University of Alberta

Internet Control in China: A Digital Panopticon

by

Yin Zhang ©

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements for the degree of Master of Arts

in

Humanities Computing

Department of East Asian Studies

Edmonton, Alberta

Spring 2004

Your file Votre référence
ISBN: 0-612-96427-2
Our file Notre référence
ISBN: 0-612-96427-2

Abstract

According to Western politicians and journalists, the Internet, is an open medium with certain characteristics that make it difficult to control. They believe that the efforts to control the Internet are doomed to fail. Some of them even expect the Internet to be a medium that will instinctively seek to undermine, and overthrow authoritarian regimes such as China. This study attempts to counter these views and discuss to what degree the Chinese government can control the Internet. It offers a legal, technical, social and cultural, and economic perspective in answering these questions. The conclusions are that the Chinese government is quite capable of controlling the Internet in China and that the Internet can even be used as a means for control. Rather than undermine the authority of the Chinese government, the Internet actually serves the purpose of the regime as much as it helps to loosen governmental control over freedom of expression and the everyday life of its citizens.

Acknowledgements

I have been fortunate enough to receive the assistance of a number of people in the course of researching and writing this thesis and would like to take this opportunity to offer my thanks.

I would like to thank my supervisors, Dr. Laifong Leung and Dr. Sean Gouglas for their direction, assistance, and guidance. Their recommendations and suggestions have been invaluable for the project. The writing of this thesis would not have been possible without their support and encouragement.

Thanks are due to Ms. Ania Dymarz and Ms. Pat Barford for taking the time to proofread and comment upon my work.

Thanks also go to the Department of East Asian Studies and the Program of Humanities Computing who provided financial support for me.

Finally, words alone cannot express the thanks I owe to my parents and Liqiang Wang, my husband, for their encouragement and support that enabled me to be here today. I am immensely grateful for the many sacrifices they have made for me.

亲爱的爸爸妈妈, 亲爱的立强, 谢谢你们无私的爱和长久的支持.

我的每一点收获都是因你们才能成就, 也因为你们而有意义.

我愿意是你们心中永远的骄傲!

Contents

List of Tables

Introduction

> In the new century, liberty will spread by cell phone and cable modem ... We know how much the Internet has changed America, and we are already an open society. Imagine how much it could change China. Now, there's no question China has been trying to crack down on the Internet --- good luck. That's sort of like trying to nail Jello to the wall.
>
> --- Bill Clinton, 8th March 2000. (Kalathil, Drake & Boas, 2000)

The Internet, since it made the transition from military and academic experiments to mainstream global communications network, has been viewed by Western politicians, libertarians and journalists alike as a kind of catalyst for freedom, justice and democracy. It is seen as a medium that will instinctively seek to undermine, and perhaps, overthrow authoritarian regimes such as the People's Republic of China (PRC) while simultaneously espousing democratic ideals and bringing the North American and European type of representative government to the rest of the world. The above quote from Bill Clinton, the former US President, shows what appears to be the general consensus in the West and in particular the United States. One cannot but agree with Clinton when one keeps hearing from journalists and politicians that the Internet is the harbinger of freedom without boundaries. According to them, although the Chinese government attempts to block websites deemed undesirable, the information can still travel in China[1] due to the "inherent characteristics" of the Internet by re-routing the information around filters. As a result, the Internet eventually will pose an insurmountable threat to the Chinese government (Taubman,

[1] China in this thesis refers to the Mainland China, excluding Hong Kong, Taiwan and Macao.

1998). Authoritarian regimes such as China that relies on information control will be defenceless against the Internet. "The state is too big, too slow, too geographically and technically limited to regulate a global citizenry's fleeting interactions over a mercurial medium." (James, 1997).

While many countries have restricted Internet access to varying degrees (e.g., Cuba only allows Internet access from approved institutions [Kalathil, Drake & Boas, 2000] and Internet access was completely prohibited in Taliban-controlled Afghanistan [Lebowit, 2001]), the Chinese government has actively encouraged and invested in the growth of the Internet. In 1998, the government invested RMB 3.1 billion into Information Technology facilities. This number has seen yearly increases, with investments reaching RMB 100 billion by the end of 2002. It is estimated that China will invest RMB 250 billion into IT infrastructures in 2003 and the next few years (Li, 2003). Faced with these facts, one cannot help asking: why is the Chinese government promoting the use of the Internet? By doing so, will they not be digging their own graves? How can China benefit from the development of the Internet? Lev Manovich offers a completely different interpretation that seems to be able to answer these questions. According to him, the West and the East have a quite different understanding of digital media, the Internet being the prime representative:

> For the West, interactivity is a perfect vehicle for the ideas of democracy and equality. For the East, it is another form of manipulation, in which the artist uses advanced technology to impose his/her totalitarian will on the people.... A western artist sees the Internet as a perfect tool to break down all hierarchies and bring the art to the people.... In contrast, as a post-communist subject, I cannot but see the Internet as a communal apartment of the Stalin era: no privacy, everybody spies on everybody else,

always present line for common areas such as the toilet or the kitchen (1996).

Before the advent of the Internet, Noam Chomsky, a linguist, political activist, and public intellectual who is well-known for his criticism of the mass media, argued in *Manufacturing Consent* that mass media is "serving a societal purpose" and this purpose is to "inculcate and defend the economic, social, and political agenda of privileged groups that dominate the domestic society and the state" (Chomsky, 2002, p.298). He states in *Necessary Illusions* that the dominant groups of a state "frequently cannot wait for the people to arrive at even general understanding", leaders must "play their part in . . . engineering . . . consent to socially constructive goals and values", applying "scientific principles and tried practices to the task of getting people to support ideas and programs". He also points out that only the dominant groups are in a position to judge what is "socially constructive". Therefore, mass media is just a means to "control the public mind" so as to realize their ultimate task of "engineering consent" (Chomsky, 1989, p.16). To perform this task, as Chomsky and Edward Herman further explain through the propaganda model, mass media needs to make sure all the contents available through the media have gone through a number of filters. As a result, money and power leave "only the cleansed residue fit to print"; "marginalize dissent, and allow the government and dominant private interests to get their messages across to the public" (Chomsky, 2002, p.2). In a word, mass media must be tolerated by those in authority and they must serve domestic power interests (Chomsky, 2002).

As a matter of fact, Chomsky's media theory and the propaganda model are

based on his discussion about media control in the U.S., the representative of Western democracies. However, I argue that these theories see universal application around the world, in both democratic and authoritarian countries. In my opinion, directly related to power, thought controls through propaganda and media censorship exist in all kinds of societies at any time. As long as power exists, thought control and censorship will not disappear. That is what Michael Scammell has remarked, "Censorship is a political tool, it is the extension of physical power into the realm of the mind and the spirit" (Scammell, 1988, p.5). To my understanding, whoever is in power, they see some information unfavorable to their reign and they will make every effort to stop those information from circulating among people. William Blum states that "propaganda is to a democracy what violence is to a dictatorship" (2000, p.11). It is undeniable that propaganda is widely used in a dictatorship and censorship seems to be indispensable to non-democratic countries. However, with the above statement, Blum argues that in authoritarian countries propaganda does not really matter too much what people think. The reason is because whatever people may think, they still have to do what the government tells them to do. Violence enacted by the government can ensure people's obedience. He points out that people are inclined to believe that democratic societies do not need propaganda. However, propaganda is, contrary to these popular postulations, more important and vital to a democratic society because people living in those societies have some rights in expressing what they think. Since people can talk, those who are in power need to make more efforts to ensure that only the correct words come out of the people's mouths. From his argument, I conclude

that democratic and non-democratic societies are indeed sharing some common characteristics in manipulating people's thoughts. Both kinds of societies use propaganda and media censorship to realize thought control out of the same purpose and the concrete measures they adopt in this process are almost the same. This is the reason why I am able to apply Chomsky's theory based on examinations of democratic countries into the discussion of Internet control in China that obviously is an authoritarian society. At the same time, I need to point out that because the Internet had just made its debut around the world when Chomsky published these works, the Internet is not explicitly one of the objects examined and discussed by Chomsky. However, Chomsky's theory should not be confined to traditional media either. His theory can be applied to the Internet as well as radio, newspaper, and TV. Continuing in the tradition of Chomsky's theory, Lev Manovich has described the Internet, a very important part of today's mass media, through its shared characteristics and purpose with traditional media. It unexceptionally serves the dominant groups in a country and it is effectively utilized and strictly scrutinized by the ruling class.

Based on Chomsky's media theory, my thesis offers an administrative, legal, technical, economic, social and cultural perspective in answering the following questions: Why does the Chinese government make efforts to maintain its control over the Internet? Do the inherent characteristics of the Internet really make it impossible to control in China? What means does the Chinese government currently employ to control the Internet? Is China capable of controlling the Internet? To what degree is the control of the Internet by the Chinese Government possible?

Through a careful examination, this thesis supports the findings of Lev Manovich by arguing that the Internet in authoritarian countries is merely another effective tool in manipulating common people's ideologies. Living in an era with the Internet as an important communication channel, people still have access only to what the government wants them to know. Instead of getting more democracy or equality, people are more likely to be supervised or spied on.

However, we cannot overlook the fact that since the emergence of the Internet in China, Chinese society has witnessed an unprecedented free flow of information, more discussion, and more openness. Taking these facts into account, this thesis should not be considered to be a complete denial of the constructive role the Internet plays in building up a society with more democratic characteristics. Instead, this thesis seeks to modify the hypothesis that the diffusion of the Internet invariantly brings about the decline of authoritarian regimes in the nation-states. My research on the development and control of the Internet in China suggests that this argument does not hold water. Because the Chinese government is capable of imposing legislative, administrative, technical and social measures to make effective controls over the Internet, China's Internet, in retrospect, has taken a route of development deviating from its anticipated mission of democratization. As a result, the Internet has not paralyzed the Chinese authorities so far. In contrast, it serves the purpose of the regime as much as it helps to loosen governmental control over freedom of expression and the everyday life of its citizens. Taking current research a step further, I combined recent research results concerning Chinese people's value orientations with the topic

of the Internet, giving an in-depth explanation as to why the Internet could hardly fulfill its function of bringing democracy or more political transitions to China as the West has expected. In 1996, Edgar Huang conducted a field observation on China's Internet. He adopted the bottom-up approach while doing his research. He examined the BBS[1] messages in four Chinese commercial BBS stations which represent communication patterns among ordinary users. He found that Chinese Internet users seemed not interested in engaging in "hard topic discussions" about democracy and other political topics (1997). My analysis on Chinese people's values can explain why this happens. My research shows that Chinese people's values have undergone great changes over the past two decades and these changes play an undeniable role in forming current attitudes towards so-called democracy and freedom. Communism, the predominant value orientation for the Chinese populace between the 1950s and 1980s, has increasingly lost popularity among the public since the Chinese Communist Party (CCP) began implementing economic and structural reforms. In contrast, Materialism, defined as a persistent pursuit of immediate rewards and physical happiness, has been adopted by a significant portion of the populace in contemporary China and has become the most influential value orientation dominating most Chinese people's daily lives. The direct result of this value shift is that "few people care to challenge the ruling regime during the present period of economic and political stability" (Hartford, 2001). People are now more concerned about whether their basic demands for a

[1] BBS is an electronic message center. Most bulletin boards serve specific interest groups. They allow users to dial in with a modem, review messages left by others, and leave their own message if they want.

well-to-do life are satisfactorily met. They are apathetic to politics, democracy, the possibility of free flow of information on the network, and the measures the government has taken to control the Internet. Moreover, they lack the desire to resist governmental control or to struggle for the building up a democratic nation with the help of the Internet as described by the West. In observing the relationship between democracy and the Internet, my thesis addresses an important factor usually ignored by Western scholars while doing research on this topic.

This thesis also finds that the control over the Internet enacted by the Chinese government in legal, technical, social and economical spheres has culminated in a situation that can be described by Foucault's Panopticon. The Panopticon, originally an eighteenth-century architectural plan for a prison devised by Jeremy Bentham (1748-1832), was later mediated and employed by Michel Foucault (1926-1984) as a general theory of modern surveillance. At the heart of the Panopticon was a system of surveillance whereby through a carefully contrived system of lighting, prisoners would be unable to discern when they were being watched, and control was thus maintained by the constant sense that unseen eyes were monitoring prisoners. Foucault argued that this model of surveillance was not confined to prisons, but had deep metaphysical roots in modern societies as a whole (Deibert, 1997, p.166). The "state" becomes the equivalent of the guard in the panoptic tower, which according to Foucault, has the power of "permanent, exhaustive, omnipresent surveillance, capable of making all visible, as long as it could itself remain invisible" (Foucault, 1995, p.217). In China, laws and regulations codify this panoptic infrastructure of

surveillance, stipulating that each network level is responsible for itself and the one below, resulting in a situation where each level engenders a mode of self-regulation and self-censorship. Users also keep a check on each other for behavior that is out of line. In addition, Internet business has all the economic incentives to keep in line with the government, since non-compliance means no business. At the same time, there is a big demand for software that helps to shield away, filter out, censor and block information deemed undesirable, whether it is porn or Falungong. The market for this kind of filtering software continues to grow and is expected to become a billion dollar industry in 2004 (Silva, 2001). Although existing technologies enable circumvention of online censorship, they all suffer from flaws that prohibit large-scale usage. My thesis explicates through a detailed analysis how the Panopticon constrains the liberalizing effects of the Internet.

The Internet control in China should be understood not as an isolated phenomenon but as a part of China's history of media control. It is also the result of particular attitudes of the Chinese people towards technology that have been formed over the past centuries. Consequently, after outlining the history and current state of the Internet in China in the first chapter, I trace the history of censorship in China and how Chinese people view mass media and technology in the second chapter. CCP's social and political considerations towards the diffusion of the Internet are also discussed in this chapter. In my opinion, all the practices in contemporary China, a country with thousands of years of civilized history, are the direct or indirect results of its pervasive ideology and philosophy. Explaining the needs to control the Internet in

China from a historical and philosophical perspective is the third contribution this study has made.

In the following three chapters, I will concentrate on how control is enacted in China and which developments can strengthen this control. The administrative, legal, technical, social and cultural, and economic measures the Chinese government has used to control the Internet will be discussed respectively. Chapter Five examines how social norms and lack of privacy awareness among Chinese people help strengthen government control over the Internet. It also tries to answer the question: why have a couple of websites and Bulletin Board Systems (BBSs) featuring sharp criticisms against the Party or government policy been allowed to exist and prosper in recent years? I attribute it to a longstanding Chinese philosophy- a minor attack in words but a major help in deeds (小骂大帮忙). In my opinion, allowing a couple of critical websites or forums to exist, the government loses nothing, instead, it gives common people a place to vent their anger and dissatisfaction and thereby the government obtains a channel to know the public opinion. To some extent, being able to vent anger through words in public reduces the possibility of fierce rebellion through grassroots actions. Furthermore, to get more recognition from the international community and also to seek more room for its development on the world stage, CCP clearly understands that more tolerance must be given to voices unfavorable to the party. Freedom to voice disagreement can be interpreted as progress for the government in promoting democracy. Tolerance of dissent helps win the approval of Chinese citizens, and scores points in improving the Party's international image. Of

course, making sure the critical websites or forums are still controllable and limiting the critiques within acceptable range are prerequisites to delivering tolerance. As far as I know, this issue has never been explored by other researchers. I regard this as the fourth and final major contribution in this study.

Appendix A holds a list of all the abbreviations used in this thesis while Appendix B is a chart consisting of the main body responsible for the Internet control in China.

Methodology

While doing this thesis, I adopted both top-down and bottom-up approaches. In particular, I employed document analysis and online participation for my research. First of all, I used document analysis to examine the history and development of the Internet in China and the controls that are present in China's hierarchical structure. At the same time some online participation helped me explore how the top-down measures work at a grassroots level in this country.

Online documents provided by official organizations are the most direct and reliable sources for getting a general understanding of China's Internet. Authorized by China's State Council, China Internet Network Information Center (CNNIC) conducts *Statistical Survey on the Internet Development in China* twice a year since 1997. All the reports are available at its website http://www.cnnic.net.cn. It always provides the latest and the most authoritative data about Internet's development in China at the earliest time possible. I made use of this source frequently and benefited from it

greatly. In addition, I obtained the original texts of laws and regulations related to Internet control from websites sponsored by national and regional regulators as well as quasi-official publications such as the website of the Ministry of Information Industry (MII) at http://www.mii.gov.cn/mii/index.html, *China Information Industry* at http://www.cnii.com.cn/ and *Law Library* at http://www.lawbook.com.cn/. At the same time, I collected news clippings from newspapers and journals such as *People's Daily* (in Chinese), *Legal Daily* (in Chinese), *China PC World* (in Chinese), *Wired, Time, New York Times, South China Morning Post,* and *Asian Wall Street Journal*, all of which also informed me of the recently issued laws or regulations as well as the latest changes in Internet control in China. Combining official documents with media coverage helped me gain a better understanding of these laws and regulations,

For some political reasons, news coverage about Chinese Internet dissidents, especially the first group which had been detained or jailed in the 1990s, is not available in Mainland China. Therefore, the above-mentioned foreign media, especially online journals sponsored by some international human rights organizations, are particularly helpful for collecting these materials. Those that I frequently visited and quoted include: *Human Rights Watch* at http://www.hrw.org/, *Human Rights in China* at http://iso.hrichina.org/iso/, *Hong Kong Voice of Democracy* at http://www.democracy.org.hk/EN/index.html, *Amnesty International* at http://www.amnesty.org/, and *Committee to Protect Journalist* at http://www.cpj.org/ . Renowned Western news agencies' websites such as that of CNN, BBC, and VOA were also very informative for my purposes.

Online participation was very beneficial for me in better understanding the state of the Internet in China. Since I was living in China during the last summer vacation, I was able to pay some visits to a couple of representative BBSs and chat rooms all of which are public and require no membership fees. To see how postings are filtered and checked on BBSs, I personally have registered as a user and tried to post some comments on *People's Daily*'s *Strong Country Forum*. My experience proved that if a posting passes through the machine-based filtering system smoothly, it takes nearly one minute before the user sees it online. To see the efficacy of China's network filtering, I personally did some experiments with some nationally well-known search engines such as that of Yahoo! China, Sina.com and Sohu.com. My experience is that a search on those search engines using the phrase "Taiwan independence" or "Falungong" as keywords would show no results. I believe that the results of this research will add much value to the topic, especially with regard to the amount of control and censorship conducted in the BBS and how the Great Firewall functions on the Internet.

Chapter One

The Internet in China

To lay the foundation for further discussion, in this chapter I will provide some background information on the Internet in China. The first section is a short overview of the history of the Internet infrastructure in China. The second part focuses on its recent development. This second part also explores the demographic characteristics of the current Internet users.

The Origin and History of the Internet in China

As in most other countries, the development of the Internet infrastructure in China commenced in academic and scientific circles. "Crossing the Great Wall to join the world"—was 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. This network was set up in the same year to provide support for academic and scientific research in computer science. Other academic networks soon sprang up, including the network of the Institute of High Energy Physics (IHEP) and the China Education and Research Network (CERNET). These early networks all shared the same limitations: they had no direct connection to the Internet. The US government was still regulating the Internet and forbidding any communist country access. This changed in April 1994, when the appeal for direct linking to the Internet was accepted

during the Sino-American Federation of Science and Technological Cooperation meeting in Washington DC. The first network directly connected to the Internet became active after the National Computing Facilities of China (NCFC) project opened up a circuit dedicated to the Internet through Sprint Corporation in America on 20 April 1994 (Zheng, 1994).

The year 1995, however, proved a crucial turning point. Infrastructure in China really took off after commerce on the Internet began to take root around the country (Tsui, 2001). In January 1995, China began its first public Internet service operated jointly by Sprint and China Telecom with the support of the former Ministry of Post and Telecom (MPT) (Wilson, 1995, p.27). The linkages belonged to China Public Computer Network (ChinaNet). In May the same year, ChinaNet allowed individuals to purchase Internet accounts from its network directly (Cullen & Choy, 1999). According to Tse and Tsang, researchers of China's Internet, within the first month of ChinaNet's operation, 800 subscribers signed up for the service (1995). After nearly a decade of vigorous growth, ChinaNet has grown to be the largest and the most powerful Internet Service Provider (ISP[1]) in China, offering services in all major cities, with backbone bandwidth[2] of 16500Mbps[3], over sixty percent of China's total gateway bandwidth to the Internet. Operated by China Telecom, a fully integrated telecommunications operator with local access networks in thirty-one provinces

---

[1] An agency or company that provides access to the Internet.

[2] Bandwidth is the amount of data that can be transmitted in a fixed amount of time.

[3] Mbps stands for megabytes. Bit is the smallest unit of information on a machine. Eight bits compose a byte, which is a measurement of memory storage. Date transfer rate, the speed with which data can be transmitted from one device to another, is often measured in megabits per second.

across the country, ChinaNet provides multiple access choices and the most reliable service: dial-up, dedicated lines and through data networks. Other access methods include Integrated Services Digital Network (ISDN[1]) and Asymmetric Digital Subscriber Line (ADSL[2]). Users could now expect a full range of Internet services from ChinaNet, including web access, e-mail, content search, personal web pages, chat rooms, BBS, instant messaging, online shopping, games, Terminal Emulation Program (Telnet[3]), File Transfer Protocol (FTP[4]), Usenet[5] and e-commerce (ChinaNex, 2003a).

Before ChinaNet's establishment, China Science and Technology Network (CSTNet) started operations as early as 1989 as a local network service in Beijing's Zhongguancun district, a prominent location for education and high-tech research. At that time, CSTNet provides information for its users involved in scientific research. These resources included a comprehensive science database, education, management and literature archives. Today CSTNet service has expanded beyond scientific

---

[1] ISDN is a standard for digital telecommunications that allows fast digital dialup connections over the public telephone network. Whereas traditional phone lines can only carry data at around 56kbps using analogue modems, an ISDN line can provide two data channels each operating at 64kbps (for a total throughput of 128kbps if required). ISDN can be used for voice data calls, faxing, videoconferencing, and high-speed data access.

