Vistas

JOURNAL OF HUMANITIES & SOCIAL SCIENCES

Volume 5 *December 2009*

Chinese Panopticon: Political Control of Cyberspace in China

Athulasiri Kumara Samarakoon

Abstract

This paper examines the systemic factors motivating China to regulate cyberspace activism and also presents a typology of mechanism that she follows in operating a panoptical surveillance on the Internet. As a rising power, in terms of economic and military capabilities, China also exploits the Internet's potential as the latest mode of capital accumulation on an international scale. In spite of the state sponsorship for bringing the Chinese economy into the digitalised space, the state becomes more concerned with the cross-border political activism on cyberspace. The enormous resistance that the state generates in order to create a counter-strategy against this activism finds its justification in claims for inalienable state sovereignty and sacrosanct national security.

Introduction

Why does China, the world's fastest rising power, ban, control, regulate, and censor information and activism on cyberspace? And how China manages to filter a huge amount of data on cyberspace and how far it has succeeded in this regard are the major preoccupations of this paper. While answering these two questions, this paper primarily expects to provide a typology of Chinese control of cyberspace and reveal its implications at the global and regional level. The paper is organized into three major sections, *viz.* the state's role in developing information technology, structural issues emanating from the introduction of the Internet on Chinese territory and how China politically controls and regulates Cyberspace in China. The chapter employs a descriptive and analytical method and draws from the existing secondary studies on the Chinese cyberspace and statistical data mainly provided in Online Network Initiative (ONI), and *Handbook of Online China* - 2008.

Role of the State in IT Industry

China is a late comer to the IT industry. However, because of the role the state plays in the industry, China has leaped forward. China has a top-down investment policy in key IT industries such as telecommunication and semiconductor manufacturing. The National Information Leading Group of China has initiated and carried forward many programs to 'upgrade information systems in government departments and to develop the nation's IT industry as a whole' (Mengin 2004a: 60). Although it seems that the Chinese government has retained the ownership of the material infrastructure of the IT sector, it is not the complete story. China has always attempted to maintain the public-private partnership in the face of a globalised economy. In China, the privately managed companies (known in Chinese as *minying qiye*) are linked to the "development of high-tech industries and the authorization given during the 1980s to universities and research institutes to set up units, at the time of their being established , selling services and seeking profit" (Mengin 2004b: 60). The private sector companies are given a high autonomy and some of them have become shareholders of the Shanghai stock as well. As expected by many, today, China has built an indigenous IT industry. A major push for the Chinese IT industry came in 1998 when China established "Super Minister of Telecommunication and New Technologies" (2004:59). Thus, analysts of the rise of "Silicon Dragon" have pointed out that new ITCs have not caused the disintegration of the Chinese state but the further integration as a nation.

Commercialization of ICTs and National Security

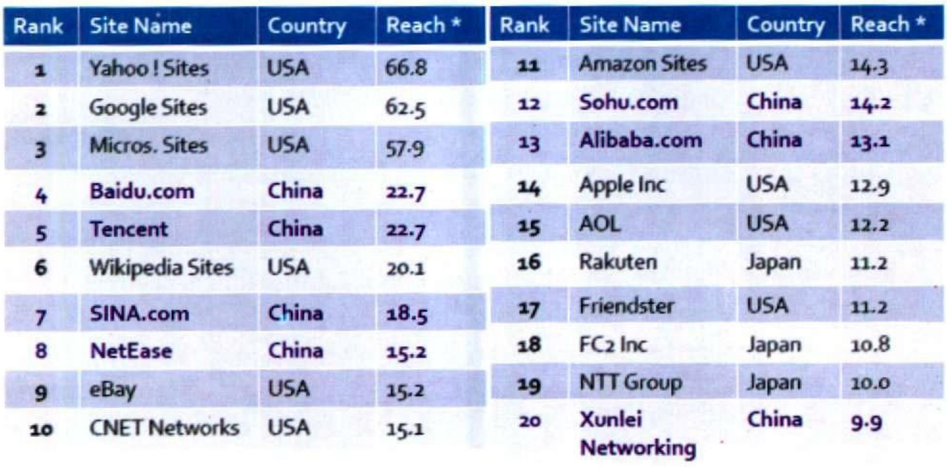
With the process of economic globalization, for which China has opened its doors, the state controlled and semi-governmental IT industry in China has faced a challenge to retain ICT architecture as designed by the state. Hughes (2004) discusses the issue of commercialization of the ICT and points out that the Chinese state has retained 'a considerable leverage over the behaviour of foreign firms and investors in the telecom market under the World Trade Organization's (WTO) rule' (2004: 76). The behaviour of the foreign firms certainly bears political implications, especially for national security of China. Subsequently, the impact of the commercialization of ICT on national security seems to lead to the imposition of rigorous regulatory mechanisms over the information diffusion on cyberspace At first, the state had ordered the ICT firms to separate 'sensitive' data from the Internet using firewalls. However, as Walton (2001) mentions, 'the sheer volume of data that is now flowing across ICTs, fuelled by the move toward broadband, means that the technology to control communications is now moving away from old-style firewalls in favour of dispersing monitoring and censorship architecture throughout the system' (Mengin 2004a:76). In this scenario, now, the Chinese state seeks more cooperation from foreign firms such as Microsoft and Red Flag Linux which can carry information to their websites without the knowledge of the users. So, dependence on such foreign software firms has been a major concern of Chinese policy makers. The Ministry of Industry and Information Technology (MIIT) and security agencies have expressed their concern over the technological lead enjoyed by foreign firms. In Hughes' study, we see that a combination of regulation and market mechanisms harnesses the expertise possessed by foreign entrants into the domestic market in ways that strengthen the power of the State and not the reverse (Hughs 2004:76).

