Issue 4, Winter 1999/2000

VIRTUAL CENSORSHIP IN CHINA: KEEPING THE GATE BETWEEN THE CYBERSPACES

by

Jack Linchuan Qiu

A. Introduction: the Cyberspace, or the Cyberspaces?

The Internet, as the means of online political communication (OPC), is not only a stimulant of cross-border interactions but also a tranquilizer of academic debates. The relationship between technology and democracy, for example, is a topic producing binary opposition for decades: some hold that advanced technology leads to democratization (McLuhan, 1954; Boorstin, 1978; Toffler, 1980; Naisbitt, 1982; Barber, 1984; Hauben, 1996), while others contend it leads to monopoly (Innis, 1964; Horkhaimer and Adorno, 1973; Vig, 1988; Luke, 1989; Postman, 1992). Although the contradiction ascended to a pinnacle in late 80s following the diffusion of satellite television, it has declined since mid-90s with the prevalence of "technological utopianism" (Segal, 1985). Today's new medium is the Internet. It sets the academic agenda with its interactivity, global accessibility, infinite channel capacity and other pro-democracy properties. It engulfs the critics of technology, whose voice nearly disappears after Herbert Schiller denounces the information superhighway as the "latest blind alley" that "is being promoted with uncritical acclaim" "under the control of a handful of private, giant, communications conglomerates" (1996:87-88).

The diffusion of Internet also contributes, at least in part, to pacifying polemics about global system and information sovereignty[1]. This controversy is linked with the aforementioned debate since democratization associated with the Net can be regarded as the global homogenization of political communication in accordance with western liberal democracy[2]. The global computer network knows no law but "Jeffersonian information policy" (Kapor, 1993). It fosters a new "transnational public sphere" in the process of "deterritorialization" (Frissen, 1997:115). National boundaries are melting. *The territories* of the nation-states are superceded by *the cyber-*

---

1 The arguments between globalization and national information sovereignty are best known in the heated debates about New World Information and Communication Order in the 80s (McPhail, 1987; Galtung and Vincent, 1992; International commission for the study of communication problems, 1993). Information sovereignty means that national sovereignty, the supremacy of the State over other authorities in its territory, encompasses the right to regulate their media systems (Alexamdre, 1993:345-46; Guan, 1995:406-408).

2 In this sense, media democratization is part of the multi-faceted globalization process centered to the West, the English-speaking countries, and ultimately, the United States (Hall, 1991). It can be therefore accused of "media imperialism", "electronic colonialism" and "peaceful evolution" from the perspective of local authorities such as those in Mainland China.

space, where there is no central government, where the "free flow of information" takes the supreme rein, where the notion of "information sovereignty" makes no sense, where global democratization becomes the dominant discourse for OPC.

However, the halt of debates does not imply overall changes in the real world. That the Internet is globalizing democracy is at most an acquiescent consent in the academia, which may not be accepted by policymakers in the nation-states. This is the situation in Mainland China, where legislative, administrative and technological measures are employed by government officials who imagine the world of computer-mediated communication (CMC) as *the cyberspaces* divided along real-world boundaries. The traditional tangible space is ruled in a mutually exclusive manner by the modern states. Why not the cyberspace?

The difference between the virtual and nonvirtual spaces has not entered the mentality of traditional authorities in that their decision still has its potency on the Net. As will be demonstrated, China still can maintain certain boundaries between the "domestic cyberspace" and the "foreign cyberspace", between the open arena of apolitical discussion and the taboo area of nonofficial OPC. The reason is simple but crucial: *so far no cyberspace can exist without tangible subsistence including the devices, the technicians, the users and the sociopolitical context in which all these nonvirtual components are put together to support and arrange the mediascape of the virtual world.* When the nation-state imposes control over the subsistence of the cyberspace, the latitude of OPC is constrained.

How shall we conceive the measures taken by the Chinese authorities to extend their rule from the real space to the virtual space? Are they unimportant abnormalities or warning signals of conceptual inadequacies concealed behind the recent quiescence of the age-long debates? Even if they are ephemeral phenomena that will be swept away by the forces of technology, they deserve critical analysis in themselves because the existence of government control over OPC, though undesirable to many, is an undeniable corner of the Web *per se*. Even if globalization, westernization and democratization may be claimed as the major trends in the virtual land, they do not dismiss the existence of localization, dewesternization and the continuation of authoritarian rule as constituents of the empirical world online, and therefore, as legitimate subject matter for academic inquiry.

How does China control the new means of public political communication? What are the characteristics of China's Internet regulations, the structure of regulatory body and patterns of policy implementation? What are the implications of these regulatory efforts? These are questions to be explored in this paper. In doing so, we are shifting our attention from the West to the East, from *the global cyberspace* to one domain of *the local cyberspaces* reclaimed by the People's Republic of China.

This is not only a geographical shift but also a conceptual one. The bulk of today's research about the Internet and politics regard technology as the independent variable that changes political institutions. This is a valid approach, but not the only one. In this paper, the presumed causal relationship is reversed. The focus is on the institutional responses of the Chinese party-state to the challenges of the new medium. In doing so, I hope to propose a concept based on the largely unexplored terrain of China's cyberspace that may revitalize the old dialogues concerning the political aspect of media globalization: *virtual censorship*.

Virtual censorship is a series of defensive policies undertaken by the Chinese authorities to prevent China's "domestic cyberspace" from being merged with "foreign cyberspaces" and keep apart the apolitical and political domains of CMC. It is *virtual* because the control mechanisms, albeit implemented in both the tangible and intangible spaces, aim at constraining nonofficial OPC in the virtual sphere. It is *censorship* because the policies reduce the interactions between the cyberspaces and the scope of political discussion by means of prohibition, supervision and punishment. From the perspective of democratization, virtual censorship is an undesirable segment of the emerging virtual reality defined as "a simulation of existing realities" and "the creations of a new reality" (Frissen, 1997:113), which attempts at rendering boundaries in the cyberspace and those in the real space congruent. Yet from the angle of globalization, it is natural and readily comprehensible since various forms of local resistance are constituents of the globalization process (Sreberny-Mohammadi, 1991; Appadurai, 1990).

The phrase has another implication: it is not *real domination*. As will be discussed in detail, the political restrictions exerted upon China's cyberspace are less rigid, suppressive and manipulative than the ways in which the Chinese party-state controls the mass media. Although employed by traditional authorities to maintain the existing order of political communication, they constitute a new mode of local media control with distinct features. Virtual reality seldom *copies* real realities. Neither does virtual censorship. Being projected by the Chinese officials upon the new realm of political communication, it bears some features of the new medium that enhances its efficacy on the one hand and gives rise to obviation on the other. These characteristics will be discovered when we bring Mainland China from the margin of the cyberspace to the center of our attention.

B. Literature Review: Studying China's Cyberspace

In contrast to voluminous publications about OPC in America and Western Europe, there have been only four works regarding computer networks and the democratization of China. One of them examines how Mainland Chinese students in the United States utilized CMC to facilitate their political activities in the late 80s (Li, 1990). Although informative, it does not demonstrate how the development of Internet may weaken China's authoritarian rule within its national boundaries. A second study relies on existing documents (Taubman, 1998). It makes a plausible argument that the Chinese Communist Party (CCP) faces a dilemma of policymaking posed by the liberalizing potentials of the Net and its economic prospects. Yet the author assumes the "built-in incompatibility between nondemocratic rule and the Internet" (p.256) and does not consider the defensive measures of the Chinese party-state systematically.

