commercial actors to promulgate code that conforms to less open standards. He further discusses how influencing the choice of code embeds values and social norms into the use of the Internet and demonstrates how choices of certain applications and architectures over others could enable whoever can exercise authority over the choices of the infrastructure and applications running on the Internet to gain control over cyberspace.[16]

Moreover, Lessig highlights that these factors are not affecting behaviour independently, but instead are all interlinked and should be understood and assessed as a single interdependent regulating structure, constituted by distinct elements, which are malleable and can also influence the function of the rest.[17] When the case of China is discussed, this interplay between the regulatory modalities will become more obvious. What seems crucial for the current analysis is his highlighting of how adequate regulation cannot possibly achieve, but does not even require, perfect effectiveness in order to be considered satisfactory. Arguably, all that is needed for achieving adequate control is the creation of numerous incentives and micro-controls, enforced with relative consistency, to render the various regulatory measures and the general regulatory philosophy behind them as the default.[18]

As Mayer-Schonberger clarifies, Lessig's theory is premised on the importance of maintaining transparency and variety of choice of Internet applications for users in order to preserve an open, unrestricted network, with his hopes lying with the beneficial power of the free market trying to maintain competition and innovation.[19] In an era, where major Internet companies such as Microsoft, Google or Apple could have a great financial and political influence, one could, naturally agree with Lessig's view on the influence of such companies, at least partly. However, whether the conditions in the PRC would allow the market to maintain control and safeguard transparency and freedom of choice is another issue. This potential of the CCP to steer its market towards its desired direction will become clearer below when the function of Lessig's identified modalities will be discussed in relation to the PRC more specifically.

---

[13] *Ibid*, 62-7.

[14] *Ibid,* 72.

[15] *Ibid*, 80.

[16] *Ibid,* 112-4.

[17] *Ibid*, 121,4.

[18] *Ibid,* 68, 73.

[19] Mayer-Schonberger, see note 7 above, at 722-4.

3. Chinese Internet and the four modalities

The Internet became quickly integrated in China as the ruling Chinese Communist Party (CCP) linked its reformative, developmental goal and, consequently, its legitimacy to the adoption and promotion of new technologies.[20] The public embraced the Internet and China had 384 million users by the end of 2009, which, in turn, built and nourished a bustling indigenous information technology economy, backed by international corporations that remained profitable even during the current global crisis.[21] The PRC now has more Internet users than the US and is also above the global average on Internet coverage despite its gargantuan size.[22]

Nevertheless, the Internet's economic boost threatened the CCP's overall control of society and the maintenance of its communist social values by facilitating behaviours considered immoral, criminal and undermining of national unity, such as gambling, access to pornography and mainly the proliferation of dissenting views.[23] Increasing information flows also hindered the Party's propaganda and information control policies – a presumably expected consequence of introducing information technologies to authoritarian regimes that suppress free speech.[24] The response of the CCP was to promote state ownership and control of main Internet infrastructures and use of the Internet, developing a comprehensive, elaborate structure for regulating the Internet. Beyond legislation, this regulating structure relies on the cooperation of corporations, the intensification of prolific normative standards of the Chinese state and the deployment of technical measures in order to create an isolated web, where the information can be monitored and controlled extensively.[25] The aspects of this multifaceted structure will be reviewed below, in order to demonstrate the relation of the Chinese Internet realities to Lessig's analysis and his concerns for the direction Internet regulation could take in the future.

3.1 The legal structure and the CCP's control over it

The first and main element of regulation is law. Chinese cyberlaws are generally based on the moral dictates of the CCP and are promulgated by its various public agencies, such as the Ministry of Information Industry (MII) and the Public Security Bureau, which together manage Internet gate-keeping and connectivity, designate the

---

[20] M Mueller and Z Tan, *China in the Information Age: Telecommunications and the Dilemmas of Reforms* (Westport Conn.: Praeger, 1996) Centre for Strategic and International Studies, Washington DC, at 57; Information Office of the State Council of the People's Republic of China, see note 4 above.

[21] Internet World Stats "China" (2012) available at www.internetworldstats.com/asia/cn.htm (accessed 26 Jul 12); CCTV, "China's Internet Economy Upbeat" (2009) available at http://www.china.org.cn/video/2009-11/03/content_18818834.htm (accessed 26 Jul 12).

[22] B Liang and H Lu, "Internet Development, Censorship, and Cyber Crimes in China" (2010) 26 *Journal of Contemporary Criminal Justice* 103-120, at 105

[23] Information Office of the State Council of the People's Republic of China, see note 4 above.

[24] J Zittrain, *The Future of the Internet and How to Stop it* (Virginia: Yale University Press, 2008), at 113-4.

[25] This regulatory structure has been named the 'Great Firewall of China'.

types of filtered information and more.[26] The regime has also shaped regulations organising Internet use under a direct licensing/monitoring scheme of users and Internet Service and Content Providers (ISPs, ICPs) by state agencies.[27] After the Internet's popularisation, though, the burden of regulating connectivity and controlling access and information gradually became too elaborate for the public sector to handle by itself. Thus, additional statutes were generated, promoting the delegation and decentralisation of responsibility of control in order to frame every aspect of Internet use under the CCP's dogma.

The extensive web of legal regulations, which are only a small part of the web-like regime of regulations and restrictions, form the basis for entrapping all other regulatory actors into realising the goals of the CCP.[28] Apparently, the government still maintains the command over legislative directions and enforcement, creating a structure of overlapping and vague provisions which it can interpret and implement according to its desired goals, with minimal internal and external resistance.[29] Moreover, the unchallenged discretionary interpretation of law by state-officials as well as the state's monitoring of private service providers' compliance with their mandatory regulatory duties, further empowers the state and disempowers the regulatees, leaving citizens and private actors ultimately unaware of the limitations of their actions.[30]

3.1.1 Internal pressure

In terms of internal, formal political resistance, mechanisms of legislative control are minimal. Constitutional challenge processes or a dissenting official political party do not exist, while popular protests focus more on low-level political corruption, misuse of powers and unjust trials, rather than regulations at the highest level of political principles.[31] There have been characteristic examples where online communities have

---

[26] L Solum, "Models of Internet Governance" (2008) *University of Illinois Public Law Research Paper No. 07-25,* at 69.

[27] For an account of the whole history and tendencies of Chinese cyberlaw and its changes in character, see: A Cheung "The Business of Governance: China's Legislation on Content Regulations in Cyberspace" (2005-6) 38 *New York University Journal of International Law and Politics,* 1-37, at 12-25; M Nawyn "Code Red: Responding to the Moral Hazard facing US Information Technology Companies in China" (2007) 2 *Columbia Business Law Review* 505-564, at 515-9.