Further, John Lagerkvist observes that 'new communications technology, effects of globalization and commercialization, and public demand for alternative sources of news' affect the ideological and political framework of China's hitherto tightly controlled media system (Lagerkvist 2006: 12). As the public demand for information increases, the level of state's democratization has always been an issue in China. The policy of information regulation in a market economy has been viewed negatively by many who take libertarian stances. Nevertheless, some analysts have seen that in the face of high commoditization of information by profit-oriented foreign firms, there has occurred a "controlled commoditization" that would create an understanding between the government media relationship within the material context of global capitalism. As Weber and Jia examines, China's 'balancing act between opening up through the WTO agreement and its political sensitivities', 'the process of thinking globally and acting locally is vital to understanding the country's fundamental contradiction in relation to its information management strategy' (Weber and Jia 2003). On the other hand, ONI data indicates that Chinese domestic search engines have outpaced some global search engines which in fact, prove the state's ability to run its own websites and search engines, as counter mediums in a commercialized information milieu.

> *Chinese netizens have access to a wide variety of well developed Internet platforms for the domestic market that have typically outpaced foreign services such as search engines (Baidu's market share is at 63 percent compared to Google's 28 percent), online portals (the top four portals –*
>
> *Sohu, Sina, Tencent, and Netease – claim 73 percent of sector revenue), bulletin board services (BBS) and discussion forums, online video sites, blogs, social networking (the service Kaixin has an estimated thirty million daily users), and booming business-to-customer e-commerce (OpenNet Initiative 2009:05).*

While commercialization as a systemic incentive for the development of e-commerce in China has buttressed its economy, it has brought another variant of systemic pressure in questioning the level of democracy the State has allowed to its netizens.

Table 1: Relative Dominance of Chinese Search Engines in Asia



Rank	Site Name	Country	Reach *	Rank	Site Name	Country	Reach *
1	Yahoo ! Sites	USA	66.8	11	Amazon Sites	USA	14.3
2	Google Sites	USA	62.5	12	Sohu.com	China	14.2
3	Micros. Sites	USA	57.9	13	Alibaba.com	China	13.1
4	Baidu.com	China	22.7	14	Apple Inc	USA	12.9
5	Tencent	China	22.7	15	AOL	USA	12.2
6	Wikipedia Sites	USA	20.1	16	Rakuten	Japan	11.2
7	SINA.com	China	18.5	17	Friendster	USA	11.2
8	NetEase	China	15.2	18	FC2 Inc	Japan	10.8
9	eBay	USA	15.2	19	NTT Group	Japan	10.0
10	CNET Networks	USA	15.1	20	Xunlei Networking	China	9.9

Source: Handbook of Online China 2008:05

IT and Democratization

As we see, 'the link between advances in information technology (IT) and the development of democracy' becomes an important research agenda among scholars and policy makers. Scholars have discerned a co-relation that exists between IT and democratic improvement. Political Science as a discipline has gained many new terms such as "digital democracy," "electronic democracy," and "cyber democracy" which refer to the Internet and democracy as working closely together and mutually reinforcing each other (Tsagarousianou *et al* 1998:04). 'Generations of political thinkers have identified the trends of commercialisation', and technological transformation and their impact on the public sphere from members of the Frankfurt School—Horkheimer and Adorno (1979) and more recently.