[2] ADSL is a high-speed Internet connection through an ordinary telephone line. Users pay a fixed monthly charge for unlimited Internet surfing, e-mail and chat etc. ADSL is up to 100 times faster than an ISDN connection.

[3] Telnet is the main Internet protocol for creating a connection with a remote machine. It gives the user the opportunity to be on one computer system and access another, which may be across the street or thousands of miles away.

[4] FTP is the simplest way to exchange files between computers on the Internet.

[5] Usenet is a worldwide system of discussion groups in which millions of people participate. There are tens of thousands of different Usenet groups, and anyone on the Internet may participate for free.

research. It has become a rich resource for a broad range of basic and applied research, including agriculture, medicine, seismology, weather, transportation, power, electronics, and environmental protection. The network is connected with major industry networks and information centers so that users can share information and online resources (ChinaNex, 2002b).

In 1994 China's State Development Planning Commission (SDPC) approved to establish the China Education and Research Network (CERNet) whose mission is to develop network services for Chinese universities and, to a lesser extent, for high schools. Although CERNet is one of the largest ISPs in China, its service is limited to education and academic research areas such as curricula, class teaching, distance education, and database searches (ChinaNex, 2003b).

In 1996, the Chinese government designated ChinaGBN (China Golden Bridge Network) as both a national information network and an ISP. The main service offered on ChinaGBN is business information, including "China BIG", an online business-to-business yellow page service with more than 600,000 company listings. ChinaGBN also offers voice and videoconferencing services through its IP network (ChinaNex, 2002a).

Today, eight major ISPs, regulated by the Ministry of Information Industry (MII), operate international telecommunication circuits and network facilities. They are ChinaNet (中国公用计算机互联网), CSTNet (中国科技网), CERNet (中国教育和科研计算机网), CNCNet (China Network Communications Network 中国网通公用互联网), China169 (宽带中国), UNINet (China United Telecommunications Network

中国联通互联网), CMNet (China Mobile Communications Network 中国移动互联网或中国移动梦网), and CIETNet (China International Economic Trade Network 中国国际经济贸易互联网). These networks form China's Internet backbone, and connections to this backbone make up ninety percent of the costs of Internet businesses (CNNIC, 2004). Among the eight, both CNCNet and China169 are subordinate to China Network Communications (China Netcom 中国网通) that was created in 2002 by the government in an effort to break the market monopoly by China Telecom. China Netcom, which successfully merged with ChinaGBN only one year after its establishment, has shown a great momentum in its development. By the end of 2003, the company had nearly three million broadband customers, amounting to thirty percent of the nation's total customers. China169 is one of the broadband services it offers to residential customers. In addition, Netcom provides videoconferencing, intelligent network (IN), and leased line services to both domestic and international customers. CNCNet, Netcom's traffic backbone, has a bandwidth up to 3600Mbps and operates in seventeen switching centers. The second largest ISP only next to ChinaNet, Netcom plans to add five million more broadband customers in 2004 (ChinaNex, 2004).

UNINet is the traffic backbone of China United Telecommunications Co., Ltd. It is also the third largest ISP, covering 330 cities across the country (ChinaNex, 2004). CMNet is provided by the China Mobile Communications Group, the largest mobile operator in China. Its current market share is seriously affected by its relatively narrow bandwidth of around 555 Mbps (CNNIC, 2004). CIETNet was built up and

operated by China International Electronic Commerce Center (CIECC). It is the smallest among the eight major ISPs in China, with a bandwidth of two Mbps (CNNIC, 2004).

In addition to these major ones, there are over 500 small-scale ISPs in China. Most of them provide some form of Internet access and other services for a particular geographic market such as in a province or certain parts of province. There are a few that also offer cross region or even nationwide access service (ChinaNex, 2002c).

The Current Development of the Internet in China

Year	Users	Online computes	Domain Names	Websites	Bandwidth
1997	670,000	330,000	5,100	N/A	N/A
1998	2,100,000	630,000	18,396	5,300	143.25 MB
1999	8,900,000	3,500,000	48,695	15,153	351 MB
2000	22,500,000	8,920,000	122,099	265,405	2,799 MB
2001	33,700,000	12,540,000	127,319	277,100	7,597 MB
2002	59,100,000	20,830,000	179,544	371,600	9,380 MB
2003	79,500,000	30,890,000	340,040	595,550	27,216 MB

Table 1 - Internet Development in China (1996-2003) **(CNNIC 1996-2004)**

The above table summarizes the major findings of the nationwide Internet surveys conducted by CNNIC since its establishment in 1997. According to their report of January 2004, the Internet population in China amounts to roughly seventy-nine million (CNNIC, 2004). Several other companies that specialize in

market research sometimes contest these statistics and point out that the figure from CNNIC is inaccurate. Interactive Audience Measurement Asia (IAMAsia) and NetValue both settled on a figure that had two million fewer users by the end of 2000 (Narayan, 2001). Nonetheless, evidence of the significant growth in numbers is undeniable. In view of the world's growth in Internet usage, some estimate that, if the current trend continues, China could have more Internet users than any other country by 2020 (Tan & Foster, 1998) and the Chinese Internet would become the largest in the world (Pfaffenberger, 2000). According to the International Telecommunication Union (ITU) and the World Intellectual Property Organization (WIPO)'s estimates, Chinese would become the most used language on the Internet in 2007, surpassing English, merely because of China's large population (WIPO, 2002).

Examining CNNIC's annual reports, I summarized some characteristics of the Internet population in Mainland China as follows: Roughly sixty percent of the Chinese Internet users are male, although the proportion of Chinese women using the Internet has grown steadily over the past several years; Internet users are heavily concentrated in prosperous provinces and municipalities in China's economically dynamic coastal areas, primarily Beijing, Shanghai, Jiangsu, Zhejiang, Shandong and Guangdong. Users from these areas make up over 43.7 percent of the Internet population alone; More than seventy percent of all Internet users in China are thirty years of age or younger, and more than eighty-two percent are under thirty-five; Approximately eighty-seven percent of the Internet users have attained at least a high school diploma, and more than fifty-seven percent have attended college (CNNIC,

2004).

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 gain access to computer facilities and to acquire the technological know-how essential for Internet access.

Meanwhile, although the number of the Internet users jumped 120 times from 1997 to 2003, I should note that seventy-nine million Internet users still account for only about 6.1 percent of the whole Chinese population. Not all 1.3 billion people will go online in the foreseeable future. China still has a long way to go before becoming the largest Internet-consuming country in the world. But for the short term, further growth is predictable. PC penetration per household in China is about two percent. While this is relatively low, this figure provides much room for growth (Souza, 2003). The Chinese government is also promoting Internet usage by slashing its Internet fees to stimulate competition between providers (ChinaOnline, 1999).

Apart from the increase in the number of users, the nature of Internet usage has widened. *People's Daily*, for example, an organ of the Chinese Communist Party, and other government and military controlled media are now offering daily online services. A central government initiated nation-wide project, known as the Government Online Project, has put a large number of government institutions from all levels onto the Internet in an attempt to provide better government administration and services. Many well-known Chinese universities, like Tshinghua and Peking Universities, now provide distant education via the Internet. Most tertiary level academic institutions are

also connected to the Internet. China's first digital library system was established in the city of Shenyang in October 1998 (CHINAINFOBANK, 1998). Popular Chinese Internet companies, both Internet Service Providers (ISP) and Internet Content Providers (ICP) like Sina.com, Sohu.com, Netease.com, and 8848.com, etc., have become among the largest and most successful private businesses in China. Although telecommunication and information industries are highly sensitive sectors of China which for security reasons have not been opened to overseas investors, foreign ICPs like Yahoo! and Google are widely used by Chinese netizens[1]. Moreover, as one observer points out, because the majority of its telecom infrastructure has been built in the last five years, China has a higher percentage of digitized lines than the U.S. and is, thus, "well-positioned for the increasingly high-speed and broadband demands and opportunities of e-commerce" (Dougan, 2003). The first electronic business in China, run by the Xinhua Bookstore, started operation in the spring of 1996. Today, using the Internet for advertising and exchanging commercial information has become fairly common across the country. Shopping on-line has also become increasingly popular. According to Craig Barrett, President and the CEO of Intel, e-commerce in China generated combined revenue of US$8.1 million in 1999 (*People's Daily Online,* 2000). By 2003, the figure reached US$900 million and is projected to hit to US$2.4 billion in 2005 (Chinaview, 2003). Some researchers remarked that, in absolute terms, "China is the most networked country among the developing nations and second only to the US among the developed nations" (Hong, 2003).

[1] Netizen is a combination of "citizen" and "net". It refers to every citizen on the Internet.

Chapter Two

China's Need to Control the Internet

This thesis argues that the Chinese government has been making full use of and strictly censoring the Internet instead of letting the Internet promote democracy or other social transitions. The CCP's control over the Internet is a continuance of ancient China's censorship history. It is also either a direct or an indirect result of the Party's and the nation's attitudes towards media, advanced technology, and their perspectives towards the international situation. As with some other countries around the world, China also has some social considerations that help to validate the government's position and to justify its control policy. Therefore, after a short review of China's censorship history, this chapter makes a deep exploration of the significance of these aspects. The last section of this chapter also focuses on how the Chinese government has made use of the Internet in order to serve its political purpose. The reason I examine this issue is because in my opinion this is another motivation that drives China to make the Internet under control.

The History of Censorship in China

What is censorship? Censorship can be defined in a variety of ways. It generally refers to official prohibition or restriction of any type of expression believed to threaten the established order (Olga & Hoyt, 1970, p.9). It is supervision and control

of the information and ideas that are circulated among the people within a society. In modern times, censorship refers to the examination of books, periodicals, plays, films, television and radio programs, news reports, and other communication media for the purpose of altering or suppressing parts thought to be objectionable or offensive. The objectionable material may be considered immoral or obscene, heretical or blasphemous, seditious or treasonable, or injurious to the national security. Thus, the rationale for censorship is that it is necessary for the protection of three basic social institutions: the family, the church, and the state (@cess Censorship, 2000).

Michael Scammell, an internationally recognized expert on censorship, looks at censorship in the contemporary world from a political perspective. He defines censorship as "the systematic control of the content of communication by a government through various means" (Scammell, 1988, p.10). He views censorship as a political tool and limitations of freedom of expression as "an instrument to assist in the attainment, preservation or continuance of someone's power". For Scammell, censorship is merely "the extension of physical power into the realm of the mind and the spirit". He also states that "the more centralized the physical power and the more total its claims, the more intolerant, wide-ranging and complete the censorship will tend to be" (Scammell, 1988, p.5).

Censorship and the ideology supporting it go back to ancient times. Some may assume that "In non-democratic societies, censorship is a dominant and all-pervasive force, felt on all levels of artistic, intellectual, religious, political, public, and personal life" (@ccess Censorship, 2000). Nevertheless, censorship is not practiced only in

non-democratic societies. Every society, including the democratic ones, has had customs, taboos, or laws by which speech, play, dress, religious observance, and sexual expression were regulated. For example, in ancient Greece, known for its democratic practices, Socrates was one individual who was constantly under scrutiny for his intellectual teachings. He questioned many things, including the government, religion, and his society at large; he advocated the tabooed position that the Greek gods did not exist. Powerless to censor Socrates for questioning and criticizing, Athenians charged him with corrupting the minds of youths and offending the gods. Socrates defended himself, saying that he had never meant to offend gods, that his ultimate goal was only to seek the truth. Socrates' defense fell on deaf ears, and he was sentenced to death. In 399 B.C., after drinking poison, he gave his life for his principles (Riley, 1998, p.4).

The United States is also well known for having one of the most speech-protective regimes in the world. Its record is by no means perfect, however; American history is full of examples of government officials using their power to punish political opponents and dissenting groups. In 1791, the First Amendment to the U.S. Constitution went into effect. It stated that

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances (Olga & Hoyt, 1970, p.15).

The First Amendment was drawn to keep the government from controlling individual freedoms. Nevertheless, in cases dealing with the First Amendment, the United States Supreme Court has ruled that censorship is permissible in certain limited situations,

generally when such censorship is intended to protect individuals or national security (Riley, 1998, p.4). In 1918, the U.S. Congress enacted the Sedition Act of 1918. This act stated that it was crime to communicate disloyal or profane comments-about the government, flag, or uniforms-through speech, print, or publication. Displaying any support for a country at war with the United States was also a crime (U-S-History.com, 2004). Under the Sedition Act of 1918, thousands of Americans were sentenced by their peers, whose passionate, misguided patriotism ran like a train out of control. By 1919, the United States was caught in the grip of the "red scare", when the fear of communism dominated people's reason. People were arrested because they looked like Communists or because they made casual comments about Russia. Another scare arose in the late 1940s and early 1950s, when it was feared that Communists had found their way into positions of influence across the country. The House Un-American Activities Committee (HUAC) investigated musicians, actors, politicians, academicians-anyone in an influential position. People were afraid to speak, not knowing how their comments might be interpreted (Riley, 1998, p.13). Even in the late 20th century, the U.S. government still had strong power over freedom of expression, especially during wartime when censorship can function legally. When the United States invaded Grenada in 1983, the press was barred from the scene. The government held that press had been given great freedom in covering the Vietnam War and their coverage had caused negative public reaction. The government did not want it to happen again. Likewise, during the Persian Gulf War, limitations were again placed on reporters. Censors read stories before they could be submitted for print, and

the censor's word, with rare exception, was the law (Riley, 1998, p.26).

Compared with the U.S. or any other country around the world, China has an even longer history of censorship. As a matter of fact, one of the world's first and most widespread forms of censorship occurred in ancient China. It was in 221 B.C. when Emperor Shi Huang (246-210 B.C.) founded the Qin Dynasty (221-206 B.C.), the first power-centralized, multi-national and unified regime in the history of China. Qin's establishment marked the end of the riotous Warring States Period (475-221B.C.), a time of endless brutal wars among seven independent states. Emperor Shi Huang's main goal was to have a unified empire, so after he had annexed the other six states, he ordered the construction of the Great Wall of China to halt enemies; he standardized the measurement of weight and length, written script, legal system and currency. He also wanted to impose his own ideals of government on the other Chinese states he had conquered. However, the presence of books from a diversity of schools of thoughts was one of the biggest threats. To eliminate these threats and to standardize human thoughts, Emperor Shihuang ordered all the books to be burned unless they involved math, science, agriculture or medicine. All books that dealt with history before Qin Dynasty were also not spared, as Emperor Shihuang wanted to be remembered as the first king. To destroy the literature was to burn the bridge that connected people's common knowledge to the possible deeper thought and introspection through reading diverse texts. Common people, therefore, had access to nothing but the knowledge or thoughts that the rulers wanted them to have. Moreover, Emperor Shihuang once ordered 460 scholars to be buried alive for misleading the

public through their unfavorable commentaries on his governance. Those events were later called "the burning of books and the burying of Confucian scholars". Emperor Shihuang's attempt at censorship was motivated by a desire to control the thoughts of all his citizens and make them loyal to him. By establishing intellectual conformity, Emperor Shi Huang hoped to stymie criticism of imperial rule that could lead to revolution. In reality his efforts only served to fortify the people's hatred for him and arouse opposition against his tyranny throughout the country. Qin is a short dynasty with a span of only fifteen years. An army of peasants overthrew the harsh Qin regime just one year after the death of the Emperor Shi Huang (Chinn & Worden, 1988, p.10-12).

In China's history, censorship has never really left center stage. On the contrary, it has played an increasingly important role throughout the different dynasties. Countless writers and scholars have been dismissed or imprisoned because of what they wrote or what they commented on. During the Ming Dynasty (1368-1644), Eastern Esplanade (y t) and Western Esplanade (q t) were set up to supervise even common people's words and deeds. These two organs acted as the secret police, spies and *agent provocateur,* taking advantage of their limitless and secret powers to blackmail and corrupt people. They pried about and reported to the emperor whatever activities they deemed conspiratorial. The emperor, deprived of any means of obtaining information or checking it, condemned all those who were denounced to him without even giving them a hearing (Gernet, 1996, p.407).

Censorship reached its zenith of power and influence in the Qing Dynasty

(1644-1911), the last feudal dynasty in Chinese history that was founded by Manchu people. As a minority reign in China, Qing had a strong desire to impose a reign of moral order and at the same time to justify the Manchu domination. As early as the reign of Emperor Kang Xi (1662-1723) there had been signs of a reaction against unorthodox works and "corrupting" novels, which were put on the index of prohibited books in 1687. This policy became harsher under Emperor Yong Zheng (1723-1736) and ended in the great "Literary Inquisition" of 1774-1789 in the reign of Emperor Qian Long (1736-1796): 10,231 works in 171,000 chapters were put on the index of prohibited books and over 2320 of them were completely destroyed. For some twenty years a hunt went on throughout the empire for books deserving condemnation because they displayed a lack of respect for the Qing Dynasty, either by using some forbidden characters (characters appearing in the emperor's personal name are forbidden to be used by common people) or by criticizing the Manchu as barbarians and questioning the legitimacy of their domination of the country. The reign did not confine itself to censoring and destroying works which could injure the moral order; it persecuted the authors and their relatives. Brutal measures were taken against them-execution, exile, forced labor, confiscation of property, and so on. Informing was encouraged by large rewards, and the possession of suspect works or the withholding of information about them was punished with the most serious penalties (Gernet, 1996, p.477, p.508).

The compilation of the *Complete Works of Chinese Classics* or *Si Ku Quan Shu* (ㄙ ㄎㄨˋ ㄑㄩㄢˊ ㄕㄨ) is another example of censorship in the Qing Dynasty. One of the greatest

contributions made by the Chinese nation to world civilization is its tradition of compiling scattered texts into collections for later generations. Every dynasty of China compiled its own collections of classics. This practice reached its pinnacle during the Qing Dynasty. During the reign of Qian Long, the Qing government organized 360 accomplished scholars from various academic circles to compile *Si Ku Quan Shu*. This encyclopaedia-type series of books was completed in ten years. A collection of important documents and classics before Qian Long, it has become one of the most important books for later generations to learn about China's over 5,000-year old scholarly achievements.

However, as all books were subject to a thorough censorship during the reign of Qian long, the *Si Ku Quan Shu*, was no exception. During the entire course of collection, all writings that were cited as "taboos" or "rebellious stuff" were cast aside or even destroyed. During the course of compilation, nearly 3,000 tiles of books were destroyed, with the number almost equalling that of books taken in by the collection. At the same time, many original texts were cut out or revised. Writings charged with vilifying and humiliating the Manchu people were revised or even deleted in paragraphs or complete pieces of writings (China News and Report, 2002). The compilation of the *Si Ku Quan Shu* was influenced in large through this censorship. As a result, censorship left this masterpiece with irreparable drawbacks.

Mass Media in China: the Party's Mouthpiece

Censorship continues to exist and function in China well into modern times. It is well known that, the Chinese government has subjected the press to the most rigorous censorship since the CCP took over the country in 1949. In addition to the major historical influence, another major explanation for the presence of censorship is that the function of the media in socialist communities is different from that of Western countries. In the West, the standard conception of the mass media is a "cantankerous, obstinate, and ubiquitous press" that always searches for "truth and their independence of authority" (Lewis, 1987). Mass media is supposed to be "vigilant, defiant and courageous" (Lewis, 1987). Its mission is to "root about in our national life, exposing what it deem right for exposure without regard to external pressure or the dictates of authority" (Lewis, 1987). However, socialist communities portray the mass media in a totally different way. The Soviet Communist theory states that mass media should be used instrumentally to suit the needs of state power and Party influence (Zhang & Cropp, 2002). In *Party Organization and Party Literature*, Vladimir Ilyich Lenin has said that all the mass media, literature and literary criticism in socialist Soviet must become a part of the general cause of the proletariat (1962, p.46). Originally adopting its system of media control from the former Soviet Union, the CCP also has a long history of using mass media as a propaganda weapon (Schell, 1995; Zhao, 1998). In May 1942, Mao Zedong (1893-1976) delivered a speech on the Yanan Forum on Art and Literature which quickly became the doctrine for all future media coverage and art production in China. In this speech, Mao

articulated his philosophy on the role of media and art in society as something that should only be created for "the people, the workers, peasants and army soldiers". Journalists and artists should be regarded as nothing more than "cultural workers" (Mao, 1967, p.69-98). This influential speech outlined the principles underlying all official journalism and artwork in China for the next 60 years. In 1948, Mao Zedong delivered a speech in which he emphasized the required tasks of Chinese newspapers. Mao said, "The role and power of the newspapers consists in their ability to bring the Party program, the Party line, the Party's general and specific policies . . . before the masses in the quickest and most extensive way" (Mao, 1961, p.241). After the founding of the People's Republic of China in 1949, the CCP further defined the general tasks of the Chinese media as "serving the cause of socialism and the people" (Chang, 1989). The Chinese leaders in the post-Mao era, both Deng Xiaoping (1905-1997) and Jiang Zemin (b.1926), continued to insist on Chinese media's role as a propaganda weapon or Party organ. Prior to the market reforms China launched in the 1980s, the role of the Chinese media was to function as the "mouthpiece" of the party-state. The Chinese media was a tool used by the government for political purposes (Liu, 1998). Since 1949, the Chinese media, consisting of newspapers, magazines, publishing houses, broadcasting stations and TV stations, have been under the control of the propaganda authorities at all levels (Li, 2001).

Since the introduction of the Open Door Policy at the Third Plenum of the Eleventh Party Congress in December 1978, China has gradually opened up to the West. The role of the media has changed, becoming more independent both in

economy and in organization management. However, the Chinese Communist Party has never given up its domination of the media. Although Marxism and Leninism, as economic and revolutionary doctrines respectively, are largely outdated forces in China, they remain the keystones of the continuing political structure in the country. A fundamental tenant of Leninism is the requirement that the state must control the media. The metaphor often used to describe this dynamic is that the media must be both the "throat and tongue" and "the eyes and ears" of the party (Cullen & Choy, 1999). The media in China is still regarded as an essential political instrument, and functions under the Party's apparatus to educate the masses and disseminate ideology. The function of the media is thus to ensure the loyalty and unity of the organization's members, to induce not only correct thinking but also correct behaving. The Party continues to be the owner, the manager and the dictator of the media.