[28] A typical example would be the restriction on Internet organisations citing foreign news without official approval and also the mandatory inspection and approval of all online publications: B Liang and H Lu, see note 22 above, at 108-9.

[29] For example, according to the **"**Computer Information Network and Internet Security, Protection and Management Regulations", it is punishable to access materials considered (*a*) subversive of state power or the socialist system; (*b*) damaging to national unity; (*c*) inciting discrimination between nationalities; (*d*) disturbing to social order; (*e*) propagating feudal superstition; (*f*) related to pornography, gambling, or violence; (*g*) insulting or libellous; and (*h*) violating the Constitution or other laws." The vagueness of the above criteria is characteristic of the arbitrariness allowed by cyberlaws. L Solum, see note 26 above, at 69.

[30] B Liang and H Lu, see note 22 above.

[31] T Kellog and K Hand "NPCSC: The Vanguard of China's Constitution" (2008) 8 *The Jamestown Foundation, China Brief* available at http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=4666 (accessed 26 Jul 12); S Shroeder, "*The Internet as a Tool for Political Activism in China"* (2005) available at http://globalmon.civiblog.org/_attachments/1774557/Chinainternettoolforpoliticalactivism2.pdf, at 15-

come together to uncover and criticise public officials' or even plain citizens' criminal or immoral acts, with satisfactory results, eventually even initiating a response from the state.[32] One could perhaps argue that the Chinese blogger and Internet user community in general could provide some sort of corrective mechanism against the state's inefficiencies and excesses. The Chinese government seems to also think that this could be so.[33] Localised Internet engagement events, such as the "hiding from the cat" incident,[34] indeed demonstrate the potential of online grassroots organising, which could impose a level of popular control on the potentially corrupt actions of state officials. However, the state has often appropriated these online civic efforts by taking advantage of the many different levels of political authority existing in such a vast country as the PRC. More particularly, the blame is often put on low-level officials, who are subsequently paradigmatically punished by the highest ranking rulers in accordance with public sentiment and CCP's ideological/moral standards.[35] Consequently, public criticism online rarely touches the actually high-ranking officials of the Party and the corrupt low-level public servants can be portrayed as deviations from the just dictates of the regime and not as an actual part of the CCP and its systemic flaws.

Moreover, some of those cases of cybercommunity organising have also raised concerns for their vigilantist consequences, which, in turn, have legitimised the government to produce legislation restricting such online initiatives in order to limit any feared excesses of public censure. More particularly, regulations have been promulgated in order to prevent "human flesh searches", where users collaborate in order to find citizens that have acted reprehensibly and express their disapproval and condemnation of their acts, sometimes reaching even to the point of threatening the safety of those identified as the perpetrators.[36] One cannot but suspect, though, that under the conditions of arbitrary enforcement of laws, common in the PRC, such laws could be employed to generally restrict civil initiatives online under alleged fears of vigilante reactions.

In effect, the CCP manages, due to its size and multiple degrees of government agencies, to localise and detach any political conflict from its ideological core and make the requested political changes at a low-level, without the high-ranking officials shouldering any blame for the corruption or the inefficiencies of their inferiors. On the other hand, the Party passes laws that give it the power to arbitrarily turn against

---

6 (accessed 26 Jul 12); on the protests and the aims of Chinese civil society see Z Tai "*The Internet in China: Cyberspace and Civil Society"* (New York: Routledge, 2006), at 216-253, 259-68.

[32] Z Tai, see note 31 above; B Liang and H Lu, see note 22 above.

[33] Information Office of the State Council of the People's Republic of China, see note 4 above, Part III.

[34] This case refers to the death of an inmate in a Chinese prison, where officials attempted to conceal the true facts by saying that the death had been caused by the inmate's participation in a game with other inmates called "find the cat". Research initiated by Internet users and bloggers led to the uncovering of the true facts, which proved that the inmate had been beaten to death by other inmates. This investigation eventually led the government to appoint Internet users as part of an assessment committee that would attempt to provide a report of the true facts, which ultimately led to the deposition of an official and the punishment of the inmates responsible for the injuries that led to the inmate's death. B Liang and H Lu, see note 22 above, at 111.

[35] *Ibid*.

[36] *Ibid*, 115-6.

online civic engagement that might seem controversial. Essentially, even if the CCP allows incidents of political activism, it has developed a capacity for taking advantage of such grassroots organising events and even promotes them at times. These practices thus, provide users with the illusion that Internet-based politicisation and democratisation is taking place with the tolerance or even support of the state. From the above one can infer that Internet-facilitated politicisation does take place in China, yet at a micro-level. However, micro-resistance does not automatically develop into macro-resistance, the latter being the kind of resistance that could seriously challenge the foundational principles and overarching political system of the Chinese regime.[37] If resistance is anticipated and co-opted by the power-holders, in this case the CCP, it will remain at a micro-level.[38] Micro-resistance would improve conditions locally, but will not lead to a challenge to the legitimacy and ultimate authority of the CCP, thus preventing dissent from developing into a generalised move towards establishing citizen rights and democracy in China.

3.1.2 External pressure

The legislative prowess of the CCP is not ardently challenged from outwith the PRC either. Although many Non-Governmental Organisations (NGOs) and rights groups have highlighted the restrictive policies of the CCP, enforced external pressure is low on behalf of states, as China's political and financial influence and prospects hinder any potential criticism for fear of alienating the CCP.[39] China's limited concessions to international community admonitions mainly relate to its World Trade Organisation (WTO) obligations, but even these have not been thoroughly realised, causing many actions to be brought against China, mainly by the US, for inconsistent enforcement of its trade obligations.[40] The PRC has lost many of these cases, relating mostly to preferential treatment of indigenous companies.[41]Despite governmental assurances that China will conform to the WTO accession agreements' terms, in many cases, the changes have not been implemented or alternative regulations have substituted those abandoned, demonstrating a lack of capacity or willingness of the WTO constituents to impose the various obligations on China.[42] Moreover, when confronted for its

---

[37] M Kelly, *The Political Philosophy of Michel Foucault* (New York: Routledge, 2009), at 109-10.

[38] *Ibid.*

[39] D Dickson, "China holds more US Debt than indicated" (2010) available at http://www.washingtontimes.com/news/2010/mar/02/chinas-debt-to-us-treasury-more-than-indicated/ (accessed 26 Jul 12); B Levisohn and O Biggadike, "China Euro Policy Denial Prompts Detection of Changes (Update2)" (2010) available at http://www.businessweek.com/news/2010-06-01/china-euro-policy-denial-prompts-detection-of-changes-update2-.html (accessed 26 Jul 12); A Guiora and S Riotte "China: Trade or Human Rights: Which comes First: The Canadian Model" (2007-8) 33 *United States-Canadian Law Journal* 11-24, at 12.