Habermas (1989) —through to contemporary media analysts concerned with the 'impact of the transformation of public service broadcasting at the end of the millennium' and the rise of the Internet technology' (Tsagarousianou *et al* 1998:04).

According to Camilleri, the State cannot be understood in isolation from the 'contingencies of contemporary political, cultural, and economic life' (Camelleri 1995 in Camilleri, Jarvis and Paolini 1995:209). Following a similar line, we can state that the contingencies of contemporary political, cultural, and economic life today are mainly due to the politics in cyberspace. Thus, the State encounters such contingencies very often as it cannot completely make it isolated from the interconnectivity created by the Internet. The economic globalization and its ideological project of democratization and commoditisation of information have direct implications for the politics of the State and its national security. China, as a powerful player with a huge economic clout, has interestingly faced this encounter of commercialized cyberspace while making it a tool of economic growth and counter state propaganda.

Together with the economic gains from the Internet, China's political identity has been affected by the political and cultural impact of cyberspace (Zhang 2004). In *Political reform: China will change in its own way*, Zhang points out a paradox that China's economic success as economic reform has been achieved without political reform but 'any sharp break with the Communist economic system inevitably entails political change' (Zhang 2004). The core-relation between economic development and political modernization thus has not been experienced simultaneously in China. As the Chinese state is attempting to exert control over the Internet for political reasons, while the state is attracted by the economic advantages offered by the technological modernization of information and. communication the Chinese state has not completely disregarded the modernization in several other spheres, except in the one party rule (Chase, Mulvenon *et al* 2006). As a nation-state which enjoys internal sovereignty of the state, China has always foreseen the transformative power of the new communication technology.

As many scholars explicates, today, 'As a result of the rapid growth of the Internet in China, the leadership of the Chinese Communist Party faces a series of challenges that are testing its ability to balance the competing imperatives of modernization and control' (Chase, Mulvenon *et al* 2006). Further, there is a particular importance of linking economic growth to social stability for the Beijing leadership, and, 'in the absence of communism or any other unifying ideology, maintenance of prosperity has become the linchpin of regime legitimacy and survival' (2006: 59). Thus, the economic modernization linked with IT has encountered the problems of political modernization leading to internal political and social insatiability.

Whatever the political reforms China has brought, they all are aimed at further economic modernization. As Zhang (2004) shows, political reform experiments are being carried out, such as e-government and the practice of "small government and big society," which reduces bureaucracy and forsakes its many functions that can be better performed by society. However, China's political reforms essentially attempts to facilitate economic development, not democratization, and to improve the efficiency of the existing political system, not to abandon it.

Human Rights Activism on Cyberspace

International Human Rights activists and organizations have produced reports that put blame on management of humanitarian affairs related to the freedom of internet usage in China. For instance Amnesty International Report (2007) records that;

> *Hundreds of international websites remained blocked and thousands of Chinese websites were shut down. Dozens of journalists were detained for reporting on sensitive issues. The government strengthened systems for blocking, filtering, and monitoring the flow of information. New regulations came into effect requiring foreign news agencies to gain approval from China's official news agency in order to publish any news (85).*

It seems that China has viewed these reports as undermining its sovereignty and to have reflected vested interests of the Western countries in interfering with her domestic affairs. Also the existence of a huge amount of anti-Chinese propaganda based on the adverse record of human rights of China on cyberspace has been seen as threat to its survival and influence in the region. Mostly, the case of Tibetan claim for autonomy has become a hot ground for human rights activists. The 56th UN Commission on Human Rights debated "The question of human rights and fundamental freedoms." According to a news report on the website of the Government of Tibet in Exile, in this forum, "A large number of NGOs strongly criticized China for its human rights failures in China, Tibet and Eastern Turkestan". Further, it reported that; 'more NGO statements were expected to be delivered before the Commission concluded its debate on this topic. ...a number of government statements also expressed concern on the human rights situation in China". Moreover, the website of Asian Human Rights Watch continuously updates the Chinese military's suppression of the Tibetan protests and activists of freedom. Just searching on Google, one gets at least **136,000,000** results on 'human rights record of China'.