As with their predecessors, China's new generation of leaders never hesitate to express their opinion on the freedom of media. They repeatedly emphasize the importance of the media's obedience to the Party. China's former President Jiang Zemin once told Mike Wallace in an interview with CBS,

> Freedom of the press should be subordinate to the interests of the nation. How can you allow such freedom to damage the national interests? ...We need to be selective. We hope to restrict as much as possible information not conductive to China's development (Lin, 2001).

In a country that has a long-standing tradition of strict control over the media, the Internet, regarded to be one facet of the media, can hardly be an exception to the control.

Technology: A Double-Edged Sword

Being a country subjected to the West's invasions and colonization since the Opium Wars in 1841, Chinese people have formed their own attitudes towards technology, in particular towards advanced foreign technology. I will include these psychological and cultural factors that influence the unique status of the Internet in China into my research.

As early as the 16th century, there have been discussions about how to implement western technology while preserving Chinese values. The concepts of *Ti* & *Yong* were introduced in the middle of the 19th century and stand for "Zhong Xue Wei *Ti* (X , E), Xi Xue Wei *Yong* (q X , я)[1]". These concepts mean that Chinese learning is cultural essence while Western learning is for practical use. Put another way, the study of Chinese learning is meant for developing fundamental principles while the study of Western learning is just for utility (Teng & Fairbank, 1963). The concepts of *Ti* & *Yong* imply a view of social and cultural superiority to the West and demonstrate a reluctance on the part of China to wholly accept foreign (especially Western) ideas and technology. Since the late 19th century, especially after the Opium Wars (1839-1842), it was assumed by most Chinese that foreign domination of China was based on the superiority of Western weapons. The understanding was that the only way to drive foreigners out would be to learn how to make and use Western

[1] It was first proposed by Zhang Zhidong (1837-1909), a scholar, educationist, and one of the foremost reformers in the late Qing Dynasty. He has searched for a way for China to survive in the modern world that could accommodate Western knowledge but preserve traditional ways. The ways he and other reformers advocated to strengthen the nation included building up professional schools, modern industrial plants, railways, and arming the military with foreign advanced weapons.

machinery in order to be able to compete on an equal footing with the West (Sinclair, 2001). From then on, China has tried to use technology to strengthen herself while carefully attempting to prevent this decision from damaging her societal fabric. In the 20th Century, China still views technology as the key to her progress and believes that, amongst other technologies, the Internet is a vital factor in the transformation of China from a developing country into a superpower. However, in the eyes of Chinese leadership, the Internet, like any other technology, is a double-edged sword. Failing to properly use and control the Internet can bring a threat to the regime. The CCP can never forget the nightmare brought on by new technology. During the Student Democratic Movement in 1989, fax machines—the new communication technology at that time—demonstrated their subversive power. The dissidents used these machines inside China to exchange information among themselves and to release information to the outside world. The application of this technology almost led to the collapse of the Chinese government at that time (Cullen & Choy, 1999).

Keeping this "nightmare" in mind, the CCP has viewed the Internet, an even more powerful communication tool than the fax machine, with great suspicion as well as great anticipation. The government is well aware of the "harmful" effects that this new technology could have that it will not allow this new technology to develop without intervention.

Stop the Internet from being Used by Hostile Forces

So far, I have talked about how the CCP views mass media and how the Chinese people view technology. In this part, I am going to discuss China's opinions about the international situations and how these perspectives influence its decision concerning the strict control of Internet usage.

In recent years, there has been a rise of transnational social movements that represent the emergence of what Lipschutz has called a "global civil society", that is, transnationally organized political networks and interest groups largely autonomous from any one state's control (1992). Deibert also notes that "transnational social movements have exploded" (1997, p.158). The Union of International Associations now recognizes some 40,000 international nongovernmental organizations (NGOs) (UIA, 2004). As Spiro notes, "Environmentalists, human rights advocates, women, children, animal rights advocates, consumers, the disabled, gays, and indigenous peoples have all gone international" (1994). According to Deibert, the rise in the visibility and density of these transnational social movements cannot be divorced from the communications technologies that have empowered them. He further notes that although telephones and faxes have long been staples for international coordination, "it has been computer networks—and in particular the Internet—that have vastly transformed the scope and potential of these transnational movements" (1997, p.159). Deibert points out that the Internet does not generate these new social movements, it does, however, create a communications environment in which such activities dramatically flourish. In fact, some NGOs "were among the first to realize

the potential of the early computer networks as facilitators of their organization" (1997, p.159).

Among all the NGOs, the Association for Progressive Communications (APC) is the most extensive global computer networking system dedicated to social and environmental issues. With the help of the Internet, APC members can share enormous databases containing everything from government department phone numbers and addresses to scientific studies to calendars of events to various government regulations and accords, which are all hyper-linked and searchable by keyword (APC, 2004). Members can also engage in electronic conferences, communicate directly through electronic mail, and distribute information, including urgent human rights or environmental violations. Besides formal networks like APC, there are many informal transnational social movements linked through Internet BBSs, newsgroups, and mailing lists. For example, Asian democracy activists exchange information through computer mailing lists such as China News Digest (cnd-info@cnd.org). In sum, as Deibert has described,

> Thousands of niche political movements from across the political spectrum and from all points of the planet have built a presence on the web. Through this presence, these movements can distribute alternative sources of news and information, maintain a repository of data related to their particular niche interest, or provide an informal hyperlinked gateway to other complementary movements (1997, p.161).

Regarding these movements' significance for contemporary politics, Deibert argues that these movements taken as a whole present a fundamental challenge to the modern world order paradigm. In other words, "the importance of these movements lies not in their potential substitutability for the state, but rather in their collective 'unbundling'

and 'de-territorializing' of political authority and processes of political participation" (1997, p.164). However, my study finds that the Chinese government pays more attention to the former instead of the latter point of importance. This difference in focus serves as a good reason why the authorities in China need to control the Internet.

As Neuman explains, the special character of the Internet is that "it can as easily be extended horizontally (among individuals and groups) as vertically (in the more traditional connection between the centralized authorities and the mass populace)" (1992, p.13). The Chinese government has realized that, compared with other communication technologies, the Internet makes it more difficult for the government to control the flow of information, and more difficult to prevent individuals from having access to information that the government deems undesirable. What is more, with the help of the Internet, international activists are more capable of educating and motivating Chinese populations with ideas of "freedom", of organizing so-called democratic activities within China's territory, and finally of seeking opportunities to overthrow the socialist regime. If the government does not take effective precautions against these possibilities, the domestic dissidents and political movements could further collude with their international counterparts. This process could lead to China playing a part in a transnational social movement, thereby making the domestic organizations in China more influential on the international arena. This is absolutely what the Chinese authorities do not desire.

At home, the Chinese government has already witnessed how the arrival of the

Internet has enabled dissidents, Falungong practitioners, Tibetan activists, Taiwan separatists, other niche political groups and individuals regarded as subversive by the Chinese authorities to organize and communicate. They use the Internet to share information with each other and with their counterparts in the exiled dissident communities, to access banned information and to draw support from a global network of activists and NGOs. Groups such as *Human Rights in China* and the *Committee to Protect Journalists* post news of arrests and human rights violations, circulate online petitions, and maintain e-mail databases of Chinese dissidents and other activists. The Internet has provided these groups a means of communication that is easier and faster to use than any technology ever before. As with any other authoritarian regime, the Chinese government is struggling to prevent activists from using the Internet to erode government controls over the flow of information and from promoting political or social agendas that the government finds threatening. Additionally, the Western democratic world (China's presumed outside enemy) has never hidden their intention to overthrow the only few remaining socialist states in the world. The following words from Litan and Niskanen will ensure that China will never relax its vigilance:

> The Berlin Wall came down not because it was demolished by tanks or armies from the West but because western television and radio coupled with diffusion of computer technology robbed communist governments of their information monopolies and thus their ability to hold the allegiance of their people. ..... It should be only a matter of time when the same thing happens to China (1998, p.2).

George. W Bush echoed this bold statement when he said straightforwardly in 1999 during a GOP Debate, "Imagine if the Internet took hold in China. Imagine how

freedom would spread" (Tsui, 2002). In my opinion, it would be difficult to refute China's perception of this statement as a threat if we hear these words and witness the Western democratic world's applause over the former Soviet Union's fall.

"Enemy forces at home and abroad are sparing no effort to use this battlefront (the Internet) to infiltrate us" (Lin, 2001). This quote is taken from an editorial published on the *People's Daily* in 2001. It illustrates a very common and basic understanding China holds towards those forces which are hostile towards its regime, either domestically or internationally. My research finds that this pervasive understanding is the most important reason why the Chinese government has never loosened its grip on the Internet.

Social Considerations

The Internet has not only provided an unprecedented convenience in human communication, but it has also facilitated the rise of transborder criminal activities, including pornographic distribution, terrorist activities, money-laundering schemes, Internet based business frauds, and Internet hacks. The new social, economic and cultural problems created by the adoption of the Internet have already aroused global concerns from all the networked nations. It is these social and cultural concerns that have instigated legislation on content censorship since the 1990s. This has happened even in the U.S., the representative of the Western democracies, even though most of the American netizens believed that the Internet should remain wide open for the free exchange of ideas without any censorship. In 1995 and 1996, a variety of legislation

involving the Internet came before the U.S. Congress. Most of the legislations addressed the interests of minors and were designed to protect them from pornography. Two of the most important were the Telecommunications Act of 1996 and the Communications Decency Act of 1996 (CDA). CDA criminalized the use of interactive computer services and telecommunications services, the sending of harassing communications and the displaying of "indecent" material to minors. Another section of CDA made it a crime to use a facility to coerce or entice minors to engage in criminal sexual activity (Riley, 1998, p.31).

Shortly after the CDA passed in February 1996, it met with sharp criticism from both liberals and conservatives who criticized that CDA's definition of "indecent materials" was too vague. The American Civil Liberties Union (ACLU) even filed a lawsuit against the "indecent" and "patently offensive" provisions of the CDA. The U.S. Supreme Court finally declared the CDA unconstitutional and granted an injunction in June 1997, (Riley, 1998, p.31). Nevertheless, over the past decade, the American legislators and the courts have gradually formulated standards and tests that recognize First Amendment rights while protecting the public in general, and children in particular. By 1996, seventeen states in the U.S. had either enacted or promulgated Internet regulation statutes. Many of the statues focused on the content which was accessible to juveniles; others focused on "explosive materials" and "terrorist acts" (Riley, 1998, p.32). The 21st century has seen more progress in regards to legislation. In 2000 the US Congress imposed laws that made libraries across the country filter all of their Internet connections (not just those used by children) or risk losing assistance

with Internet access. At this time, 2003, the US Supreme Court has upheld Congress's requirements; so libraries are now faced with choice of censorship or loss of funds (Ockerbloom, 2003).

Again, as with other countries across the world, Chinese authorities have social and moral issues to consider in terms of the impact of the Internet. This is another factor that has made the Chinese government hesitant in accepting the Internet without imposing a certain degree of censorship. China has its own definition of the vast array of "indecent" materials available on the Internet. The CCP used to call these materials a "spiritual pollution", a term formed in the early 1980s suggesting the extent of the damage brought on by decadent influences from the West (Spence, 1991). In October 1983, an article published on *Hong Qi,* a theoretical journal run by the Central Committee of the CCP, described various forms of spiritual pollution including pornography, obscenity, vulgarity, violence and the ideology of putting money above all else. The article called them "deadly poisons" which have an extremely corrosive effect on the minds and lives of the masses, particularly on the minds and lives of the young people. The writer mobilized the Chinese people to combat spiritual pollution thoroughly in order to build a "spiritual civilization" (Li, 1995).

Did the CCP crack down on the alleged spiritual pollution merely out of social and moral concerns? An article published one month later on the *People's Daily* provides us with another perspective through which to understand the CCP's stand on this issue. This article states that spiritual pollution falls into two categories:

> The first type includes pornographic books, pictures, tapes and films. These things must be confiscated... The other type is bourgeois liberalization and the commercialization of spiritual products in the theoretical, literary, and art circles. Some examples of this would include propaganda in support of abstract humanism; theses concerning Western ideologies; literary and art works that distort history and reality, concentrate on the dark side of our society, and encourage "self-expression" and vulgar, low-class performances. This type of spiritual pollution makes the people, especially the young, pessimistic and lethargic, creates discord, promotes individualism, and causes some people to doubt and even deny socialism and party leadership (Li, 1995, p.205).

It should be noted that political concerns, here, take the place of the social or moral concerns.

Since the "spiritual pollution" comes from the bourgeois ideology and lifestyle, an anti-bourgeois liberalization campaign is an inevitable result of the anti-spiritual pollution campaign. This campaign reached its zenith in the late 1980s. At that time, the CCP leadership illustrated its political considerations more clearly than before. While talking about the harm of the bourgeois liberalization, Deng Xiaoping once said,

> bourgeois liberalization is an attempt to turn China's present politics in the direction of capitalism...Its exponents worship the "democracy" and "freedom" of western countries...if we engage in idle talk of democracy, the country will be taken over by extreme democratization and anarchism. Political stability and unity will be undermined (Li, 1995, p.593).

In the following years, Deng took every opportunity to denounce this ideological trend fiercely. By the end of 1986, students took to the streets in demonstrations in several major cities. This climaxed in 1989, on June 4th in Tiananmen Square. All the movements demanded democracy, liberty and political reforms. Among them, the June 4 incident, an anti-revolutionary riot in the CCP's viewpoint, caught worldwide

attention, severely undermined the CCP's legitimacy, and almost led to the collapse of socialist China. Deng claimed that all these disturbances were the result of a failure on the part of some individuals from the CCP's leadership to take a firm, clear-cut stand against bourgeois liberalization.

Today, the domestic political situation in China has changed a lot. The dispute between socialism and capitalism is not intense. The CCP's current leadership, however, can continue to draw on the experiences of the Party in the 1980s to remind them of the potential risk they will face if the Western ideology overruns the country. One difference is that nowadays, the politicians use neither terms like "spiritual pollution" nor "bourgeois liberalization" to describe the flood of incoming Western ideology. Instead they compare this sort of information with electronic opium and highlight the impact it has in lowering social and moral standards. This approach seems to have a better effect than the past political movements (ChinaOline, 2000). Chinese people are very sensitive to opium because it was the disruptive influence of opium introduced by the British colonialists in the 19th century that finally led to the Opium Wars. Losing the war, the Qing government had to sign unequal treaties and cede some territories to Western countries. Chinese people regard the Opium Wars as the beginning of their miserable modern history. As a result, there are heated discussions about the corrupting influence of the electronic opium even among common people. It is not difficult for the government to persuade its people that China needs to find ways to restrict the flow of Internet information. The government is justifying its Internet control policy by positioning it as a safeguard of moral values,

trying to combine its political and social concerns.

Making the Internet Serve the Party's Political Needs

One of my thesis's arguments is that the Chinese government has been actively exploiting the Internet for its own political advantage. In the Chinese authority's understanding, if its control over the Internet is successful, the government can make the Internet serve the Party's political needs. I believe this is also one of the motivations that drive China to control the Internet. In this section I would like to give an introduction into how the government can benefit from the Internet.

Discovering What Citizens are Thinking

With the strict online censorship, there are large quantities of rhetoric in support of the regime prevalent in BBSs and chatrooms. At the same time, there are, to a much lesser degree, some anti-party comments. The Internet does allow people to speak their minds and vent their anger to some extent. Hachgian notes that Internet forums "offer officials who lack the benefit of a free media a way to discover what citizens are thinking" (2001). Therefore, when criticism of the government is brought up on the Internet, the government can be updated with the latest sentiments and opinions of the public. The government can then choose to react quickly to this by inundating the media with its own message to quell any unrest.

In March 2001, an explosion at a primary school in Jiangxi Province killed forty-two people and injured twenty-seven (Jiang, 2001). Local officials tried to cover up the tragedy because illegally forcing primary school pupils to hand make

firecrackers was the cause of this accident. However, unofficial news about it had begun to circulate in some BBSs long before it was published in the official news media. Chatrooms from some popular websites were flooded with messages condemning local officials' covering up the truth. Netizens also condemned the central government's powerlessness and inefficiency in dealing with this affair. The discussion over the school blast became so heated that Sina.com was forced to shut down its forum for a couple of days. Alarmed by the information, the central government immediately dispatched a specially appointed working team to the explosion site. Severe punishments were given to local officials based on the working team's report. Premier Zhu Rongji (b.1928) even offered a rare public apology to the families of some forty children killed in the explosion; he apologized for allowing the abuses that led to the accident and failing to handle it properly in the early stages. Shortly after this, the Ministry of Public Security launched a new round of campaigns concerning the management of explosives and firearms (BBC News, 2001). The authorities finally quieted down public turbulence with grand-scale publicity of Premier Zhu's official apology, and with news about all the actions the government had adopted to deal with this incident, and with measures to prevent the recurrence of such incidents. My research found that the Internet played an indispensable role in this affair in helping the government timely find and pacify the public's dissatisfaction with its malpractice. The Internet "served as a catalyst of public opinion and led to greater government accountability" (Harvard International Review, 2001).

E-government

To build up a more transparent and open government, the Chinese government started its E-government movement in 1992 (Westland, 2000). E-government is defined as the "use of technology to enhance the access to and delivery of government services to benefit citizens, business partners and employees" (Deloitte & Touch, 1998). Since 1993, the Chinese government has concentrated on funding the Golden Projects, the collective telecommunication projects introduced as the first step to realize the E-government. By establishing a data communications network, China expects the Golden Projects to modernize the country's information technology infrastructure and to be able to lead to more efficient centralized government organizations (Tan, 1995).

Originally starting out with three projects in 1993, the number of the Golden Projects has grown steadily over the years as more plans have been initiated. The projects fall into four tiers. Tier one consists of four projects, they are Golden Bridge, the infrastructure for the China National Economic Information Network, China's version of the information superhighway; Golden Gate (Customs), a foreign trade information network linking the Ministry of Foreign Trade and Economic Cooperation with the Customs Bureau; Golden Card, an electronic money project whose goal is to use telecom networks to replace cash transactions with an electronic system for savings, withdrawals, and payments; Golden Sea, an information system interconnecting China's top government leaders and providing them with immediate access to reference data from other institutions, organizations, and offices under the

direct jurisdiction of the Communist Party Central Committee (Lovelock & Petrazzini, 1996).

The projects in tier two were designed to apply information networks to economic reform. They comprise Golden Macro, a network serving the Government's Central Economic and Financial Leading Group for macro-control over national economic activities; Golden Tax, a data network designed to link State Tax Administration's auditing center in Beijing with fifty regional offices and 800 bureaus. Projects in tier three have to do with sector-specific applications of the new IT program. They include Golden Enterprise, an internal network linking China's 12,000 large- and medium-sized enterprises; Golden Agriculture, a databank service network providing agricultural information, weather reports, and market information; Golden Health, the Ministry of Public Health's high-speed information exchange system for hospitals; Golden Information, a network linking the various statistical collection departments across the country; and Golden Housing, a nationwide sharing of information on real estate. The final tier of projects comprises Golden Cellular, a consortium of China's large domestic mobile communications manufacturers; and Golden Switch – a program to build China's domestic digital switch manufacturing industry (Yurick, 1997).

Following the initial success of the Golden Projects, in January 1999, the Chinese government announced an ambitious program calling for sixty percent of the ministries to have websites by the end of 1999 and eighty percent by the end of 2000 (Press, Foster & Goodman, 1999). A website, www.gov.cn, was set up for the

coordination and orientation of this nation-wide Government Online Project. After five years, facts show that China's achievements far outstripped the government's original ambitions for E-government. Up to February 2003, the government online project has put information from over 10,000 Chinese government offices online, helping those operations establish homepages or put databases and archives on the Web (Chinese Government Online, 2004).

The Government Online Project is multi-purpose. The authority expects it to reduce the administrative costs of the governments at various levels, to improve government efficiency and transparency, to promote communication between various departments of the government and various walks of society and to build government websites into convenient service windows for citizens. I have paid more attention to the last point listed here. My research finds that one of the major points of importance of this project is to popularize laws and to promote common people's awareness of law. Since the 1980s, the nation's leadership has come to a consensus that making laws more accessible to common people and promoting people's awareness of laws is a crucial step in constructing a developing country's legal system. They have attached great importance to this issue since China, for a long period of time, has been a country where a large proportion of crimes were committed through people's ignorance of the relevant laws. To change this situation, over the past decades, Chinese regulations have gone from being largely unpublished, confidential, in-house edicts, meant for officials, to published texts that are more detailed with each new reiteration. The emergence of the Internet, especially the Government Online Project,

played some active roles in making this change come about. A very important trend present on the government operations' WebPages is the increasing availability of the full text of Chinese laws and regulations. For example, all regulations concerning telecommunications and the Internet are now published and available to anyone interested at the website of MII (http://www.mii.gov.cn/mii/zcfg.html). Although this is still very unusual, some Chinese government agencies have even published proposed regulations or policies online and asked for comments from the public (Report from U.S. Embassy in Beijing, 2001).

Putting government organizations online is sometimes a tool used in battling corruption. The central government is promoting online bids and auctions to increase transparency and reduce kickbacks in awarding government contracts. These measures are all meant to address the long-standing problem of corruption (People's Daily Online, 1999).