[40] W Morrison, "China-U.S. Trade Issues" Federal Publications Paper (Cornell University, 2011); A Wang, L Hornby and G Dyer, "Geithner softens his Stance on China" (2010) available at http://www.ft.com/cms/s/0/e62286e6-6697-11df-aeb1-00144feab49a.html (accessed 26 Jul 12); B Johnson, "US asks China to explain Google hacking claims" (2010) available at http://www.guardian.co.uk/technology/2010/jan/13/china-google-hacking-attack-us (accessed 26 Jul 12).

[41] W Morrison, see note 40 above, at 22 onwards.

[42] *Ibid.*

human rights violations, China rejects any criticisms as an intrusion on its sovereignty. This prevents any interference with its perception of punishable criminal and dangerous activity especially since many countries have imposed similar restrictions themselves on the bases of national security or intellectual property rights protection.[43]

From the above facts, one can infer that the CCP is not endangered by what has been characterised as the "Iron Cage of Liberalism". This signifies the situation where international condemnation towards an authoritarian regime flows from the need of democratic states to maintain a condemning position in relation to rights-violations by such governments, eventually preventing any formal interaction.[44] Although for smaller states, for example Iran, such condemnation could mean international diplomatic and economic isolation, the economic and political global influence of the PRC renders it impervious to these isolation and delegitimisation threats. Additionally, China is currently a crucial trade partner of the US and the EU, also holding, or being seen as a great candidate for taking over, large sums of these countries' high debts.[45] Therefore, a very realistic concern has been expressed that even the most powerful democratic states would be reluctant to incur the wrath of the CCP by openly and actively criticising its restrictive policies, thus, also its Internet-related restrictions.[46]

3.2 Market controls in China and their effects on regulation

3.2.1 Established controls

The Chinese market has traditionally been strongly regulated, entailing discouraging requirements for foreign telecommunications investments and financially burdensome compliance policies, which demonstrate a firm governmental grip on Internet market growth, especially since many large infrastructural companies remain state-affiliated despite their privatisation.[47] As research has demonstrated, despite the extensive

---

[43] BBC News, "G20 summit agrees on deficit cuts by 2013" (2010) available at http://news.bbc.co.uk/1/hi/business/10429446.stm (accessed 26 Jul 12); A Guiora and S Riotte, see note 39 above, at 15; L Solum and M Chung, "The Layers Principle: Internet Architecture and the Law" *University San Diego Public Law Research Paper No. 55*, available at http://ssrn.com/abstract=416263 (accessed 26 Jul 12), at 73.

[44] D Ritter and A Trechsel, "Revolutionary Cells: On the Role of Texts, Tweets, and Status Updates in Nonviolent Revolutions", (2011) Paper presented at Conference: *Internet, Voting and Democracy* (Laguna Beach, California), at 4-5.

[45] Many EU states even support the lifting of the arms embargo, which was imposed in 1989 after the Tienanmen Square protests were brutally repressed. W Morrison, see note 40 above; D Steibock, "EU Centre Policy Brief No.3: The Eurozone Debt Crisis and the Role of China" (2011) Policy Paper of the EU Centre in Singapore available at http://aei.pitt.edu/33650/ (accessed 27 Jul 12).

[46] J Groves, "Silence on Human Rights...The Price Europe Must Pay for China's Billions" available at www.dailymail.co.uk/news/article-2054929/EU-debt-deal-China-buys-Europes-silence-human-rights.html (accessed 26 Jul 12).

[47] G Wacker, "The Internet and Censorship in China" in C Hughes and G Wacker (eds), *China and the Internet: Politics of the Digital Leap Forward* (London: Routledge, 2003) 58-79, at 64-5; J Goldsmith and T Wu, see note 3 above, at 93; P Sohmen, "Taming the Dragon: China's Efforts to Regulate the Internet" (2001) 1 *Stanford Journal of East Asian Affairs* 17-26, at 17.

obligations the PRC was supposed to fulfil in terms of trade liberalisation and market openness policies, the Chinese state has often created conditions that promote indigenous businesses and create hurdles for foreign companies, consequently maintaining a stricter control on its market and promoting indigenous businesses.[48] Furthermore, as seen above, it has demonstrated a disinclination to conform to the open competition standards that the WTO has demanded, allowing the state to maintain a firm grip on commercial activity.[49]

Additionally, international information technology (IT) corporations invest in Chinese companies with similar interests, such as filtering technologies, becoming stakeholders and supporting the rise of the indigenous Internet conglomerates, which have structured their business plans and products based on the CCP's restrictive philosophies.[50] This internal, self-serving market, the products of which are also appealing for many regimes around the world like Iran, Saudi Arabia etc, strongly reinforces China's growing influence in information technologies and its potential autarky in managing its internal IT needs, with many domestic Internet platforms outpacing western ones.[51] The CCP's extent of control reaches from Internet Service Providers down to small, private companies, such as Internet cafes and content providers, as it promulgates regulatory incentives or obligations to have the commercial sector also assist in filtering content and monitoring of ambiguous use.[52]

Moreover, foreign corporations, like Yahoo, Google, Cisco etc have colluded with the CCP in order to partake in PRC's market, filtering search engine results, blogs and even disclosing dissidents' data to the government, subsequently provoking international condemnation and even Congressional hearings.[53] Nevertheless, despite the criticisms, no ban on US information technology exports has ensued. Although many organisations and even the US Congress have tried to pressure these

---

[48] W Morrison, see note 40 above.

[49] *Ibid.*

[50] K Regan, "Yahoo investing $1billion in Chinese Internet Company" (2005) available at http://www.ecommercetimes.com/story/45411.html?wlc=1276283884 (accessed 27 Jul 12); Electronics Design Strategy News, *"Intel invests in 3 Chinese Companies"* (2005) available at http://www.edn.com/article/469101-Intel_Invests_in_3_Chinese_Companies.php (accessed 27 Jul 12).

[51] OpenNet Initiative, *"Internet Filtering in China 2009"* (2009) available at http://opennet.net/research/profiles/china (accessed 27 Jul 12), at 5; R Winfield and K Mendoza, "Does China Hope to remap the Internet in its own Image? A Memorandum by the World Press Freedom Committee" (2007) available at http://www.wpfc.org/site/docs/pdf/Does%20China%20Hope%20to%20Remap%20the%20Internet%20in%20its%20Own%20Image.pdf (accessed 27 Jul 12) at 4; H Zhang, "China's Technology Companies Achieve Over 1,000% Growth" (2007) available at http://www.lifeofguangzhou.com/node_10/node_34/node_190/node_493/2007/10/26/119335887029179.shtml (accessed 27 Jul 12).