The third research in a book named *Cyberpolitics* (Hill and Hughes, 1998) reports a content analysis of Usenet messages representing 41 countries including China. 41 Usenet groups are selected to stand for the countries. After running multivariate tests, the authors conclude, "[t]here must be a true relationship between democratization in a nation and the likelihood that someone will post an anti-government message directed at that nation's government" (p.106). Remarkably, China lies exactly on the regression line of their analysis, which means China's OPC can be perfectly predicted in one of their models (p. 105).

As I was skeptical of their operationalization, I ran a small test in *socio.culture.cn*, the Usenet chosen by Hill and Hughes to stand for China[3]. I found what they analyze is not how the new medium leads to democratization within the country but how it allows people abroad to criticize the Chinese authorities in a place where few people in China can access. Internet systems in China do not support Usenet since "the communication volum[e] is too large" and the network administrators "can't afford [for] about 500MB volum[e] each day"[4]. As a result, few domestic Chinese users have access to the Usenet. The democratizing effect of the Internet is thus far from established insofar as China is considered. The inappropriate operationalization indicates a methodological deficiency shared by the previous researches about China's OPC, namely inadequate understanding of actual situations in China's cyberspace. This shortage is best overcome in the fourth study (Huang, 1997).

This research conducted by Edgar Huang combines field observation and interpretive content analysis of messages in bulletin board systems (BBSs). The fieldwork was carried out in 1996 in four Chinese commercial BBS stations. An America-based ISP was included for comparative purposes. It is found that, pressed by various "discussion rules" and the "webmaster's censorship" in domestic arenas, Chinese Internet users seldom engage in "hard topic discussions" about democracy and other political topics. However, when they attend the oversea BBS, they tend to talk more about democratic development in China. My observations in various BBS communities confirm these findings.

Huang's research approach is bottom-up. He first examines the BBS messages, representing communication patterns among ordinary users, and then attributes the lack of OPC to political censorship. This analytical trajectory is appropriate for Huang's study, which attempts to identify online censorship as a potential obstacle for the Internet to democratize China. But it is not adequate for a systematic depiction of China's virtual censorship. Therefore, my study adopts the top-down institutional approach widely used in political science and China studies, also known as Sinology. It is presumed that users' OPC patterns in China's cyberspace has to be understood as contingent upon the institutional barriers set by the Chinese authorities between the domestic and foreign cyberspaces, between the apolitical arenas and the sphere of OPC. The totality of these constraints is virtual censorship, which governs not only BBS but also other channels of CMC such as http, ftp and email, which confines ordinary users as well as techni-

---

3 A total number of 3333 messages were identified. Sorted by date, they extend from January 19 to March 4, 1999. 202 of them are selected using systematic sampling (sampling interval=18). Following the procedures specified in the book (p. 102), I coded the origins of the Usenet messages basing on the email addresses of the sources. No message was from Mainland China, whereas most of them were posted by people in North America (87.1 %). Breaking down the sources by nation yield following results: the US (166), Canada (10), UK (8), Australia (4), Singapore (3), Taiwan (2), France (2), Malaysia (2), Germany (1), Denmark (1), Hungary (1), Japan (1), Indonesia (1). Moreover, none of them is written in Chinese.

4 The quotations are from the "Internet" board of *bbs.mit.edu*, where I posted the question "why China does not have Usenet?" to solicit answers. *bbs.mit.edu* is an electronic bulletin board system (BBS) operated by overseas Chinese students at the Massachusetts Institute of Technology. It accommodates Chinese users both inside China and worldwide.

cians, media managers, network facilities and online services in a nationwide administrative infrastructure. It is the aim of this paper to sort out the control mechanisms of virtual censorship in China and discuss their implications in terms of formal regulation and actual implementation.

C. Methods

Document analysis, participant observation and interviews are employed because this paper examines both the formal and the operational dimensions of the regulatory measures in China's cyberspace. Computer-mediated communication (CMC) greatly facilitates data collection. Online search engines are particularly helpful for collecting regulatory documents. Meanwhile, I attend China's virtual communities and talk to my informants without leaving Hong Kong, where this research is conducted. Real-life means are used to check the validity of online data and explore the structural aspect of virtual censorship, which may not be available otherwise. Comparative methods are also used to demonstrate the characteristics of virtual censorship imposed by the Chinese government.

In order to survey China's Internet and its OPC regulations, I collect news clippings from magazines and newspapers such as *Wired, Time, New York Times, South China Morning Post, Asian Wall Street Journal* and *China PC World* (in Chinese). The original texts of the regulations are copied from websites sponsored by national and regional regulators as well as quasi-official publications such as *China Communications News* and *Telecom Trade*, both published in Chinese and English. Useful statistics come from CNNIC Reports at the website of China Network Information Center (http://www.cnnic.net.cn), which is authorized by China's State Council to provide statistical reports about the development of Internet in the nation. I also make use of an online survey conducted in March 1999 by Sohu (http://168.160.224.208/survey), the second most popular domestic website in China according to the CNNIC Report of July 1999.

Since January 1998, I have joined electronic bulletin boards systems (BBS) located at seven Chinese universities in Wuhan, Shanghai, Beijing, Shenzhen, Guangzhou and Hefei and paid regular visits to BBSs and chatrooms hosted by commercial companies in Guangzhou, Shanghai and Beijing. These virtual communities are representative of China's public CMC arenas since the diffusion of Internet is restricted to the urban areas[5]. The BBS I attend most frequently is *bbs.whnet.edu.cn* in Wuhan, where I served as the boardmaster (*banzhu*), a low-rank regulator, of two electronic bulletins -- one for Beijing University alumni, the other about Hong Kong for nearly one year until May 1999 when all boardmasters are required to register with real-life identifications. By average I spent one hour each day from January 1998 to May 1999 in this BBS. I grew up in Wuhan. I know the local environment before I logged into the virtual community. This advantage facilitates my participation as well as my application to be a boardmaster. In June 1998, I traveled to Wuhan to conduct face-to-face interviews with other boardmasters as well as an associate-station-master (*fuzhanzhang*), who was in a position to know more about the operation of the entire virtual community. Participant observation and interviews,

[5] The concentration of Internet users in the central cities is demonstrated in Table 1.

both in the virtual and nonvirtual spaces, allow me to examine not only the formal arrangements announced by the Chinese authorities but also the dynamics of policy implementation.

Virtual censorship should be understood not as an isolated phenomenon but as part of China's history of media control. Thus I bring in China's manipulation of traditional mass media to make comparisons. I know mass media regulations in China through reading official Chinese propaganda, taking courses in China's journalism, and conducting summer intern in Chinese mass media organization.

In this paper, I will first outline the history and current state of Internet in China, providing background information for the discussion of virtual censorship in terms of general development, user demographics and online activities. Then, I will concentrate on the formal content, regulatory structure and technological constraints of virtual censorship, by which the Chinese authorities attempt to create boundaries in the virtual space. The comparison between Internet regulation and mass media manipulation in China summarizes the distinct features of virtual censorship. Broader implications are discussed in the end of the paper.

D. China's Nets and Netizens: A Sweeping View

"Surmounting the Great Wall, walking towards the world" (*yueguo changcheng, zouxiang shijie*)[6] – this is the first email ever sent from Mainland China. It was delivered on 20 September 1987 through the China Academic Network (CANet) from Beijing to Germany. Using international long distance telephone line as its channel, CANet was slow, expensive and unreliable. In March 1993, the Institute of High Energy Physics (IHEP) established a dedicated data line linking up to Stanford University with a channel capacity more than ten times larger than that of the CANet[7]. Meanwhile, a project named "the National Computing and Networking Facility of China" (NCFC) was under way with funding from the World Bank and China's State Council. It was accomplished in April 1994, when more than 30 research institutes and two universities in Beijing were directly connected to Internet terminals located in the United States. Unlike CANet and IHEPnet, the server of NCFC supported both email exchange and TCP/IP, which means all major Internet functions such as http, ftp, telnet, gopher and WWW, were then available in Mainland China[8].