Spreading Propaganda and Promoting Nationalism

The CCP, as I have said, sees the Internet, a powerful part of the mass media, as an important play ground for the Party's propaganda. An example of "inundating the media with Party-preferred information" is China's official website for Human Rights (http://www.humanrights-china.org) that sets out the government's human rights policy. Some may argue, websites like that sponsored by state agencies are not as influential among Chinese users as the government expected (Qiu, 1999-2000). One possible reason is their lack of interactivity. The websites are designed to facilitate one-way indoctrination instead of interactions. Seldom do they reflect nonofficial

opinions except when they are hacked. Moreover, it is well known that despite the efforts of CCP's propaganda especially that which concerns human rights policies frequent criticism and attacks against the policy continue to spring up. However, persistently interpreting its own policies from its own perspective is one of CCP's countermeasures. The CCP always believes that long-term existence of the official perspectives will always have some effect regardless of fluctuations in public opinion. It also believes that the large investment in putting government operations online can act as a favorable counter to the increasing number of online critics of the Party. By building attractive websites and posting regularly updated policy interpretations the CCP hopes to influence the public's opinions. It also should be noted that the Chinese government began to realize the drawbacks of its propaganda and it is actively improving its propaganda skills. Propaganda organs tried to use the Internet as a powerful tool for disseminating material that was less ideologically minded, and more acceptable to people at home and abroad. Needless to say, common people, sometimes, benefit from the propaganda. They get more and more useful and timely information from the Web and with this information they can better safeguard their own citizen rights. For example, with the updated information offered by the Customer Rights Protection agencies on the latest results of their anti-counterfeit raids via http://www.cqi.gov.cn (a website used by this agency to show off their working achievements), people are able to keep themselves away from the troubles or problems might be caused by fake and shoddy goods.

While some people, such as Nicolas Negroponte, the Director of the M.I.T.

Media Lab, argues that the Internet will signify the end of nationalism because it facilitates greater mutual understanding, some others observe that the Internet has not erased but has rather facilitated a strong sense of nationalism. Martin Regg Cohn said,

> The delicate dynamic of government regulation and corporate compliance has dampened the democratization trend that so many had predicted soon after the Internet took off in China. Now, nationalism is gaining ground by default (2001).

Nationalism, in China, is a concept that lies within the accepted range of social norms. It is often mentioned in the mass media and brought up during political events. My research has found that when a couple of important international events took place, the government was able to take advantage of the power of the Internet to help sway public opinion towards its own views. Most of these views center around the idea of nationalism (Qiu, 1999-2000). For example, shortly after the United States bombed the Chinese Embassy in Belgrade in 1999 and killed three Chinese journalists there, the *People's Daily* set up a chat-room called the *Anti-bombing Forum* on its website, which was later changed to the name of *Strong Country Forum*. This forum, together with all the other government-sanctioned chat-rooms, became a space offered by the government for Internet users to amplify their nationalistic sentiments. A great deal of anti-Western rhetoric focused on accusing the U.S. of deliberately undertaking the bombing; messages questioning the status quo view were promptly deleted. Despite the prohibition on using the Internet to plan demonstrations, "most observers believe that the government not only encouraged but actively aided students who used the Internet to plan days of violent protests outside the U.S. Embassy" (Pfaffenberger, 2001). "The great attraction of the Internet...as a sounding board against America,

and a rallying point for patriotism, is a source of comfort to the Communist Party. And it is no accident" (Cohn, 2001).

This was also the case during the aftermath of the U.S. Spy Plane incident off the coast of Hainan Island in 2001. The plane collision killed a Chinese jet fighter named Wang Wei. It also caused much heated discussion and roused nationalistic sentiments in the Chinese BBS. Some of the comments reported in the chatrooms included

> --We can forgo joining the WTO but we cannot afford to lose face.
> --Why can't the US show any human rights concern to the poor missing pilot?
> --The whole nation is waiting to see if China can play hardball with the US?

Furthermore, soon after this collision, www.netor.com, a host of a leading mourning site in China, established an online shrine to Wang Wei. Here citizens could light a virtual candle, leave digital flowers, dedicate digital melodies, or offer written expressions of their grief online. "We salute the hero in the sky", wrote one, while another citizen said, "You have fallen but millions like you live on to fight for the motherland". In just three days, Wang's site received the third most visits of the nearly 5,000 sites hosted by Netor.com (Chandler, 2001).

China has a long history of censorship of information, and the Internet is no exception. The CCP's deeply rooted attitude towards media and foreign technology, its judgment concerning the current domestic and international situations, and its social considerations all add to the CCP's strong determination to actively seek to control the use of the Internet. Further, it is clear that the Chinese government is developing a more sophisticated understanding of the Internet's function; it is gradually learning how to make the Internet serve the political purpose of the Party.

My research also suggests that China does have its historical, psychological, social and cultural aspects to consider in regards to the issue of Internet control. However, none of these aspects are as prominent as the CCP's political motivation. As a matter of fact, all these varying aspects promote the same goal albeit through different routes, that is namely to safeguard the CCP's leadership, the political stability, and the national unity of the country.

Chapter Three

Administrative and Legal Measures

The control of the Internet by the Chinese government began with the building up of a hierarchical administration structure. In this chapter I will first outline this hierarchy and then give a brief introduction to the different organs of this structure. After that, I will focus on the legal measures the CCP has taken in controlling the Internet, from the laws and regulations it has made, to the intimidation tactics it has practiced. I will also talk about the Chinese characteristics of those laws, regulations and their executions.

Building Up A Hierarchical Administration Structure

For a number of years, a power struggle ensued between the former Ministry of Posts and Telecommunications (MPT) and the former Ministry of Electronics Industry (MEI) over the control of the lucrative Internet. The lack of clarity over which department would be responsible for the Internet was the cause of the power struggle. To deal with this dispute, the central government created the Ministry of Information Industry (MII) in an overall organization reshuffle in March 1998, which finally brought the chaos to an end (Tsui, 2001). As a super ministry, MII is primarily responsible for planning and overseeing the development of China's electronics, telecommunications and electronic information industries. The MII is also responsible

for laws and regulations and the coordination of China's information industry. Wu Jichuan (b.1937) was elected as the first Minister of the MII in March 1998. The current head of MII is Wang Xudong (b.1946) who was promoted to this position in March 2003.

In China, MII is at the top of the hierarchy of the Internet control. Under MII are the Ministry of Public Security (MPS) and its subordinate bureaus in the provinces and cities. They are responsible for network security by looking after abuse of the network, like for example, the leak of state secrets, political subversion or the spread of pornography or hatred on the Internet. The MPS has the legal rights to monitor network traffic. Qiu argues that policemen from MPS and its local bureaus are actually the most superior gatekeepers against the "inappropriate" uses of the Internet since MII always gives its priority to routine administration (Qiu, 1999-2000). Under the MPS and its local bureaus, there lies the entirety of China's cyberspace, which is, first of all, managed by major ISPs. Although in different sizes, ChinaNet, CSTNet, CERNet, CNCNet, China169, UNINet, CMNet, and CIETNet have parallel administrations. Each has several regional network centers that control Internet services in provinces and cities. Among the regional network administrators, some technicians called "system operators" are directly involved in the daily maintenance of cyberspace communities. In BBS, they are called "stationmaster", assuming the most visible power of administrative control in the community. They can choose, install or uninstall, and modify the platform on which the online public communication is going on. They are the technocrats that are positioned in the middle

of the Internet regulation hierarchy. According to Qiu, a common practice adopted by these ISPs is to assign young teachers, researchers or graduate students majoring in computer science to be the stationmasters. Being members of the regulatory body who regularly receives monetary rewards, these people should be seen as an interest group different from ordinary users. The lowest rank of regulators in cyberspace is the boardmaster. Boardmasters are responsible for cleaning messages on one or a few electronic bulletin boards. Unlike the system operators, boardmasters are not necessarily members of the network centers. This means an external user can be a boardmaster within the entire system. Another significant feature distinguishing a boardmaster from a system operator is that the former is *electorate* whereas the latter is *selectorate* (Qiu, 2000). Most of the boardmasters are winners of online elections, in which ordinary users vote via the Internet. Subsequently, their source of legitimacy is supplied by ordinary users rather than by the higher ladder of the hierarchy.

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 are expected to supervise the technocrats and the netizens and penalize disobedient actions. The technocrats are to follow instructions from the cyberpolice and use various means in order to prevent users in their networks from accessing prohibited websites or expressing harmful information. The duty of the netizens is expressed in but one command: no trespassing is allowed into forbidden cyberspace.

If these duties are not performed, there is a system of punishment mechanisms

directed both at the technocrats and the netizens. The cyberpolice must also be subject to certain checks from the State Council and the Chinese Communist Party Center, but this is not specified in any regulation (Qiu, 2000).

Various other ministries and government bodies have an influence with regard to the Chinese Internet control as well, some of the more important ones are as follows: The Ministry of State Security (MSS) is responsible for the regulation of encryption software. Encryption is the technology responsible for conversion of data into a form that cannot be easily understood by unauthorized people. China Internet Network Information Center (CNNIC) is a non-profit organization founded on June 3rd 1997. It takes orders from the MII to conduct daily business, while being administratively operated by the Chinese Academy of Social Science (CASS). CNNIC is mainly responsible for the registration of domain names and the allocation of IP addresses. Its major responsibilities also include the annual Internet Usage Survey conducting, international liaison, technology and policy researches (Li, 2003). The State Council Information Office and the Propaganda Department of CCP Central Committee also work closely together and oversee much of the Internet content policy. In addition, all the levels of local, municipal and provincial government organizations of the information industry also play certain roles in managing and supervising the Internet.

To some extent, the jurisdictions of the above organizations might overlap in some areas. However, it should be noted that they all serve the same purpose that is namely to keep the Internet under their strict political, economic and cultural control and to keep the Internet from jeopardizing the Party's leadership and social stability.

Because of this common goal, there are no evident disputes among the different levels or organizations so far.

Laws and regulations

As the Internet grows, the Chinese government keeps tightening its control, making great efforts in legislation. From 1994 to 2004, at least sixty sets of laws and regulations on Internet control have been issued. The laws have become progressively more comprehensive, moving from efforts to regulate Internet business to restrictions on news sites and chat rooms (Law-lib.com, 2004).

Laws and regulations concerning Internet control can be divided into three different categories: those that govern the network infrastructure and international network connections; those that handle illegal activities related to the Internet; and those that deal with monitoring organizations and individuals. The main regulation for governing the network infrastructure and international network connections is the Temporary Regulation for the Management of Computer Information Network International Connection (Temporary Regulation) that was formally announced on February 1st 1996 and verified on May 20th 1997. Article Six of the Temporary Regulation provides that "no units or individuals are allowed to establish direct international connection by themselves," and that "all direct international networking traffic must use international incoming and outgoing channels provided by the national public network of the MPT" (Cullen & Choy, 1999). This means that every bit of Internet traffic that comes from foreign servers must pass through the network

of the former MPT (now MII), making it easier for authorities to monitor the traffic.

In December 1997, the Ministry of Public Security (MPS) issued the Security Management Procedures in Internet Accessing. The Procedures lists five kinds of "harmful activities" related to network infrastructure including

> (1) Intruding computer information network or making 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) (China Communication News, 1998).

In March 1994, the revision of China's Criminal Code first specifies the illegal activities related to the Internet, it announced that

> 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 285); whosoever, in violation of State regulation, 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 case, imprisonment of five years or more may be imposed (Section 286) (Qiu, 2000)

The latest law dealing with individuals' Internet-related illegal actions is the one issued on 21 January 2001 which rules that those who cause "especially serious harm" by providing "state secrets" to overseas organizations and individuals over the Internet may be sentenced to death:

> Those who illegally provide state secrets or intelligence for units, organizations and individuals outside the country through Internet with serious consequences will be punished according to stipulations of the Criminal Law; in especially serious cases, those who steal, make secret inquiries or buy state secrets and intelligence and illegally provide gathered

> state secrets and intelligence to units outside the country will be sentenced to ten or more years of fixed-term imprisonment or imprisonment for life and their properties may concurrently be confiscated by the state. In case of a gross violation of law and where especially serious harm is caused to the state and people, law offenders may be sentenced to death and their properties will be confiscated by the state (Amnesty International, 2002).

In my opinion, these regulations themselves are not unreasonable. For example, state subversion and endangering national unity are illegal in every other country (Tsui, 2000). The problem lies in the fact that the interpretation of the law can be quite arbitrary in China. The most noteworthy clause in the legislation is the one pertaining to the leak of "state secrets". This clause is so vague that it can be interpreted in multiple ways. Because of its ambiguous meaning, the leaking of "state secrets" has been often used as a pretext for detaining people (Amnesty International, 2000). Ambiguity in law thus is very useful for authorities in terms of justifying their control.

The government's determination to censor on-line content has grown with Internet usage. The Temporary Regulation for the Management of Computer Information Network International Connection was also the first issued regulations on managing the Internet information service. It prohibited all ISPs from publishing information that incites hatred, viruses and subversive acts meant to overthrow the state. Article Thirteen reads,

> Units and individuals engaging in Internet business shall strictly enforce safety and security control systems according to relevant state laws and administrative regulations, and shall not make use of the Internet to conduct criminal activities-including activities prejudicial to state security and the leakage of state secrets-or to produce, retrieve, duplicate, and disseminate information prejudicial to public order or pornographic materials (Human Rights Watch Backgrounder, 2001).

Information that is prohibited on the Internet was described in more detail by the

Telecommunications Regulation of the People's Republic of China, issued in September 2000 by the State Council. According to Article Fifteen, no unit or individual may use the Internet to create, replicate, retrieve, or transmit

(1) Information that goes against the basic principles set in the Constitution;
(2) Information that endangers national security, divulges state secrets, subverts the government, or undermines national unification;
(3) Information that is detrimental to the honor and interests of the state;
(4) Information that instigates ethnic hatred or ethnic discrimination, or that undermines national unity;
(5) Information that undermines the state's policy for religions, or that propagates heretical organizations or feudalistic and superstitious beliefs;
(6) Information that disseminates rumors, disturbs social order, or undermines social stability;
(7) Information that disseminates pornography and other salacious materials, that promotes gambling, violence, homicide, and terror; or that instigates the commission of crimes;
(8) Information that insults or slander other people, or that infringes upon other people's legitimate rights and interests; and
(9) Other information prohibited by the law or administrative regulations (Amnesty International, 2002).

In November 2002, the regulations controlling Internet Content Providers (ICPs) demanded that, "sites publishing news must obtain special licenses, may never generate their own content, and instead may only republish stories from official sources" (Sinclair, 2002). As a result, Chinese web sites do not have any option but to copy most of the news articles from the official sources. An example of this process can be found in portals such as Sina.com and Sohu.com, which have partnerships with the Western media companies Dow Jones and Reuters. Both portals stopped publishing non-financial news after a warning from the central government. They also stopped carrying news sources that were not officially state-sanctioned, fearing a loss of licenses. Content providers must also be wary of the State Secrets Protection

Regulations for Computer Information Systems on the Internet issued by the Bureau for the Protection of State Secrets in January 2000. Article Eight of this regulation states,

> The management of secrets concerning information on the Internet shall be based on the principle of "whoever places materials on the Internet takes the responsibility". Information provided to or released on Web sites must undergo a security inspection and approval. Inspection and approval should be carried out by related departments. Related units shall, in line with state laws and regulations on guarding secrets, establish and improve a leadership responsibility system for the examination and approval of information intended for the Internet. Units that provide the information shall establish a security system for information examination and approval in accordance with certain work procedures (Human Rights Watch Backgrounder, 2001).

The latest regulation on managing Internet information services is the one issued in January 2002. It stated that all ISPs operating in sensitive and strategic sectors such as news sites and bulletin board services must record details about users, including viewing times, addresses, phone numbers and account numbers. ISPs are also required to install software that could record every message sent and received by their users. ISPs also should maintain users' records for sixty days and provide these to the relevant state authorities when required (Amnesty International, 2002). If an ISP finds a message that it thinks violates the law, the ISP must send a copy of the message to three government agencies (the MII, the MPS and the Bureau for the Protection of State Secrets), then delete the message (Qiu, 2000). All key network management systems are now required to use domestically produced software. Since Internet chatrooms and electronic bulletin systems are particularly liable to become public political forums, which is quite a sensitive issue for the central government, Internet-related companies in China practice a high degree of self-censorship in order

to gain the trust and cooperation of the government. Almost all the ICPs and Internet Cafes have issued their own set of guidelines for both users and administrators. CERNet's Regulation of BBS Management 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) (CNNIC, 1997).

Sohu.com, a Nasdaq registered portal based in Beijing, also gives a very detailed message to clients who want to enter their chatrooms:

> Please take note that the following issues are prohibited according to Chinese law:
> (1) Criticism of the PRC Constitution;
> (2) Revealing state secrets, and discussion about overthrowing the Communist government;
> (3) Topics that damage the reputation of the state;
> (4) Discussions that ignite ethnic animosity, discrimination or regional separatism;
> (5) Discussion that undermine the state's religious policy, as well as promotes evil cults and superstition;
> (6) Spreading rumors, perpetrating and disseminating false news that promotes disorder and social instability;
> (7) Dissemination of obscenity, sex, gambling, violence, and terror. Cyber-sex is not permitted within the English chat-room;
> (8) Humiliating or slandering innocent people;
> (9) Any discussion and promotion of content which PRC law prohibit.

The message ends with the following warning: "If you are a Chinese national and willingly choose to break these laws, Sohu.com is legally obliged to report you to the

Public Security Bureau" (Sinclair, 2002).

Self-censorship even sees the involvement of transnational ICPs. A "Public Pledge on Self-Discipline" was introduced in August 2002 under which signatories agree not to post or disseminate "pernicious" information that may "jeopardize state security, disrupt social stability, contravene laws and regulations" and not to "spread superstition and obscenity". Over 300 companies have signed this pledge, including the popular international search engine Yahoo! (CNET, 2002).

On November 15, 2002, tough new regulations introduced by the Ministry of Culture restricting access to the Internet and operations of Internet cafes came into effect. These regulations obliged proprietors of Internet cafes to install software preventing users from accessing information considered "harmful to state security", as well as preventing the dissemination, downloading, copying or browsing of material on "heretical organizations", violence and pornography. Those aged under eighteen years old were banned from Internet cafes. Operating licenses could now be withdrawn and fines could be imposed if these regulations were not properly implemented (Amnesty International 2002).

Even before this regulation came into effect, Internet cafes had already taken measures to protect themselves from possible punishment. Personnel of the Beijing-based Feiyu Internet Cafe routinely checked screens by walking along the 800 computer units and reading over the shoulders of the clients. A note that was placed on a user's monitor to indicate the start of his or her login time says,

> Feiyu Web Bar warns its clients: Please do Not Download Web Pages with Illicit, Violent or Reactionary Content. Content considered "reactionary"

could include Falungong-related material, dissident web pages or sites promoting the independence of Taiwan or Tibet. Feiyu's website has a link to all major Internet regulations and added some additional ones. Under these rules, mostly issued by the Bureau of Industry and Commerce, Feiyu management is obliged to turn violators in to the local police station (Human Rights Watch Backgrounder, 2001).

Laws and regulations with Chinese characteristics

The enforcement of laws and regulations in China comes in waves. Laws are strictly enforced at first, then after a while, the enforcement situation relaxes. When the government feels it needs to issue a warning the laws and regulations are tightly enforced again (Cowhig, 2000). These enforcement swings are best illustrated in the Internet cafe sweeps that occur from time to time to make sure that they adhere to the regulations. On April 10, 2001, the State Council announced a three-month investigation into Internet cafes. China's *Legal Daily* gave what it termed an "incomplete" progress report on June 14, 2001. By that time, police had investigated more than 56,800 web bars, of which 6,071 were ordered to disconnect from the Internet. Between April and July 2001, over 2,300 cafes had been closed down altogether (2001).

Another characteristic of Chinese laws that needs to be borne in mind by Chinese Internet business insiders is that even though one can have a knowledge of law, the laws can not be relied upon as a stable factor. In order to be able to assess the situation correctly, it is more important to have good relationships with the government. For example, the Sina office has a direct hotline to relevant officials who help clarify when the policy is unclear and who give warning in advance of sensitive topics (Heim,

2000). Thus, companies exhibit anticipatory conformity, showing the behavior deemed appropriate by the government. A new law therefore does not realistically result in any big changes, since most companies were already adhering to the government policy. In other words, law codifies what is already common practice.

This last point is likely to be a universal characteristic of developing countries. That is, the actual implementation of regulations varies greatly in different geographical regions, at different administrative levels and during different period of time. For instance, message eradication is usually more frequent and strict in websites located in Beijing, the nation's political, economical and cultural center, than in other parts of the country. In distant provinces such as Yunnan, it is said that the registration of Internet cafes had not been put into practice until 2000 although the relevant regulations took effect as early as in 1997 (Qiu, 1999-2000). Virtual censorship also usually tightens up when the date of June 4th approaches and when the National People's Congress is under way, while it is loosened for the rest of the year. The uneven implementation of Internet regulations therefore results in controls of different intensity. Remote areas, lower administrative levels and periods when the political atmosphere is relatively open definitely see comparatively lenient controls.

To Punish One to Warn One Hundred (2 Ч Э р)

Law, as a means of control, depends on the threat of sanctions by the state. Intimidation is a very strong weapon in the battle for Internet control and something at which the Chinese government excels. Its goal is to set a "standard", so everyone

knows which boundaries they should not cross. "To punish one to warn one hundred": this is what the Chinese proverb *sha yi jing bai* means. Actually, another Chinese idiom has the same meaning. It reads: *sha ji xia hou*, which literally means "to kill the chicken to frighten the monkeys". Looking back to all the previous political movements, I found that the CCP has become more and more proficient in making use of this tactic, and it has never hesitated to make examples out of certain situations in order to intimidate the public. Finding ICPs which violate the government's relevant laws or regulations, the government can close the website for a few days. This happened, for example, to Sohu.com in early 1999, when a pornographic link was detected on its site. In another case, the China Finance Information Network's site was closed down when content was found that "spread rumors that damaged the government's image" (Hartford, 2001). After that, news portals such as Sina, NetEase, Sohu and Yahoo! tried their best to stay clear from politics in general and focus on entertainment and sport instead.