[52] J Goldsmith and T Wu, see note 3 above, at 96-7; L Solum, see note 26 above, at 69-70. Especially for cybercafes, the state has promoted schemes of chain-store model standardisation for management, which could facilitate the tightening of control, putting many cafes under specific monitored plans, while unregistered cafes would be hunted and closed down. B Liang and H Lu, see note 22 above, at 114.

[53] Amnesty international, "Undermining Freedom of Expression in China: The Role of Yahoo!, Microsoft and Google" (2006) available at http://web.amnesty.org/library/pdf/POL300262006ENGLISH/$File/POL3002606.pdf (accessed 27 Jul 12); M Nawyn, see note 27 above.

corporations, market liberalisation philosophies prevent the imposition of any actual governmental restriction on the commercial policies of those multinational corporations doing business in China.[54] Therefore, western companies are able and usually do make all the necessary concessions in order to be allowed to operate within China and benefit from its huge consumer base. There has been one exception, that of Google eventually leaving China after continued conflicts with government practices.[55] However, the CCP and PRC's market have remained unfazed, with indigenous companies absorbing Google's market share, while the political motives of Google's move have also been doubted - its move to Honk Kong being attributed mainly to business management choices.[56]

3.2.2 The changes of market liberalisation

On the other hand, one could argue that the new technologies, in addition to some undoubted efforts at liberalising the market in PRC, have brought changes to the operation of various Internet and media companies in relation to information generation and distribution. Inevitably, the commercialisation processes introduce western perceptions and operational models in the information industries, disconnecting such companies from governmental desires, mainly by increasing competition and linking financial survival to audience satisfaction.[57] More particularly, the development of Internet branches of official news agencies and the need to attain a broad audience to support Internet growth and investment in the agencies, has led to a more liberal enforcement of restrictions, even allowing media outlets to create their own news, despite the formal prohibitions.[58] Many unofficial sites also republish news, either downloaded or translated from foreign websites, disregarding the governmental dictates.[59]

---

[54] R Winfield and K Mendoza, see note 51 above, at ; A Lin and Y Shan, "Global Online Freedom Act would create dilemma for Beijing", (2010) available at http://www.theepochtimes.com/n2/content/view/28531/ (accessed 27 Jul 12); C Li, see note 2 above, at 66.

[55] J York, "Google.cn redirects to Hong Kong... for Now" (2010) available at http://opennet.net/blog/2010/03/googlecn-redirects-hong-kongfor-now (accessed 27 Jul 12).

[56] E MacAskill, "Google shift to Hong Kong played down by US" (2010) available at http://www.guardian.co.uk/technology/2010/mar/23/us-google-china-reaction (accessed 27 Jul 12); A Tse, "Google vs China vs Baidu, who wins?" (2010) available at http://www.thestreet.com/story/10712603/2/google-vs-china-vs-baidu-who-wins.html (accessed 27 Jul 12). Aljazeera, "Fallout from Google China Row grows" (2010) available at http://english.aljazeera.net/business/20english.aljazeera.net10/03/201032525940733731.html (accessed 27 Jul 12); M Helft, "For Google, a Threat to China With Little Revenue at Stake" (2010) available at http://www.nytimes.com/2010/01/15/world/asia/15google.html?ref=asia (accessed 27 Jul 12).

[57] Z Tai, see note 31 above, at 110-1; J Zhu, "Roadblock and Roadmap: Circumventing Press Censorship in China in the new media dimension" (2008-9) 30 *University of La Verne Law Review* 404-466.

[58] B Liebman, "Watchdog or Demagogue? The Media in the Chinese Legal System" (2005) 105 *Columbia Law Review*, 1-157, at 60-1.

[59] J Wang, "The Internet and the E-commerce in China: Challenge of the WTO" available at http://home.etf.rs/~vm/cd1/papers/93.pdf (accessed 27 Jul 12) 1-54, at 17.

However, the CCP seems to be finding alternative, indirect ways to restrict the dangerous consequences of liberalisation by integrating many state agencies into the various market sectors, thus perpetuating its original incumbent position in the new IT and media market.[60] Moreover, even after the introduction of the Internet, most regulations were, and up until today are,[61] aiming at containing the flow of information and securing the economic interests of the state-owned media.[62] The authorities have also been demonstrating their control capabilities by shutting down web TV sites and promoting extra regulation on Internet publishing, singling out bloggers and webcasting, as the sources through which foreign news are being "smuggled" into Chinese cyberspace.[63] Arguably, the regime has even attempted to hack into Google's servers in order to gain access to activist and other politically interesting and potentially threatening email communications, demonstrating a very aggressive, yet only implicitly connected to the government, tactic to enforce controlling policies, when companies decline to consolidate voluntarily.[64] This attack is significant symbolically as it establishes the willingness of the regime to go to extremes against companies that would try to evade its controlling policies. Furthermore, the Chinese government retains absolute control over the physical gateways to the global Internet and therefore ISPs connecting to these government-controlled backbone networks must be licensed, which inevitably means that ISPs will have to follow government dictates in order to maintain their operability within the PRC.[65]

The above facts indicate clearly how the CCP has the potential to shape its Internet market based on its demands and standards and it is extensively exercising its control,

---

[60] P Lovelock and J Ure, "*E-Government In China"* in J Zhang and M Woesler (eds) "*China's Digital Dream: The Impact of the Internet on the Chinese Society"* (Bochum: The University Press Bochum, 2002), at 13; Z Wen, "Traditional Chinese Media fights Crisis, embraces New Era*",* (2010) available at http://china.globaltimes.cn/diplomacy/2010-03/515835.html (accessed 27 Jul 12).

[61] Commercial portal sites must normally obtain permission from the Central Government Information Office to carry news. Even with permission, they can only publish news provided by official government information organs such as the *People's Daily* and the Xinhua News Agency, and are banned from carrying any news items based on their own interviews or from other sources. Also, no China-based websites without separate approval by the State Council Information Office, is allowed to link to overseas news websites or carry news from overseas news media or websites. See L Li, "China's Information Policy" (2003) TPRC, available at http://ssrn.com/abstract=2060570 (accessed 27 Jul 12) at 6; Major search engines and portals must not post their own commentary articles and instead make available only opinion pieces generated by government-controlled newspapers and news agencies. Private individuals or groups must register as "news organizations", which most of the time might prove problematic, before they can operate e-mail distribution lists that spread news or commentary. Existing online news sites, like those run by newspapers or magazines, must give priority to news and commentary pieces distributed by the leading national and provincial news organs. J Khan, "China Tightens Its Restrictions for News Media on the Internet" (2005) available at http://www.nytimes.com/2005/09/26/international/asia/26china.html?ex=1189137600&en=2cecba9398a679ae&ei=5070 (accessed 27 Jul 12).