NCFC is the ancestor of today's China Science and Technology Network (CSTNet) operated by China's Academy of Science[9]. Since April 1994, several universities in China have also obtained access to the Net. They are interconnected in the China Education and Research Net-

---

6 Qian, Tianbai. "The development of Internet in China" (Internet zai zhongguo de fazhan). Beijing: *China PC World (zhongguo jishuanji shijie).* pp. 131.

7 Qian, Hualin. "China Science and Technology Network". Published online in December 1997 at http://www.cnnic.net.cn/jb/9711/cnnic-53.html.

8 Qian, Tianbai. "The development of Internet in China" (Internet zai zhongguo de fazhan). Beijing: *Computer World (jishuanji shijie).* pp. 132.

9 CNNIC Report. January, 1999. http://www.cnnic.net.cn/99'cnnic/p1.htm.

work (CERNet) under the auspices of the Ministry of Education. CSTNet and CERNet are designed for exclusive academic usage. In January 1995, China began its first public Internet services operated jointly by Sprint in America and China Telecom supported by the former Ministry of Post and Telecom (MPT) [10]. The linkages belong to ChinaNet, which is the largest nationwide computer network in China. Another national Internet access provider (IAP) is GBNet (China Golden Bridge Network) owned by China Unicom (Jitong), representing the interests of the former Ministry of Electronic Industry (MEI). Although MPT and MEI were merged into the Ministry of Information Industry (MII) in 1998, ChinaNet and GBNet are now kept apart. According to the No.195 Ordinance of the State Council in 1996[11], CSTNet, CERNet, ChinaNet and GBNet are the only nationwide "interconnecting units" (*hulian danwei*) with state permit to have direct linkage with the global computer network. In another word, the existence of other Internet Access Providers (IAPs) in China's cyberspace is illegal.

	Total number of users	**Total number of online computers**	**Total number of domain names[12]***	**Total bandwidth for international connection***
Jan. 1996	40,000	6,000	--	--
Oct. 1997	620,000	299,000	4066	25.41 MB
Dec. 1997	670,000	330,000	5100	--
Feb. 1998	820,000	400,000	6450	--
June 1998	1,175,000	542,000	9415	84.64 MB
Dec. 1998	2,100,000	630,000	18396	143.25 MB
June 1999	4,000,000	1,460,000	29045	241.00 MB

Table 1. The development of Internet in China

Table 1 summarizes the major findings of the nationwide Internet surveys conducted by China Network Information Center (CNNIC) since its establishment. The growth rate is dramatic. From June 1998 to June 1999, the total number of users and domain names both more than tripled, whereas online computers and international connection bandwidth increase at lower speed, which means by average each user has fewer facilities to enter the global cyberspace than before. And the diffusion of the new technology is still highly limited if China's huge population is considered[13].

---

10 Wilson, H.W. "China Logs On to the Internet". *The Economist.* 7 January 1995. p. 27.

11 Accessible at http://www.gznet.com/serassociate/mynews/law1.htm

12 Some data is missing in the reports.

13 As shown in Table 1, China had 4 million users by the end of June 1999. This figure accounts for merely 0.32% of the nation's total population and 1.07% of the nation's urban population.

	Nationwide Statistics	CNNIC Report (July 1999)	Sohu Report (March 1999)
Age (%)			
Younger than 20	34 *	10.5	14
20 – 35	29 *	78.4	74
Older than 35	37 *	11.1	12
Gender (%)			
Female	49 **	15	16
Male	51 **	85	84
Education (%)			
Below college level	75 **	14	13
College & higher level	25 **	86	87
Average monthly salary (yuan)	784 **	1520	1307
Geographical concentration (%) * **	7.9 **	41.5	44.5

Table 2. The demographics of China's Internet users[14]

As shown in Table 2, currently Internet users in China are predominantly male, young and with college or higher level of education. Their average income is nearly twice as much as that of the non-users. And geographically, they are highly concentrated in Beijing, Shanghai and Guangdong Province, the relatively more developed regions of the nation. Such a distribution of user demographics is not surprising because, in China as in other developing countries, educated young males in large cities are more likely than others to acquire computer facilities and technological know-how, both essential for Internet access.

	Location	Search Engine	News		Free Email	Chat Room	Bulletin Board
			Technology	Politics			

14 The CNNIC Report of July 1999 and Sohu Report of March 1999 use volunteer sampling by linking the questionnaires to established commercial and academic websites. The sample sizes are 52549 and 2227, respectively. Figures from *China Statistical Yearbook* (1998) and *1% Sampling Tabulation on the 1995 Population Census of PR China* (1997) are listed for the purpose of comparison.

* = 1% Sampling Tabulation on the 1995 Population Census of PR China (1997); ** = China Statistical Yearbook (1998); *** = The proportion of population living in Beijing, Shanghai and Guangdong Province.

1. Sina Net www.srsnet.com	*Beijing*	*	*	*		*	*
2. Sohu www.sohu.com	*Beijing*	*	*	*	*		*
3. Capital Online www.263.net	*Beijing*	*	*	*		*	*
4. Yahoo www.yahoo.com	*U.S.*	*	*	*	*	*	
5. Netease www.netease.com	*Guangzhou*	*	*	*	*	*	*
6. 163 Post Office www.163.net	*GuangZhou*		*	*	*		
7. GB Chinese Yahoo gbchinese.yahoo.com	*U.S.*	*	*	*	*	*	
8. China PC Weekly www.cpcw.com	*Chongqing*		*				
9. Shanghai Online www.online.sh.cn	*Shanghai*	*	*	*			
10. 21st Century *www.21cn.com*	*Guangzhou*		*	*	*	*	*
11. Chinabyte www.chinabyte.com	*Beijing*	*	*	*	*		*
12. China Central Television www.cctv.com	*Beijing*			*			
13. Guangzhou window *www.gznet.com*	*Guangzhou*	*	*	*		*	*
14. 263 freemail *freemail.263.net*	*Beijing*				*		
15. Hotmail www.hotmail.com	*U.S.*				*		
16. Shenzhen window *www.szptt.net.cn*	*Shenzhen*	*	*	*		*	*
17. Yeah Search www.yeah.net	*Guangzhou*	*				*	*
18. PC Home www.pchome.net	*Shanghai*	*	*				
19. CNNIC www.cnnic.net.cn	*Beijing*		*				
20. Microsoft www.microsoft.com	*U.S.*	*	*				

Table 3. Services provided by popular websites in China

There is strong utilitarian orientation among Chinese users. This is evident in Table 3 presenting services provided by the top twenty popular websites listed in the CNNIC Report of July 1999. Search engine, technological news and free email are of special strength in attracting users, indicating that Internet usage in China is still predominantly pragmatic and instrumental. The report also mentions that most users access the Net in order to check email (90.9%), use search engine (65.5%), upload or download software (59.6%), whereas only 28% of them join bulletin board systems.

BBS is the most important venue of public discussion in China's cyberspace because it is publicly accessible, its content is chronologically accumulative, and the users have relatively stable identity shown by their membership IDs. However, my observations in Chinese BBS concur with Edgar Huang (1997)'s study, which finds that political and ideological content is usually

outnumbered by discussions about technology, economy, entertainment, sports and other apolitical topics. In this sense, only a small portion of China's 4 million Internet users can be called "netizens", defined as those who engage in OPC.