The foreign search engines which publish content in English language provide information that challenges the legitimacy of the CCP rule. Therefore, the PRC attempts to filter theses websites locally. Additionally, the Chinese government maintains its own websites in English to counter the anti-Chinese propaganda by human right activists. The Propaganda Department of Xinhua News Agency (Hong Kong Branch) maintains the website. From a comparative reading of the websites on human rights by various actors, one can discern a certain view of the human rights of a State. Commenting on the 'problem of global ICT governance' Hughes (2004) notes that States have to adhere to certain norms in their behaviour in the international system, but 'self-interest of the States receive more support than the advocacy of human rights and democracy'. "While the case of China shows that the globalization of IT does have a political impact on states, this tends to reflect attempts to manipulate architecture and the collection and processing of data for the causes of strengthening the legitimacy and security of security regimes, rather than the promotion of liberal-democratic transformation" (Hughes 2004:87). The international system is such that the State has no help other than self-help (Waltz 1979). Therefore, the existing regimes, and institutions are always looked at suspiciously by the State actors because the embedded interest in them always reflects the hegemonic politics that aspire to stretch its power and influence.

Building Chinese Panopticon

The notion of a virtual panopticon on Chinese cyberspace is brought into discussion by Karstein Giese (2004) in "Speaker's Corner or Virtual Panopticon: Discursive Construction of Chinese Identities Online". Foucault (1977) proposes that not only prisons but all hierarchical structures like the army, the school, the hospital and the factory have evolved through history to resemble Bentham's Panopticon. The notoriety of the design today (although not its lasting influence in architectural realities) stems from Foucault's famous analysis of it. In *China and the Internet: Politics of the digital leap forward,* Giese (2003) further brings the conception into the field of cyber politics. The concept in the context of the Chinese "fire walled" and "golden-shielded" cyberspace explains simultaneously the surveillance system and the limits (amount of freedom) of the users of cyberspace in their access to information. The Chinese control of cyberspace has been metaphorically explained by using the same Foucauldian concept of the Panopticon, a prison in which every cell has a window facing a central tower from which an unseen warden just might be watching what any individual prisoner does at any time. The prisoner thus has to act as if he is under constant surveillance all the time, even though such surveillance is not physically possible for the single warden. By applying such a model to the kinds of technologies that are being built into the Internet, Boyle argues that effective censorship has indeed become possible (Wacker 2003, 67-68).

According to Giese (2004) in the panopticon system of network access, the user is not denied access to each and every website. For instance, the local Chinese web users are allowed to surf many of the Chinese language websites while some foreign sites are barred. As the government is in close contact with the Internet Content Providers (ICPs) and Internet Service Providers, they have to act according to the rules and regulations of the government on the one hand, and on the other, as Net cafes are registered and the users have to prove their identity; the user is always aware of the political control of Internet use. As such, the virtual panopticon is structured around the users of web, ICPs, ISP, the owners of "Netcafes" and the government regulation. Above all, there exists a plethora of State controlled websites that could provide most of the information the web user asks for. In place of English language websites, China had 126,000 domains and 293,000 web sites at the beginning of this Millennium. Wacker (2004) and Tai (2006) have devoted space to discuss the National Policy of Chinese regulation of the Internet. In his study Wacker outlines 'various provisions that were included in a raft of regulations that was introduced in the year 2000 to govern telecommunications and the publication of news and electronic information on the Internet' (Wacker 2004:61-65). He provides a typology of internet filtering under the categories of 'forbidden contents', 'restrictions on the distribution of news', 'licenses', 'storage of user data', 'surveillance', 'judicial liability', and 'penalties'.

Forbidden Contents

Contents that are banned from distribution or electronic publication involves that which (1) contradicts the principles defined in the constitution [of the PRC], (2) endangers national security, discloses state secrets, subverts the government, and destroys the unity of the country, (3) damages the honour and the interests of the State, (4) instigates ethnic hatred or ethnic discrimination, destroys the unity of [China's] nationalities, (5) has negative effects on the State's policy on religion, propagates evil cults or feudal superstition, (6) disseminates rumours, disturbs social order, and undermines social stability, (7) spreads lewdness, pornography, gambling, violence, murder, terror or instigates crime, (8) offends or defames other people, infringes upon the rights and interests of other people, (9) and other contents that are forbidden by law or administrative regulations (Wacker 2004: 62-63).