BBSs or other virtual communities carrying forbidden political contents can be shut down for a period of time, during which time the technocrats are required to remove the inappropriate contents. This process is also employed for the purpose of prevention. For instance, in recent years in early June, most BBSs hosted by universities are denied network connections for a week or so due to the anniversaries of the student movement on Tiananmen Square on June 4 1989. If there is serious violation, the responsible website or virtual community can be closed indefinitely. The *Untitled BBS* station of Peking University (*Beida Weiming BBS*) provides a good

example. This BBS, formerly renowned for zealot political discussions, was closed for nearly three years between September 1996 and 2000 for the reason that it mobilized a nationalist protest movement against Japan despite official objection on the part of the government. The shutdown of the BBS shows that the government has no problems with closing a popular service to make a political statement.

The *New Culture Forum* site (www.xinwenming.net), the first China-based website started by veteran democracy activists, was closed down only four months after its birth in 2000 to scare away potential websites of the same kind. This forum was run by a group of dissidents from Shandong Province. It aimed at spreading the messages that Chinese politics should adopt compromise and conciliation to enable democratic change. This was undoubtedly intolerable to the government and the state security officials shut down the forum with the charge of posting "reactionary materials" on its website.

Regarding legal punishment imposed on individuals, I found that before the summer of 1999, only one person was detained due to improper online transactions. However, in August 2000, China's first civilian Internet police force was reported to make its debut in Anhui Province, with several other provinces planning to follow suit. Part-time online surveillance jobs were offered to graduate and undergraduate students majoring in computer science and technology. The troop was reported to have approximately 5,000 members in 2000. As a result, between 2000 and 2001, at least thirteen people who circulated "politically sensitive" information over the Internet were detained or imprisoned, one for posting anti-Party messages to BBS,

another for starting a web site about the Tiananmen Massacre. All the remaining eleven cases were Falungong practitioners, who transmitted or disseminated online materials of the officially prohibited "evil sect" (Qiu, 1999-2000).

The recorded intimidation of individuals because of Internet misconduct began with the case of Lin Hai, a computer engineer from Shanghai. He was arrested in March 1998 and is considered to be the first person to have been sentenced for improper use of the Internet in China. The Chinese authority accused him of providing 30,000 email addresses to VIP Reference, a US-based online pro-democracy magazine. Lin was also charged with subversion and was sentenced to two years in prison in June 1999 (Amnesty International, 2002). Considered as the first "Internet dissident" in China, Lin gained worldwide attention. The Western media portrayed him as a political martyr, but actually he was just hoping to make a few bucks by selling the email addresses. It is very ironic that Lin Hai did not act out of political motives but out of commercial interest. However, the Chinese authorities successfully sent a message through Lin's case to others who might use the Internet for democratic aims or for the purpose of challenging existing institutions. Lin's case also undoubtedly alerted all Chinese Internet users to the fact that the government was indeed actively monitoring email and that it would not hesitate to take action if they suspected someone is abusing the Internet.

In June 2000, the Chengdu-based Internet activist Huang Qi was arrested for "subverting state power". Huang had set up and operated his own website, www.6-4tianwang.com by which he exposed corrupt practices and criticized the

government's military action against the 1989 Tiananmen protest. He also called for political reforms, and helped dissidents trace missing relatives following the crackdown on the 1989 pro-democracy incident (Report from U.S. Embassy in Beijing. 2001). Huang's trial began in secret in February 2001, but the trial was suspended after he reportedly fell ill. It was re-scheduled for June in the same year, but again postponed (Human Rights Watch Backgrounder, 2001). In August 2003, the Sichuan High Court confirmed on appeal his five-year sentence that was passed by a lower court. In September 2003, he was transferred to the top security prison of Nanchong, 200 kilometers east of the provincial capital Chengdu (Reporters Without Borders, 2003).

One of the longest sentences for Internet misconduct has been passed against a former police officer, Li Dawei, who has been sentenced for 11 years in prison for downloading articles from Chinese democracy websites abroad. All his appeals have been turned down (Amnesty International, 2002). Li Zhi is the highest level official who has been detained for Internet activities. Li, thirty-two, is a graduate of the Xinan Institute of Finance, and prior to his arrest on September 3, 2003 was a finance official in the Dazhou municipal government in Sichuan Province. According to Human Rights organizations, Li Zhi frequently expressed his views on BBSs and chatrooms. Police told Li's wife that he was found to have communicated with overseas dissidents through Internet chatrooms. Sichuan Province State Security Police formally arrested Li Zhi on charges of "conspiracy to subvert state power". Under the present charge of subversion Li could be sentenced to up to fifteen years in

prison (Human Rights in China, 2003).

Miss Liu Di, a 22-year-old psychology major at Beijing Normal University, is the youngest Internet dissident China had detained. In 2001, she started her own chatroom, "A Life Like Fire". Since then, she kept publishing articles that criticize government restrictions on the Internet. Using the pseudonym "the stainless steel mouse", she posted messages urging fellow Internet users to "ignore the Chinese regime's propaganda and live in full freedom" and to spread "reactionary" ideas via the Internet. On November 7, 2002, the day before the inauguration of the sixteenth Chinese Communist Party Congress, Liu Di was arrested on campus. Public Security Bureau officials later searched the family home, removing her computer, notebooks, and floppy disks. She has been held in solitary confinement on charge of "jeopardizing national security" (Human Rights Watch, 2003). With hundreds of Chinese people taking the risk of signing an online petition calling for her release, Liu Di was finally freed on bail on November 28, 2003, one week before Chinese prime minister Wen Jiabao (b.1942) traveled to the United States (Reporters Without Borders, 2003). The government gives no mercy to Internet dissidents even if they are young students who have limited life experience - this is the message conveyed to Internet users through Liu Di's case.

Chomsky notes that the government uses the media to manufacture consent. He states that "the primary targets of the manufacture of consent are those who regard themselves as 'the more thoughtful members of the community', the 'intellectuals', the 'opinion leaders'" (Chomsky, 1989, p.45). Reviewing these cases, I would

conclude that this is indeed what the Chinese government does in regards to the Internet. If the government needs to punish one to warn one hundred, those who regard themselves as "the nation's conscience", "people's rousers " or "gravediggers of an unjust social system" would more likely to be selected as the instructive example.

According to Foucault's Panopticon theory, a prison needs a surveillance system to make a permanent and ubiquitous supervision on its prisoners. It is the same in the case of a modern society (Deibert, 1997, p.166). Comparing China's cyberspace to a Panopticon, I found that China's regulatory hierarchy works as the prison's guards at different levels and positions with different responsibilities. From the custodial officers to common jailors, these aspects help form a very basic and necessary part of a surveillance system. The laws and the regulations related to the Internet work as a legitimate and effective weapon through which the guards can punish the prisoners, i.e. the Chinese netizens. For the purpose of executing laws and regulations, the CCP has its own techniques. The CCP chooses to pick up and punish some representative violators as a first step, either an Internet business or an individual dissident, to intimidate any like minded violators. However, this process does not imply that once the representative dissident is punished, the rest are safe. Indeed, the government can choose to punish quite freely because of the ambiguity encoded in law. Since only the government has the right to interpret laws and regulations, the government can make use of some vague provisions. Whether the business organizations or netizens are "anti-revolutionary", "jeopardizing state security" or "leaking state secrets" totally

depends on the authority's arbitrary interpretation of law. Secondly, since the "one hundred" always needs intimidation to be kept in line, in the Chinese authority's understanding, there is no end to the government's efforts to pick out and punish the "one".

Chapter Four

Technical Measures

"If governments were to think that the Internet needs some type of regulation...Laws and regulations are one solution, and technological solutions are another" (Spinello, 2000, xi). My study supports this argument. Following the chapter about laws and regulations, this chapter will review the major technical measures the Chinese authorities have adopted in curbing the Internet. It also outlines some major anti-control measures and discusses to what degree these measures have been effective.

Filtering

In China, an important government measure to implement Internet control is the control of the main Internet infrastructure. As we have mentioned in Chapter Three, the 1996 Temporary Regulation for the Management of Computer Information Network International Connection (Temporary Regulation) stated, "all direct international networking traffic must use international incoming and outgoing channels provided by the national public network of the MPT" (Cullen & Choy, 1999). This means that every bit of traffic that came from foreign servers had to pass through the network of the former MPT, making it easier to monitor the traffic. Since then, government organization reshuffles happened from time to time. The MPT has

already been replaced by the MII. However, the government monopoly in Internet access has not changed greatly. For the ISP business sector, the MII is still the one agency authorized to review, approve and grant operation licenses, and ban any foreign investment into the market. As a result, the Central Government and its functional departments have so far controlled the vast majority of the Chinese telecom infrastructure, with all the ISPs being local and within the regime's jurisdiction. I have mentioned in Chapter One that there are eight major ISPs in China. Of the total bandwidth (27216Mbps), state controlled ChinaNet has 16500Mbps, or sixty-one percent of the total. The rest are distributed among the other seven government department controlled Internet networks, among which China169 has 4475Mbps or sixteen percent, CNCNet has 3592Mbps or thirteen percent, UNINet has 1490 Mbps or five percent, CMNet has 555Mbps or two percent, CERNet has 447Mbps or two percent, CSTNet has 155Mbps or 0.6% and CIETNET has 2Mbps or 0.01%. It is evident that the government is a monopoly supplier of the ISPs. All the private ISPs across the country have to rent their space from these state-owned Internet companies. In other words, the central government, through different departments, controls all network traffic that travels outside China.

Upon these connection lines, China imposed what the Western media called "the world's largest firewall" or "the Great Firewall" (South China Morning Post, 1997), that blocked access to selected websites with "harmful information" and automatically screened online content by targeting at words such as "June Fourth". Therefore, even today, no one can access a website that is deemed undesirable and blocked out of the

gateway of the eight ISPs because the ISPs are at the top of the hierarchy of the network structure. Filtering does not stop at ISPs. After a fire in an Internet cafe in Beijing in June in 2002, the authorities closed thousands of Internet cafes and demanded that those allowed to reopen do so only after installing filtering software to block Web sites considered "politically sensitive" or "reactionary". The software further prevented access to various foreign websites that were deemed undesirable by the government but that happened to have escaped from the filtering net (Amnesty International, 2002). In late August 2002, China even blocked access to apolitical search engines such as Google and AltaVista for a brief period, diverting users to local Chinese search engines instead. Sometimes, Chinese authorities shift tactics by opening up some previously blocked websites, but making it impossible for users to open documents on those sites that relate to China (Amnesty International, 2002).

In mid-September 2002, China introduced new filtering systems based on key words, regardless of site or context. Filtering software has reportedly been first installed on four public access networks in China. Prohibited words or strings of words on websites, e-mail, foreign news sites and search engines were affected by these new filtering systems. The filtering process works in the following way: when users try to access information that includes key words such as "human rights", "Taiwan", "Tiananmen", "Falungong" or "Tibet", the filter program that screens out forbidden contents would recognize the web pages. The request would then be thrown away, with the user receiving a banal message: "Operation timed out" or "Page cannot be displayed". One Hong Kong's human rights group reports that by the end of 2003,

over 500,000 foreign websites had been blocked in China on the grounds that Chinese people might be exposed to pornography and other "unhealthy elements" from abroad. Among such "unhealthy" websites are news sites for Cable News Network (CNN), the Voice of America (VOA), British Broadcasting Corporation (BBC), the Washington Post, the Sydney Morning Herald, and the Falungong websites (Zhang, 2003). Geocities and Tripod, although very popular for providing opportunities to have anonymous homepages free of charge, are also blocked since their services are used by Chinese dissidents to publish some underground newsletters such as *Tunnel* or *VIP Reference* (Lyon, 2001, p.102).

This filtering system has displayed its tremendous power over the years. Ethan Gutmann, a researcher on China's Internet, gives us one example. According to him, when he worked in China in 2002, he received an e-mail from a U.S. friend in a browser-based Hotmail account, which in his mind should have been difficult to monitor. However, contrary to his judgment, words in that email such as "China", "unrest", "labor", and "Xinjiang" were in queer half-tone brackets, as if the words had been picked out by a filter. Gutmann notes that "I now realize that it was a warning; any savvy Chinese user would have sensed it instantly". He also points out that during his stay in China, e-mail to Tibet took three days to get through, if it even ever reached its final destination, while Falungong e-mail was completely eradicated (2002). While working on this thesis in China in July 2003, I tried to search on Yahoo.com using the phrase "Taiwan independence" and "Falungong". For the former, the search engine first told me it found 15,700 results but none of them could be

connected when I clicked on it; trying for the second time, all the 15,700 results disappeared, the statement that "Page cannot be displayed" replaced them, which was the same as what I got for the latter request.

Filtering out undesirable contents from outside China or doing keyword searching inside e-mails and web addresses is not a foolproof process for the eradication of dissident information on the Internet. Chinese authorities also need software and devices that allow them to recognize who the offenders are. Cisco, an American company that is known (among other things) for building corporate firewalls to block viruses and hackers, helped China solve the problem. They developed a router device, integrator, and firewall box specially designed for the Chinese government's Internet monopoly. At approximately $20,000 a box, according to Gutmann's report, "China bought many thousands" and "IBM arranged for the 'high-end' financing". An engineer with Cisco China confirms, "Cisco made a killing. They (the boxes) are everywhere" (2002). How do these boxes work and how does China detect those offenders through the devices? Gutmann said the engineer did not know or would not say. However, Gutmann gives another example. In April 2002, Chi Shouzhu, a veteran activist, was picked up and arrested in a crowded train station minutes after printing out online materials promoting Chinese democracy. Gutmann notes that incidents such as this have mushroomed in China, suggesting that Cisco's system is more powerful than expected and Cisco may not be the only one capable of helping the Chinese authorities in looking deeply into Internet traffic (2002).

Control vs. Anti-control

John Gilmore once said, "The Net interprets censorship as damage and routes around it" (Internet Quotation Appendix, 2003). Lokman Tsui explains this process in the following way:

> The Internet is a packet-switched network, meaning it is designed so that data are [sic] sent around in small packets and are able to take another route if one part of the network is down. Censorship is thus treated as if one part of the network is down. The Internet will find a way around the censorship to reach its target (2001).

There are ways to get around the obstructions of censorship and this is what Clinton and others who believe that the Internet will eventually bring democracy to China base their conjectures on. In this part, I will examine some major countermeasures to censorship and discuss to what degree they are successful.

Proxy Servers

As I have mentioned earlier, the Chinese government prevents access to certain websites by blocking certain Internet Protocol (IP) addresses through a national "firewall". A firewall is a system or group of systems that enforces an access control policy between two networks (Drakos, 2000). However, breaking through the firewall is theoretically a simple task. Using a proxy server, "another computer that acts as an intermediary between surfers and websites, helping to hide their web footprints and evade the filters" (Gutmann, 2002), the audience is able to view those blocked sites. Actually, the use of proxy servers to circumvent existing filters is the most often mentioned countermeasure to content control. Requests for websites are forwarded to the proxy server, which in turn requests the website you request. Since the proxy

server is not hampered by the restrictions, it retrieves blocked websites like that of CNN and forwards it back to you. The result is that you retrieve the CNN website not directly from CNN but by way of the proxy server.

A study in 2000 by researchers at CASS reveals that from 1037 people surveyed "more than a quarter of Internet users admitted to occasionally using Internet proxy computers...while ten percent admitted to frequent use" (Lee, 2001). Ethan Gutmann comments that the "most common search words in China were... 'free' and 'proxy'" (2002). Furthermore, Chinese newspapers, have indirectly taught readers, how to use proxy servers for "faster" connections and informed them of how to reach banned materials. In the summer of 2000, through the use of proxy servers, many people in China were able to read the text of Taiwanese President Chen Shuibian's inaugural address although it did not appear in any of the mainland official publications (Hachigian, 2001).

However, there are some complications inherent in this process which are often neglected in articles that mention the use of proxy servers as the savior of "free speech". It must be pointed out that, like addresses of websites, the IP addresses of proxy servers can also be blocked. It is true that the Internet users are able to switch servers to avoid the blockades. However, as Gutmann points out, "a user, frantically typing in proxy addresses until he finds one that isn't blocked, effectively provides the government with a tidy blacklist" (2002). For the time being, the search for proxy servers can be simplified by using programs that specialize in searching for proxy servers. Proxy Hunter is such a program, which is available in China. The problem is

of course that if it is easy for the users to locate a new server, it will also be easy for the government to locate it. The success of the proxy surfers relies on the fact that new proxy servers appear every day and depends on the assumption that the government cannot possibly block them all. With the new century's advent, rumors even started to go around that the government would deploy fake proxies, using them as a so called "honey pot" (Chen, 2000). A honey pot acts like a real proxy, but monitors the activity and gathers data necessary for prosecution. Once these "honey pots" come into effect, Internet users would look at any proxy with suspicion and might be hesitant about using the proxy.

Furthermore, keeping practical considerations in mind, countermeasures need to have a high degree of accessibility, user-friendliness and continuity to be successful. For a proxy server to be efficient, it needs to be accessible. First of all, the speed a proxy server connection to a website should not be much slower than a direct connection. The speed is dependent on the physical distance between the host and the proxy server itself and on the number of users using the bandwidth of the proxy server; if more people use the same proxy server, the server will clog up and it will get slower. Proxy servers are useful as long as the traffic is not too high. As long as the number of users using the proxy is not alarming, the proxy can continue to run. When the number of users starts to rise, the performance of the proxy will suffer, rendering the proxy server useless. There is also no commercial incentive in running a proxy server, therefore continuity of the service is not guaranteed.

E-mail

Perhaps the most common use of the Internet is electronic mailing. This allows information to be sent over the Internet from user to user or more importantly from one user to numerous users at a speed unimaginable for communication in the past. Nina Hachigian remarks, "E-mails can replace dangerous personal meetings among dissenters. Furthermore, the instant dissemination of information about a political event to thousands of people can build momentum behind a cause faster than past media ever could" (2001). Naturally, E-mail is the weapon of choice for Chinese dissidents. Despite the blocking of Falungong websites hosted overseas, e-mail has become a lifeline for practitioners organizing meetings and protests. Likewise underground dissident magazines such as *VIP Reference* and *Tunnel* use e-mail to disseminate their regular issues to Internet users in China. Nina Hachigian explains that "e-mail was critical to the growth of the now-outlawed China Democracy Party" (2001). Veteran Chinese dissident Dai Qing admitted, "Whenever I get back to my apartment, the first thing I do is to check my e-mail" (1997).

It has long been assumed that, while it is not an immense undertaking to filter out certain websites, the censorship of e-mail is close to impossible. In the past, it was also widely believed that signing up for one of the many web-based non-Chinese e-mail providers such as Hotmail (it is now available in Simplified Chinese characters), can get around the Chinese government's censorship on e-mail. The reason is that the Chinese government cannot feasibly block websites like Hotmail because companies like Microsoft (owner of Hotmail) form a powerful lobby whose

support China requires in order to expand its rapidly growing Information Technology sector. These suppositions have proved to be a little shortsighted. Kathleen Hartford provides us with the chilling warning that "any digitized communication can be recorded, categorized, and searched. If the thought that they cannot possibly read every e-mail message gives you comfort, keep this in mind: they don't need to" (2001). As I have already mentioned, the government utilizes software and devices to monitor and filter out certain keywords in e-mail communications. Hartford also confirms that

> sophisticated search software can pluck a handful of potentially suspect messages out of millions. Traffic analysis – a technique that Chinese security agencies already use – can identify communication hot spots or trace messages emanating from particular sources (2001).

This could be a worrying proposition for those who regard e-mail as undetectable and use it for their own causes. This could be a problem for groups such as the China Democracy Party, Falungong, *Tunnel* magazine, *VIP Reference*, *Chinese News Digest* (CND), and some other underground newsletters. Meanwhile, the example given by Gutmann (outlined in the previous section entitled "Filtering") undermines people's overoptimism of e-mail providers such as Hotmail. While this example may work as a simple warning demonstrating that the government is watching, the warning's efficiency depends on the Internet users. The warning may not frighten the truly determined activist or hacker, but it is credible that for the vast majority of the Internet users these measures would serve their purpose. Orville Schell is quoted by Andrew Leonard as having said,

> I think a lot of digital revolutionaries...believe that the information revolution is uncontrollable but I'm not so sanguine. I think it's uncontrollable for the hard-core hackers, but for ordinary people it's quite controllable (Leonard, 1997).

This argument highlights my concerns.

Encryption

Encryption potentially forms a big problem for the Chinese government. It allows individuals to communicate in private and prevents a third party from eavesdropping. A normal e-mail message is inherently insecure, comparable to a postcard. However, if you encrypt the message, the government cannot read it unless it has the key to decrypt it. Nevertheless, a few existing problems prevent encryption from gaining widespread use. First of all, not a lot of people care about privacy on the net (with the one exception of where credit cards are concerned). Security awareness is not very high among the general public (an issue I will discuss in more details in next chapter), and therefore not a lot of people install encryption software (Declan, 2001). The second factor in the relative unpopularity of encryption is the high technical barrier; encryption software is hard to use, a fact acknowledged by Phil Zimmerman, the creator of Pretty Good Privacy (PGP) which is the most popular encryption software (Wired, 2001). Additionally, both the sender and receiver need to have PGP installed in order to have it work. The fewer PGP users you know, the less useful it is. Another problem is that the encrypted messages will look very suspicious and draw attention, since communication nowadays is generally unencrypted. After all, why would you encrypt the message if you did not have something to hide?