A special group of netizens is the external users, who enter China's virtual territory from the outside, playing a key role in linking China's cyberspace with the global computer network. Most of them surf domestic websites and exchange information with others as ordinary users. Some directly oppose the rule of the Chinese authorities distributing emails with overt anti-CCP content. More aggressively, there are hackers breaking into China's Internet systems to put up humiliating messages on the websites owned by the Chinese party-state[15].

Meanwhile, the Chinese authorities also reclaim their territory in the cyberspace. Dozens of newspapers and TV stations in the country have established their websites to propagate the party line in the virtual sphere. A nationwide Government Online Project has been also launched, hoping to provide homepages for official organs of the State apparatus[16]. But these websites, sponsored either by the mouthpiece of CCP or state agencies, are not influential among Chinese users[17]. One possible reason is their lack of interactivity. The websites are designed to facilitate one-way indoctrination instead of OPC interactions. Seldom do they reflect nonofficial opinions except when they are hacked.

E. Bamboo Curtains Unfurled

I. Formal regulations

China's Internet regulation started in January 1993. So far there have been three regulations issued by China's central government concerning Internet usage. The most important one is the Temporary Regulation for the Management of Computer Information Network International Connection (the Regulation) passed in the 42nd Standing Convention of the State Council on 23 January 1993[18]. This regulation was formally announced on 1 February 1996 and verified on 20 May 1997. Detailed Implementation Measures for the Temporary Regulation (the Measures)[19] were issued on 8 December 1997. According to the Regulation, China adopts "the principle of overall planning, unified standard, stratified management, and advance in development" towards international network connection (Item 4). No units or individuals are allowed to establish direct international connection by themselves (Item 6). All direct linkage with the Internet must go through ChinaNet, GBNet, CERNet or CSTNet (Item 8, the Measures). License is

---

13 Hesseldahl, Arik. "Hacking for human rights?" *Wired*. 14 July 1998.

16 Information about this project is accessible at http://www.gov.cn.

17 According to the CNNIC Report of July 1999, no propagandist website belongs to the top forty most favorable websites among Chinese users except China Central Television and *People's Daily*, ranking the 12th and the 21st, respectively.

16 Accessible at http://www.gznet.com/serassociate/mynews/law1.htm

17 Accessible at http://www.gznet.com/serassociate/mynews/law2.htm

required for anyone to provide Internet accesses to users (Item 8) and registration for users to obtain access (Item 10). Except control over the facilities, the service providers and the ordinary users,"harmful information" that is either "subversive" or "obscene" is forbidden (Item 13). Punishment measures are specified in monetary terms (Item 14, 15).

The second regulation is the Ordinance for Security Protection of Computer Information Systems (the Ordinance) issued on 18 February 1994 by the State Council. It stresses that the responsible organ of Internet security protection is the Ministry of Public Security (Item 6), which is entitled to "supervise, inspect and guide the security protection work", "investigate and prosecute illegal criminal cases" and "perform other supervising duties" (Item 17). The Ordinance led to a subsequent regulation approved by the State Council and issued by the Ministry of Public Security in December 1997, namely the Security Management Procedures in Internet Accessing (the Procedures)[20]. In addition to further specifying the "harmful information" mentioned in the Regulation, the Procedures also lists the five kinds of "harmful activities"including:

> *(1) Intruding computer information network or make use of network resources without authorization; (2) Canceling, altering or adding functions in computer information network without authorization; (3) Canceling, altering or adding data and application software for the purpose of memory, processing or transmission in computer information network without authorization; (4) Intentionally producing, disseminating destructive software such as computer virus; (5) Other activities that are harmful to the security of computer information network (Item 6).*

Another result from the Ordinance was the revision of China's Criminal Code in March 1994[21]. Related provisions include:

> *Section 285: Whosoever, in violation of State regulations, intrudes into a computer information system involved in State matters, construction of the national defense or advanced technology shall be punished by imprisonment or detention of three years or less. Section 286: Whosoever, in violation of State regulations, deletes, alters, adds, or disturbs the operation of a computer information system so that it cannot operate properly, shall, in serious cases, be punished by imprisonment or detention of five years or less; in especially serious cases, imprisonment of five years or more may be imposed.*

It was reported that the Ministry of Public Security has established its computer investigation unit since 1996, which has processed over a hundred computer crime cases until July 1998[22]. Educational materials have been published and distributed to 170,000 police offices in Public Security Bureaus of the provinces and cities for the control over computer networks[23].

---

20 "Policy and regulation", *China Communications News* (*zhongguo tongxin xinwen*). March 1998, 2(2):45-49.

19 "Computer security in China". Washington: *East Asian Executive Reports*. 15 July 1998. pp. 10-11.

20 *Ibid.*

21 *Ibid.*

In addition to regulations issued by the State Council and the Ministry of Public Security, various managerial measures are also formulated at the level of the four major networks. ChinaNet, GBNet, CSTNet and CERNet all have announced their own regulations that either reiterate or substantiate the requirements of "public security" according to the unique features of the networks. For instance, in the Management Procedures of GBNet's Public Multimedia Information Services[24], it is stipulated that, while using the GBNet, it is prohibited to "produce, view, disseminate and announce harmful information that disturbs social security and contains obscene content"(Item 16). "National security regulations must be strictly abided by". Offenders may have their license rebuked and serious ones will be handed to organizations of public security (Item 17).

Because Internet chatrooms and electronic bulletin systems are particularly liable to become public political forums, national network authorities and local community managers issue specific regulations to circumscribe OPC as a dangerous field in cyberspace. CERNet's Regulation of BBS Management[25] provides that "the content of services in BBS systems shall be limited to the scope of academic exchange, which is mostly concerning science and technology. No service is allowed for non-academic content."(Item 2) And when there is an "emergent situation", system operators should "report immediately" and "resolutely delete the articles with political problems" (Item 5.1). "When the emergency is out of control, network centers in every region must immediately shut down the telnet and http interface linking up to the BBS where the emergency occurs" (Item 5.2).

Another example standing for cyberspace communities operating under commercial circumstances is the Community Basic Law of Netease[26], a website on ChinaNet located in Guangzhou, which is the most popular website in the country according to the CNNIC Report of January 1999. The Community Basic Law stipulates that

> *"citizens in the community must not talk or behave in violation of all regulations issued by ChinaNet" (Item 23). "If a discussion board contains anti-revolutionary, pornographic, personal attacking or other illegal articles, the community of Netease has the right to delete the board" (Item 32). "Those who overtly disseminate obscene, pornographic and anti-governmental speeches and opinions will have their user accounts suspended temporarily or deleted permanently in serious occasions"(Item 38).*

II. The national firewall and Intranet technologies

The formal regulations are implemented with the aid of network security technologies. As been specified in the regulations, network connection between China's domestic cyberspace and

---

22 Accessible at http://www.gb.com.cn/Chinese/information/fg3.htm.

23 Accessible at http:// bbs.whnet.edu.cn.

24 Accessible at http://club.netease.com /law.htm.

the foreign cyberspaces is monopolized by IAPs with state permit. In October 1997, China had no more than 25 direct international lines[27]. Upon these connection lines, China imposes what *Wired* magazine calls "the world's largest firewall" or "the Great Firewall"[28], that blocks access to selected websites with "harmful information" and automatically screens online content by targeting at words such as "June Fourth". The national firewall is in fact not a large project with respect to the small number of cross-border connection lines operating under state monopoly. With undeclared rationale and unspecified number of blocked sites, the national firewall blacks out http and www websites and ftp servers. But it can be easily penetrated especially through email. Most importantly, firewall software and devices do not allow the authority to recognize who the offenders are.