Political and Social Content Filtering

The political and social content filtering is high on the Chinese agenda of the regulation of the Internet. The above forbidden categories display the government's intention of preventing all the imaginable threats in terms of national security, survival of the CCP and social and religious harmony. Thus, by forbidding certain information on cyberspace, Chinese authority has aimed to continue its internal and external sovereignty uninterrupted. Faris and Villeneuve (2006) have studied the breadth and depth of filtering in global scale. In this study, China's breadth and depth of filtering are just below Iran, another State which has repressively regulated the Internet on its territory. Their study has identified data from forty countries which practice social and political content filtering vigorously (some countries are omitted in Figure 1). At a glance, an analyst would recognize that most of the countries are labelled as authoritarian that deny much of media freedom in their territories. But, in a structural perspective, these States attempt to resist the system wide distribution of new technology, which could bring qualitative changes in their existing rules or create chaos at the collapse of such authoritarian control of the polity.

Figure 1 Breadth and Depth of Filtering

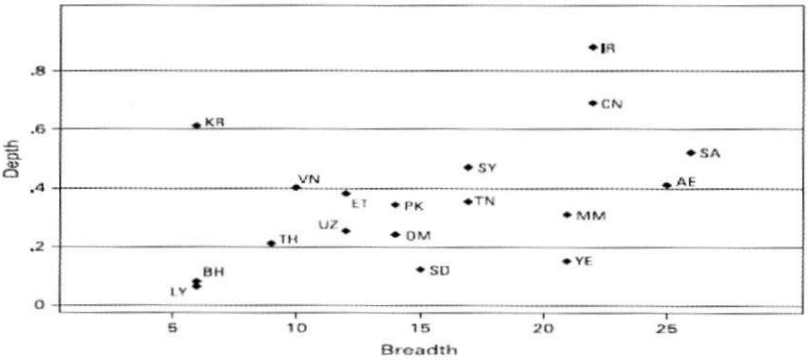


Figure 4:7 Comparing the breadth and depth of filtering.
AE—United Arab Emirates; BH—Bahrain; CN—China; ET—Ethiopia; IR—Iran; JO-- Jordan; KR—South Korea; LY—Libya; MM—Burma/Myanmar; OM— Oman; PK—Pakistan; SA—Saudi Arabia; SD—Sudan; SY—Syria; TH—Thailand; TH—Tunisia; UZ— Uzbekistan; VN—Vietnam; YE -Yemen. (Faris and Villeneuve 2006:08)

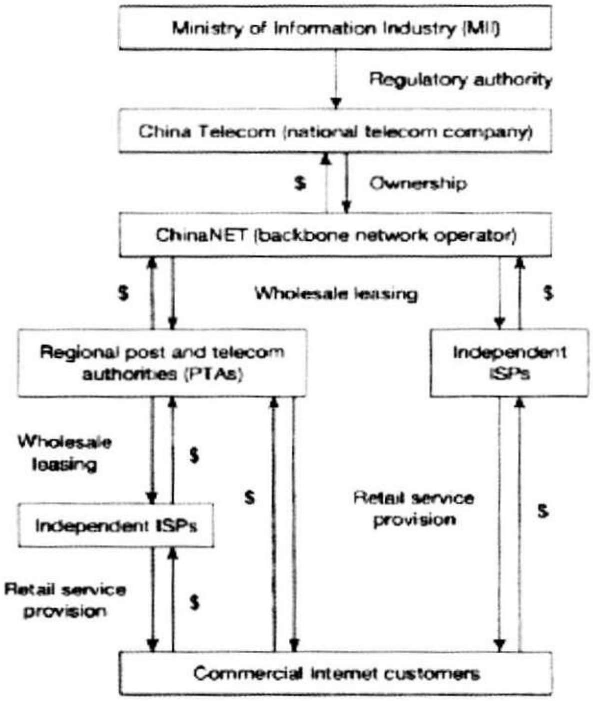
Restrictions on the Distribution of News and Information