Bulletin Board System (BBS) and Chat Room[1]

BBSs and chat rooms are notoriously hard to regulate because of their spontaneous nature. However, as I have noted, stationmasters and boardmasters, both parts of China's hierarchical network administration force, play different roles in keeping the BBSs and chat rooms under maximum control. Within BBSs, all the postings by registered users are filtered by key words. If they contain targeted key words, they will be placed in a queue where they wait to be approved by boardmasters. If approved, postings will appear on the BBS with other safe postings. Otherwise, they will be deleted. I personally have registered as a user and tried to post some comments on *People's Daily*'s *Strong Country Forum*. My experience proved that if a posting passes through the filter smoothly, it takes nearly one minute before the user sees it online. A circumvention of key words is possible by using homophones, characters that have the same pronunciation but have a different meaning. However, inside knowledge is required to understand what is meant, which raises barriers to access. If undesirable content is found, the technocrats and boardmasters can give different penalties to ordinary netizens including message eradication, temporary or partial suspension of membership or even cancellation of membership accounts. Message eradication is the most widely used means of virtual censorship. It is a form of punishment transmitting a lucid negative feedback to the responsible netizen: what you wrote is not acceptable in this online arena. If infringement is repeatedly

---

[1] A chat room is a place on the Internet where people with similar interests can meet and communicate together by typing messages on their computer. The messages in a chat room appear instantly to everybody who is connected to that particular chat room.

committed by the same netizen, the boardmasters generally suspend his or her access to the virtual community for a certain period of time. In some minor cases, the punishment is a temporary suspension of some network applications such as voting, posting articles and chatting with other users. In the most serious cases, the offender's membership account in a virtual community is removed. According to relevant laws and regulations, the technocrats shall hand over severe violators to public security offices. Since most netizens use pseudonyms when they really want to challenge the authorities on the Web, tracing those violators in the reality is beyond the boardmasters' jurisdiction. The Ministry of Public Security, the Ministry of State Security and other departments armed with more sophisticated technologies can take on these responsibilities. Therefore, eliminating the virtual existence of the offender is the gravest punishment the boardmasters are able to carry out.

As with the BBSs, all the chat rooms in China's cyberspace have a "big mama" (Gutmann, 2002), that is, a supervisor for a team of censors who wipe out politically incorrect comments immediately after they are posted. Gutmann examined the way Yahoo! China handles things and described it in the following way,

> If in the midst of a discussion you type, "We should have nationwide multiparty elections in China!!" no one else will react to your comment. How could they? It appears on your screen, but only you and Yahoo!'s big mama actually see your thought crime. After intercepting it and preventing its transmission, Mother Yahoo! then solicitously generates a friendly e-mail suggesting that you cool your rhetoric (2002).

Moreover, cybersleuthing companies are developing various software for the industry that make it possible to spot undesirable contents (for example, a rumor posted online) within 15 minutes or even less (Kumar, 2001). This software would form a great first

line of defense for moderators who are responsible for detecting and eliminating unwelcome contents. China's Internet censorship has long been benefiting from the global technology upgrading. I will also develop this topic in next chapter. I argue that the government will spare no efforts in obtaining and utilizing the latest and most advanced technologies in making the Internet users obedient. This trend refutes the argument that BBSs and chat rooms are impossible to be controlled.

Anonymous Networks

Networks that protect users' privacy and let them surf anonymously are sometimes mentioned as a countermeasure to the all-seeing eye of the government. Instead of their computers being monitored, the privacy network is monitored. However, this solution has the same fatal problem as what proxy servers suffer, that is, it can also be blocked. Furthermore, anonymous network services are either free like Anonimyzer, but flawed or painfully slow to operate (Wired, 1999) or, ironically, demand payment, like a service called "Freedom" (Freenet available at www.zeroknowledge.com). The former drives the users away for its instability and other inherent shortcomings while the latter also makes it difficult for Chinese Internet users to access. The latter option is undesirable because firstly, Internet users prefer free service, and only use those costing money if the service is deemed indispensable. As a matter of fact, spending on Internet is still a luxury to most households in China. Secondly, even if individuals can afford and are willing to buy access to a privacy network, electronic payment has long been considered unsafe therefore is almost non-existent in China. In one word, both of these privacy network

options are currently inaccessible to ordinary Chinese Internet users.

Building Up Architecture for its Own Benefit

In *Manufacturing Consent*, Chomsky points out that to manipulate the media into following a special agenda and framework, the national authority takes many different routes. One such route is "to help chase unwanted stories off the front page or out of the media altogether". Another is to inundate the media "with stories, which serve sometimes to foist a particular line and frame on the media". Chomsky also notes that this strategy can be traced back to at least as far as World War I when it was discovered that "one of the best means of controlling news was flooding news channels with 'facts', or what amounted to official information" (2002, p.23).

Examining China's Internet control, I found that the authorities have adopted both of the ways of controlling media mentioned by Chomsky. We can compare the filtering of information in China to the first way of media control through chasing unwanted stories out of the media (Internet). Furthermore we can compare the process whereby nationwide government-controlled networks are built up and filled with authority-approved contents to the second option for the control of media: the inundation of media with official information. Chinese authorities believe that nationwide networks filled with only government-sanctioned contents can greatly contribute to building a safe environment for Chinese netizens. Within this environment, only the content that falls in line with the government's propaganda requirements is filtered through, while everything else remains inaccessible. A result

of this process noted by media analyst W. Lance Bennett is that

> The public is exposed to powerful persuasive messages from above and is unable to communicate meaningfully through the media in response to these messages...Leaders have usurped enormous amounts of political power and reduced popular control over the political system by using the media to generate support, compliance among the public (1988, p.178-179).

This is actually a clear depiction of the Chinese government's endeavor to promote national ICP services.

At the same time, it is beneficial to note that there are also some objective causes driving the government's activities. Language is one of the big issues. An often-made assumption is that having access to the Internet automatically means access to all the information on the Internet. This is simply not true. Mere accessibility of information says nothing about issues concerning diversity and quality of information. The fact that so much information is available only in English raises barriers to Chinese people's access to information on the Web. Seen in this light, the building up of government-controlled networks is not only reasonable but also necessary if the Chinese people are to gain access to information.

In the late 1990s, about eighty percent of the Internet content was in English (Newsbytes News Network, 1998). Although this number sees yearly decrease, by the end of 2001, still something over sixty percent of Internet content was in English, the mother tongue of ten percent of the world's population (Wade, 2001). Simply because English is the dominant language on the Web does not mean that it is necessarily

popular among surfers. An IDC[1] research pointed out that Asian web surfers all prefer content in their own languages, as opposed to content in English, the lingua franca on the Internet (Bonisteel, 1999). In China, although the majority of Internet population consists of relatively high-educated young people that live in the big cities, their low English literacy still prevents them from widely accessing foreign web content. That explains why current Internet users in China visit domestic websites eighty percent of their time while the other twenty percent is split between overseas Chinese websites and English-language ones (Zhu & He, 2002). Language barriers become more poignant when Chinese users try to interact with foreign Internet users. In such a case, Chinese users need to be fluent in written English to be accepted in foreign virtual communities (North, 1994). A foreign community, which is in its essence defined by its exclusiveness and borders, will find easy ways to exclude members who do not have full command of the English language. This reality affects not only Chinese or Asians but also all non-native English speakers in general. Of course, the same thing happens if a foreigner tries to participate in a Chinese online community. Indeed, it is mainly Chinese people who gather in Chinese BBSs and chat rooms where everything is conveniently communicated in their own language.

Learning English is officially promoted by the Chinese government and it is seen as a necessary ability to be able to compete in the world market. As a result, English proficiency does keep improving in China. However, it will be a long time before the

[1] IDC is the premier global market intelligence and advisory firm in the information technology and telecommunications industries. It has branches in 50 countries providing local expertise and insights on technology markets.

English literacy of a significant number of Chinese people does not form a barrier in accessing worldwide Internet information. Since most of the websites on the Internet are still written in English, a pressing concern of the moment is that of how to meet an increasingly high demand from Chinese netizens for accessible content, namely content in Chinese. It seems that building up national networks and providing most of the content of the portals are the only viable options available to the Chinese government.

By December 2003, after nearly a decade's efforts, China had owned 595,550 websites registered with the domain name of .cn. All of these websites are available to seventy-nine million net users through 30.9 million computers connected to the Internet. These are the parameters of Chinese users' designated protected environment; this is what Hartford calls "a safe sandbox environment" (2001). This is also an environment Chinese users desire. By providing "safe and healthy" content to meet the people's demands, China's policy seems to have succeeded. CNNIC's yearly report shows that more users are satisfied with the amount of Chinese content available on the net. According to its surveys, the percentage of users discontented with Chinese content in 1997 and 1998 was over forty-five percent, but this decreased to nine percent in 1999 and in the latest survey conducted in January 2004, this percentage had decreased even further to 2.5 percent (2004). Among all the national networks, Sina.com, Sohu.com, and Netease.com have become the largest and most successful portals, enjoying great popularity among net users across the country.

Based on all the discussions in this chapter, my thesis arrives at the following

conclusions: first of all, to make sure all the prisoners (netizens) in the panopticon (cyberspace) have access only to the "safe and healthy" information, China imposed "the Great Firewall" to websites, emails, and search engines on the Internet. Although it is still not yet explicitly known how the government traces and detects some offenders with the firewall system, it is doubtless that this system is powerful enough to frighten the vast majority of the common netizens. Secondly, to occupy the propaganda play ground and to meet people's high demand for accessible content on the Internet at the same time, China has made great efforts in building up national networks that are inundated with government-approved content. To my understanding, by making the panopticon a comfortable and satisfying space the prison's defensibility can be strengthened.

My research does support the claim that some technical anti-control measures can be used to get around the "Great Firewall". However, it must be recognized that each of these measures suffers from some fatal drawbacks. For common Chinese netizens, the money or technical knowledge required to get around the "Firewall" are distinct barriers. For instance, it is possible to dial into a foreign ISP but this is such an expensive solution to the "Firewall" that few Chinese netizens can afford it. On top of this, technical knowledge is needed to use encryption, a proxy server or any other method to evade the blocks of government control. Depending on some free services on the Internet is also not a viable option because as the Internet becomes more commercialized over the last few years these free services are harder to maintain (Tsui, 2001). To sum up, in my opinion, the war between governmental control and

anti-control forces in China is a long-term battle. At the moment, in any case, there is little sign that the Chinese government will ultimately lose.

Chapter Five

Social, Cultural and Economic Measures

Legal, administrative, and technical measures are visible, and firmly fixed. Social norms, lack of privacy awareness, and the newly developed value orientation of recent years are like "invisible and gentle hands" that help strengthen the government's control over the Internet. In this chapter I will first concentrate on the above topics. Chomsky notes in *Necessary Illusions* that for the media, "to confront power is costly and difficult" (1989. p.8). This is absolutely true. In China, for Internet corporations, especially those ICPs, to confront government means no business. To maintain their business, all the Internet-related companies conform to government regulations. Similarly, to grab the largest possible share of the global market, transnational companies supply China with sophisticated technology or are directly involved in helping the government build a national Internet firewall, leaving their pursuit of democracy at home. Market economy has its own laws. The second part of this chapter examines how the Chinese government takes advantage of market laws to strengthen its Internet business management and to arm itself with advanced technologies.

Social Norms

Social norms differ depending on the community and culture in which they

operate. A universal example of social norms regulating behavior is watching porn in a public place, such as an Internet cafe, an act that is generally frowned upon. Statistics from CNNIC survey in January 2004 shows that 66.1 percent of users access the Internet at home, 43.6 percent at work, 18.4 percent in school and 20.3 percent from Internet cafes (this is a multi-choice question) (CNNIC, 2004). Although the trend is growing towards access at home as more people can afford to buy PCs, in the short run, work units and Internet cafes will remain the most common places for users to access the Internet. Accessing the Internet from a public place puts users in a vulnerable position because social control in public is much stronger than in private. The sense of being watched in public can work as a deterrent to accessing or spreading socially unacceptable materials, not only porn but also the politically unacceptable ones.

Meanwhile, like other Chinese regulations or policies, online social norms have Chinese characteristics. The BBSs help with observing how the Chinese government uses social norms to regulate Internet users' behavior. As mentioned in the hierarchical administration structure, every news forum or BBS has its own boardmaster. They are responsible for weeding out messages that are not in line with government policy, news forum policy or those that are off-topic. Besides the boardmasters, the online community itself also influences what one can say in the BBS. Community members can keep each other in check and correct behavior when needed. For example, within the community, netizens often used "hanjian" (; j) which translates as "traitor of the Chinese people" and has a strong negative

connotation to label people who were sympathizing with the Americans in the spy plane incident of April 2001. Upon finding a person labeled as a "hanjian", community members rallied together to attack them, making them feel too ashamed to publish any more pro-American postings. The boardmaster sometimes stepped in when things got out of hand, calling for an "orderly and rational discussion" (Qiu, 2001). This example indicates clearly that the community itself was chastising and censoring those who did not conform. People in the online community still need to conform to the moral order to maintain the harmony of the community or risk being flamed and becoming an outcast.

Privacy Awareness

Before 1980s when China adopted the reforms and opening-up policy, Chinese people knew little about privacy. What's more, in China, the notion of privacy has long been conceived of as a typical product of Western society. Noble-minded people, in China's culture, were expected to do everything with brightness, fairness and straightforwardness instead of holding something back. People should not have anything that cannot be spoken about in public. As Stephen Lau, former privacy commissioner for personal data in Hong Kong said, "We didn't have the word 'privacy' in the Chinese vocabulary until relatively recently... We had no words for 'privacy' because it was never in our culture" (Tsui, 2003). Things have changed somewhat since the 1990s. However, although comprehensive works have been written and published on privacy and the implications of information technologies in

the West, the lack of research on Chinese privacy studies, if such a discipline exists, has been glaring. Currently, almost no work exists that deals with the concept of privacy in a specific "Chinese" context, let alone online privacy in China. In other words, research on online privacy in modern China and, in specific, the implied impact of information technologies, has been almost non-existent.

Lack of common people's privacy awareness is likely responsible for this.. For the same reason, Western issues, such as governments' infringements upon privacy through the Internet, will not likely be an issues of concern for the Chinese public. The following case may be a good comparison. In April 1999, Singapore's state-sponsored telecommunications monopoly, SingNet, made a public apology for intruding into its subscribers' personal computers in the name of "virus scanning" (Sessor, 1999). 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 shows that Singapore's Internet regulation respects citizens' right to privacy, at least while facing the public, and the regulatory body permits bottom-up resistance. However, neither of these characteristics exists in China's virtual censorship. Only two months later, as I mentioned in Chapter Three, Lin Hai, a computer engineer from Shanghai was sentenced to two years in prison for providing a number of email addresses to a US-based online pro-democracy magazine. During this case, China seemed unconcerned about exposure of the fact that the government actively monitors

personal email, or the possible bottom-up protest against this action. In fact, people at that time were not even aware of the privacy rights they should enjoy legitimately.

Things have not changed greatly. A Beijing-based company set up a personnel database that functions as a blacklist for bad employees. Company officials claimed that their service met a great market demand. More than 10,000 corporations applied to make use of this database immediately after the service was launched (Zhou, 2001). This is an issue that will become paramount with the increasing capacities of database. The possibility of linking databases will certainly appeal to the central government, which is exactly what they are trying to achieve with some of the Golden Projects. As I have also mentioned in Chapter Three, ICPs are required to keep records for sixty days of all information posted on the websites and bulletin boards. ISPs should maintain users' records for sixty days and provide them to the relevant state authorities when required. Special facilities were installed to trace how long users were online, from where they logged on and what websites they visited. Since there are still no laws in China determining exactly what records are too private for release, things that would be impossible in the West met with little protest in China, sometimes no disagreement at all.

Value Orientation in Contemporary China

Value orientation refers to an individual's preference for a value system. The preference is a psychological state and behavioral pattern underlying all domains of beliefs, perceptions, opinions, attitudes, actions, and lifestyle. In societies undergoing

a dramatic transition, there are often several major value orientations competing for followers. China is a country of this kind that has witnessed unprecedented political and social changes over the past decades. Jonathan J. H. Zhu and Zhou He, in 2000, conducted a survey attended by 2,600 adults in Beijing and Guangzhou on value orientation change in Mainland China. According to their study, Communism, defined as selfless dedication to the well-being of society and mankind, starting from the 1980s when CCP began to embark on economic and structural reforms and improve the standard of living for Chinese citizens, unexpectedly invited the rise of Materialism. Undoubtedly the predominant value orientation for the Chinese populace between the 1950s and 1980s, Communism, has increasingly lost popularity over the past twenty years (He, 2000a). In contrast, Materialism has had a completely different journey. This value orientation, defined as a persistent pursuit of immediate rewards and physical happiness, had been a notorious symbol and disappeared almost completely from the public discourse as the CCP launched one campaign after another to divest private ownership, assault self-concern and self-rewarding behaviors, and promote non-materialistic values. However, it returned in the 1980s when the Chinese people were allowed to seek well-being for themselves. Zhou and He's observations of the ideological landscape in China have revealed that Communism has become the least popular value orientation among Chinese audiences, whereas Materialism has been adopted by a significant portion of the populace. As a matter of fact, Materialism has already taken the place of Communism and become the most influential value dominating Chinese daily life (He, 2000b). It is easy to understand why the

Communist slogan "Looking Forward (и ? в pronounced as xiang-qian-kan in pinyin)" has been replaced by the Materialistic motto "Looking For Money (и а в pronounced also as xiang-qian-kan)".

Coming back to Internet development in China, I notice that while many argue that the freedom brought to China by the Internet will act as an incentive to organize a democracy movement, there is a more compelling argument that "few people care to challenge the ruling regime during the present period of economic and political stability" (Hartford, 2001). Why does the second viewpoint hold water? On the one hand, Chinese people's apathy to politics or democracy can be partly attributed to what they have suffered and the lessons they have learned from all previous political movements such as the Cultural Revolution (1966-1976) or the Tiananmen massacre 1989. Fear keeps people from getting involved in political issues. As well, the value orientation change among the Chinese is a major factor. Materialism has most Chinese now more concerned about whether their clothing, food, housing, travel and other basic demands for a well-to-do life are satisfactorily met. Politics and democracy, including the possibility of free flow of information on the Internet, to some extent, are not their concern. As long as their stable jobs and incomes are guaranteed by the government, it is absolutely unnecessary for them to care about what measures the government takes to control the Internet or how to resist the government's control, let alone to struggle for building up a so-called democratic nation as described by the West. As Pfaffenberger points out "almost all Internet users have powerful incentives to support the government and to refrain from voicing any

criticism". In China, those incentives can be interpreted partly as enjoying and lengthening the most stable and peaceful, therefore the rarest time in China's history to a maximum degree and making a good living within this period of time. Chinese people began to realize that the more stable society is, the more profit they can make. A society of political conflict in the past left them with a backward economy and endless poverty. People are inevitably apathetic to political movements. They are not willing to tolerate social turbulence as in the past. That may also explain why "despite the technical possibility of accessing banned sites, the flow of external Internet access is best described as a mere trickle". Blocked sites such as Human Rights in China and China News Digest report "receive only a few dozen hits per week from within China" (2001). Oliver Kwan of Netease says that the chatrooms are "contrary to what people in the West have imagined", for most of the time "there's very little negative or political material posted...The hottest bulletin boards are love and relationships" (Sinclair, 2002). It would seem that, much like the rest of the world, Chinese Internet users are more interested in entertainment rather than politics, stocks and shares rather than revolt, and cyber-dating rather than secret society-forming. Individually oriented materialism displays its tremendous power in influencing people's preferences, leading them to pay attention to nothing but those which bring immediate profits or physical pleasures. Hachigian maintains that "the Net can not create rebellious social forces" (2001), but can only nurture those that are already there. Chinese Internet users have

> little incentive to use the network for seditious purposes...(netizens know that they) have little to gain from undertaking actions that would lead the

> government to crack down on the Internet; in contrast, their futures depend on rapid Internet growth and keeping out of trouble with the government (Pfaffenberger, 2001).

Indeed, the growing economic significance of networked information and the exploitation of real or imagined threats (from minor hacker damage on websites to national security perils) may elicit—as it already has in some developed countries—user acquiescence to tighter government controls. A combination of fear of punishment, contentment with the current situation and potential benefits, and apathy to politics will prevent the Internet from being used to its full advantage in bringing democracy or more political transitions to China, a quite necessary result of the Internet's advent in this country assumed by the West.

A Minor Attack in Words but A Major Help in Deeds

(ж t ю к)

Some Chinese intellectuals want to make the Internet a communication medium that can promote political reform and free speech. In recent years, they have been surprised to see one or two websites in China regularly post frank critiques of Chinese society, the Party and the government. Wenxuecity.com is a website of this kind. More surprisingly, the government did not smother this website as before. Wenxuecity.com has survived and prospered.

Likewise, in recent years, despite stringent content controls, it is not unusual to find sharp critiques against the Party and certain government policies posted on *Strong Country Forum* that was sponsored by *People's Daily*, the Party's highest

propaganda organ. Following the "Strong Nation Forum", almost all government controlled online media set their own BBS for netizens to air their views. Take for example, the Development Forum run by *Xinhua News Agency* (http://forum.xinhuanet.com), Chinese Youth Forum run by the *Chinese Youth Daily* (http://202.99.23.162/index.php), Oriental Forum run by Shanghia Municipal Government (http://bbs.eastday.com/index.jsp), Jinghua Forum of *Qianlong News Network* run by Beijing Municipal Government (http://bbs.qianlong.com/bbs.jsp), etc. More importantly, messages posted on these BBSs are quickly spread among net users and through them to a wider community in reality.

But these forums were not shut down. Sometimes they became more transparent. On December 10, 2000, the World Human Rights Day, *Strong Country Forum* invited two members of China's Human Rights Research Association to hold an online discussion session on human rights and democracy. During the discussion, opinions from multiple perspectives were exchanged and heated debates occurred. This might be the most lively human rights discussion in China with the largest number of participants in history (Report from U.S. Embassy in Beijing, 2001). Contrary to some Chinese conservatives expected, the government lost nothing by allowing this discussion, instead, it won public approval for regime's tolerance to a wide diversity of opinions on human rights issue. People from every walk of life were delighted to voice their viewpoints, some of which were undoubtedly prohibited from being publicized in the past.

Examining this issue through a cultural perspective, I find that the online

critiques are--a minor attack in words but a major help in deeds (ж t ю к). This longstanding Chinese philosophy can partly explain why the government allows the above-mentioned to happen. As I have discussed in Chapter Two, by allowing a couple of critical websites or forums to exist, the government gives people a place to vent their anger and dissatisfaction. By doing so, it gains a channel to learn what citizens are thinking and can take necessary steps to quell possible unrest through the mass media. In addition, being able to vent anger through words in some public places, to some extent, reduces the possibility of fierce rebellion through grassroots action. CCP also realized that for recognition from the international community and also to seek credibility as a player on the world stage, more tolerance must be given to voices undesirable to the party. Freedom to voice disagreements can be interpreted as progress the government makes in promoting democracy. Tolerance of disagreement helps it not only win applause from Chinese citizens, but also score points in improving its international image.