The really menacing technical measures taken by the Chinese government is therefore not the selected blockage of information from outside but the construction of the China Wide Web since 1996. This project enables China's policemen to trace all online activities of any targeted network terminal located within the firewall, including surfing, chatting, downloading and email exchange by using devices such as proxy servers. These technologies are usually used for Intranets of large commercial corporations. However, China is applying them to an entire nation.

Why the Chinese gatekeepers can utilize advanced network security technologies so quickly? A decisive but usually overlooked reason is the imports of such technologies from the United States. For instance, the Sun Microsystems obtained a US$15 million deal to build the Intranet backbone of the China Wide Web in December 1996[29]. And in January 1997, the Bay networks of California won a bid over other American computer companies, including 3Com Corp and Cisco Systems, to provide another multi-million dollar infrastructure for the China Wide Web[30]. The contractor standing for the Chinese authority is China Internet Corp., which is controlled by China's Xinhua News Agency[31].

Obviously, there is a dilemma in the global diffusion of Internet technology, which is not purely an instrument of political democratization. On the one hand, political consideration is not the only or most important factor in the global market. More often than not, commercial benefit is the predominantly influential goal. This is especially so when the commodity is Inter-

---

25 The CNNIC Report of October 1997. Among the 25 international lines, 16 are in ChinaNet, 4 in CERNet, 3 in CSTNet, 2 in GBNet. Updated reports no longer release information about international lines.

26 Mckay, Niall. "China: the Great Firewall". *Wired*, 1 December 1998.

27 Coale, Kristi. "China Shines Intranet Contract on Sun", *Wired*, 2 December 1996.

28 "Bay Networks wins CWW Bid", *South China Morning Post*, 21 October 1997.

31 It may be unfair to accuse these American companies of selling firewall and Intranet technologies to China so that the cyberpolice can use them for political purposes. The deals are first of all announced as targeting at network crimes such as online pirating that disturbs commercial order. Moreover, were there no such network security technologies reassuring the skepticism of high-level party leaders, China's construction of the Internet might have been in a slower pace, and ordinary Chinese people must have to wait longer to have access to the Web.

net technology, upon which American legislators have exerted little control. On the other hand, what Internet means is not a single technology that favors free flow of information. Rather, it is a set of technologies including those protecting stability and order. This dualistic nature of the new medium should be stressed.

III. The hierarchical structure of administration

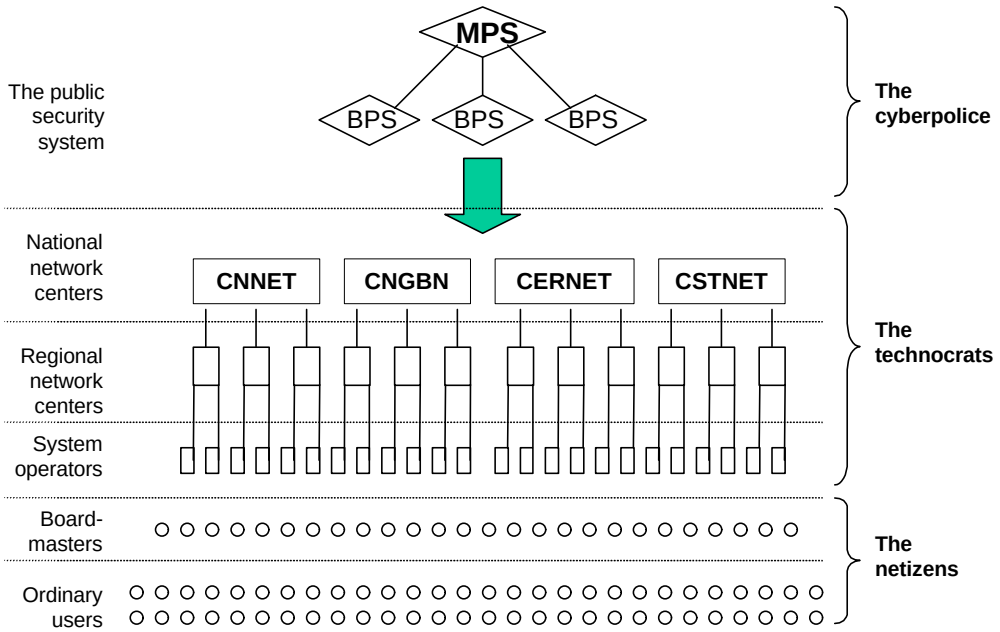

Figure 1. The hierarchical structure of regulation

Internet regulations stipulated by the Chinese party-state are not merely formal deterrence with technological supports. For the cyberspace communities such as BBS, there is also a hierarchical system of regulators (see Figure 2) since this is the place where nonofficial OPC content is most likely to emerge and accumulate. At the top of the hierarchy is the Ministry of Public Security (MPS) and its subordinate bureaus (BPS) in the provinces and cities. According to the regulations, the policemen are the most superior gatekeepers against the "inappropriate" uses of the Internet. They are called cyberpolice in this paper.

Under the shadow of the cyberpolice, there lies the entirety of China's cyberspace, which is, first of all, managed by the national network centers of the Internet oligarchies. Although in different sizes, these four networks are administratively parallel to each other. Each of them has several regional network centers that control Internet services in provinces and cities as for ChinaNet and GBNet or those in universities and research institutes as for CERNet and CSTNet. Among the regional network administrators, some technicians are directly involved in the daily maintenance of cyberspace communities. They are called "system operators" or simply "sysops". In BBS, they are also called "*zhanzhang*" (station-master) and "*fuzhanzhang*" (associate-station-master) as they assume the most visible power of administrative control in the community. They can choose, install or uninstall, and modify the platform on which CMC is going on.

They can set automatic screening software targeting at a list of "inappropriate" keywords and punish those who violate the regulations. The sysops and other administrative officials in the national and regional network centers are the technocrats in the middle of the Internet regulation hierarchy.

Most sysops are technicians at the lowest bureaucratic level of the regional network centers. In CERNet and CSTNet, a common practice is to assign a young teacher/researcher of Internet technology to be the station-master, while all other sysops are graduate students majoring in computer science or telecommunications[32]. Being members of the regulatory body in terms of both physical location and monetary rewards, they should be seen as an interest group different from ordinary users. Their subordinate relations with the state distinguish them from the lowest rank of regulators in cyberspace: boardmasters (*banzhu*).

Boardmasters are the regulators who are responsible for "cleaning" messages on one or a few electronic bulletin boards. Unlike the sysops, boardmasters are not necessarily members of the network centers. Like ordinary users, most of them use pseudonyms to log in. This means an external user can be a boardmaster within the Great Firewall until real-life identification is required in May 1999. Another significant feature distinguishing boardmaster from sysop is that the former is *electorate* whereas the latter is *selectorate*. Most of the boardmasters are winners of online elections, in which ordinary users vote via the Internet. Subsequently, their source of legitimacy is from ordinary users rather than the higher ladder of the hierarchy. Boardmasters and ordinary users are netizens in China's public OPC arenas.

The regulatory hierarchy is more than a cluster of post and rank. As in real-world institutions, human beings in China's cyberspace are tied to certain duties and subject to constraints. The cyberpolice is expected to supervise the technocrats and the netizens as well as the online OPC content and penalize disobedient actions. The technocrats shall follow instructions from the cyberpolice and use various means, including technological ones, to prevent users in their networks from accessing prohibited websites and expressing harmful information. The duty of the netizens is but one command: no trespassing upon the forbidden cyberspaces in their Internet exposure and online expression.