Restrictions on news act as hindrance and prohibition of the distribution of news through the Internet, unless this news has either been published on the Internet by the official state-owned media. The restriction could emanate from various sources - from political, legal, market or self-censorship. In examining the hierarchical organization of the political authority and the commercial distribution of the Internet facility in China, this is further realized. In study titled "Government policy and political control over China's Internet", Harwit and Clark (2006) has drawn a structure underlying the regulatory authority, ownership, wholesale leasing, retail services and the commercial internet customers ranked in hierarchical fashion. The final arbiter of this hierarchical structure derives its power from the centralized ruling elite. While the State draws revenue upwards, the power of regulation has reached the bottom layer, which is the netizen (commercial customer). Both local and foreign news sites undergo a similar fate. As Wacker notes;

> *With respect to links to foreign news sites or the publication of news taken from foreign media – some portals had signed agreements with foreign information services like Dow Jones and others – the regulations stipulate that the prior consent of the Information Office of the State Council is necessary (Wacker 2004: 63).*

The state not only uses its political power to rule over the ICP and ISP, but it uses its economic might to increase the competition among the pro-state news portals. In 2000, the Chinese government granted special funds (USD 121 million) in order to strengthen the competitive position of such official organs. In issuing the 'Licenses' for the ICP and ISPs, China has always imposed comprehensive and detailed rules. Separate licenses are also required for each category of service. Storage of user data is a must for the ISPs. The registration of the customer number of the user, the telephone number used for logging on, web addresses or domains visited during the session and for how long, are the data required to be stored for sixty days and submitted when ordered by the authority. Regulations introduced in January 2002 are the most disturbing so far for requiring ISPs and ICPs to screen e-mails, which depict the omnipotent power of the State for surveillance of personal communication. Judicial liability of the ISPs and ICPs is stringent in China. Posting and uploading of information on the Internet could be legally barred if detected for threats. Heavy penalties await those ISPs, ICPs and individual users who violate the regulation of publishing and providing information. Fines ranging between RMB 5,000–50,000 could be imposed (Wacker 2004: 60-65)

Figure 2 Control of hierarchy and revenue flows of Internet service Provision under the Ministry of Information Industry (MII) in China


Ministry of Information Industry (MII)
Regulatory authority
China Telecom (national telecom company)
$
Ownership
ChinaNET (backbone network operator)
$
Wholesale leasing
$
Regional post and telecom authorities (PTAs)
Independent ISPs
Wholesale leasing
$
$
Retail service provision
$
Independent ISPs
Retail service provision
$
Commercial Internet customers

Source: Harwit and Clark (2006)

Giese (2004: 25) views that the hierarchical network architecture and the vertical responsibility system and multilayered policy measures have exerted the 'highest possible degree of control on the Internet in China as opposed to general decentralized nature of network architecture mostly observed in the Western democracies. Further, he points out that '[A]ll institutional and economic actors of each level within this hierarchy hold responsible to ensure compliance with the relevant laws and regulations policing the Chinese Internet and can be sanctioned for any failure to comply' (2004:25).

The matrix of technological, political, legal and coercive surveillance, control, censoring, penalizing and regulation of the Internet ownership and users thus has convincingly brought us the notion of 'absolute control of cyberspace'. In the words of Giese (2004), this absolute control could be possible because,

> *...many observers conclude that not a single byte of information disseminated via the Chinese part of the Internet will evade the eyes of the censor and the long arm of the state- at least potentially, as public reports on arrests of individuals and revoking of licenses for economic actors as sanctions for non-compliance seem to prove" (2004:25-26).*

From this analysis of Giese, we can conclude that the right of the internal sovereignty of the Chinese State is highly regarded and enacted by the Chinese State as its capability allows it to act so in the international system. Thus, Chinese behaviour in regulation of the Internet, a global variable of analysis on the domestic front, has much system wide impact that will be the topic of a forthcoming discussion.