[62] G Wacker, see note 47 above, at 62-3.

[63] Amnesty International, "People's Republic of China the Olympics countdown: Repression of Activists Overshadows Death Penalty and Media Reforms" (2006) available at http://web.amnesty.org/library/index/ENGASA170152007 (accessed 27 Jul 12), at 25-26.

[64] W Morrison, see note 40 above, at 26.

[65] L Solum, see note 26 above, at 69-70.

not just on information generation and distribution, but also on the software and hardware generated by both indigenous and foreign companies. This power is mainly realised by either enforcing compliance of local incumbents or implicitly integrating compliant state agencies in important industry areas and also by inducing compliance through the allure of its profitable market for overseas corporations. Consequently, this means that the state dictates which Internet- and telecommunications-related companies are allowed to operate within its Great Firewall. The Party's choices also relate to the hardware and software these companies employ, which will naturally have to conform to the Party's prescribed standards and regulations. Such practices ultimately reduce transparency and limit the choice of accessible information to what is prescribed by the ideology, morality and public safety notions that the government dictates.

3.3 Code: regulating versus liberating

The above argument becomes even clearer once the actual nature of code which is employed and promoted by the CCP has been reviewed. Despite the CCP's denial that organised censoring is taking place on its Internet communications, extensive regulations have gradually set up a multilayered filtering network essentially supervised by the state as a main method of controlling content.[66] The capabilities of this state-controlled Internet infrastructure were greatly expanded after the introduction of a fiber-optic, CN2 network supporting a pyramidal filtering structure. Filtering begins at the state-managed international gateways, spreading to governmental ISPs through which private ISPs connect, with the filtering and blocking even reaching down to individual user level.[67]

Filtering techniques employ various, overlapping types of filtering, such as keyword searches, domain name level and search engine filtering, email and bulletin board monitoring and erasure.[68] The topics being censored and the level of blocking strictness vary, with sensitive political content like Tibet Independence sites, as well as pornography sites and blogs being frequently blocked.[69] Social networking sites like YouTube or Facebook are also blocked extensively, while most western media and human rights sites are seldom unavailable, yet the extensiveness of filtering combined with its erratic application hinders any precise assessment of its extent.[70]

This fluctuating vagueness and the overlapping webs of filtering and blocking, some automated, some man-monitored, create even more opaqueness in relation to the

---

[66] R Winfield and K Mendoza, see note 51 above, at 3; R Nawyn, see note 27 above, at 513; N Anderson, "Internet Governance Forum takes on China, US" (2006) available at http://arstechnica.com/news.ars/post/20061031-8115.html (accessed 27 Jul 12); Z Tai, see note 31 above, at 102-3; T Lum, "Internet Development and Information Control in the People's Republic of China" (2006) *Congress Research Service Report for Congress* available at http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA462477 (accessed 27 Jul 12); L Li, see note 61 above, at 24-5.

[67] J Goldsmith and T Wu, see note 3 above, at 96-7; M Nawyn, see note 27 above, at 516-9.

[68] A Cheung, see note 27 above, at 9; OpenNet Initiative, see note 51 above, at 17-8.

[69] OpenNet Initiative, "Internet Filtering in China in 2004-2005: A Country Study" available at http://www.opennetinitiative.net/studies/china/ (accessed 27 Jul 12); OpenNet Initiative, see note 51 above.

[70] *Ibid.*

allowable materials and the extent to which users could access information. This arbitrariness further increases information restriction due to the lack of any independent controlling mechanisms based on publicly accessible standards, which could in turn allow for the monitoring of filtering excesses by the citizens or any independent authority. Technical filtering is also inevitably supplemented by a self-regulatory over-reaction by plain users, who, being unaware of the exact limitations they should abide by, often end up limiting themselves far more than they might have to. After all, solely the knowledge of existence and application of digital measures of surveillance could be enough to restrict activity and effect censorship, consequently limiting public civic discourse that might threaten the CCP's supremacy.[71]

It would appear that the CCP has managed to impose strong limitations on the ability as well as the ultimate willingness to view and publish content that would be undesirable by the CCP, employing code-based controls on many different levels, from central infrastructures, such as international gateways, to plain service providers, such as cybercafes. In parallel, the size of the PRC market also creates a great incentive for the generation of code that conforms to the designated CCP standards, thus extensively influencing the current, as well as the prospective code developments. As Lessig argues, code creation is synonymous to power and this power is now mainly in the hands of commercial enterprises.[72] However, in the case of China, these private actors are induced or restricted by governmental regulations in order to align their code with the state's operational standards. Most companies, being naturally more interested in the profits the booming Chinese market can offer, often conform to governmental standards of code-design.[73] Therefore, the CCP's grip on code seems unchallenged, since infrastructure and software come either from colluding foreign companies, like Microsoft and Cisco[74] or from developing indigenous manufacturers originally set on following the government's provisions and technological standards.[75] Simultaneously, China's expanding IT market allows it to also export standards of network design, influencing the nature and orientation of global production of code. Finally, the global proliferation of similar filtering and surveillance technologies, even in western countries, also voids any political pressure in relation to code development that western democracies could exercise against the restrictive code employed by the PRC, since many western state agencies and legislatures sponsor similar technologies and standards.[76]

On the other hand, one could say that technology also compromises the CCP's capacity to control information through code, since circumventive methods, such as anti-blocking/encryption software, mirror sites, anonymous e-mail services, peer to

---

[71] G Wacker, see note 47 above, at 60.

[72] L Lessig, see note 5 above, at 79.

[73] J Mulvenon, "Golden Shields and Panopticons: Beijing's Evolving Internet Control Policies" (2008) 9 *Georgetown Journal of International Affairs* 115-120, at 119.

[74] OpenNet Initiative, see note 69 above, at 6-7; A Cheung, see note 27 above, at 29-30.

[75] R Winfield and K Mendoza, see note 51, at 4.

[76] G Wacker, see note 47 above, at 71-2; Electronic Privacy Information Centre *"Carnivore"* (2005) available at http://www.epic.org/privacy/carnivore/ (accessed 27 Jul 12); J Peronne, "The Echelon Spy Network", (2001) available at http://www.guardian.co.uk/world/2001/may/29/qanda.janeperrone (accessed 27 Jul 12).

peer technologies and more could bypass most of the above limitations abound on the Internet.[77] Such measures are being extensively used by activists and users that desire to communicate – protected from governmental controls – and access restricted information and websites from abroad.[78] However, many of those measures require more than average technical knowledge, are time-consuming and can entail a relative risk of exposure to state sanctions – difficulties which discourage everyday users. Consequently, such tactics are adopted by a small minority of users. It is questionable whether such small groups could turn the tide against the vast majority; particularly, since the majority is still either incapable or reluctant to circumvent the existing technical controls and happy with the Internet experience already provided to them, having known no different, free cyberspace.