If the duties are not performed, there is a system of punishment mechanisms directed both at the technocrats and the netizens. The cyberpolice must be also subject to certain check from the State Council and the CCP Party Center. But this is not specified in any regulation. The announced means of punishment and those I observed as a member of the regulatory hierarchy include:

1. Penalties exercised by the cyberpolice upon the technocrats

(1) *Real-world personnel punishments*: the sysops and responsible administrators who fail to meet the political standards are censured, fined, removed from regulatory positions and/or subject to administrative sanction.

---

30 Information was collected in an interview with an associate-station-master conducted in June 1998.

(2) *Temporary suspension of network connection*: the websites or the virtual communities carrying forbidden OPC content are shut down for a period of time, when the technocrats are required to remove the inappropriate content. This mechanism is also employed for the purpose of prevention. For instance, every year in early June, most BBSs hosted by universities are denied network connection for a week or so due to the anniversaries of the massacre in 1989.

(3) *License revocation:* Serious violation leads to the revocation of license to provide Internet services. As the result, the responsible website or virtual community is closed *sine die*. So far there is only one such case, which is the Untitled BBS station of Peking University (*Beida weimin BBS zhan*). This BBS, formerly renown for zealot political discussions, has been closed for nearly three years since September 1996 when it mobilized a nationalist protest movement against Japan regardless of official objection.

2. Penalties exercised by the technocrats and boardmasters upon ordinary netizens

(1) *Message eradication:* sysops and boardmasters erase the articles containing undesirable content without using any other punishment mechanisms. The regulator may not even contact the offender. But this is nevertheless a form of punishment transmitting a lucid negative feedback to the responsible netizen: what you wrote is not acceptable in this online arena. Message eradication is the most widely used means of virtual censorship.

(2) *Temporary/partial suspension of membership:* if infringement is committed by the same netizen repetitively, the sysops suspend his/her access to the virtual community for a certain period of time. Or in some minor cases, the punishment is temporary suspension of some network applications such as voting, posting articles and chatting with other users. Boardmaster can also punish those who express harmful information by denying their right to post articles on the bulletin board s/he is in charge of.

(3) *Cancellation of membership account:* in the most serious cases, the offender's membership account in a virtual community is removed. Although it is stipulated that the technocrats shall hand severe violators to public security offices, never does this happen according to the reports I collected and my experience in China's cyberspace. Most netizens use pseudonyms when they really want to challenge the authorities on the Web. The gravest punishment is thus to eliminate the virtual existence of the offender.

F. Virtual Censorship vs. Mass Media Regulation

The modern space of politics relies heavily on symbolic construction. The polity has expanded to the extent that mediated communication has replaced obtrusive interactions as a major buttress for the "imagined community" of nation-state (Anderson, 1990). China's nationalization of political imagination may exceed many countries due to its tradition of collectivism and the dominance of communism. The Party and the State possess the exclusive ownership of all print and broadcast media in the nation. The Central Propaganda Division of CCP gives explicit instructions about reports concerning political affairs. The Chinese government censors

every medium flowing across its national boundaries, from newspaper to VCD, from cassette tape to satellite TV, in order to keep Chinese people imagining themselves politically as nothing but sons and daughters in the socialist family of China. In these regards, virtual censorship is logically consistent with its predecessors in the realm of China's mass mediated political communication. However, the geography of the virtual land is different. Though perhaps with repugnance the Chinese authorities nevertheless formulate virtual censorship to govern the new medium in a way inconsistent with previous control mechanisms over the mass media. The dissimilarities can be put into the following categories:

I. The genesis of regulation

There is a remarkable difference between virtual censorship and mass media regulation with regard to their genesis. In the history of the People's Republic of China, the press, radio and television have been controlled by the authorities since the very beginning of their operation. However, there was no formal rule for the Internet from 1986 to 1993, a period longer than the six-year history of China's regulation of the Internet. This was partly due to the medium's immaturity before 1993 and partly due to its limited scope of influence that was restricted to a few scientists at the time.

II. Media ownership

As for ownership, China's Internet Access Providers (IAPs), i.e. the four national networks, are similar to mass media as being monopolized by the State. However, private ownership of Internet Service Providers (ISPs) is allowed. And Since December 1998, CHINANET and GBNET, have been reforming to establish non-official ownership as a response to Premier Zhu Rongji's call for the split between public offices and their enterprises[33]. If the separation is successful, the state ownership of the Web will be significantly reduced.

Meanwhile, personal computers and modems also constitute an indispensable part of the Internet. These facilities are possessed by party-state offices, commercial organizations as well as households and individual users. The dispersion of media ownership in regard of network terminals is most conspicuous. And unlike television sets and radios, computers with network connection allow individuals to engage in the processes of symbolic production and message dissemination in addition to information consumption.

III. The manipulation of media content

China's mass media have been known as the "mouthpiece" of the authorities. By controlling media ownership, the nation's powerful ideologists govern the personnel system in media organizations and establish strict censorship mechanisms such as "stratified checks" (*ceng ceng shen pi*) to ensure that the publicized political content advocates the party line. However, the cyberpolice is not entitled to appoint and dismiss managers in the national networks. Neither is there a vertical relationship from the Central Propaganda Division to the ISPs concerning what

33 "China Telecom at crossroad, new uncertainties". *Asia Pacific Telecommunication*. 1 January 1999.

should be exhibited online. Freed from the burden of "propaganda tasks", the sysops and boardmasters can be more dedicated to pursue commercial or professional goals. In this sense, the present proliferation of apolitical information in China's cyberspace, though not fully supporting democratization, is nevertheless a progress in comparison with the manipulated political facade of the mass media.

Moreover, due to the technological attributes of the Internet, ordinary netizens are allowed to speak out in the forums hosted by nonofficial ISPs. Technical detours bypassing the regulatory obstacles are also possible in case the user has more computer literacy.

IV. The invisibility of the Party

Another difference is the role of CCP. So far the "Party press" like *People's Daily* is still monopolizing the mass-mediated political arena of the nation. In contrast, CCP's portion of the Web is trivial. So far there is nothing that can be called a nationwide "Party Net". Even if technically there are some "Party ISPs", they are few in number and feeble in influence. Meanwhile, different from the penetration of CCP in the mass media system, Party groups are not established at least at the lower levels of the regulatory hierarchy.

The conceivable decline of the Party as a direct regulator of media content in cyberspace means that the authoritarian control over CMC in China depends more on the Chinese government. State ownership of both IAPs and ISPs is overwhelming. Regulations of the Internet are issued by the State Council rather than the Central Propaganda Division. The enforcement relies on various government officials rather than the cadre system of CCP. Additionally, legal adjustments were formulated and announced as the state regulation of the Net began, whereas the mass media are still suffering form the lack of stable regulation.

The distinction between the Party and the State is meaningful in the analysis of virtual censorship since government officials are supposed to be more professional and ideologically less committed. An intriguing comment is that Beijing's attempt to block foreign websites is but a strategic ritual employed by the technocrats to satisfy the hard-liners[34]. This is possible since government agencies do have interests different from party organs. However, it is naïve to regard the State as an autonomous regulator totally separated from the CCP, which may still have an "invisible hand" at work, although there is no explicit indication of its role in the alleged measures of Internet regulation.

V. The efficacy of the regulations

Virtual censorship may not be as effective as mass media regulation because of the following reasons. First, the efficacy of punishments is reduced by the virtuality of CMC. Chinese journalists in mass media organizations face real risks if they hope to deviate from the Party line, whereas their counterparts in cyberspace face mostly virtual ones especially when they use pseudonyms. Although China announced some real-world means for virtual censorship such as the

---

32 *Ibid.*

invalidation of ISP license and criminal charges against offenders, the actual utilization of such measures is infrequent. Real-word punishments thus function mostly as potential deterrence rather than direct penalty like message eradication, which hurts only the virtual existence of the netizens rather than their tangible life.