Preventive and Repressive Regulation and Building 'Chinese Special' Websites

As Krasner (2001) explains "...technological change has made it very difficult, or perhaps impossible, for states to control movements across their borders of all kinds of material things (from coffee to cocaine) and not-so-material things (from Hollywood movies to capital flows)". In the case of China, Krasner's analysis has to be reformulated. We would say that while China accepts the capital flows into the State, it has managed to keep some of the intrusive ideas, and norms at the border. The Chinese commitment in regulating the Internet also deserves attention as no other State has attempted to do so in that fashion. The Chinese matrix of regulation can be explained under three terms following the typology of Mengin; preventive, repressive and self-propaganda. China has succeeded in all the three dimensions as we have shown above. China bans most of the foreign websites like CNN, BBC, or Time under preventive methods. The repressive methods constitute the "Internet policing', which we have already discussed. Also, improving of soft power via proliferating much information on cyberspace becomes a major pillar of Chinese strategy.

In fighting propaganda by the West, Taiwan or Tibet, China duplicates such websites or builds their own to spread counter propaganda. The dialectical effect of such counter propaganda would certainly add to the confusion of the netizen immersed in a sea of information.

Concluding Remarks: Influence of China's Cyber Strategy on Sri Lanka

The hierarchical network architecture and vertical responsibility, iron hand of political power, judicial procedures, coercive measures or economic incentives for the pro-Chinese media and technological surveillance are among the major strategies of Chinese regulation of the behaviour of the Internet, which could be discerned from the above discussion. Thus, China has used power to get the actors engaged in information business on cyberspace to act in the way China wants them to act. The control of the material cyberspace, primarily, has led to the acquiescent reflection of the symbolic cyberspace. China's efforts have paid off from many points of view.

If political modernization introduced state sovereignty as an unalienable right of the state, China has fought for that right. And by doing so China has worked against the emergence of political chaos domestically. China has mainly fought against the political discourse aimed at 'overthrowing the current regime' (Mengin 2004: 56). China's future behaviour could certainly influence several other regimes which face similar threats, once the Chinese hegemony is established as predicted in many studies.

In the present context, Sri Lanka makes an obvious example for adopting similar strategies that China adopts for control of her cyberspace. Sri Lanka which has long been confronted with the challenges of separatist guerrilla movements on the physical terrain as well as on the virtual space of the Internet, seems to have been influenced by the Chinese architecture of cyberspace control. Though, technologically small, States are not in a position to create their own 'panopticons' with 'firewalls' or 'golden shields'. It seems that at the domestic front, they tend to adopt all the coercive measures in the style of the Chinese. The ban on the "www.tamilnet.com" of the LTTE (Liberation Tigers of Tamil Eelam) (Vidanage: 2009) and the creation of military websites (www.army.lk, www.navy.lk, www.defence.lk, etc.) testified to the Sri Lankan state's desire to have control on cross-border political activism on cyberspace against the State.

Thus, China's approach of cyberspace control seems to reject the chaos of politics and rather aims to achieve normalization through surveillance, though the severity of such behaviour could be highly contested.

References

Adorno, T and Horkheimer, M (1979) *Dialectic of Enlightenment*,London: Verso

Amnesty International (2005) *Amnesty International Report 2005*, Amnesty International, [Online Web] Accessed 17/04/2009

Camilleri, Joseph A. (1995), *The State in Transition: Re-imagining Political Space Critical Perspectives On World Politics*, Lynne Rienner Publishers

Damm, Jens and Thomas, Simona (eds) (2006), *Chinese Cyberspaces Technological changes and political effects*, London and New York: Routledge

Deibert, R. J. & Villeneuve, N. (2004), "Firewalls and power: An overview of global state censorship of the internet". In: M. Klang & A. Murray (eds.), *Human Rights in the Digital Age*. London: Cavendish Publishing

Deibert, Ronald *et al* (2008), *The Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, Massachusetts and London: The MIT Press

Fannin, Rebecca A. (2008), *Silicon Dragon: How China is Winning the Tech Race*, New York: McGraw-HillFaris, Robert and Villeneuve, Nart (2006), "Measuring Global Internet Filtering" in Ronald Deibert et al (eds), *The Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, Massachusetts and London: The MIT Press

Foucault, Michel (1977) *Discipline and Punish: The Birth of the Prison*, Harmondsworth: Penguin

Gies, Karsten (2003), "Construction and Performance of Virtual Identity in the Chinese Internet" in K.C Ho, Randy Kluver and C.C. Yang (eds) (2003) *Asia Encounters the Internet*, London: Routledge

Giese, Karsten (2004), "Speaker's Corner or Virtua Panopticon: Discursive Construction of Chinese Identities Online", in Francoise Mengin (ed) (2004a) *Cyber China Reshaping National Identities in the Age of Information*, New York: Palgrave Macmillan