Nevertheless, to the government, making sure the critical websites or forums are still controllable and limiting the critiques within acceptable range are prerequisites to delivering tolerance. That means, the government still enjoys the final say in web content and is able to censor any content it regards as unacceptable to the regime. Like its management over other Internet communities, it can impose punishment or suspension on violators anytime the government finds they go beyond its maximum tolerance. Under this principle, the inclusion of different voices on websites or forums may therefore serve as a new method to dampen political communication in

unlicensed virtual spaces. Monitoring a couple of licensed critical websites featuring complaints to the government on the whole is much easier and feasible than tracing and struggling with numerous potential opponents.

"Business Is the Primary Objective"

I have mentioned in previous chapters that portals, such as Sina.com and Sohu.com, had partnerships with Western media companies Dow Jones and Reuters, but both stopped publishing non-financial news after a warning from the central government. They also stopped carrying news that was not officially state-sanctioned, fearing a loss of licenses. Discarding these news sources does not mean they are insignificant. Tony Zhang, CEO of Chinanow.com commented, "nobody wants to irritate the government if business is the primary objective" (Tsui, 2001).

Since the basic principle behind the concept of Internet regulation in China is that "one is responsible for what one publishes", internet-related companies practice a high degree of self-censorship to protect themselves from possible punishment. Self-censorship is also necessary to gain the trust and cooperation of the government. Almost all the ICPs and Internet Cafes have issued their own sets of guidelines for both users and administrators. The Sina office even has a direct hotline to relevant officials who help clarify when the policy is unclear and warn in advance on sensitive topics, making sure that Sina will not offend the government at any time (Heim, 2000). Foreign Internet companies employ different means to build their relationships with the government. I have mentioned in Chapter Three, that hundreds of companies in

China's Internet, including famous foreign ICPs such as Yahoo!, signed a "Public Pledge on Self-discipline" in 2002, expressing willingness and determination to regulate their information dissemination, chat rooms and BBSs in accordance with China's laws and regulations (CNET, 2002). Yahoo!'s eagerness to placate the Chinese government does not begin and end with the online news, chat rooms or BBSs. It extends to search engines. My experience is that a search on Chinese Yahoo! using the phrase "Taiwan independence" or "Falungong" as keywords would show no results. Yahoo! China has its own explanation, "We are not a content creator, just a medium, a selective medium" (Gutmann, 2002). On the one hand, Yahoo! China had no choice but to obey the rules; on the other hand, it did so of its own accord to cement its relationship with the government and secure its overwhelming popularity in Mainland China. It is also interesting to note that Yahoo! China "rejected an attempt by VOA to buy ad space" (Gutmann, 2002). Undoubtedly, this is an action expected and welcomed by the Chinese government who has long regarded VOA as a notorious propaganda agency used by the West to promote their so-called freedom and democracy in Asian countries. Similarly, AOL-Time Warner, shareowner of China.com (McDonald, 2001), is eager to gain further entry into the lucrative market and has been "weighing up the pros and cons of informing on dissidents if the Public Security Bureau so requests" (Gutmann, 2002). It appears that AOL-Time Warner thinks it is worthwhile to eliminate any doubts of the Chinese government to pave the way for economic development, at the cost of free speech and democracy. These companies simply adapt their religions to the specific environment they are involved

in China. Once again, "business is the primary objective".

"It's Not the Gun But the Way It's Used"

In the 1980s, the U.S. did not allow any socialist country to have Internet access. It took China almost eight years to be linked up with the worldwide Internet. As in many other fields, developed countries' high-tech protection policies made it hard for China to get the latest and the most advanced information technology. In recent years, however, the U.S. relaxed its export restrictions for advanced technology, as foreign policy set by Clinton and continued by George W. Bush is based on the belief that once China enters the world market, democracy will flow into China (Tsui, 2001). The latest example of the relaxation of U.S. export control policy is the case of encryption technology. U.S. companies are now allowed to export any encryption technology to individuals, commercial firms or other non-governmental end-users in any country, including China (U.S. Bureau of Industry and Security, 2003). As a practical result of this policy relaxation, China is able to import advanced technology it needs for developing the Internet, including technology that enables Internet control such as monitoring and surveillance tools.

Consequently, the late 1990s witnessed a great number of technologies from the United States used by China to build up its Internet infrastructure. Eager for a slice of this largepie, the major global networking companies--Sun Microsystems, Cisco Systems and Bay Networks, among others--cheerfully competed to supply the gear to make this construction possible. Sun Microsystems obtained a US$15 million deal to

build the Intranet backbone of the China Wide Web in December 1996 (Kristi, 1996). 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 (*South China Morning Post*, 1997).

Building a national Internet firewall and strengthening its Internet control as well cannot be achieved by China on its own. Taking advantage of the global market competition, China relies a lot on Western companies to supply sophisticated technologies to meet its targets. The Golden Shield Project shows what is possible when Western companies meet the Chinese government against a background of fierce market competition. This Project was started in 2000 by the government to facilitate "the adoption of advanced information and communication technology to strengthen central police control, responsiveness, and crime combating capacity, so as to improve the efficiency and effectiveness of police work" (Chen, 2000). In the same year, the Security 2000 exhibition was held in Beijing for multinational companies to display and promote sales of their information technology to the Golden Shield Project. Here Fortune 500 companies, such as Sun, Hewlett-Packard, Compaq and Cisco, and a whole group of lesser-known Silicon Valley companies such as Websense were anxious to do business with the Chinese government (Marshall & Kuhn, 2000). Websense is a company specializing in systems that block access to websites. The software is, of course, not designed with authoritarian regimes in mind, but is used by corporations to monitor and restrict access for employees to

inappropriate websites such as porn websites. As Websense spokesman Ted Ladd states, "We have no control over the categories of websites customers choose to block. It's up to them" (Marshall & Kuhn, 2000). In other words, Websense does not care about how its product is used, even if it is used by the Chinese government to block websites undesirable to authoritarian regimes. Today, this is a business philosophy followed not only by unknown companies striving for its survival, but also by almost all the IT giants. For example, Cisco Systems developed a router device, integrator, and firewall box specially designed for the government's telecom monopoly. These devices have been sold in thousands to China, making it easier for Chinese cyberpolice to intercept and look into the information sent around the Internet. David Zhou, a Cisco engineer, said in an interview with Gutmann "We do not care about the Chinese government's rules. It's none of Cisco's business." Gutmann further commented, "It's not the gun but the way it's used, and how can a company that builds firewalls be expected to, well, not build firewalls?" (2002). Only one company with a track record with the Chinese government has refused to do business out of "ethical motives" and that is InfoGlide (Hartford, 2001). InfoGlide sells a technology that is able to search and detect patterns in huge databases. It refused to deliver this technology to China, but the question is, how many others did? Endeavoring to grasp market share as much as possible, few of them would do as InfoGlide did. As Bryan Pfaffenberger points out, the "regime is getting plenty of help from foreign investors and IT corporations, who leave their high-minded, free speech ideals at home" (2001).

China's target and demand became more specific and straightforward as time

passed. According to Gutmann, China Telecom had rounds of discussions with an Israeli company called iCognito in 2001, which invented a program called "artificial content recognition". Similar to but more mature than Websense's product, the software learns which sites to filter as the user surfs the Internet. It was designed to filter gambling, shopping, job search, pornography, stock quotes, or other non-business materials. But the first question from their Chinese buyers is invariable: Can it stop Falungong? (2002)

It might be unfair to accuse these foreign companies of selling firewall or Internet technologies to China so the cyberpolice can use them for political purposes. Some deals were first announced as targeting at network crimes such as online pirating. Moreover, political consideration can never become the only, or most important factor in the global market. More often than not, business is the primary influence.

There is a tendency in market competition that a new technology will quickly overtake another one. In February 2002, a new piece of software called "Peek-a-booty" appeared. It promised to "circumvent government censorship" (Knight, 2002). But iOpus Software announced shortly after that their newly launched STARR monitoring software could easily detect the use of Peek-a-Booty on a computer (Reuters, 2002). To meet endless market demands, Western businesses offer not only control-oriented technologies but also anti-control-oriented ones. New products target consumers from two different standpoints come into the market one after the other, stimulating upgrading and optimization. Countries like China can

profit a great deal from the competition. What they need to do is just to keep a close eye on the upgrading to get technologies that best serve the regime's interests.

Still using Foucault's Panopticon theory to examine China's cyberspace, I can draw the following conclusions based on discussions in this chapter: Within the Panopticon, prisoners (netizens) keep each other in check and correct behavior to make sure everyone conforms to the basic social norms (prison regulations) so that the harmony of the Panopticon can be protected. The sense of being watched by other prisoners works as a deterrent to accessing unacceptable material; Lack of privacy awareness makes the prisoners almost completely ignorant of the right infringement committed by the guards (the regulatory body and the government); Materialism makes the prisoners pay attention to merely their basic living requirements, and apathetic to make great changes about the order or the situation of the Panopticon; The guards sometimes allow prisoners to have a couple of small-scale assemblies where they can voice their dissatisfaction within an acceptable range. In Chinese vocabulary, this is a Win-Win (ΦT) situation meaning that both the prisoners and the guards benefit from the limited freedom, in this case, I believe the latter gets more.

In *Capitalism and the Information Age*, Edward Herman argues that there is no evidence for the Internet as a supporter of interactive democratic media. He said, "although the new technologies have great potential for democratic communication, left to the market, there is little reason to expect the Internet to serve democracy" (1998. p.201). I believe my analysis about the power of the market in this chapter works as a good annotation of Herman's remarks.

Conclusion

The Internet arrived in China in 1987 on a rather small scale but has grown exponentially ever since and continues to do so. The Chinese government has a mixed reaction towards the development of the Internet. On the one hand, it recognizes that the Internet is an important carrier for China's social, cultural and economic development. Chinese leaders have stated on numerous occasions that since China reacted too late to the Industrial Revolution, they definitely do not want China to miss the Information Revolution. As a result, they call for all levels of government to realize that the application of network technologies and the construction of the Internet is a fundamentally important task. On the other hand, the Chinese government keeps warning that the Internet itself has become a "domestic and international battlefield for ideological struggle" and that "enemy forces at home and abroad will spare no effort to use this battlefront to infiltrate China" (Lin, 2001). Indeed, tension between Chinese government's desire to exploit business opportunities brought about by the digital revolution and its concern about the possible unwanted political consequences constitutes the central issue of the Chinese Internet development. In the past decade, compared with western countries, Internet development in China has shown "Chinese characteristics". The Chinese government's policies towards the Internet are polarized. While actively promoting business-related Internet development, China has also tried to control the use of the Internet. In other words, China has gone to great pains to strike a balance between its

desires and anxieties.

This thesis starts with a quotation from Clinton, saying that the Internet is impossible to control. In his and other Westerners' opinions, the Internet is bringing new means to evade state control, and it will break down the information monopoly of the Chinese government. They believe that the Internet will function as a political Trojan horse, and will bring democracy to any authoritarian regime and eventually help overthrow those regimes. However, my research on the development and control of the Internet in China suggests that this argument does not hold water. To date, no cyberspace can exist without tangible subsistence such as devices, technicians, users and the sociopolitical context in which all these non-virtual components are put together to create and support the virtual world. When the Chinese government imposes legislative, administrative, technological, social and economic measures to control the subsistence of the cyberspace, the latitude of the Internet is constrained. My analysis in this thesis indicates that the current measures the government has taken are quite effective in preventing users from accessing prohibited content, from making use of the Internet as a communication tool to set off political movements, and from promoting so-called democracy and freedom across the country, let alone overthrowing the regime. The government is not powerless in its effort to control the Internet.

It is appropriate to draw a few conclusions from what I have presented in this thesis. China has a long censorship history and CCP has a long-standing tradition of strict control over the media. As a part of the mass media, the Internet has not been an

exception, being subject inevitably to censorship. China's deeply rooted attitude towards foreign technology, its judgment about the current international situation and its social consideration leave it determined to control the use of this new medium. The CCP has exerted various constraints upon the Internet: laws and regulations are issued and enacted; the Great Firewall is constructed; the hierarchical regulatory body is established to further exclude users that are politically unreliable and contents that are ideologically undesirable; and intimidation serves to remind Internet users that they are monitored and action can be taken against them anytime. In addition to the pursuit of economic gain, the government is using the Internet for its own political advantage. In particular, the regime, with the help of the Internet, is seeking to streamline many of its government operations through networked information management, distribute propaganda and promote nationalism online at the national and local levels, and consolidate Beijing's central authority through more efficient communication with provincial governments. There are clear signs that the Internet serves the purpose of the regime as much as it helps loosen government controls over freedom of expression and the daily life of citizens (Dalpino, 2000).

Besides, prying eyes can help prevent one from wandering too far from the socially accepted standard, Internet businesses self-censor themselves out of commercial interest and market competition and technology updating enable the government to monitor each individual user. Lack of awareness of privacy issues mean that control measures impossible in the West are feasible in China. Low English literacy forms a barrier to users' access to worldwide Internet content. Requirements

for money or technical knowledge stop countermeasures from being used to their full advantages. These all constrain the liberalizing effects of the Internet.

Despite these constraints, we cannot overlook the fact that since the emergence of the Internet in China, Chinese society has witnessed an unprecedented free flow of information, more discussion, and more openness. It is evident that the Internet offers a faster and more convenient channel for the Chinese to gain access to Western culture and products. They can sometime participate in online interactions to voice their anger or dissatisfaction with the government as long as their comments are within an acceptable range. All these were impossible, even unimaginable in the past when traditional mass media functioned only as the Party's "throat and tongue". These will absolutely be constructive to build up a government with more democratic characteristics. In light of these facts, this thesis should not be considered a total denial of the Internet's function on promoting democracy. Instead, this thesis seeks to modify the hypothesis that the diffusion of the Internet invariably brings about the decline of authoritarian regimes in the nation-states. Hartford has said,

> Smart authoritarians do not try to control everything; they focus on controlling what really matters...keeping the vast majority from politically sensitive areas, and preventing the nonconforming small minority from organizing enough to mount a challenge. The imperfect controls that already exist, even applied with the velvet glove outermost, are sufficient to move the vast majority (2001).

My study found that China's Internet, in retrospect, has taken a route of development deviating from its anticipated mission of democratization since the Chinese government is clever enough to make imperfect controls sufficient. As a result, the Internet has not paralyzed the Chinese authorities as yet. In contrast, it serves the

regime as much as it helps to loosen governmental control over freedom of expression and the everyday life of its citizens. It remains uncertain whether Internet control in China will become more menacing or less so. In the short term, however, it seems that China is still determined to control the Internet which may in fact help strengthen the Party's hold over the people. The Chinese government's expectations and fears about the Internet mean it will continue to walk a delicate balance between promotion and restriction, between investment and clampdown and between encouragement and deterrence. However, everything is still under the government's control. The Panopticon still exists.

Bibliography

Books & Articles

Alan, H. (1999). *Contemporary China.* New York: St. Martin's Press.

Bennett, W. L. (1998). (2nd Ed.). *News: The Politics of Illusion.* New York: Long-man.

Blum, W. (2000). *Rogue State: A Guide to the World's Only Superpower.* Monroe: Common Courage Press.

Bristow, D. (2000, February). Cyber-warfare rages across Taiwan Straits. *Jane's Intelligence Review.* pp.40.

Brodsgaard, K.E., & Strand, D. (Eds.). (1998). *Reconstructing Twentieth-Century China: State Control, Civil Society, and National Identity.* Oxford: Clarendon Press.

Chai, C. H. (1997). *China: Transition to A Market Economy.* Oxford: Clarendon Press.

Chandler, C. (2001, April 18). For Chinese pilot, martyrdom on earth and in cyberspace. *The Washington Post.*

Chang, W. (1989). *Mass Media in China.* Ames: Iowa State University Press.

Cheng, Y. S. (1998). *China in the Post-Deng Era.* Hong Kong: Chinese University Press.

China Communication News. (1998 Mar). *Policy and Regulations.* pp.45-49.

Chomsky, N. (1989). *Necessary Illusions.* Boston: South End Press.

Chomsky, N., & Herman, E. S. (2002). *Manufacturing Consent.* New York: Pantheon Books.

Cohn, M. R. (2001, July 21). China seeks to build the Great firewall. *Toronto Star.*

Colin, M. (2001). *The New Cambridge Handbook of Contemporary China.* Cambridge, UK: Cambridge University.

Cullen, R., & Choy, P. (1999). The Internet in China. *Columbia Journal of Asian Law,* 13. pp.99-134.

Deibert, R. J. (1997). *Parchment, Printing and Hypermedia: Communication in World Order Transformation.* New York: Columbia University Press.

Edmonds, R. L. (Ed.). (2000). *The People's Republic of China after 50 Years.* Oxford: Oxford University Press.

Fang, B. (1998). Chinese "Hacktivists" Spin a Web of Trouble: The Regime is Unable to Control the Internet. *U.S. News and World Report.* pp.47.

Far East Economic Review. (2001, September 21). *Chinese Organ Screens Web Site.*

Foster, W., & Goodman, S. E. (2000). *The Diffusion of Internet in China.* Center for International Security and Cooperation, Stanford University.

Foucault, M. (1995). *Discipline and Punish: The Birth of the Prison.* New York: Vintage Books.

Gernet, J. (1996). (2nd Ed.). *A History of Chinese Civilization.* New York: Cambridge University Press.

Guangzhou Daily. (2001, May 11). *Military Expert Comments on "May Day" Cyber War between China and the United States—Interview with Zhang Zhaozhong.*

Guo, Y. J. (2004). *Cultural Nationalism in Contemporary China: the Search for National Identity under Reform.* New York: Routledge.

Hachigian, N. (2001). China's Cyber-Strategy. *Foreign Affairs*, 80 (2).

Hamrin, C. L. (1990). *China and the Challenge of the Future.* San Francisco: Westview Press.

Harvard International Review. (2001). *Speaking Out: The Internet in China*, 23, pp.7-8.

He, Z. (2000a). Chinese party press in a tug of war: A political-economy analysis of the Shenzhen Special Zone Daily. In C. Lee (Ed.) *Money, power and media: Communication patterns in cultural China* (pp. 112-151). Evanston: Northwestern University Press.

He, Z. (2000b). Working with a dying ideology: Dissonance and its reduction in *Chinese Journalism Studies*, 1, pp. 599-616.

Herman, E., & McChesney, R. (1998). *Capitalism and the Information Age.* New York: Monthly Review Press.

Hill, K. A., & Hughes, J. E. (1998). *Cyberpolitics: Citizen Activism in the Age of the Internet.* Lanham, MD: Rowman & Littlefield.

Hoyt, O. (1970). *Censorship in America.* New York: Seabury Press.

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

IPI Survey. (1959). *The Press in Authoritarian Countries.* Zurich: International Press Institute. No.5.

Jansen, S. C. (1988). *Censorship: The Knot that Binds Power and Knowledge.* New York: Oxford University Press.

Lee, J. (2001, August 30). United States Backs Plan to Help Chinese Evade Government Censorship of Web. *New York Times.*

Legal Daily. (2001, June 4). *Police from Various Regions See Success in Clearing "Web Bars".*

Lewis, A. (1987, November 26). *Freedom of the Press -- Anthony Lewis distinguishes between Britain and America.* London Review of Books.

Lieberthal, K.(1995). *Governing China: From Revolution Through Reform.* New York: W.W. Norton.

Li, K. (1995). *A Glossary of Political Terms of the People's Republic of China.* Hong Kong: The Chinese University Press.

Lin, B.J., & Myers, J. T. (1996). *Contemporary China in the Post-Cold War Era.* Columbia, SC: University of South Carolina Press.

Lin, G. & Hu, X. B. (2003). *China after Jiang.* Stanford, Calif: Stanford University Press.

Li, T. (1990). Computer-mediated communications and the Chinese students in the U.S.. *Information-Society*, 7, pp.125-137.

Lipschutz, R. (1992). *Reconstructing World Politics: The Emergence of Global Civil Society.* Millennium: Journal of International Studies, 21 (3). pp. 398-420.

Litan, R. E., & Niskanen, W. (1998). *Going Digital! A Guide to Policy in the Digital Age.* Washington, D.C.: Brookings Institution Press and Cato Institute.

Liu, H. (1998). Profit or ideology? *Media, culture & society, 20* (1), pp. 31-41.

Lynch, D. (1999). *After the Propaganda State: Media, Politics and "Thought Work" in Reformed China.* Stanford, CA: Stanford University Press.

Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life.* Buckingham, Philadelphia: Open University Press.

Mao, Z. (1961). A talk to the editorial staff of the *Shanxi-Suiyuan Daily.* In *Selected Works of Mao Zedong.* Beijing: Foreign Languages Press. Vol. 4.

Mao, Z. (1967). Talks at the Yanan forum on literature and art. In *Selected Works of Mao Zedong.* Beijing: Foreign Languages Press. Vol. 3.

McClellan, G. S. (1967). *Censorship in the United States.* New York: H.W. Wilson Co..

McConnell, G. (2001). The expansion of English as a language of science and communication: east and southeast Asia. In U. Ammon (Ed.). *The Dominance of English as A Language of Science: Effects on Other Languages and Language Communities.* Berlin, New York: Mouton de Gruyter. pp.119.

Neuman, R. (1992). *The Future of the Mass Audience.* London: Cambridge University Press.

Olga, G., & Hoyt, E. P. (1970). *Censorship in America.* New York: The Seabury Press.

Orwell, G. (1992). *1984.* New York: A.A. Knopf.

Peleg, I. (Ed.). (1993). *Patterns of Censorship around the World.* Boulder, Colo.: Westview Press.

Perry, E. J., & Selden, M. (Eds.). (2000). *Chinese Society: Change, Conflict, and Resistance.* New York: Routledge.