Second, there is no visible reward system to encourage users to comply with the rules or sysops to improve their "network security work". The hierarchical structure of regulation is held together by a series of negative feedback from the cyberpolice to the technocrats to the netizens. Yet there seems to be no channel for positive feedback the other way round. Incentives are an important part of institutional constraints. In China's mass media industry there are various incentive mechanisms such as the election of best news stories and best journalists. But so far this aspect is underdeveloped in virtual censorship.

Third, different from the relatively standardized implementation of central policies in the mass media, the actual implementation of virtual censorship varies greatly in different geographical regions, at different administrative levels, during different period of time. For instance, message eradication is usually more frequent and strict in websites located in Beijing, the nation's political center, than in other parts of the country. In distant provinces such as Yunan, it was reported that the registration of Internet Cafe had not been put into practice until recently[35]. Virtual censorship also tightens up when the date of June 4th impends and the National People's Congress is under way, while it is loosened for the rest of the year. Meanwhile, there is resistance from lower-level technocrats. Many sysops are reluctant to follow the instructions of closedown during the sensitive dates. In my interview with a sysop, my informant even disclosed some technical tricks he used to keep the BBS station open to ordinary users but look like closed when the cyberpolice supervises it. The uneven implementation of Internet regulations therefore results in freer OPC and the reduction of actual censorship in remote areas, at lower administrative level and during periods when the political atmosphere is relatively open.

Admittedly, new facilities, new staff and new methods are employed to tackle the new space. But comparing with political control over the mass media, China's censorship over the Internet is still primitive. The regulatory structure of Internet regulation is less developed, the implementation processes are less predictable and the institutional constraints are less confining. The reduction of gatekeepers' manipulative power is clear.

Thus far I have discussed the measures employed by the Chinese government to impose national border and political boundary upon the cyberspace. Relatively ductile as it is in comparison with China's mass media regulation, virtual censorship nevertheless has legislative, technological and administrative teeth, in virtual and nonvirtual spaces alike, that reduces the latitude of OPC in China's cyberspace. The best showcase is the imprisonment of Lin Hai, a software engineer in Shanghai, who sent 30,000 Chinese email addresses to an electronic dissident publi-

---

33 Information was collected in an interview with Stan Sessor, a technology columnist at *Asian Wall Street Journal.*

cation based in America[36]. This transaction infringes the lines of both geographical and political demarcations presumed by the Chinese authorities in the virtual land. He was arrested by cyber-police in March 1998, accused of "subversive act", and sentenced to two-year imprisonment on 20 January 1999.

G. Beyond the Great Firewall: Discussions

It remains uncertain whether virtual censorship in China will become more menacing or they will collapse someday, leaving OPC free at last among the Chinese netizens. But it is appropriate to draw a few conclusions from what I presented concerning China's OPC regulation *per se*.

(1) Existing institutions with authoritarian control over political communication *still have their potency* to respond to the challenges of CMC. Institutional constraints are formulated and imposed directly upon Internet facilities, service providers, and domestic users in the real space and thereby indirectly upon the latitude of political discussion in the virtual space. In doing so, the Chinese government is still viable to establish national, political boundaries in "China's cyberspace" and change the Net before the Net subverts it.

(2) The current regulatory measures against nonofficial OPC, albeit employed for old purposes, have their new characteristics. They depend more on imported network security technologies and government agencies than on CCP's propaganda apparatus. They constitute a yet immature administrative system comparing with that of mass media in terms of both ownership and the manipulation of media content. The regulatory body is less hierarchical. The punishments are less confining. Consequently, virtual censorship should be conceived of as *a new mode of media control* in Mainland China.

(3) This paper is not a total denial of global democratization. Rather, it modifies the hypothesis that the diffusion of Internet invariantly brings about the decline of authoritarian regimes in the nation-states. Being content with the grand narrative is not helpful for us to understand what happens in China, whose cyberspace accommodates incentives as well as constraints of democratization. And the interaction between the opposing forces may produce merely *limited transformation* of the traditional media system towards equality, plurality and openness rather than sudden paralysis of the Chinese authorities in cyberspace.

To see broader implications of these findings, it is necessary to locate China's Internet regulation in a larger spatial scope. One useful way is to briefly compare China with Singapore, another important component of the global Chinese community that is also known internationally for its efforts to regulate CMC. Singapore and China both control the Internet in a way stricter than Taiwan, Hong Kong and other parts of the world. Moreover, these two countries are often confounded with each other as the world's "most extreme version of governmental

---

[36] Faison, Seth. "China sentences Internet entrepreneur to 2 years in jail". *The New York Times*, 21 January 1999.

and political control over the nets" (Rash, 1997:162). Comparing them is therefore of primary significance for us to map the landscape of the cultural China in the virtual world in terms of OPC.

A case may be a good start for the comparison. In April 1999, three months after Lin Hai was sentenced in Shanghai, Singapore's state-sponsored telecommunications monopoly, SingNet, made a public apology for intruding into its subscribers' personal computers in the name of "virus scanning"[37]. The intrusion was discovered by a college student, who contacted the police and the mass media for help. Under public pressure, SingNet was forced to apologize publicly that "we should have informed the subscribers in advance". This event, albeit reflecting the patriarchal role of the regulators, nevertheless illuminates that Singapore's Internet regulation respects citizen's right to privacy, at least while facing the public, and the regulatory body permits bottom-up resistance. Both these characteristics are non-existent in China's virtual censorship.

Moreover, according to Singapore's Internet Code of Practice[38], taboo areas in its cyberspace are much specified, comparing with Mainland China, and the target of regulation is the ISPs rather than individual users[39]. Regulatory power is not monopolized by Singapore Broadcasting Authority (SBA), the state agency in charge of CMC. Industry self-regulation and parental guide in households are encouraged with technical supports[40]. A "light-touch" enforcement policy is adopted, which means, "an offender will be given a chance to rectify the breach before SBA takes any action"[41]. Obviously, Singapore's Internet regulation is less centralized and more transparent than virtual censorship exerted by the Chinese authorities, who seldom explain their policy rationale, set up specified industry guidelines, or acknowledge basic rights of ISPs and ordinary netizens. The periodical suspension of BBS services in CERNet during sensitive dates like June 4th is a good example. Administrators at higher level of the regulatory hierarchy never bother to explain why such a punishment of virtual communities in a national scale should be taken.

Certainly, Singapore also sets constraints against nonofficial OPC. Unlike commercial ISPs, those who set up websites with political content in Singapore are required to apply for state approval. Although references to seditious material were dropped in the revision of Singapore's Internet Code of Practice in October 1997, there are still political boundaries since "the prohibition is covered by other laws"[42]. Thus generalizing Singapore and China as representative of the same "prevention model" (Rash, 1997:162) is meaningful only when the West is used as

---

37 Sessor, S. "SingNet apologized for virus scanning". *Asia Wall Street Journal*. 7 May 1999.

38 Available at the site of Singapore Broadcasting Authority (*http://www.sba.gov.sg*).

39 Tee, Edmund. "Revised Internet code makes taboo area clear". *Straits Times*. 23 October 1997.

40 "SBA's approach to the Internet". Available at http://www.sbs.gov.sg/internet.htm.

41 *Ibid.*

42 Tee, Edmund. "Revised Internet code makes taboo area clear". *Straits Times*. 23 October 1997.

the comparative reference. Both countries hope to protect their OPC arenas against invasions from other cyberspaces. Yet the generalization should not be carried to the extent that their internal variance is completely ignored. And virtual censorship in Mainland China should be conceptualized as a distinct mode of media control not only in the Chinese history but also in the world at large.