Habermas, J. (1989), *The Structural Transformation of the Public Sphere*. Cambridge, Mass: MIT Press

Harwit, Eric (2001): The impact of WTO membership on the automobile industry in China. In: *The China Quarterly*, Vol. 167, 655-670

Harwit, Eric and Clark, Duncan (2006), "Government policy and political control over China's Internet" in Jens Damm and Simona Thomas (eds), *Chinese Cyberspaces*, New York: Routledge

Hughes, Christopher R. (2004), "Controlling the Internet Architecture within Greater China" in Francoise Mengin (ed) (2004a), *Cyber China Reshaping National Identities in the Age of Information*, New York: Palgrave Macmillan

Hughes, Christopher R. and Wacker, Gudrun (2003), *China and the Internet Politics of the digital leap forward*, London and New York: Routledge Curzon

Hung, Chin-fu (2004), "The Internet and the Changing Beijing- Taipei Relations: Toward Unification or Fragmentation?" in Francoise Mengin (ed) (2004), *Cyber China: Reshaping National Identities in the Age of Information*, New York: Palgrave Macmillan,

Jarvis, Anthony P. & Paolini, Albert J. (1995), "Locating the State", in Joseph A. Camilleri, (ed) (1995), *The State in Transition: Reimagining Political Space Critical Perspectives On World Politics*, Lynne Rienner Publishers

Krasner, Stephen D. (1999), *Sovereignty: Organized Hypocracy* , Princeton, New Jersey: Princeton University Press,

Krasner, Stephen D. (2001), "Sovereignty", *Foreign Policy*, Jan-Feb 2001:21

Lagerkvist, Johan (2006), "In the crossfire of demands: Chinese news portals between propaganda and the public" in Jens Damm and Simona

Mengin, Francoise (ed) (2004a), *Cyber China Reshaping National Identities in the Age of Information*, Palgrave Macmillan, New York

Mengin, Francoise (ed) (2004b), "New Information Technologies and the .Reshaping of Power Relations: An Approach to Greater China's Political Economy" in Mengin, Francoise (ed), *Cyber China Reshaping National Identities in the Age of Information*, Palgrave Macmillan: New York

OpenNet Initiative (2009) "Internet Filtering in China", [Online Web] Accessed 20/06/2009, Organisation for Economic Co-operation Development (2006), *OECD Information Technology Outlook 2006,* OECD publishing; [Online Web] Accessed 02/03/2009

Shirk, Susan L. (2007) *China Fragile Superpower,* Oxford University Press

Tai, Zixue (2006) *The Internet in China: Cyberspace and Civil Society,* Routledge: London and New York

Tan, Zixiang (1995), "China's information superhighway," *Telecommunications Policy,* 19:9, 721–31 Thomas (eds) (2006), *Chinese Cyberspaces Technological changes and political effects,* London and New York: Routledge

Tsagarousianou, Roza; Tambini, Damian and Bryan, Cathy (eds) (1998) *Cyberdemocracy,* London: Routledge

Vidanage, Harinda (2009) "Rivalry in cyberspace and virtual contours of a new conflict zone: the Sri Lanka case", in Athina Karatzogianni (ed), *Cyber Conflict and Global Politics,* Routledge: USA and Canada

Wacker, Gudrun (2004) "The internet and Censorship in China", quoted in Kartsen Gies, "Speaker's Corner or Virtual Panopticon: Discursive Construction of Chinese Identities Online" in Francoise Mengin (ed), *Cyber China Reshaping National Identities in the Age of Information,* Palgrave Macmillan: New York

Walton, Greg (2001) *China's Golden Shield Corporations and the Development of Surveillance Technology in the People's Republic of China,* International Centre for Human Rights and Democratic Development

Waltz, Kenneth N.(1979)*Theory of International Politics,* Random House: New York

Weber, Ian and Jia, Lu (2003) "Handing over China's Internet to the Corporations". In IIAS Newsletter, issue 33, p9. [Online Web] Accessed 03/09/2009,

Zhang, Wei-Wei (2004) "Political reform: China will change in its own way", [Online Web] Accessed 03/10/2009, URL http://www.nytimes.com/2004/05/21/opinion/21iht-edzhang_ed3_.html