China has even managed to block access to the Tor anonymising network, which normally allows users to encrypt their communications and send them through a network of volunteer relay computers, making tracing of the original sender impossible. As research has shown, the two major telecoms companies (China Telecom, China Unicom) have taken up this task and have managed to block access to the initial Tor gateways, essentially preventing the use of Tor for PRC users.[79] The regime has also reportedly attacked Virtual Private Networks (VPN), creating software that could monitor such encrypting connections that are very commonly used by Chinese users for bypassing the technological filters of the PRC, inducing further self-censoring in Universities and businesses, where the restrictions on VPN have mostly focused.[80] All these efforts demonstrate the advanced sophistication and extent to which the PRC would go in order to prevent uninhibited communications between Chinese users and with the rest of the world. In extreme cases, the regime has even resorted to temporarily shutting the Internet down to maintain control of the information flows in specific areas during critical periods.[81]

Moreover, the main strength of the Internet for democratisation, openness and resistance to restrictive regulation is the convergence of interconnected, innovative applications and platforms consisting of multiple contributions from a constant flow

---

[77] J Lacharite, "Electronic Decentralisation in China: A Critical Analysis of Internet Filtering Policies in the People's Republic of China", (2002) 37/2 *Australian Journal of Political Science* 333 – 346, at 339-341; R McKinnon, "Flatter World and thicker Walls? Blogs, Censorship and civic Discourse in China" (2008) 134 *Public Choice* 31-46, at 33-4.

[78] Many different groups of users, from nationalists and political dissidents to hacker teams and marginalised social groups, dare to defy the restrictions posed, using many alternative means, like p2p technologies, online games, blogs and chat forums. This paints a more diverse picture, marring the image of discipline the regime is trying to maintain and impacting much more radically on the morphology of the internet, both within and without the PRC, see: J Qiu, "The Internet in China: Data and Issues", (2003) Working paper, *Annenberg Research Seminar on International Communication*, available at http://arnic.info/Papers/JQ_China_and_Internet.pdf (accessed 27 Jul 12).

[79] Technology Review, "How China Blocks the Tor Anonymity Network" available at http://www.technologyreview.com/blog/arxiv/27697/ (accessed 27 Jul 12).

[80] C Arthur, "China Cracks Down on VPN Use" available at www.guardian.co.uk/technology/2011/may/13/china-cracks-down-on-vpn-use (accessed 27 Jul 12)

[81] M Chase and J Mulvenon, "You've got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter Strategies" (2002) RAND Corporation Monograph Report, at 62.

Reuters, "China allows Internet Access in Xinjiang 10 Months after Riots" (2010) available at http://www.reuters.com/article/idUSTOE64D02Y20100514 (accessed 27 Jul 12).

of users, without any informational identification or prioritisation or any central controlling factor.[82] Chinese policies, though, have negated such unhindered interoperability to a large extent through filtering and blocking of the various interconnected platforms, even erratically. As seen above, the Chinese state has instituted core controlling mechanisms that prioritise certain information and applications over others that are deemed controversial, hindering or blocking access to various west-originating communications' sites (Skype, YouTube) and even monitoring mobile use.[83] Consequently, interoperability also becomes a controlled experience, where platforms and online applications are either banned or modified before allowing the Chinese users to employ them. This partial "castration" of the interoperability of the various code-based applications for information generation and distribution maintains the illusion that code propagates the free exchange of information. In reality, though, this alleged multi-faceted information exchange has first been "purified" by the various regulatory filters, both technical and rule- or policy-based that the companies offering these platforms and the applications running on them have to abide by.

3.4 Social norms in the PRC

Unavoidably, the extensive grip of the CCP on law-making, market structuring and subsequently, code promulgation has influenced Internet-usage norms, while simultaneously the goals of the CCP are facilitated by additional, traditionally endemic norms of the Chinese society. The dominant norm both inherent in Chinese society, but also reinforced by the various aforementioned controls, is self-censorship. Initially, self-restrictions are adopted for fear of sanctions, due to legal uncertainty, which is pervasive in China. As mentioned before, vague and arbitrarily interpreted legal provisions, reinforced by cyber-police and surveillance mechanisms, inevitably give rise and perpetuate a feeling of constant scrutiny for users and businesses.[84] As Wacker states, the best way to create "a firewall in one's head" is to introduce vague terminology and arbitrary interpretation of regulations, with sporadic incidents exhibiting enforcement capabilities, something the CCP seems to be expertly realising.[85] The Chinese government has even attempted to globally introduce its views on information and communications technologies by suggesting the adoption of

---

[82] J Zittrain, see note 24 above, at 31, 70; L Lessig, see note 5 above, at 44-5, at 111-112.

[83] T Branigan, "China blocks YouTube" (2009) available at http://www.guardian.co.uk/world/2009/mar/25/china-blocks-youtube (accessed 27 Jul 12); L Hornby, "China blocks Twitter Service ahead of Anniversary", (2009) available at http://www.reuters.com/article/idUSTRE5512HT20090602 (accessed 27 Jul 12); OpenNet Initiative, see note 51 above, at 15-6.

[84] For legal vagueness and arbitrariness and its combination with enforcement powers and technical measures in order to facilitate self-censorship see: G Rawnsley, "The Media, Internet and Governance in China" (2006) China Policy Institute, Discussion Paper 12, presented at the "*International Conference on the Development of the Nonstate Sector, Local Governance and Sustainable Development in China",* available at http://www.nottingham.ac.uk/chinapolicyinstitute/publications/documents/Discussion_Paper_12_China_Media.pdf (accessed 27 Jul 12) at 13; J Qiu, see note 78 above, at 12.