Plato. (1961). *Laws.* London: Heinemann.

Plato. (1987). The *Republic.* London: Penguin Books.

Reuters. (2002). *STARR- the Anti Peek-a-Booty Software.* Taken from *In China, the Net Grows Up: To Avoid Censors, "Web Worms" Police Themselves.*

Riley, G. B. (1998). *Censorship.* New York: Facts On File, Inc.

Scammell, M. (1988). Censorship and Its History-A Personal View. In Kevin Boyle (Ed.). *Article 19: Information, Freedom, and Censorship (World Report 1988).* New York: Times Books.

Schell, O. (1995). Maoism vs. Media in the Marketplace. *Media Studies Journal,* 9 (3).

Schurmann, F. (1966). *Ideology and Organisation in Communist China.* Berkeley: University of California Press.

Sessor, S. (1999, May 7). SingNet apologised for virus scanning. *Asia Wall Street* Journal.

Sikkink, K. (1993). Human Rights, Principled Issue Networks, and Sovereignty in Latin America. *International Organization,* 47. pp. 418.

Sinclair, G. (2001). Do Falungong's origins in popular religious tradition provide an alternative definition of "Chineseness" which threatens the Communist Party's present construction of nationalism? (Nationalism & Ethnicity in China-EAST 2580). *Department of East Asian Studies,* University of Leeds.

South China Morning Post. (1997, October 21). *Bay Networks Wins CWW Bid.*

Spence, J.D. (1991). *The Search for Modern China.* New York: Norton Company.

Spinello, R. (2000). *Cyber Ethics*. London: Jones and Bartlett.

Spiro, P. J. (1994). New Global Communities: Nongovernmental Organizations in International Decision Making Institutions. *The Washington Quarterly* ,18 (1). pp.47.

Tan, Z. (1995). China's Information Superhighway: What Is It and Who Controls It. *Telecommunications Policy*,19 (9), pp. 721-731.

Tan, Z., & Foster, W. (1998). Internet diffusion in P.R. China. *Global Diffusion of the Internet*, March, pp.114.

Taubman, G. (1998). A not-so World Wide Web: the Internet, China, and the challenge to non-democratic rule. *Political Communication,* 15, pp.255-272.

Teng, S., & Fairbank, J. K. (Eds.). (1963). *China's Response to the West: A Documentary Survey 1839-1923.* New York: Atheneum.

Timothy, C. (1997). *Propaganda and Culture in Mao's China.* Oxford: Clarendon Press.

Unger, J. (1996). *Chinese Nationalism.* Armonk, N.Y.: M.E. Sharpe.

Lenin, V. I. (1962). *Party Organization and Party Literature.* Moscow: Collected Works.

Wilson, H. W. (1995, January 7). China logs on to the Internet. *The Economist.*

Zhang, W. W. (1996). *Ideology and Economic Reform under Deng Xiaoping.* New York: Kegan Paul International.

Zhao, Y. (1998). *Media, Market, and Democracy in China: Between the Party Line and the Bottom Line.* Urbana: University of Illinois Press.

Zheng, C. (1994). Opening the digital door. *Telecommunications Policy*, No.18. pp.236-242.

Zheng, Y. N. (1999). *Discovering Chinese Nationalism in China: Modernization, Identity, and International Relations.* Cambridge: Cambridge University Press.

Bibliography

Online Resources

@cess censorship. (2000). *History and Definitions of Censorship.* Accessed March 1, 2004 at http://www.wam.umd.edu/~gjbush/history.html#HIS2Definitions

Amnesty International. (2000). *State Secrets—A Pretext for Repression.* Accessed June12, 2003 at http://www.web.amnesty.org/ai.nsf/index/ASA170421996

Amnesty International. (2002, November 26). *People's Republic of China: State Control of the Internet in China.* Accessed June 12, 2003 at http://web.amnesty.org/ai.nsf/Index/ASA170072002?OpenDocument&of=COUNTRIES%5CCHINA

APC. (2004). http://www.apc.org/english/index.shtml. Accessed March 13, 2004.

Barme, G., & Ye, S. (1997). The Great Firewall of China. *Wired Magazine.* Accessed July 2, 2003 at http://www.wired.com/wired/archive/5.06/china_pr.html

BBC News. (2001, March 15). *Chinese Leader Sorry Over School Blast.* Accessed July 5, 2003 at http://news.bbc.co.uk/1/hi/world/asia-pacific/1222991.stm

Black, J. (1997, June 27). Golden Projects. *CNET NEWS.com.* Accessed July 4, 2003 at http://news.com.com/2009-1033-200931.html?legacy=cnet

Bonisteel, S. (1999, November 6). *Asian Surfers Prefer Native.* Accessed July 5, 2003 at http://www.computeruser.com/newstoday/99/11/06/news6.html

Buruma, I. (1999, Novermber 4). *China in Cyberspace.* Accessed June 14, 2003 http://www.nybooks.com/nyrev/WWWfeatdisplay.cgi?19991104009F#top

Chen, J. (2000, Novermber 10). IT multinationals: willing partners to repression in China? *Human Rights China.* Accessed March 24, 2004 at http://bobson.wong.home.mindspring.com/research/china/multinationals.htm

CHINAINFOBANK. (1998, Oct 30). *Internet Users Spur Growth of On-line Service.* Accessed July 23, 2003 at http://www.chinainfobank.com

China News and Report. (2002). *Building the Treasure House of Ancient Chinese Books and Records.* Accessed February 24, 2004 at http://www.china.org.cn/baodao/english/newsandreport/2002august1/16-3.htm

ChinaNex. (2002a). *ChinaGBN.* Accessed February 1, 2004 at http://www.chinanex.com/company/internet/chinagbn.htm

ChinaNex. (2002b). *CSTNet.* Accessed February 1, 2004 at http://www.chinanex.com/company/internet/cstnet.htm

ChinaNex. (2002c). *Other ISPs.* Accessed February 1, 2004 at http://www.chinanex.com/company/internet/other.htm

ChinaNex. (2003a). *ChinaNet.* Accessed February 1, 2004 at http://www.chinanex.com/company/internet/chinanet.htm

ChinaNex. (2003b). *CERNet.* Accessed February 1, 2004 at http://www.chinanex.com/company/internet/cernet.htm

ChinaNex. (2004). *China Netcom.* Accessed March 10, 2004 at http://www.chinanex.com/company/netcom.htm

ChinaNex. (2004). *China Unicom.* Accessed March 10, 2004 at http://www.chinanex.com/company/unicom.htm

China Online. (1999, Oct 26). *China Cuts Internet Access Fees to Spur Online Growth.* Accessed July 23, 2003 at http://www.chinaonline.com

China Online. (2000, August 8). *Dependence on Foreign Hardware, Software, Net Content Concerns China, Report Says.* Accessed June 24, 2003 at http://www.chinaonline.com/topstories/000808/1/C00080701.asp

Chinaview. (2003, November 12). *Internet Changes Life in China.* Accessed March 12, 2004 at http://ecommerce.about.com/gi/dynamic/offsite.htm?site=http://news.xinhuanet.com/english/2003%2D11/12/content%5F1174514.htm

Chinese Government Online. (2004, February 6). Accessed March 8, 2004 at http://www.gov.cn/frontmanger/contant.jsp

CNET. (2002). *Yahoo! Yields to Chinese Web Laws.* Accessed July 8, 2003 at http://news.zdnet.co.uk/story/0,,t269-s2120830,00.html

CNNIC. (1996-2004). Accessed February 1, 2004 at http://www.cnnic.net.cn/en/index/index.htm

Committee to Protect Journalists. (2001). *The Great Firewall.* Accessed July 9, 2003 at http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html

Cowhig, D. (2000, December). New Net Rules not a Nuisance? *China Online.* Accessed June 20, 2003 at http://www.chinaonline.com/commentary_analysis/internet/NewsArchive/secure/2000/December/c0012016.asp

Dalpino, C. (2000). *The Internet in China: Tame Gazelle or Trojan Horse?* Accessed June 4, 2003 at http://www.brook.edu/dybdocroot/views/articles/dalpino/2000_hap.htm

Declan, M. (2001, May 9). Public: Take our privacy, please. *Wired.* Accessed July18, 2003 at http://www.wired.com/news/print/0,1294,43657,00.html

Dougan, D. (2003). *Scaling the Great Wall of E-Commerce.* Accessed July 4, 2003 at http://www.virtualchina.com

Drake, W. J., Kalathil, S., & Boas, T. C. (2000). *Dictatorship in the Digital Age: Some Considerations on the Internet in China and Cuba.* Accessed August 2, 2003 at http://www.cisp.org/imp/october_2000/10_00drake.htm

Drakos, N. (2000). *Internet Firewalls:Frequently Asked Questions.* Accessed June 5, 2003 at http://www.interhack.net/pubs/fwfaq/#SECTION00031000000000000000

Goldsmith, J. (2003). Against cyberanarchy. *Occasional Papers from the Law School the University of Chicago.* No. 40. Accessed August 4, 2003 at http://www.law.uchicago.edu/Publications/Occasional/40.html

Gutmann, E. (2002, February 25). *Who lost China's Internet?* Accessed June13, 2003 at http://www.weeklystandard.com/Utilities/printer_preview.asp?idArticle=922&R=4

Hachgian, N. (2001, April). China's cyber strategy. *Foreign Affairs*, 80. Accessed June 5, 2003 at http://www.rand.org/nsrd/capp/cyberstrategy.html

Hartford, K. (2001). *Cyberspace with Chinese Characteristics.* Accessed August 8, 2003 at http://www.pollcyber.com/ch/pubs/home.htm

Heim. (2000, September 19). China Keeps Firm Hand on Net Use. *Mercury News.* Accessed September 3, 2003 at http://www0.mercurycenter.com/svtech/news/indepth/docs/china091900.htm

Hong, L. (2003). *Chinese Government Online Project-A Reapproach.* Accessed March 12, 2004 at http://www.arts.monash.edu.au/chinese/icassets/SISU-Intern-teaching%20plan-03.pdf

Huang, Y., Hao, X., & Zhang, K. (1997). *Challenges to Government Control of Information in China.* Accessed August 19, 2003 at http://www.oneworld.org/wacc/media/china.html

Human Rights in China. (2003, September 23). *Internet Activist Li Zhi Arrested for Subversion.* Accessed February 2, 2004 at http://www.democracy.org.hk/EN/2003/sep/news_02.html

Human Rights Watch. (2003, November 30). *Internet Dissident: China Liu Di.* Accessed March 15, 2004 at http://www.hrw.org/advocacy/internet/dissidents/8.htm

Human Rights Watch Backgrounder. (2001). *Freedom of Expression and the Internet in China.* Accessed September 23, 2003 at http://www.hrw.org/backgrounder/asia/china-bck-0701.htm

James, B. (1997). *Foucault in Cybersapce.* Accessed August 20, 2003 at http://www.law.duke.edu/boylesite/fouc1.html

Jiang, Z. (2001, April 19). Explosives face stricter controls. *China Daily Online.* Accessed September 17, 2003 at http://www3.chinadaily.com.cn/en/doc/2001-04/19/content_51800.htm

Kalathil, S., Drake, W., & Boas, T. (2000, October). Dictatorships in the Digital Age: Some Considerations on the Internet in China and Cuba. *Information Impacts.* Accessed March 6, 2004 at http://www.ceip.org/files/publications/dictatorships_digital_age.asp?p=5&from=pubdate

Knight, W. (2002, February 19). Peekabooty aims to banish Internet Censorship. *NewScientist.com.* Accessed August 3, 2003 at http://newscientist.com/news/print.jsp?id=ns99991948

Konvitz. M. R. (1998, December 12). *History and Definitions of Censorship.* Accessed March 2, 2004 at http://www.wam.umd.edu/~gjbush/history.html#HIS1

Kumar. (2001, February 24). Concern about new web monitors. *Wired.* Accessed August 25, 2003 at http://www.wired.com/news/privacy/0,1848,41931,00.html

Law-lib.com. (2004). Accessed February 28, 2004 at http://www.lawbook.com.cn/

Lebowitz, R. (2001, July). Taliban Ban Internet in Afghanistan. *Digital Freedom Network.* Accessed June 9, 2003 at http://dfn.org/focus/afghanistan/Internetban.htm

Leonard, A. (1997, February 20). Chairman Rupert's Little Red Bucks. *Salon 21st.* Accessed June 4, 2003 at http://www.salon.com/feb97/21st/article970220.html

Li, H. (2003). *Internet Usage and Regulations in China.* Accessed July 28, 2003 at http://www.tukkk.fi/tjt/OPETUS/TJTS11/Arkisto/china.pdf

Li, X. (2001). *The Internet's impact on China's press.* Accessed July 25, 2003 at http://www.rthk.org.hk/mediadigest/20020115_76_10450.html

Lin, N. A. (2001). The great firewall. *Committee to Protect Journalists.* Accessed July 28, 2003 at http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html

Lovelock, P., & Petrazzini, B. (1996). *China's Golden Projects: Reengineering the*

National Economy. Accessed August 20, 2003 at http://www.asiacase.com/ecatalog/NO_FILTERS/page-EC_DEVT-529579.html

Manovich, L. (1996). *On Totalitarian Interactivity.* Accessed March 9, 2004 at http://www.manovich.net/text/totalitarian.html

McDonald, J. (2001, October 22). AOL signs Landmark Deal with China. *Washington Post.* Accessed Junel, 2003 at http://www.washingtonpost.com/wp- srv/aponline/20011022/aponline124610_000.htm

Newsbytes News Network. (1998, February 4). *Internet World Canada - Alis & Mitsui Sign Translation Deal.* Accessed July 17, 2003 at http://www.findarticles.com/cf_dls/m0NEW/n25/20212077/p1/article.jhtml

North, T. (1994). *The Internet and Usenet Global Computer Networks: An Investigation of Their Culture and Its Effect on New Users.* Accessed August 19, 2003 at http://www.vianet.net.au/~timn/thesis/chap5.html

Ockerbloom, J. M. (2003). *The Online Books Page.* Accessed March 12, 2004 at http://onlinebooks.library.upenn.edu/banned-books.html

People's Daily online. (1999, July 13). *Much Achieved by Government Online Project in China.* Accessed October 15, 2003 at http://english.peopledaily.com.cn/199907/13/enc_19990713001047_TopNews.html

People's Daily online. (2001, January 5). *China Telecom to Merge and Enlarge 163/169 Network.* Accessed March 14, 2004 at http://english.peopledaily.com.cn/200101/05/eng20010105_59697.html

Pfaffenberger, B. (2000). *Currents: the Internet in China.* Accessed August 2, 2003 at http://www.linuxjournal.com/article.php?sid=5064

Press, L., Foster, W., & Goodman, S. (1999). *The Internet in India and China.* Accessed July 20, 2003 at http://www.isoc.org/inet99/proceedings/3a/3a_3.htm

Qiu, J. L. (1999-2000). *Internet Censorship in China: Keeping the Gate between the Cyberspace.* Accessed July 15, 2003 at http://www.ijclp.org/4_2000/pdf/ijclp_webdoc_1_4_2000.pdf

Qiu, J. L. (2001). Chinese opinions collide online. *Online Journalism Review.* Accessed August 5, 2003 at http://64.87.25.234/ojr/technology/1017959697.php

Rand Journal (2002, August 26). *Political Use of the Internet in China.* Accessed August 5, 2003 at http://www.rand.org/publications/MR/MR1543/MR1543.ch1.pdf

Report from U.S. Embassy in Beijing. (2001). *Kids, Cadres and "Cultists" All Love it: Growing Influence of the Internet in China.* Accessed May 3, 2003 at

http://www.usebassy-china.org.cn/english/sandt/netoverview.html

Reporters Without Borders. (2003, May 12). *China: webmaster Huang Qi put in solitary confinement after visit from Reporters Without Borders.* Accessed March 2, 2004 at http://coranet.radicalparty.org/pressreview/print_right.php?func=detail&par=7553

Reporters Without Borders. (2003, December 26). *Charges dropped against young Internet-user Liu Di.* Accessed March 1, 2004 at http://www.rsf.org/article.php3?id_article=8418

Silva, D. (2001, October 12). *Companies take steps to combat Internet abuse.* Accessed March 10, 2004 at http://seattle.bizjournals.com/seattle/stories/2001/10/15/focus4.html

Sinclair, G. (2002). *Internet in China: Information Revolution or Authoritarian Solution?* Accessed July 1, 2003 at http://www.geocities.com/gelaige79/intchin.htm

Souza, V. (2003, Aug 25). Dousing the Dragon's fire. *Express Computer.* Accessed March 3, 2004 at http://www.expresscomputeronline.com/20030825/opinion01.shtml

Tao, W. (2001). *Censorship and Protest: the Regulation of BBS in China People Daily.* Accessed June 2, 2003 at http://www.firstmonday.dk/issues/issue6_1/tao/

Timothy, T. (2001). *The Internet in China: Civilian and Military Uses.* Accessed June 2, 2003 at http://fmso.leavenworth.army.mil/FMSOPUBS/ISSUES/china-internet.htm

Tse, S., & Tsang, P. (1995). *Internet and WWW in China: All the Right Connections.* Accessed July12, 2003 at http://www.csu.edu.au/special/conference/apwww95/papers95/stse/stse.html

Tsui, L. (2001). *Big Mama Is Watching You: Internet Control and the Chinese Government.* Accessed May 3, 2003 http://www.lokman.nu/thesis/010717-thesis.pdf

Tsui, L. (2002). *Internet Opening Up China: Fact or Fiction?* Accessed May 10, 2003 at http://cms.mit.edu/conf/mit2/Abstracts/LOKMANTSUI.pdf

Tsui, L. (2003). Online Privacy in China. Accessed June 9, 2003 at http://www.lokman.nu/archives/002250.html

UIA. (2004). http://www.uia.org/uia/. Accessed March 12, 2004.

U.S. Bureau of Industry and Security. (2003). Accessed August 15, 2003 at http://www.bxa.doc.gov/Encryption/Default.htm

U-S-History.com. (2004). *The Sedition Act of 1918.* Accessed March 2, 2004 at http://www.u-s-history.com/pages/h1345.html

U.S. Internet Council. & ITTA Inc. *State of the Internet 2000.* Accessed August 28, 2003 at http://usic.wslogic.com/intro.html

Wade. R. (2001). *Development Assistance in the Digital Age.* Accessed July 18, 2003 at http://www1.oecd.org/dac/digitalforum/docs/Wade_presentation.pdf

Westland, C. (2000). China's Golden Projects. *Global Electronic Commerce.* Accessed July 16, 2003 http://www.itheadline.com/feat_art/FA8/china_golden.htm

Wired. (1999, April 13). *Anonymous Web Surfing? Uh-uh.* Accessed July 26, 2003 at http://www.wired.com/news/technology/1,1282,19091,00.html

Wired. (2001). *E-mail Privacy Remains Elusive.* Accessed August 25, 2003 at http://www.wired.com/news/technology/0,1282,442359,00.html

WIPO. (2002). *Multi-lingual Domain Names: Joint ITU/WIPO Symposium.* Accessed June, 4, 2003 at http://ecommerce.wipo.int/domains/international/pdf/paper.pdf

Wong, B. (2000). Improving Internet access in China. *Digital Freedom Network.* Accessed June 6, 2003 at http://www.dfn.org/ccefocus/china/chinanet.htm

Yurcik, W. (1997). *The Great (Fire)Wall of China: Internet Security and Information Policy Issues in the People's Republic of China.* Accessed August 19, 2003 at http://www.sosresearch.org/publications/ica97.PDF

Zhang, E. (2003, November 8). *SARS: Unmasking Censorship in China.* Accessed March 5, 2004 at http://www.asianresearch.org/articles/1502.html

Zhang, E., & Cropp, F. (2002). *A Party Organ's Party Journalism/Market Dichotomy—The Case Study of Guangzhou Daily Press Group.* Accessed June 17, 2003 at http://www.artsci.wustl.edu/~veap/zhangarticle

Zhou, J. (2001). Internet archive to snitch on workers. *South China Morning Post.* Accessed August 15, 2003 at http://prodev.learningnetwork.com/HR_Professionals/News/0000-5077 KEYWORD.Missing.htm

Zhu, J., & He, Z. (2002). Information accessibility, user sophistication, and source credibility: the impact of the Internet on value orientations in mainland China. *Journal of Computer Mediated Communication.* Volume 7. Accessed June 6, 2003 at http://www.ascusc.org/jcmc/vol7/issue2/china.html

Appendix A

Abbreviation List

ACLU	American Civil Liberties Union
ADSL	Asymmetric Digital Subscriber Line
APC	Association for Progressive Communications
BBS	Bulletin Board System
CANET	China Academic Network
CASS	Chinese Academy of Social Sciences
CCP	Chinese Communist Party
CDA	Communications Decency Act of 1996
CERNet	China Education and Research Network
ChinaGBN	China Golden Bridge Network
ChinaNet	China Public Computer Network
China Netcom	China Network Communications
CIECC	China International Electronic Commerce Center
CIETNet	China International Economic Trade Network
CMNet	China Mobile Communications Network
CNCNet	China Network Communications Network
CND	Chinese News Digest
CNNIC	China Internet Network Information Center
CSTNet	China Science and Technology Network

FTP	File Transfer Protocol
IAMAsia	Interactive Audience Measurement Asia
ICP	Internet Content Provider
IHEP	Institute of High Energy Physics
IN	Intelligent Network
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ITU	International Telecommunication Union
Mbps	Megabits
MEI	Ministry of Electronics Industry
MII	Ministry of Information Industry
MPS	Ministry of Public Security
MPT	Ministry of Post and Telecom
MSS	Ministry of State Security
NCFC	National Computing Facilities of China
NGO	Nongovernmental Organization
PGP	Pretty Good Privacy
PRC	People's Republic of China
SDPC	State Development Planning Commission
Telnet	Terminal Emulation
UNINet	China United Telecommunications Network
WIPO	World Intellectual Property Organization

Appendix B Structure of Internet Regulatory Body

(Last Updated: 12/31/2003)