II. Unfinished inquiry

Cross-media and cross-national comparisons depict virtual censorship as new measures imposed by the Chinese government upon China's cyberspace. However, on a more abstract level, when the totality of CMC is considered in a global scope, virtual censorship can be seen as not so special. It reflects the emerging attempts of legislatures, governments and various administrative organs worldwide to incorporate the cyberspace into their sphere of jurisdiction. The Communication Decency Act of the United States issued in 1996, which outlaws the distribution of materials such as child pornography and profanity via the Net, is an example of these attempts. Although with different intention and different methods of implementation, the regulation of CMC in United States, as in other Western countries, also aims at drawing boundaries in cyberspace, if not political ones between different nation-states, then ethical ones between different groups (e.g. people of different age, with different sexual orientation). The boundaries may be different in the East and the West. But they are all boundaries that separate the cyberspace into the cyberspaces.

Looking back to media history, Herbert Schiller argues that "The high expectations for the new means of transmitting messages and images are invariably thwarted by the *institutional arrangements* that quickly enfold the new instrumentation" (1996:75, emphasis added). The kind of institutional forces he mentioned is commercial corporate management. But as shown in this paper, his argument also applies to authoritarian political censorship in China. Like many of its predecessors, the Internet may enjoy a certain period of freedom at its inception, when bureaucracies of social control experience a "new medium shock". But sooner or later, control mechanisms will be developed and imposed with features of the new medium as well as the old regulatory institution. This may be the reason why Internet regulation is burgeoning worldwide today when deregulation is the catchword in the global telecommunications industry.

III. Orientations for future study

I would like to admit some insufficiencies in my study that may shed light on orientations for future study.

First, my access to the regulatory organs is incomplete. I use document analysis to examine vertical control from higher level of the hierarchical structure and participant observation and interviews to explore how the top-down measures work at the grassroots level. As a result, the study contains inadequate information about the technocrats in the middle of the regulatory hierarchy and about the dynamics of policymaking. The study will be improved, if more access is available and more in-depth data is collected at the higher strata of the hierarchical structure.

The lack of first-hand quantitative data is also a drawback. None of the statistical reports I use in this paper is designed for the study of OPC. Their results may provide some background information. But to know exactly how OPC is going on in China's cyberspace and what may influence the efficacy of virtual censorship, new data needs to be collected by means of content analysis like in Edgar Huang's previous work. Online survey is also desirable but perhaps not feasible in China's cyberspace where ISPs are under tight political control.

Due to limited space, the comparative part of this paper can be further strengthened. It is possible to choose a specific issue of political discussion and compare its communication patterns in cyberspace with those in the mass media. Other countries representing different Internet regulation models can be added together to make typologies. It may also be promising to compare OPC with different media, such as China's big-letter posts (red posts), a traditional small medium for political communication, to generalize patterns of media control imposed by political authorities. In sum, our understanding of virtual censorship in China will be enhanced if more comparative work is conducted.

H. Concluding Remarks

"Surmounting the Great Wall, walking towards the world." In retrospect, China's Internet has taken a route of development deviating from its anticipated mission of democratization. The Chinese authorities have exerted various institutional constraints upon OPC and transform the Internet to serve their interests. Formal regulations are issued and enacted. The Great Firewall and the China Wide Web are constructed. The hierarchical structure of regulation is established to further exclude users that are politically unreliable and contents that are ideologically undesirable. All these policies of virtual censorship are implemented to constrain the liberalizing effects of the Internet so that the Chinese people will use the new medium in the old hegemonic modes of political communication.

It is evident that the Internet does not paralyze the Chinese authorities in their efforts to minimize the liberalizing impact of the new medium. However, comparing with mass media, the distinct geography of the virtual space does give rise to a more decentralized media ownership system, a less hierarchical regulatory body and a set of punishment mechanisms with less confining potency. These characteristics should be acknowledged as indicators of limited transformation towards democracy rather than reflections of global democratization that stresses the dissolution of national borders and the demise of authoritarian control. National and political boundaries are still emerging. And virtual censorship in China may nevertheless have few parallels worldwide.

Bibliography

1% Sampling Tabulation on the 1995 Population Census of PR China (1997). Beijing: China Statistics Press.

Alexandre, L. (1993). "Open skies over the South". Nordenstreng, K. and Schiller, H. (eds.). Beyond national sovereignty: international communication in the 1990s. Norwood, NJ: Ablex. pp.343-367.

Anderson, B. (1983). Imagined Communities. London: Verso.

Barber, B.J. (1984). Strong democracy: participatory politics for a new age. Berkely: University of California Press.

Boorstin, Daniel J. (1978). The republic of technology: reflections on our future community. New York: Harper and Row.

China Statistical Yearbook (1998). Beijing: China Statistics Press.

Galtung, J. and Vincent, R. (1992). Global Glasnost: toward a New World Information and Communication Order (Chapter 2). Cresskill, NJ: Hampton. pp.31-70.

Guan, S. (1995). Intercultural communication (in Chinese). Beijing: Beijing University Press.

Hauben, M. (1996). The netizens and the wonderful world of the Net: an anthology. Available at http://www.columbia.edu/~hauben/netbook/.

Hill, A. K. & Hughes, E.J. (1998). Cyberpolitics: citizen activism in the age of the Internet. Lanham, MD: Rowman & Littlefield.

Horkheimer, M. and Adorno, T.W. (1973). Dialectic of Enlightenment. London: Allen Lane.

Huang, E.S. (1997). "Flying freely but in a cage". Paper presented in the 1997 convention of Association for Education in Journalism and Mass Communication. Chicago, Illinois. July 1997.

Innis, H. (1964). The bias of communication. Toronto: the University of Toronto Press.

International Commission for the Study of Communication Problems. (1980). Many voices, one world. London: K. Page; New York: Unipub.

Li, T. (1990). "Computer-mediated communications and the Chinese students in the U.S." Information-Society. No.7, February, pp. 125-137.

Luke, T.W. (1989). Screens of power: ideology, domination, and resistance in information society. Urbana and Chicago, IL: University of Illinois Press.

Mayer-Schonberger, V. and Foster, E.T. (1997). "A regulatory Web: free speech and the global information infrastructure". In Kahin, B. and Nesson, C. (Eds.). Information policy and the global information infrastructure. Cambridge, MA: the MIT Press.

McPhail, T.L. (1987). Electronic colonialism: the future of international broadcasting and communication. (2nd revised Ed). Newbury Park, CA: Sage.

McLuhan, M. (1954) "New Media as Political Forms." Explorations, No.3, August, pp.120-126.

Naisbitt, J. (1982) Megatrends: ten new directions transforming our lives. New York : Warner Books.

Postman, N. (1993). Technopoly: the surrender of culture to technology. New York: Vintage Books.

Rash, W. Jr. (1997). Politics on the Nets: wiring the political process. New York: W.H. Freeman and Company.

Schiller, H.I. (1996). Information inequality: the deepening social crisis in America. New York and London: Routledge.

Segal, H.P. (1985). Technological utopianism in American culture. Chicago & London: University of Chicago Press.

Sreberny-Mohammadi, A. (1991). "The global and the local in international communication," in Curran, J. and Gurivitch, M. (eds.). Mass media and society. London: Edward Arnold. pp.118-138.

Taubman, G. (1998). 'A not-so world wide web: the Internet, China, and the challenges to non-democratic rule.' Political Communication. 15, 255-272.

Toffler, A. (1980) The third wave. New York: Morrow.

Vig, N.J. (1988). Technology, philosophy, and the state: an overview. In Kraft, M.E. and Vig, N.J. (Eds.). Technology and politics. London and Durham: Duke University Press.