[85] G Wacker, see note 47 above, at 68

a "World Norm" based on its censoring standards during the Athens Internet Governance Forum (IGF).[86]

Moreover, two interrelated norms have supplemented self-censorship as the CCP has emphasised nationalism and materialism in order to formulate and inscribe the image of the ideal Chinese Internet user on public conscience.[87] The desirable user, therefore, is portrayed as a docile consumer/follower of the CCP morals, who avoids controversial uses of the Internet.[88] Moreover, the CCP's control of a large percentage of the mainstream media apparatus and its extensive use of propaganda has enabled it to dominate norm-creation, since alternative online media have been and are still generally censored, while at the same time, state-affiliated, traditional media has been modernised, establishing a strong Internet presence and consequently, colonising cyberspace-generated information.[89]

The CCP, realising the new challenges technologies pose to realising absolute information control, has also adopted a new strategy called "Control 2.0". This strategy initially allows information distribution, but pre-empts it, setting the agenda for the coverage of controversial news, thus reporting information in ways that could be favourable to the regime, rather than blocking it.[90] The CCP has even employed large numbers of Internet users (the 50cent Army) that access blogs, social networking websites and media in order to post pro-Party comments to counter dissent and spread state propaganda.[91] Since information could more easily circumvent the regime's restrictions with the introduction of the new digital technologies, the more efficient strategy would be to control how information is ultimately structured and perceived, rather than try to prevent its reception, something which the Internet has shown is ultimately futile. Consequently, through such tactics, the CCP pre-empts information exchanges and influences expression and bias. Additionally, through such techniques, the aims of nurturing nationalistic ideals and fostering economic prosperity are achieved more efficiently, establishing those elements as the CCP's central aims as well as normative pillars of its own legitimacy. Nationalistic tendencies are also to be anticipated, given the socialist state structure, merging the CCP's survival with the personal interests of citizens, with most citizens being public servants in the Chinese state apparatus.[92]

Moreover, state-promoted, depoliticising consumerism has transformed the old "information superhighway" to an "entertainment superhighway", where Chinese users focus more on the entertaining uses of the Internet, such as online gaming, e-commerce etc and not so much on seeking information and promoting the politicising

---

[86] R Winfield and K Mendoza, see note 51 above, at 3

[87] Office of the State Council of the People's Republic of China, see note 4 above.

[88] J Qiu, see note 78 above, at 16.

[89] J Zhu, see note 57 above; Amnesty International, see note 63 above, at 20-2.

[90] Z Wen, see note 60 above; OpenNet Initiative, see note 51 above, at 3.

[91] Wikipedia, "50 Cent Party" available at http://en.wikipedia.org/wiki/50_Cent_Party (accessed 27 jul 12).

[92] S Shroeder, see note 31 above.

uses of the medium.[93] Such conceptions, despite being challenged by a growing Chinese civil society and an effort to inspire and nurture post-materialist ideals,[94] remain dominant, especially since capitalism and consumerism are internationally prominent normative trends.[95] Talks about the rising demands and protests against state deficiencies and corruption by a newly forming middle class in China reflect such consumerist orientations as well. Essentially, citizens still focus on demands relating to safer houses and faster means of transportation which are more localised and refrain from actually directly challenging the ruling party's policies on a more substantive, ideological-political level.[96]

4. Conclusion

Is the Internet, therefore, capable of realising its democratising effects in China or is the CCP adequately in control of the medium, nullifying its alleged potential for political change and openness? From what has been discussed above, one could at least argue that for the moment, change towards more open, democratic models of Internet organisation and regulation appears to be at a nascent, if not doubtful, stage. This is because the CCP still appears to maintain a satisfactory grip on all aspects of regulation, employing a triptych of tactics, which include:

> a. blocking in the wider sense,
>
> b. co-option/pre-emption of political initiatives and information respectively and
>
> c. ultimately resorting to open aggression in order to control all possible modalities and actors influencing the regulation of its cyberspace.

More particularly, blocking is the traditional controlling function, originally employed by the PRC. Blocking encompasses the regulations and technical measures that prohibit certain types of information and certain behaviours from proliferating online and which gradually increase in pervasiveness, accuracy and sophistication. Co-option/pre-emption includes the aforementioned techniques of "Control 2.0", where both online movements and newsfeeds are appropriated by state mechanisms. Such a process facilitates the better control of how information is shaped and perceived and ensures the public resolves its civil disputes with the authorities in ways that entail the least possible contestation to the high-ranking party politicians and the general principles of the CCP. Finally, aggression is a more activist tactic, often employed by authoritarian regimes in order to coerce and silence dissent. This combines cracking down on cybercafes and dissidents or bloggers in real-life with actually attacking code

---

[93] R McKinnon, see note 77 above, at 33.

[94] J Zhu and Z He, "Information Accessibility, User Sophistication, and Source Credibility" (2002) 7 *Journal of Computer Mediated Communication* available at http://jcmc.indiana.edu/vol7/issue2/china.html (accessed 27 Jul 12).

[95] R Winfield and K Mendoza, see note 51 above, at 3.

[96] The Economist, "The New Middle Classes Rise Up" available at www.economist.com/node/21528212 (accessed 27 Jul 12).

and code-making companies through, for example, employing denial of service attacks on dissident websites or trying to hack into the Tor or VPN anonymising networks or into Google's servers. All these three different controlling tactics allow extensive control to be exercised by the CCP.

These three tactics are based on another triptych that has increased the efficiency and consistency of these types of control, while it has also reduced potential challenges. These three elements are:

a. global reliance on the Chinese economy,

b. internal technological development and sufficiency and

c. the "ideologisation" of established socio-political realities of the Chinese state.

More particularly, the allure of the Chinese economy and market as a support for the failing western economies, but also as a flourishing market for western corporations, has resulted in the lack of any serious external sanctions to the arbitrary and inconsistent actions of the Chinese state in relation to its national trade and human rights obligations, leaving its sovereignty largely uncontested. This is also reinforced through the collusion of technological giants such as Cisco, Microsoft and Yahoo with the regime.

Partly because of the above integration of obedient corporations into the PRC market and partly due to the great investment of the state to new technologies and indigenous entrepreneurship, China has also developed an autarkic market of information technology companies and products that abides and promotes its designated informational control standards. This autarky enables China to become independent of the big, western hardware and software companies, since subsidised Chinese companies are taking advantage of lax copyright policies, taxation and other provisions, which allow them to quickly become efficient and competitive in relation to western competitors. The Chinese state, thus, develops the capacity to require very little external IT support, which subsequently, empowers it to promote whatever policy it desires without having to conform to foreign standards of technological development and functionality, even threatening to create a closed Chinese Internet, independent from the global one.

Finally, the Maoist tradition with its huge state-centred organisation, sanctified single party political structure and strict moral foundations and traditions has facilitated the political legitimisation of the aforementioned policies on the basis of national security and preservation of the ideological heritage of the Party and has greatly discouraged the evolution of an internal ideological and political initiative. The combination of the above factors has allowed the regime to remain almost uncontested ideologically. This lack of any serious ideological challenge has in turn, provided stronger legitimising bases for the aforementioned controlling policies the CCP has adopted. These controls and restrictions further reinforce the aforementioned established norms, thus creating a vicious cycle.

One cannot ignore the voices finding hope for change in various incidents of civil society political initiatives, casual bypassing of filtering controls and alternative

media sharing global news and exposing regime injustices.[97] Despite the fact that this multifaceted regulatory power might not be absolute, with the Internet having created some cracks, the levels of control are still adequately extensive, thorough and enforced with relative consistency, allowing the CCP to ultimately steer Internet use towards the direction it desires for the vast majority of citizens. [98] As Goldsmith has argued *"the question is whether regulation will heighten the cost of the activity sufficiently to achieve its acceptable control from whatever normative perspective is appropriate."*[99]

Consequently, even if filtering and policing controls are circumvented, China seems to have already set legal, technical, business and normative standards that portray such counter-control tactics as deviant, counterintuitive, criminal and even threatening of Chinese traditions. Additionally, the opaqueness of the chaotic regulatory structure results in the vast majority of users and companies being unaware of the kind and the extent of information that is being blocked or filtered and also induces them to refrain from challenging the surveillance and filtering measures employed in case they are spotted by state employed monitors. This greatly increases the potential cost of attempting these circumventions, at least for the majority. The Internet has been transformed by the CCP to become a supervisory tool for the government, an officially sanctioned governance tool, rather than a subversive medium, with many authorities having even set up informant websites dealing with corrupt officials and with the majority of citizens approving such initiatives, finding them as a positive step towards democratisation.[100]

Furthermore, the Chinese Government White Paper on the Internet is indicative of the tendency of the regime to deny any allegation of unconstitutional, excessive information controls and restrictions and to suggest that any possible control only exists for the protection of Internet security, its users and ultimately, the nation itself.[101] The White Paper is an impressive documentation of how everything relating to the Internet in China and its potential controls are portrayed by the state as being premised upon basic state principles and constitutionally-accepted laws and regulations. The presumption of normality and legitimacy is in fact so pervasive in the text that, if read without any factual knowledge, it paints an ideal image of the Chinese Internet, even for western standards. The state, thus, justifies its controls and regulations in ways that any defiance would render the objectors as enemies of the state or at least deviant and malevolent towards the development of the Internet and the safe surfing of citizens. McKinnon has excellently summed up the tactics described above as phenomena networked authoritarianism, where authoritarian

---

[97] For a full analysis on civil society and alternative online media and the optimism they inspire see Z Tai, see note 31 above; J Zhu, see note 57 above; S Hetcher, "Virtual China" (2008) 7 *The John Marshall Review of Intellectual Property Law* 469-487.

[98] L Lessig, see note 5 above, at 68, 73.

[99] J Goldsmith, see note 6 above, at 1223-4.

[100] Information Office of the State Council of the People's Republic of China, see note 4 above, Part III.

[101] *Ibid.*

practices are explicitly and implicitly blended with the everyday life functions of the public.[102]

Consequently, until some important shift in the social class balance and subsequently, in the socio-political groups' capacity to exercise political power, the CCP's restrictive policies will survive and dominate the Chinese cyberspace and define the organisational bases of the PRC. As it is reported, even during the current economic crisis, where presumably disaffection against the regime should rise, "*there's little sign that the current economic downturn is leading to widespread social unrest – still less open opposition to the government*."[103] Added to that, recent reports show that respective CCP policies have intensified, rather than abated, especially since the financial crisis has presumably created the need for more social stability and subsequently, more concretised and extensive regulation.[104] The Chinese state has repeatedly and explicitly demonstrated its dislike for any reform initiatives through the above policies and tactics, having often also resorted to severe penalties against dissenters, with some even strangely disappearing after having voiced their disagreement with regime policies.[105]

China might be making some concessions, mainly in order to achieve technological integration, better economic agreements and international cooperation, or it might modernise its perceptions and accept the inevitability of information flows despite the controls. Yet, more general reconciliation on Internet policies seems highly unlikely on a mass scale for now. Cyberspace is currently a crucial tool for the CCP's desire for development and control and the Party does not seem willing to relinquish its control over its various functions. Rather, it seems to relentlessly be making efforts to extend its control through alternative, pro-active and implicit methods to the various channels and hubs that produce and propagate information and could also potentially

---

[102] *"[...] networked authoritarianism permits – or shall we say accepts the Internet's inevitable consequences and adjusts – a lot more give-and-take between government and citizens than in a pre-Internet authoritarian state. While one party remains in control, a wide range of conversations about the country's problems rage on websites and social networking services. The government follows online chatter, and sometimes people are even able to use the Internet to call attention to social problems or injustices, and even manage to have an impact on government policies. As a result, the average person with Internet or mobile access has a much greater sense of freedom – and may even feel like they have the ability to speak and be heard – in ways that weren't possible under classic authoritarianism. It also makes most people a lot less likely to join a movement calling for radical political change. In many ways, the regime actually uses the Internet not only to extend its control but also to enhance its legitimacy. At the same time, in the networked authoritarian state there is no guarantee of individual rights and freedoms. People go to jail when the powers-that-be decide they are too much of a threat – and there's nothing anybody can do about it. Truly competitive, free and fair elections do not happen. The courts and the legal system are tools of the ruling party."* R Mackinnon, "China's Internet White Paper: Networked Authoritarianism in Action" (2010) available at http://rconversation.blogs.com/rconversation/2010/06/chinas-internet-white-paper-networked-authoritarianism.html (accessed 27 Jul 12).

[103] T Branigan, "Young, Gifted and Red: The Communist Party's Quiet Revolution" (2009) available at www.guardian.co.uk/world/2009/may/20/china-changing-communist-party (accessed 27 Jul 12).

[104] D Mermigas "China: The World's Untouchable Internet Market, Even for Google" (2009) available at http://industry.bnet.com/media/10003988/china-the-worlds-largest-untouchable-internet-market-even-for-google/ (accessed 27 Jul 12); Reuters, "US Human Rights Report hits China, Iran" (2010) available at http://www.reuters.com/article/idUSTRE62A3IO20100311 (accessed 27 Jul 12); OpenNet Initiative, see note 51 above, at 4.

[105] T Branigan, see note 103 above.

nourish dissent. Eventually, the CCP is not just changing the normative and practical structure of the medium externally, but is becoming an intrinsic part of it, attempting to project its characteristics in every aspect of it globally. As Lessig solemnly argues, the way cyberspace was when it was first created is not the only way cyberspace could be.[106] China is so far the living proof of that realisation. Its multi-faceted tactics demonstrate that, even if what cyberspace is cannot be completely shaped according to the regime's will, its will and ways can implicitly infiltrate the various aspects of the Internet, "infecting" even the remaining open and free elements and activities in it. Sadly, China is also not alone in this, since a growing number of states, even in the democratic western world, are gradually joining it in attempting to transform the Internet according to more restrictive standards. Whether a Chinese model of the Internet will prevail, even beyond China, remains to be seen.

[106] L Lessig, see note 5 above.